Send Orders for Reprints to reprints@benthamscience.ae

508 *The Open Cybernetics & Systemics Journal,* 2015, *9,* 508-511

Open Access

Multiple-Bell-Bases Parallel Quantum Key Distribution Using Feedback

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

[1]*School of Electronic Engineering, Xidian University, Xi'an, 710071, P.R. China;* [2]*School of Information and Communication, Guilin University of Electronic Technology, Guilin, 541004, P.R. China*

Abstract: There is a problem that some eavesdropping risks exist in PQKD (Parallel Quantum Key Distribution) systems for the same types of quantum channels. Using the method of adjusting measure bases, a scheme of MBB (Multiple-Bell-Bases)-PQKD is proposed based on the principle of feedback controls. In this scheme, the sample spaces of Bell bases are changed constantly to increase the difficulty for eavesdropper to steal quantum keys. The analyses results demonstrate that the eavesdropping risks in parallel quantum channels are reduced by feedback controls, and the QKD (quantum key distribution) bit rates are increased, which provides novel approaches for the algorithm designs of high-speed quantum secure communications and QKD networks.

Keywords: Feedback control, multiple Bell bases, parallel quantum key distribution, quantum communication, quantum cryptography, quantum entanglement.

1. INTRODUCTION

PQKD (Parallel quantum key distribution) is the core stage of long-distance quantum cryptography where the quantum key information is transmitted in parallel quantum channels. As a novel research field of quantum information processing, PQKD is also one of the most important feasible tools to implement the actual large-capacity quantum secure communication.

Early ten years ago, A. Ortigosa-Blanch and J. Capmany proposed originally the concept and physical principle of PQKD based on quantum mechanics and frequency coding [1], and they improved the QKD (quantum key distribution) bit rate using the approaches of SCM (subcarrier multiplexing). In 2012, José Capmany *et al.* demonstrated the feasibility of sending parallel quantum keys for the time *via* SCM [2]. The results showed that the QBER of their two-channel scheme was less than 20% with a sifted key rate of 10 Kb/s/channel, and the quantum key numbers were increased. Meanwhile, they implemented the experiments of PQKD in combination with SCM and WDM (Wavelength Division Multiplexed) [3]. The QBER and sifted key rate were as high as that of Ref. [2], while the QKD bit rates were enhanced. These researches [1-3] have open the way of PQKD in optical fiber networks. In 2013, Guhao Zhao *et al.* presented a theoretical forward spectral filtering PQKD scheme *via* polarization coding and WDM [4], and the QKD bit rates can be raised greatly. In 2014, Jian Fang *et al.* put forward a CV (continuous-variable) PQKD scheme by SCM [5], and their results of the QKD bit rate can also be improved considerably with Gaussian modulation. Recently, the PQKD systems with quantum entangled stated were modeled with the UML technique [6], and the PQKD processes were demonstrated with simulated animation software.

Compared with single channel QKD, the performances of these PQKD systems have achieved great improvements in channel capacity, QBER and QKD bit rate, which is of great significance for the developments of high-speed quantum secure communication, QKD networks and multi-user QKD. Also, these researches have provided novel ways to the engineering application of long-distance quantum communication.

However, there is a problem that potential eavesdropping risks may occur in some parallel quantum channels for the reason that the measure bases are not changed for the PQKD system [1-6]. Also, the quantum channels are of identical types, which give chances to the hidden eavesdropper (*i.e.* Eve) to steal the relevant information during quantum key transmissions. The QKD bit rates of system are not easy to be increased.

Therefore, motivated by Refs. [1-6], a novel method of MBB (Multiple-Bell-Bases)-PQKD is proposed using the principle of feedback control, and the sample space of measure bases is expanded from one Bell basis to four Bell bases. The remaining sections are arranged as follows.

The feedback control system of MBB-PQKD is constructed in Section 2. Alice (the sender) and Bob (the receiver) select one or more Bell bases, and they can change the distributions of Bell bases in parallel quantum channels. In section 3, the results of performance analyses of this MBB-PQKD control system are demonstrated, while the advantages of this control system are analyzed in Section 4. Finally, a brief conclusion of this paper follows in Section 5.

2. FEEDBACK CONTROL SYSTEM OF MBB-PQKD

2.1. Construction of the MBB-PQKD Control System

Currently, the PQKD system can be only constructed theoretically under the ideal conditions of no environmental noise. The reason is that it is difficult to implement experi-

1874-110X/15

ments in free space and optical fiber for the early development stage of PQKD, especially for that of quantum entangled channels. Here the PQKD system itself is supposed to be perfect. The main disturbances for PQKD are mainly from Eve that hides in parallel quantum channels.

To design good quantum secure communication systems, it is assumed that Eve was more powerful than Alice and Bob in each quantum channel, that is, Eve might eavesdrop on the quantum key information with a certain probability after many trials and errors. To reduce the disturbances from Eve, more Bell bases are adopted to construct the PQKD system to enhance the security of parallel quantum channels than before, which make it difficult for Eve to eavesdrop on the information of the Bell bases [7] used by Alice and Bob in parallel quantum channels. Therefore, according to the unitary transformations among four kinds of Bell bases [7], a feedback control system of MBB-PQKD is constructed as shown in Fig. (**1**).

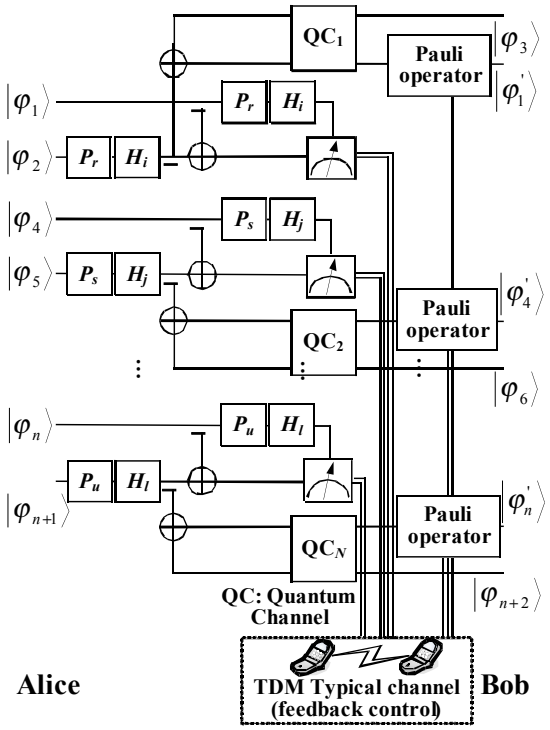

Fig. (1). Feedback control system of MBB-PQKD.

In Fig. (**1**), the independent parallel quantum channels are mapped by the quantum entanglement states of EPR (Einstein-Podorrsky-Rosen) pairs. The approaches of quantum communications with quantum entangled states can be diverse, such as quantum teleportation [7, 8], quantum entanglement swapping [9], etc. $\boldsymbol{H}_i$, $\boldsymbol{H}_j$ and $\boldsymbol{H}_l$ are four kinds of Hadamard gates. $\boldsymbol{P}_r$, $\boldsymbol{P}_s$ and $\boldsymbol{P}_u$ are quantum Pauli gates. $i, j, l, r, s, u \in \{1, 2, 3, 4\}$. Every quantum channels are corresponding to each time slot of the TDM (Time Division Multiplexing) classical channel which is also the feedback section of this MBB-PQKD system. The controlled objects are this system including the parallel quantum channels with the quantum Hadamard gates and quantum control-not gates, while the controllers are the Pauli gates.

2.2. Feedback control of the MBB-PQKD system

The unknown quantum bits of quantum keys in the last quantum channel of Fig. (**1**) can be taken as an example. It is supposed that the initial quantum entanglement states of particles n+1 and n+2 are one of the Bell states of a certain Bell Basis. Alice and Bob utilize this quantum channel and a time slot of TDM classical channel to send and receive the quantum information of unknown particle n *via* the quantum circuits including the selected Bell basis, and the feedback control processes of MBB-PQKD can be divided into three steps as follows.

Step 1, Alice and Bob select the initial Bell bases for every parallel quantum channels *via* the shared classical channel. They choose one or more Bell bases from four Bell bases [7] as the sample space of measure bases. The Bell bases of every quantum channel can be identical or different. Yet, Eve has no knowledge about the types and numbers of these Bell bases in the MBB-PQKD control system. She has to steal the relevant quantum information of Bell bases for no participation of the classical channel. Thus**,** Alice and Bob is active during PQKD, while Eve is passive.

Step 2, according to the eavesdropping distributions, Alice and Bob change the types of Bell bases in parallel quantum channels *via* the TDM classical channel. If this MBB-PQKD scheme is similar with the existing PQKD systems, that is, the parallel quantum channels are of the same types, then the measure bases are always unchangeable. As a result, Eve can eavesdrop on the quantum information of the transmitted quantum keys with a high probability when she obtains the messages of measure bases, which leading to large risks in the parallel quantum channels. For the MBB-PQKD control system, yet the sample capacity of Bell bases in every quantum channels can be more than one, and the measure bases are changeable. When Alice and Bob find that the measure bases in some quantum channels are known by Eve, then they have to transform the Hadamard gates of the quantum circuits of Bell bases with Pauli gates in Fig. (**1**). Conversely, the transformations of these quantum gates can influence the eavesdropping of Eve, thus the MBB-PQKD system can be adjusted and controlled by changing the Bell bases.

Step 3, Alice and Bob control the quantum circuits of Bell bases in parallel quantum channels by the feedback section of the classical channel. Generally, the kinds of Bell bases are more for the MBB-PQKD system, the eavesdropping probabilities of parallel quantum channels are lower. Nevertheless, under the threshold conditions of time and eavesdropping probability, more kinds of Bell bases of quantum channels do not mean better. The reason is that the total time is longer for Alice and Bob to send, transmit and receive quantum key bits than before, which prevent the QKD bit rates from increasing. The kinds of Bell bases are limited, and the sample spaces can not be always expanded constantly. The unnecessary extra costs in quantum circuits are wasteful to exploit too many Bell bases in the PQKD system. Therefore, it is necessary to control the quantum circuit compositions of Bell bases to improve the system performance by changing constantly the parameters including types

and numbers of Bell bases. Alice and Bob can obtain the changed information of mutual Bell bases *via* the feedback TDM classical channel, while Eve is confused without relevant exact information about Bell bases in every quantum channels.

According to the numbers of the unknown bits for quantum keys, the feedback control formula of the MBB-PQKD system can be expressed as:

$$\frac{n_{Alice}}{n_{Bob}} = \frac{G(n_1, n_2, \cdots, n_N)}{1 + f(p_1, p_2, \cdots, p_n)} \quad (1)$$

n_{Alice} and n_{Bob} are the inputs and outputs of this system, respectively. $n_1, n_2, \ldots, n_N$ are the unknown bit numbers of quantum keys in parallel quantum channels. Their sum is proportional to the feed forward function G which is relative to the parameters of the direction, number and kinds of measure bases. These parameters can be denoted as p_1, $p_2, \ldots, p_n$. According to the formula (1), the whole I/O (input/output) gain for this MBB-PQKD system can be improved and controlled by increasing numbers of quantum keys in every quantum channels and adjusting the feedback TDM classical channel.

2.3. Acquirement of the Key Code-Book for PQKD

Alice and Bob can implement MBB-PQKD *via* all parallel quantum channels and the TDM classical channel using current protocols (*i.e.* Ref [9]) or new protocols. According to the transmission results of unknown quantum bits, they not only need to determine whether there are eavesdroppers in every quantum channels or not, also they know about the information that the parameters of Bell bases in these quantum channels are distinguished by Eve. If there is eavesdropper hiding in the MBB-PQKD system and the directions of measure bases for Alice and Bob are identical, then the unknown quantum bits of parallel quantum channels can be combined into as quantum keys. If there exist disturbances in some of parallel quantum channels whereas the eavesdropping probabilities is far lower than the given threshold by Alice and Bob, then the transmitted unknown quantum bits in these channels can be chosen for quantum keys. In other cases, the unknown quantum bits *via* parallel transmissions in quantum channels are rejected. Finally, the unknown quantum bits in effective channels are combined into quantum key code-books for quantum secure communications with the procedures of quantum error corrections, privacy amplifications and other steps.

3. RESULTS OF PERFORMANCE ANALYSES

For the MBB-PQKD system, the unknown quantum bits can be transmitted by selecting one or several Bell bases according to the feedback steps *via* the classical channel, where the parameters (i. e. kinds, number, etc) of Bell bases need adjusting. Consequently, it is more difficult for Eve to steal the quantum bits of quantum keys than ever. In comparison with the PQKD systems using the single Bell basis, the average eavesdropping probability of Eve is illustrated as Fig. (**2**).

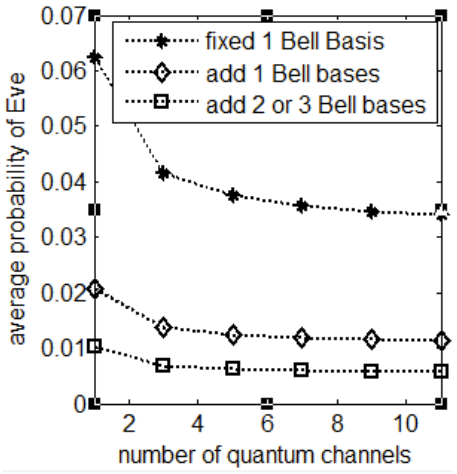

Fig. (2). Different average eavesdropping probability of Eve with the Bell bases and odd quantum channels for MBB-PQKD.

4. DISCUSSION

Differently from the existing PQKD system [6], it can be seen from the results of Fig. (**2**) that this MBB-PQKD system has two performance advantages as follows.

The statistical average probabilities of Eve's successful eavesdropping in parallel quantum channels have been reduced, and the QKD bit rates are increased. The main reason is that the eavesdropping risks are decreased by the increased sample space of Bell bases, which leads to the improvement of the MBB-PQKD system. The quantum circuits of different kinds of Bell bases are difficult to distinguish outside the system for their similarities. Several kinds of Bell bases are produced with the continual adjustments and changes of the Bell bases parameters. Then the difficulty for Eve to implement successful eavesdropping in parallel quantum channels is increased by the TDM classical channel for Alice and Bob to exchange the information of Bell bases. As a result, the average probability of the effective eavesdropping for Eve is lower than before, which is consistent with the feedback control processes by the formula (1).

The control costs of this system are relatively not high. For this MBB-PQKD system, these costs are mainly from the Hadamard gates which are transformed unitarily by Alice and Bob, and the types of Pauli gates in parallel quantum channels can be controlled *via* the feedback classical channel. According to the results of PQKD, if the probabilities of Eve' eavesdropping are far lower than the given thresholds by Alice and Bob for too many kinds of Bell bases, then the kinds of Hadamard gates in the MBB-PQKD system can be reduced appropriately. Conversely, the kinds of Hadamard gates need to be increased gradually. Thus, the overall control cost of this system *via* quantum gates remains low.

5. CONCLUSION

In this paper, a MBB-PQKD scheme has been obtained using the method of feedback controls, and the quantum information of quantum key can be transmitted in parallel with the quantum entangled state carriers of EPR pairs. Compared with the existing work, the sample spaces of Bell bases in our scheme have been expanded more than before. It has

been more difficult for Eve to eavesdrop on the quantum keys, and the QBER that is from Eve has been cut down. Under ideal conditions, the problem of low QKD bit rates has been solved to some extent by reducing the chances of the hidden eavesdropping risk. In addition, the controller costs of the MBB-PQKD have been not relatively high according to the feedback adjustment information of Bell bases. This scheme has provided some new approaches for the algorithm designs of high-speed quantum secure communication and QKD network, and it can also be utilized in the competitive fields of military, commercial, insurance, financial secrecy, etc. For the MBB-PQKD system, there remains much work, such as the QBER, channel capacity, environmental noise, system internal factors, coherence, fidelity, etc.

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).

REFERENCES

[1] A. Ortigosa-Blanch, and J. Capmany, "Subcarrier multiplexing optical quantum key distribution," *Physical Review A*, vol. 73, p. 024305, June 2006.

[2] M. José, R. A. Antonio, A. Waldimar, M. Alfonso, G. M. Víctor, C. David, and C. José, "Experimental demonstration of subcarrier multiplexed quantum key distribution system, " *Optics Letters*, vol. 37, pp. 2031-2033, June 2012.

[3] R. A. Antonio, M. José, A. Waldimar, M. Alfonso,G. M. Víctor,C. David, and C. José, "Microwave photonics parallel quantum key distribution, " *IEEE Photonics Journal*, vol. 4, pp. 931-942, June 2012.

[4] 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," *Optics Communications*, vol. 298, pp. 254-259, July 2013.

[5] J. Fang, P. Huang, and G. H. Zeng, "Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation," *Physical Review A*, vol. 89, p. 022315, Feb 2014.

[6] W. Xie, S. Ouyang, and H. L. Xiao, "Modeling of parallel quantum key distribution system *via* UML", *The Open Cybernetics & Systemics Journa*l, vol. 8, pp. 61-66, Dec 2014.

[7] W. Xie, S. Ouyang, and H. L. Xiao, "Controlled quantum teleportation schemes using generalized bell bases", *The Open Cybernetics & Systemics Journal*, vol. 9, May 2014 (online).

[8] 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, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, pp. 269-273, Sep 2012.

[9] 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," *Optics Communications*, vol. 284, pp. 4836-4842, Sep 2011.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014