A hierarchical modulation coherent communication scheme for simultaneous four-state continuous-variable quantum key distribution and classical communication

Can Yang, Cheng Ma, Linxi Hu, and Guangqiang He*
State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

We present a hierarchical modulation coherent communication scheme, which simultaneously achieves the classical communication and continuous variable quantum key distribution (CVQKD). The hierarchical modulation consists of a basic quaternary phase-shifting keying (QPSK) modulation for classical communication and a secondary four-state discrete modulation for CVQKD. Our simulation results based on practical parameters show that the maximum transmission distance is about 50km in order to satisfy the bit error rate of 10^{-9} in classical communication and secure quantum key distribution. In consideration of CVQKD able to be deployed over modern optical networks, We have reasons to believe that in the future the hierarchical modulation scheme will be used to upgrade existing digital communication systems to extend system functions.

Quantum key distribution (QKD) is one of the most practical and inspring applications of quantum information. It allows two remote parties to generate secure keys, whose security is guaranteed by the laws of quantum mechanics [1, 2]. Whereas the CVQKD system using modern transmission techniques and devices is compatible with current coherent light communication network [3], we demonstrate a novel protocol which allows classical communication and CVQKD with discrete modulation to be conducted simultaneously. The protocol is achieved by using hierarchical modulation scheme. The basic constellation carries the classical data, which is a classical coherent communication using QPSK modulation. The secondary constellation accomplishes a four-state CVQKD. The simultaneous transmission protocol using hierarchical modulation offers a different degree of protection to the transmitted messages according to their relative degrees of importance. The protocol can be used to upgrade an existing digital broadcast system, which will expand the system functions and meet the requirements of multi network convergence.

DETAILS OF NEW PROTOCOL

Alice prepares a coherent state, on which the classical information m_A and quantum key information n_A are orderly encoded. The coherent state can be expressed by $|\ \beta e^{i(2m_A+1)\pi/4} + \alpha e^{i(2n_A+1)\pi/4}\rangle, m_A \in \{0,1,2,3\}, n_A \in \{0,1,2,3\}$, as shown in Fig. 1. Note that the classical information m_A can be mapped into classical bits $ab \in \{00, 10, 11, 01\}$. The amplitude α and β , which are both real numbers, are chosen to optimize the performance of system. Alice sends the coherent state to Bob via a quantum channel.

When Bob receives the modulated coherent state, he firstly measures position $\widehat{q}$ and momentum $\widehat{p}$ of coherent state simultaneously using heterodyne detection to get the classical information. That is, if the measurement results are $\widehat{q}_m > 0$ and $\widehat{p}_m < 0$, then the classical information bits ab are assigned as 01. After determining the classical information of the basic constellation, Bob adjusts and displaces the measurement results to generate the secure quantum key as follows.

$$\widehat{q}_k = \frac{\widehat{q}_m}{\sqrt{\eta T_{ch}}} - (-1)^a \frac{\beta}{\sqrt{2}}. \tag{1}$$

$$\widehat{p}_k = \frac{\widehat{p}_m}{\sqrt{\eta T_{ch}}} - (-1)^b \frac{\beta}{\sqrt{2}}. \tag{2}$$

Where T_{ch} is the transmittance of the quantum channel and η is the detection efficiency of heterodyne detection. The coherent state becomes $|\ \alpha e^{i(2n_A+1)\pi/4}\rangle$ by eliminating the classical information, as shown in Fig. 1. Next, we can get the raw quantum key by the analysis same as the traditional CVQKD with discrete modulation. Assume the values of $\widehat{q}_k$ and $\widehat{p}_k$ are greater than zero. Then Bob determines that the quantum key information n_A is 0. Finally, Bob gets the secure key by the quantum key postprocessing [4, 5].

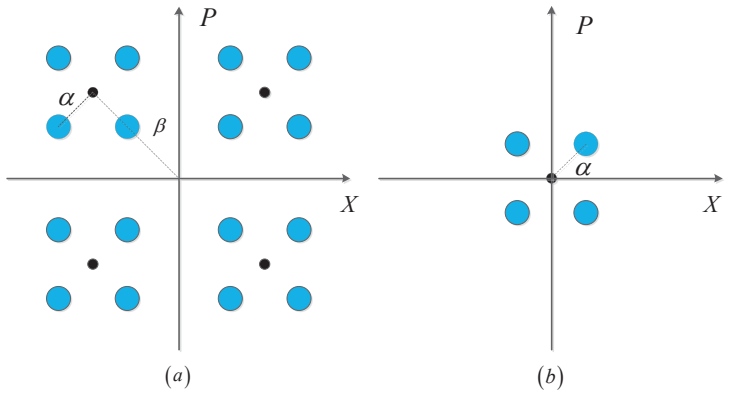

FIG. 1. Diagrammatic sketch of hierarchical modulation scheme, α and β are the amplitude of the signal field. (a) The basic QPSK modulation for classic communication and the secondary four-sate modulation for CVQKD. (b) The constellation schematic of four-state CVQKD after demodulating the basic classical information.

* gqhe@sjtu.edu.cn

[1] H. -K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photon **8**(8), 595–604 (2015).

[2] A. K. Ekert, "Quantum cryptography based on bell's theorem," Phys. Rev. Lett.**67**(6), 661–663 (1991).

[3] S. L. Braunstein and P. Loock, "Quantum information with continuous variables," Rev. Mod. Phys.**77**(2), 513–577 (2005).

[4] U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. on Inform. Theory. **39**(3), 733–742 (1993).

[5] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. on Inform. Theory. **41**(6), 1915–1923 (1995).