A Hierarchical Modulation Coherent Communication Scheme for Simultaneous Four-State Continuous-Variable Quantum Key Distribution and Classical Communication

Can Yang, Cheng Ma, Linxi Hu & Guangqiang He

International Journal of Theoretical Physics

ISSN 0020-7748
Volume 57
Number 9

Int J Theor Phys (2018) 57:2775-2786
DOI 10.1007/s10773-018-3798-z

Springer

Int J Theor Phys (2018) 57:2775–2786
https://doi.org/10.1007/s10773-018-3798-z

A Hierarchical Modulation Coherent Communication Scheme for Simultaneous Four-State Continuous-Variable Quantum Key Distribution and Classical Communication

Can Yang[1] · Cheng Ma[1] · Linxi Hu[1] · Guangqiang He[1]

Received: 5 March 2018 / Accepted: 4 June 2018 / Published online: 11 June 2018

Abstract We present a hierarchical modulation coherent communication protocol, which simultaneously achieves classical optical communication and continuous-variable quantum key distribution. Our hierarchical modulation scheme consists of a quadrature phase-shifting keying modulation for classical communication and a four-state discrete modulation for continuous-variable quantum key distribution. The simulation results based on practical parameters show that it is feasible to transmit both quantum information and classical information on a single carrier. We obtained a secure key rate of 10^{-3} bits/pulse to 10^{-1} bits/pulse within 40 kilometers, and in the meantime the maximum bit error rate for classical information is about 10^{-7}. Because continuous-variable quantum key distribution protocol is compatible with standard telecommunication technology, we think our hierarchical modulation scheme can be used to upgrade the digital communication systems to extend system function in the future.

Keywords Quantum key distribution · Hierarchical modulation · Simultaneous transmission · Coherent state

1 Introduction

Quantum key distribution (QKD) is one of the most practical and inspiring applications of quantum information. It allows two remote parties to establish a secret key, whose security is guaranteed by the laws of quantum mechanics [1, 2]. QKD has been thoroughly studied both in theory and in practice over the past thirty years [3]. Indeed, some QKD systems have begun to be applied in practice.

✉ Guangqiang He
gqhe@sjtu.edu.cn

[1] State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Continuous-variable QKD (CVQKD) protocol with Gaussian modulation, in which the continuous information modulated by Gaussian distribution are encoded on the quadratures of a coherent state, was proposed as a feasible method in practice [4, 5]. CVQKD protocol using Gaussian modulation has the maximum mutual information between Alice and Bob over Gaussian channel. And it has been demonstrated to be unconditionally secure against collective attacks [6] and coherent attacks [7] in the asymptotic limit, which are the most general attacks allowed by quantum mechanics. Recently, the composable security of CVQKD with coherent states has been proved in Ref. [8] including the finite-size effects. However, the main problem of CVQKD system based on Gaussian modulation is poor performance at present. The reconciliation efficiency is low when CVQKD protocol with Gaussian modulation works at low signal-to-noise ratio(SNR),thus severely limiting the key transmission distance. Typically, the practicable transmission distance of CVQKD protocol based on Gaussian modulation is within 50 kilometers equivalent to the distance of metropolitan area network [9]. So CVQKD protocol with discrete modulation was proposed to improve the system performance [10]. Its ability to obtain a high reconciliation efficiency conditioned on a low SNR makes it an alternative to Gaussian modulation protocol to achieve long-distance transmission. Moreover, one advantage of the discrete modulation protocol over the continuous modulation protocol is its low complexity of reconciliation procedure.

Whereas the CVQKD system using modern transmission techniques and devices is compatible with current coherent light communication network [11], in this paper, we demonstrate a novel protocol which allows classical communication and CVQKD with discrete modulation to be conducted simultaneously. The protocol is achieved by a hierarchical modulation scheme. The first layer constellation carries classical information, which is a classical coherent communication scheme using quadrature phase-shifting keying (QPSK) modulation. The second layer of the constellation carries quantum key information. Our simultaneous transmission protocol using hierarchical modulation scheme provides a different level of protection according to the degree of importance of information. The protocol can be used to upgrade an existing digital broadcast system in the future, which will expand the system functions and meet the requirements of multi network convergence.

In recent years, the simultaneous transmission schemes have received great attention. R. Kumar et al use the method of frequency division multiplexing to achieve the coexistence of continuous-variable QKD with classical channels in [12]. In Qi's scheme, the classical information is encoded on the displacements of QKD signals [13]. Different from the above schemes, our scheme uses discrete modulation in CVQKD, which is simpler and more efficient than Gaussian modulation. In addition, we use a high-order modulation format to transmit classical information in the hierarchical modulation scheme.

2 Details of New Protocol

The protocol we propose runs as follows.

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 classical channel.

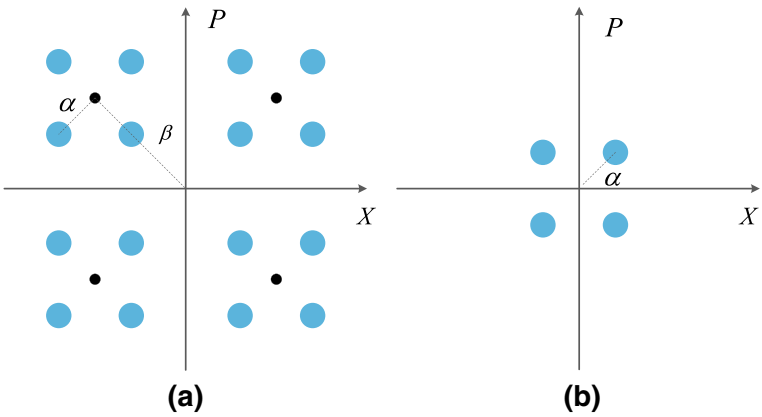

Fig. 1 Diagrammatic sketch of hierarchical modulation scheme. α and β are the amplitude of the signal field. **a** β is the modulation amplitude of the first layer constellation and α is the modulation amplitude of the second layer constellation. **b** The constellation schematic of four-state CVQKD protocol after demodulating the first layer information

When Bob receives the modulated coherent state, he firstly measures position $\widehat{q}$ and momentum $\widehat{p}$ of coherent state simultaneously by 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 first layer constellation, Bob adjusts and displaces the measurement results to obtain the secure quantum key as follows.

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

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

Where T is the transmittance of the quantum channel and η is the detection efficiency of heterodyne detector. 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 through analysis similar to the traditional CVQKD protocol with discrete modulation [10]. If 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 including error reconciliation, parameter estimation and privacy amplification [14, 15].

Because classical information and quantum information interfere with each other in the hierarchical modulation system, the first layer QPSK modulation system operates at a high noise level. In order to analyze the bit error rate of the first layer classical communication system, we define λ as the ratio of quantum signal intensity α and classical signal intensity β.

$$\lambda = \frac{\alpha}{\beta}. \tag{3}$$

λ is an important parameter to characterize the hierarchical modulation system. If $\lambda = 0$, the whole system is a classical QPSK modulation system, transmitting only the classical information. When λ is extremely small, the four coherent states in each quadrant of the phase space form a "cloud". The variation among the coherent states in a cloud has the same effect of white noise on the first layer QPSK modulation system. Under this condition,

the bit error rate of the classical communication system is low and the CVQKD system based on four-state modulation is secure in our hierarchical modulation scheme. Given that the quantum signal amplitude α should be extremely small, we are only interested in the situation where the value of λ is less than 0.5.

For the hierarchical modulation system, the carrier to noise ratio(CNR) is defined as

$$CNR = \frac{E_s}{\sigma^2} = \frac{\eta T(\beta^2 + \alpha^2)}{\sigma^2} = \frac{\eta T(1 + \lambda^2)\beta^2}{\sigma^2}. \tag{4}$$

Where E_s is the carrier power and $\sigma^2 = T\eta(1 + \chi_{line} + \chi_{het}/T)N_0$ represents the noise average power at the receiver. Note that N_0 denotes the shot-noise variance, which should be measured in real time in the experiment [16]. χ_{line} denotes the total channel-added noise referred to the channel input, expressed in shot noise units. χ_{het} refers to the heterodyne detection-added noise expressed in shot-noise units. The 1 of the last expression σ^2 refers to a quantum noise term, by which the received data are always accompanied. However, to the first layer constellation, the noise consists of two terms, the system noise σ^2 and the scattering of coherent states in the second layer constellation, $\eta T\alpha^2$ [17, 18]. So the signal to noise ratio of the first layer constellation can be accepted as the ratio of power of QPSK modulation to noise power, and it is expressed by

$$SNR_1 = \frac{\eta T\beta^2}{\sigma^2 + \eta T\alpha^2} = \frac{CNR}{\lambda^2(1 + CNR) + 1}. \tag{5}$$

The classical information bit error rate of our hierarchical modulation system will definitely increase compared with independent QPSK modulation system because of the second layer quantum information. The performance of the first layer QPSK modulation system before and after quantum information is added may be evaluated by comparing the values of CNR and SNR_1. Normally, we think the transmitting optical power of the first layer constellation is constant. Therefore, we define the difference, P_{snr}, between CNR and SNR_1 to evaluate the signal-to-noise ratio deterioration degree of the first layer QPSK modulation system due to the existence of the second layer quantum information.

$$P_{snr} = CNR - SNR_1 = \frac{\lambda^2(1 + CNR)}{1 + \lambda^2(1 + CNR)} CNR. \tag{6}$$

The P_{snr}, said a penalty, represents the additional carrier power that is needed in the hierarchical system so that the heterodyne receivers can show the same bit error rate performance as in the independent QPSK system. The larger the P_{snr} is, the worse the heterodyne receiver will perform in the system. The simulation diagram of P_{snr} is shown in Fig. 2.

In most deployed QPSK broadcast systems, the minimum operating CNR is below 7 dB [17]. This means the SNR of the first layer QPSK modulation system must be greater than 7 dB due to the interference of the second layer CVQKD system. As shown in Fig. 2, at CNR=7 dB, the P_{snr} is around 0.5 dB for λ= 0.1. The heterodyne receivers effectively get a QPSK constellation with equivalence of SNR=6.5 dB, because the penalty is 0.5 dB. The penalty increases with the increase of CNR, but the penalty becomes insignificant because there are enough margins in the CNR to meet the desired performance. According to these results, the desirable λ is under 0.1 to satisfy the operating condition of the heterodyne detections.

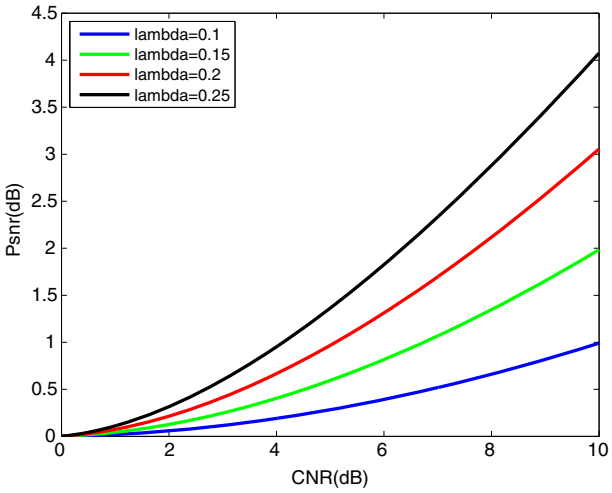

Fig. 2 The difference between CNR and SNR_1 when the value of λ varies. The SNR_1 is signal-to-noise ratio of the first layer QPSK modulation system. The CNR is the carrier-to-noise ratio of the hierarchical modulation system

3 Security Analysis of Four-State Protocol

For the CVQKD part in our hierarchical modulation scheme, we address the security of four-state protocol with the assumption that Alice and Bob's labs, and equipment, are trusted. R.Renner and J.I.Cirac have proved that the derived bounds for the secret key generation rate in the case of collective attacks remain asymptotically valid for arbitrary coherent attacks in [7], which are the most powerful attacks allowed by quantum mechanics in the asymptotic limit. So we restrict our security analysis to the case of collective attacks.

We know that a QKD protocol can be implemented by Prepared and Measure(PM) scheme or Entanglement-Based(EB) scheme, which are equivalent in the case of four-state protocols. Implementations are usually simpler for PM scheme, but EB scheme is easier to analyze theoretically. For the EB version of the four-state protocol, Alice prepares a pure two-mode entanglement state: $|\Phi\rangle = \sum_{k=0}^{3} \sqrt{\lambda_k}|\phi_k\rangle|\phi_k\rangle$ where

$$\lambda_{0,2} = \frac{1}{2}e^{-\alpha^2}\left[cosh\left(\alpha^2\right) \pm cos\left(\alpha^2\right)\right] \tag{7}$$

$$\lambda_{1,3} = \frac{1}{2}e^{-\alpha^2}\left[sinh\left(\alpha^2\right) \pm sin\left(\alpha^2\right)\right] \tag{8}$$

and

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}} (-1)^n |4n+k\rangle. \tag{9}$$

The pure state can also be rewritten as $|\Phi\rangle = \frac{1}{2}\sum_{k=0}^{3}|\psi_k\rangle|\alpha_k\rangle$ where the states

$$|\psi_k\rangle = \frac{1}{2}\sum_{m=0}^{3} e^{-i(1+2k)m(\pi/4)}|\phi_m\rangle \tag{10}$$

are orthogonal non-Gaussian states. Then Alice continues to perform the projective measurement $|\psi_k\rangle\langle\psi_k|$ $(k = 0, 1, 2, 3)$ on one of the modes. The coherent state $|\alpha_k\rangle$ is prepared

when Alice's measurement gives the result k. This coherent state is sent to Bob through the quantum channel. At Bob's trusted area, he measures both quadratures for each coherent state with a heterodyne detection. After the quantum transmission phase, the two sides of the communication share a correlated key string, which needs to be proceed with classical data processing procedures.

Under collective attacks, Eve's accessible information is written as $S_4(y:E)$ in four-state protocol, which is maximized when the state ρ_{AB} shared by Alice and Bob is Gaussian [6, 19, 20]. Therefore, the value of $S_4(y:E)$ is upper bounded by a function of the covariance matrix Γ of ρ_{AB} [21]:

$$S_4(y:E) \leqslant f(\Gamma), \tag{11}$$

where f is an entropic function depending on the symplectic eigenvalues of Γ. In the Gaussian protocol based on coherent state,the covariance matrix Γ_G of the shared state ρ_{AB} after the quantum channel can be computed and depends on Alice's modulation variance V_A in the PM version of the protocol and the transmission T and excess noise ξ of the channel.

$$\Gamma_G = \begin{bmatrix} (V_A+1)\mathbb{I}_2 & \sqrt{T}Z_G\sigma_Z \\ \sqrt{T}Z_G\sigma_Z & (1+TV_A+T\xi)\mathbb{I}_2 \end{bmatrix} \tag{12}$$

In the above formula, $\mathbb{I}_2$=diag(1,1), σ_Z=diag(1,-1). The Z_G has the form with $Z_G = Z_{EPR} = \sqrt{V_A^2+2V_A}$. For the four-state protocol, Ref. [22] has proved that the covariance matrix Γ_4 of the state ρ_{AB} has the same form as Γ_G after the quantum channel. It can be expressed as

$$\Gamma_4 = \begin{bmatrix} (V_A+1)\mathbb{I}_2 & \sqrt{T}Z_4\sigma_Z \\ \sqrt{T}Z_4\sigma_Z & (1+TV_A+T\xi)\mathbb{I}_2 \end{bmatrix}. \tag{13}$$

Note that Z_4 is a function of the modulation variance V_A. When the modulation variance V_A is small enough, Z_4 is very close to Z_G, as shown in Fig. 3. We can see that the two are almost impossible to distinguish in the region of $V_A < 0.5$ from the graph. So the Holevo quantity between Eve and Bob's classical variable is very similar in these two protocols conditioned on $V_A < 0.5$. Hence, the Holevo key rate in four-state protocol reads

$$K_{coll} = \zeta I(x:y) - S_4(y:E) \approx \zeta I(x:y) - S_G(y:E), \tag{14}$$

which is against collective attacks in the asymptotic limit.

4 Analysis and Simulation

4.1 Classical Information Bit Error Rate Analysis

To evaluate the performance of our proposed protocol, we derive the bit error rate of classical information in the hierarchical modulation scheme. In fact, two kinds of modulation are mutual interference in the hierarchical modulation scheme. The noise caused by four-state modulation for CVQKD therefore needs to be considered in classical information bit error rate analysis. In Section 3, we obtain the condition in which the modulation variance V_A of four-state modulation CVQKD scheme is less than 0.5 to ensure the security of CVQKD. Besides, the ratio λ should be less than 0.1 to ensure that the heterodyne detector works effectively. So the bit error rate of classical information is calculated in this condition. In the following simulation process, we set the classical signal intensity β to a different value to observe the effect of β on the classical information bit error rate. For each β, we set different λ values to verify the effect of quantum signal intensity α on simulation results.

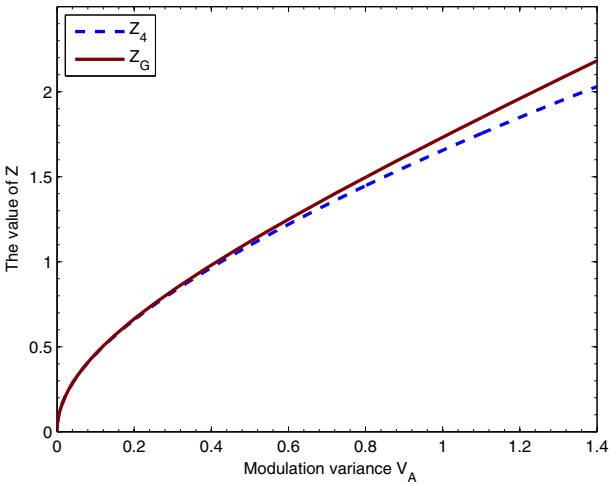

Fig. 3 Comparison of the covariance coefficient Z_4 for the four-state protocol and Z_G for the Gaussian-modulation protocol as a function of the modulation variance V_A

For the first layer QPSK modulation constellation diagram in hierarchical modulation scheme, the in-phase branch and the quadrature branch are mutually independent and can be treated separately. Because the bit error ratio of the in-phase branch and quadrature branch is equivalent, the average error probability of in-phase branch and quadrature branch over transmission medium is expressed as follows.

$$P_{eI} = P_{eQ} = \frac{1}{2} erfc\left(\sqrt{\frac{\eta T\beta^2}{(2+2\upsilon_{el}+\eta T\varepsilon+\eta T V_A)N_0}}\right). \tag{15}$$

In the above formula, the parameters are defined as follows. (1) $T = 10^{\frac{-\gamma L}{10}}$ is the quantum channel transmittance, where L is the fiber length. (2) $V_A = 2\alpha^2$ is modulation variance of the second layer four-state modulation in the hierarchical modulation scheme. (3) ε is the excess noise in the quantum channel. (4) $N_0 = \frac{1}{4}$ denotes the shot-noise variance. (5) The electronic noise of heterodyne detection is υ_{el}. The average bit error ratio of the lower layer QPSK modulation scheme reads

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{\eta}{\frac{(2+2\upsilon_{el})N_0}{\beta^2 10^{-\gamma L/10}} + \frac{\varepsilon\eta N_0}{\beta^2} + 2\lambda^2\eta N_0}}\right). \tag{16}$$

Then we use the above model for numerical simulations of the classical information average bit error rate. We use practical system parameters and take full account of the sources of noise in the numerical simulations process. The simulation data we used comes from the reference [10, 13]:$\upsilon_{el} = 0.05$, $\gamma = 0.2dB/km$, $\varepsilon = 0.005$ and $\eta = 0.5$. The simulation results are plotted in Fig. 4.

From Fig. 4, when the modulation amplitude $\beta = 5$ in the first layer of hierarchical modulation scheme, the ratio λ of the quantum signal intensity α and the classical signal intensity β is less than 0.1, which meet the simulation condition. The maximum

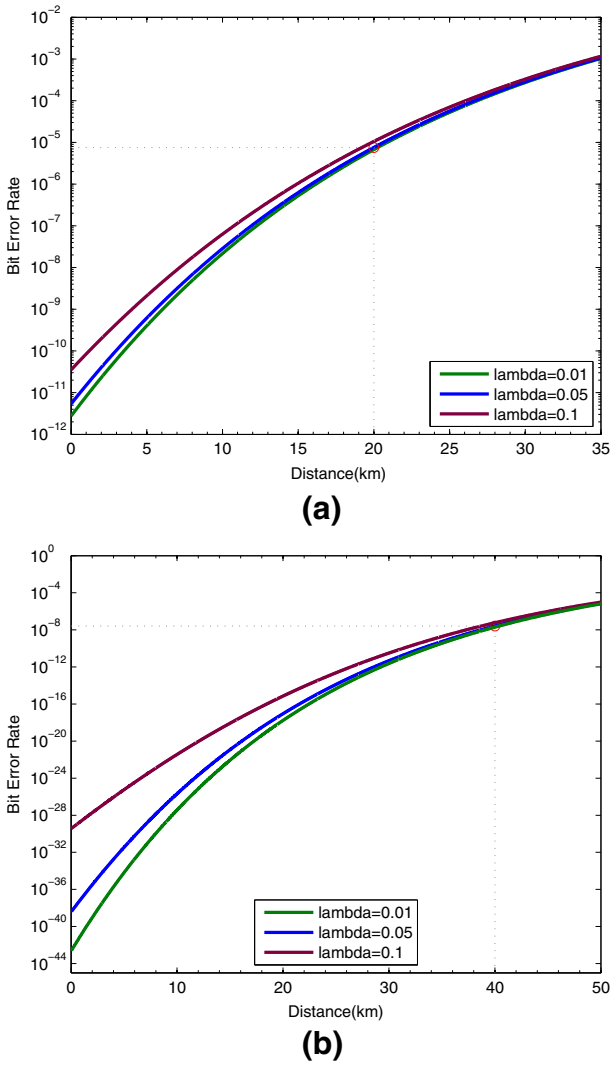

Fig. 4 The classical information average bit error rate for different modulation amplitude β as a function of the distance. **a** $\beta = 5$. **b** $\beta = 10$

transmission distance is about 5 kilometers to satisfy the average bit error rate 10^{-9} in classical communication scheme. Considering the modulation amplitude $\beta = 10$, the maximum transmission distance has increased to about 35 kilometers. As the modulation amplitude β increases, the ratio λ becomes smaller. But the performance of the first layer classical communication system is better with the increase of Euclidean distance in the first layer constellation diagram according to the Fig. 4. It is important to note that although the modulation amplitude is very large in the first layer of the hierarchical modulation scheme, the quantum key is still secure, because the quantum information is encoded into the second layer constellation diagram of our hierarchical modulation scheme.

4.2 Quantum Key Rate Analysis

In this section, we derive the secure quantum key rate of the four-state modulation CVQKD protocol in the hierarchical modulation scheme. As mentioned above, we only consider the optimal collective attacks in the asymptotic limit. The secret key rate K_{coll} is given once more conditioned on reverse reconciliation by [21, 23]

$$K_{coll} = \zeta I\left(x : y\right) - S_4\left(y : E\right), \tag{17}$$

where ζ is the reconciliation efficiency; $I\left(x : y\right)$ is the classical Shannon mutual information between Alice and Bob's data [24], and $S_4\left(y : E\right)$ is the Holevo information between Bob's string and Eve's quantum system in the four-state CVQKD protocol [25]. In practice, all we focus on is the maximum value of $S_4\left(y : E\right)$, which is computed in the Gaussian state case. It's relatively simple to derive the Shannon mutual information of Alice and Bob for the case of heterodyne detection:

$$I\left(x : y\right) = 2 \times \frac{1}{2} log_2 \frac{V_B}{V_{B|A}} = log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}}, \tag{18}$$

where V_B is the variance of Bob receiving signal, $V_{B|A}$ is the Bob's variance conditioned on Alice's measurement result, and χ_{tot} refers to the total noise at the channel input, not including the shot noise. They are expressed respectively as below.

$$V = 1 + V_A \tag{19}$$

$$\chi_{tot} = \chi_{line} + \chi_{het}/T \tag{20}$$

$$V_B = \eta T\left(V + \chi_{tot}\right)/2 \tag{21}$$

$$V_{B|A} = \eta T\left(1 + \chi_{tot}\right)/2 \tag{22}$$

As discussed in the previous section, under the assumption that V_A is small enough, the Holevo quantity between Bob and Eve in four-state CVQKD protocol is close to that in Gaussian modulation protocol. Especially when $V_A < 0.5$, the Holevo quantity in these two protocols can be treated as the same. Therefore, we can calculate the value of $S_G\left(y : E\right)$ in Gaussian modulation CVQKD protocol [21] instead of getting $S_4\left(y : E\right)$. Through simplification, the formula of $S_4\left(y : E\right)$ can be expressed as

$$\begin{aligned} S_4\left(y : E\right) = & G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) \\ & - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right). \end{aligned} \tag{23}$$

where $G(x) = (x+1)log_2(x+1) - xlog_2 x$. The symplectic eigenvalues $\lambda_{1,2,3,4}$ of Γ_4 and $\Gamma_{A|b}$, the covariance matrix of Alice's state conditioned on Bob's measurement result, are given by

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})}. \tag{24}$$

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})}. \tag{25}$$

where

$$A = V^2 + T^2(V + \chi_{line})^2 - 2TZ_4^2. \tag{26}$$

$$B = (TV^2 + TV\chi_{line} - TZ_4^2)^2. \tag{27}$$

$$C = \frac{A\chi_{het}^2 + B + 1 + 2\chi_{het}[V\sqrt{B} + T(V + \chi_{line})] + 2TZ_4^2}{[T(V + \chi_{tot})]^2}. \tag{28}$$

$$D = \frac{(V + \chi_{het}\sqrt{B})^2}{[T(V + \chi_{tot})]^2}. \tag{29}$$

In a realistic setting, only a portion of the shared data by Alice and Bob can be used to extract keys. So there is a coefficient ζ in front of variable $I(x : y)$ in (17). The reconciliation efficiency ζ depends on the SNR and modulation method. As mentioned in [10], ζ increases with the increase of SNR in Gaussian modulation CVQKD protocol. And besides, the reconciliation efficiency of a Gaussian modulation scheme is better than that of a discrete modulation shceme in the case of a high SNR. Unlike the high SNR, the reconciliation efficiency of a discrete modulation scheme is better under low SNR conditions. In our case, it is reasonable to have a reconciliation efficiency higher than 50% under low SNR conditions [9], because we use a discrete four-state modulation scheme in our protocol. So we employ $\zeta = 0.5$ in the simulation experiment. So far, we have finished the theoretical analysis of secure key rate of the second layer four-state modulation CVQKD protocol.

According to actual experimental parameters in reference [13]:$\upsilon_{el} = 0.05$, $\gamma = 0.2dB/km$, $\varepsilon = 0.005$ and $\eta = 0.5$, we have made a simulation analysis. The simulation results based on the above security analysis are displayed in Fig. 5. We discuss the quantum key generation rate of our protocol in the case of three different modulation variances:$V_A = 0.1$, $V_A = 0.3$ and $V_A = 0.5$ in Fig. 5.

The secret key generation rate is not proportional to the Alice's modulation variance V_A under the restrictions of $V_A \leqslant 0.5$ according to the Fig. 5. We know when the modulation variance V_A is 0.5, the secure quantum key rate is in the range of 10^{-3} bit/pulse to 10^{-1} bit/pulse within 40 kilometers.In this case, the maximum classical information bit error rate is on the order of 10^{-7} under the condition of $\beta = 10$. When the modulatin variance V_A is equal to 0.1, the maximum transmission distance is about 20 kilometers. And the maximum classical information bit error rate is about 10^{-5} under the condition of $\beta = 5$.

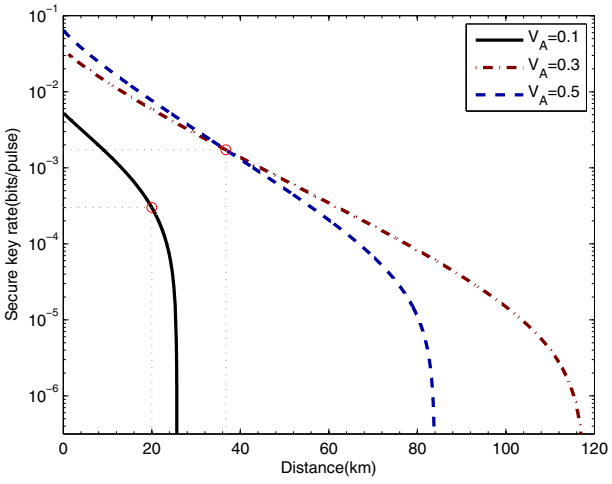

Fig. 5 Secret key generation rate as a function of distance for the second layer four-state modulation CVQKD protocol at different modulation variance:$V_A = 0.1$, $V_A = 0.3$ and $V_A = 0.5$

Furthermore, as the transmission distance is greater than 20 kilometres, the secure quantum key rates suddenly deteriorate. So the system can't perform key distribution normally after 20 kilometers in the case where the modulation variance is equal to 0.1.

Based on the above simulation results, the quantum key rate has nothing to do with modulation amplitude β of the first layer in the hierarchical scheme. When the modulation amplitude β of the classical signal is much larger than the modulation amplitude α of the quantum signal, the value of α does not have much effect on the bit error rate of classical information. We also learned that the transmission distance of our protocol is affected by the modulation amplitude α because of $V_A = 2\alpha^2$. So the appropriate modulation amplitude α is very necessary in the transmitter in order to balance the transmission distance, classical information bit error rate and secure quantum key rate. When modulation variance in the transmitter is 0.3, the classical information bit error rate is about 10^{-5} in the case of $\beta = 10$ in 50 kilometers and the quantum key rate is about 10^{-3} bit/pulse.

5 Conclusions and Perspectives

In this paper, we proposed a new protocol for simultaneous transmission of the classical information and quantum key based on QPSK/four-state hierarchical modulation scheme. We proved that the QKD process is secure against collective attacks in the asymptotic limit, when Alice's modulation variance V_A is very small ($V_A < 0.5$) in the four-state modulation CVQKD protocol. Through numerical simulations of using real parameters, we observe the maximum transmission distance of our system. Our simultaneous transmission system can achieve the secure quantum key distribution and reliable classical communication in metropolitan area network. Although our scheme does not extend the communication distances, it improves the type of transmission information under the condition of a single carrier. The proposed protocol also offers different degrees of protection to the transmitted messages, which is useful for upgrading the one-to-many server/client systems to meet the demands of different customers.

However, there are some problems that need to be studied further, such as the operation frequency of classical communication system and CVQKD system mismatch problem. Because the maximum operation frequency of CVQKD experiment is far below the demand of classical communication system, we have to sacrifice the speed of the classical communication to implement the simultaneous classical and quantum communication protocol. So we should develop high-speed (above 10 GHz) shot-noise-limited heterodyne detectors in future and the operation frequency of simultaneous transmission system will be continuously improved. Besides, the noises from the classical channel will affect the performance of QKD system in hierarchical modulation scheme. In this paper, we regard the overall excess noise as a whole ε in quantum channel. In order to minimize the impact of noise on QKD system performance, we can try to use the optical amplifier in simultaneous transmission system [26, 27]. Next, the further research in this direction are likely to bring this technology a step closer to a wide range of applications within the well laid metropolitan area network.

Acknowledgements We would like to thank anyone who made suggestions for this paper. We also acknowledge support from the National Natural Science Foundation of China(Grants No.61475099 and No.61102053), Program of State Key Laboratory of Quantum Optics and Quantum Optics Devices (KF201405), Open Fund of IPOC(BUPT) (IPOC2015B004) and Program of State Key Information Security (2016-MS-05).

References

1. Lo, H.-K., Curty, M., Tamaki, K.: Nat. Photonics **8**, 595 (2014)
2. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
3. Diamanti, E., Leverrier, A.: Entropy **17**, 6072 (2015)
4. Grosshans, F., Assche, G.V., Wenger, J., Brouri, R., Cerf, N.J., Grangier, P.: Nature **421**, 238 (2003)
5. Ralph, T.C.: Phys. Rev. A **61**, 010303 (1999)
6. García-Patrón, R., Cerf, N.J.: Phys. Rev. Lett. **97**, 190503 (2006)
7. Renner, R., Cirac, J.I.: Phys. Rev. Lett. **102**, 110504 (2009)
8. Leverrier, A.: Phys. Rev. Lett. **114**, 070501 (2015)
9. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G., Grangier, P.: Phys. Rev. A **77**, 042325 (2008)
10. Leverrier, A., Grangier, P.: Phys. Rev. Lett. **102**, 180504 (2009)
11. Braunstein, S.L., Loock, P.: Rev. Mod. Phys. **77**, 513 (2005)
12. Kumar, R., Qin, H., Alléaume, R.: New J. Phys. **17**, 043027 (2015)
13. Qi, B.: Phys. Rev. A **94**, 042340 (2016)
14. Maurer, U.M.: IEEE Trans. Inf. Theory **39**, 733 (1993)
15. Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.M.: IEEE Trans. Inf. Theory **41**, 1915 (1995)
16. Kunz-Jacques, S., Jouguet, P.: Phys. Rev. A **91**, 022307 (2015)
17. Jiang, H., Wilford, P.A.: IEEE Trans. Broadcast. **51**, 223 (2005)
18. Vitthaladevuni, P.K., Alouini, M.S.: IEEE Trans. Broadcast. **47**, 228 (2001)
19. Navascués, M., Grosshans, F., Acín, A.: Phys. Rev. Lett. **97**, 190502 (2006)
20. Wolf, M.M., Giedke, G., Cirac, J.I.: Phys. Rev. Lett. **96**, 080502 (2006)
21. Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N.J., Tualle-Brouri, R., McLaughlin, S.W., Grangier, P.: Phys. Rev. A **76**, 042305 (2007)
22. Leverrier, A., Grangier, P.: Phys. Rev. A **83**, 042312 (2011)
23. Devetak, I., Winter, A.: Proc. R. Soc. A **461**, 207 (2005)
24. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley (2006)
25. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
26. Zhang, H., Fang, J., He, G.: Phys. Rev. A **86**, 022338 (2012)
27. Fossier, S., Diamanti, E., Debuisschert, T., Tuallebrouri, R., Grangier, P.: J. Phys. B **42**, 114014 (2009)