International Journal of Theoretical Physics
https://doi.org/10.1007/s10773-019-04056-0

Phase Estimation and Compensation for Continuous-Variable Quantum Key Distribution

Ying Guo[1] · Zihang Zhou[1] · Xudong Wang[1] · Xiaodong Wu[1] · Ling Zhang[1] · Duan Huang[1]

Received: 13 September 2018 / Accepted: 8 February 2019 / Published online: 19 February 2019

Abstract
Phase estimation and compensation is one of the enabling functionalities in continous-variable quantum key distribution (CVQKD). Recently, a novel CVQKD scheme has been independently proposed to combat the local oscillator (LO) side channel attacks. Furthermore, we have carried out a proof-of-principle experimental study on the feasibility of the CVQKD without sending a LO. However, this scheme contains a serious weakness: The phase noise caused by the two different lasers between the sender and the receiver would severely destroy the quantum signal and finally reduce the secure distance. In this paper, we investigate the optical phase noise and explore the optimal approach to estimate and compensate such kind of noise with appropriate data overhead. Numerical simulations show that our scheme can successfully reconstruct the phase drifts even at low signal-to-noise ratio conditions. We also suggest that a higher accuracy of phase estimation could be achieved by using the frequency division multiplexing scheme. This opens an opportunity to employ advanced pilot-aided phase estimation techniques in quantum communication system.

Keywords Continuous-variable quantum key distribution · Phase estimation · Frequency division multiplexing

1 Introduction

Quantum key distribution (QKD) is a promising technology allowing two authenticated parties, Alice and Bob, to establish secure keys through an insecure quantum channel possibly controlled by an eavesdropper, Eve [1–4]. There has been a tremendous interest in quantum large-scale networks. In order to achieve the high rate of modern optical networks, continuous-variable QKD (CVQKD) is an attractive approach towards the next generation application, relying on the standard telecommunication fiber [5–8]. Moreover, CVQKD with coherent detection has been demonstrated a high detection efficiency, high practicability and superior compatibility with classical channels [9]. One of the most frequently-used

✉ Duan Huang
duanhuang@csu.edu.cn

[1] School of Information Science & Engineering, Central South University, Changsha, 410083, China

protocol is the Gaussian-modulated coherent state (GMCS) protocol [10], which has been demonstrated secure against individual, collective [11], and coherent attacks [12] even considering the finite-size effects [13, 14].

It's important to realize high-efficiency heterodyne detection in CVQKD protocol. However, the transmission of the local oscillator (LO) brings terrible influence and safety loopholes. For example, a strong LO sharply decreases the efficiency through a lossy channel [15] and scattered photons from the LO may contaminate the signal [16]. What's more, Eve may have the chance to perform attack by manipulating the LO [17, 18], which may cause LO fluctuation attack [19], calibration attack and so on. Taking these limitations into account, CVQKD with a locally generated LO has been proposed and its feasibility has been demonstrated in experiments [20–23]. On the other hand, there still exists an urgent problem, e.g, the phase drift. Since the transmission distance is bounded by channel's transfer characteristics, there is a phase difference $\Delta\varphi$ between receiving data and transmitting data. The phase drift has an effect on the receiver's detection, which shortens the maximal transmission distance.

Currently, there have been three solutions for environmentally-induced phase drift. The first solution is the structure improvement of the interferometric system to compensate for the phase drift, such as the plug-and-play structure [24, 25]. The second one is the passive compensation, which uses the passive methods to reduce the impact of the external environment on the interference system, such as temperature isolation and damping measures. The third is the active compensation [26], which uses the scanning method to obtain the dynamic parameters of phase drift and perform real time compensation. The phase feedback compensation algorithm, which belongs to the active compensation, adds a swept frequency testing frame to the transmitting data and determines the phase drift in the channel by observing the phase of the swept testing frame at the receiver, relying on receiver's well restoration to the signal's contour. The conventional phase feedback compensation is a convenient algorithm to conquer the phase drift. Unfortunately, there are two disadvantages of the conventional scheme. On the one hand, it can only estimate the phase drift when the signal-to-noise ratio (SNR) is much larger than 1. On the other hand, after the phase drift estimation, the conventional phase compensation scheme needs to compensate the phase drift to the receiver's phase modulator in real time, increasing the hardware's complexity of the system and introducing additional noise as well.

In this paper, we propose a phase estimation and compensation scheme for the frequency division multiplexing (FDM) based CVQKD system. We refer to the agreement of the self-referenced protocol [20–22] and use the locally generated LO in the GMCS QKD, to remove the security loopholes associated with the transmitting LO. Withal, this phase compensation scheme estimates the phase drift by adding a small numbers of testing frames to the transmitting data. We show the statistical characteristics of the corresponding segments in the receiving data to accurately estimate the phase drift. Considering that inserting testing frames directly in the time domain may result in performance weaknesses, therefore, we use a phase modulator (PM) for the FDM and insert testing frames in the frequency domain. The FDM not only improves the spectral efficiency, but also expands the dynamic range of the phase compensation. Moreover, we perform phase compensation on Alice's side, which reduces the hardware's requiements in practice. The proposed phase estimation and compensation scheme contribute to the development of CVQKD communication systems compatible with optical network requirements.

This paper is organized as follows. In Section 2, we consider characteristics of the locally generated LO that involves the phase drift, and present our phase compensation scheme

for the FDM-based CVQKD system. In Section 3, we perform the performance analysis of the FDM-based CVQKD system. In Section 4, we consider our scheme under different conditions with numerical simulation results. Finally, we discuss and draw conclusion in Section 5.

2 The Phase Estimation and Compensation Scheme for CVQKD

2.1 The Locally Generated LO Scheme

Figure 1 shows the transmitted LO design and the locally generated LO design, separately. The main advantage of the transmitted LO is the guarantee of a stable phase between signal and LO. Security of such implementation have raised doubts and questions by manipulating the LO intensity or wavelength. In the locally generated LO design, Bob performs heterodyne detection with a locally generated LO, thus estimates the relative phase by using the phase reference pulse, waiving the security loopholes from the transmitted LO.

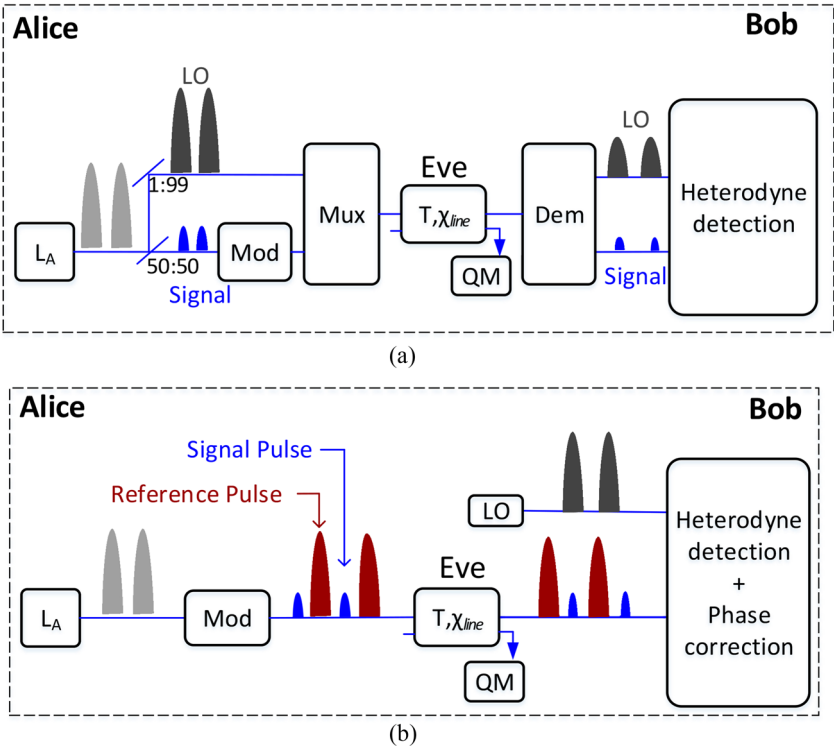

Fig. 1 The transmitted LO design and the locally generated LO design. **a** In the transmitted LO design, the phase reference (darkgray pulse) and the quantum signal (blue pulse) are derived from the same optical pulse and sent from Alice to Bob. Mod is a modulator, Mux is multiplexing and Dem is demultiplexing. **b** In the locally generated LO design, Alice sequentially sends weak quantum signal (blue pulses) and phase reference (red pulses). Bob performs consecutive coherent detections of each pulse received using his own LO pulses (darkgray pulses)

As for the loaclly generated LO, Alice selects two independent Gaussian random variables (X_A, P_A) distributed as $N(0, V_A)$ and sends a coherent state $|X_A + iP_A\rangle$ to Bob as signal pulses. Subsequently, Alice sends a reference pulse at the next time bin. The amplitude of the reference pulse, $V_R^{1/2} = (X_{A_R}^2 + P_{A_R}^2)^{1/2}$, is fixed and may be several times greater than $V_A^{1/2}$, but much smaller than the typical LO. Besides, the reference pulses can reduce the interference of signal pulses since the *long tail* of larger amplitude pulses cannot be completely suppressed. Bob performs homodyne detection of the quadrature value X_B or P_B of the received signal pulse to estimate its mean value x_B or p_B, which is defined based on his own high power LO. He performs heterodyne detection on the received reference pulse and obtains the mean quadrature value for both, X_{B_R} and P_{B_R}, based on the LO. Because of the free-running of Alice's and Bob's respective LO, the phase difference θ between their two frames is a time-varing amount. We assume that θ is a random variable at any moment, uniformly distributed over $(-\pi, \pi]$. And its fluctuating frequency (i.e., phase noise bandwidth) f_θ measured and calibrated before the start of the protocol is much lower than the rate at which the pulse is generated. Let Δt to be the time delay between the signal and the reference plus the duration of the two pulses. This duration should be much shorter than the inverse of the bandwidth f_θ given by,

$$\Delta t \ll f_\theta^{-1}. \tag{1}$$

We can derive an estimation of the phase difference $\hat{\theta}$ since Bob knows the mean quadrature values of the reference pulse both in Alice's, (X_{A_R}, P_{A_R}), and his own frame, (X_{B_R}, P_{B_R}), are described as

$$\begin{bmatrix} X_{B_R} \\ P_{B_R} \end{bmatrix} = \sqrt{T_{eff}} \begin{bmatrix} \cos\hat{\theta} & -\sin\hat{\theta} \\ \sin\hat{\theta} & \cos\hat{\theta} \end{bmatrix} \begin{bmatrix} X_{A_R} \\ P_{A_R} \end{bmatrix}, \tag{2}$$

where $0 < T_{eff} \leq 1$ is the effective channel transmittance which can be eliminated to get,

$$\hat{\theta} = \tan^{-1}\left(\frac{X_{B_R}P_{A_R} - X_{B_R}P_{A_R}}{X_{B_R}P_{A_R} + X_{B_R}P_{A_R}}\right). \tag{3}$$

Taking $P_{A_R} = 0$, we obtain

$$\hat{\theta} = \tan^{-1}\left(\frac{P_{B_R}}{X_{B_R}}\right). \tag{4}$$

Since the reference pulse's quantum uncertainty cannot be ignored, there should exist an error given by

$$\hat{\theta} = \theta + \varphi, \tag{5}$$

where the estimation error φ follows some probability distribution $P(\varphi)$.

Subsequently, Bob sends phase difference estimation, $\hat{\theta}$, and measurement of the signal pulse to Alice, while Alice rotates her tabulated values by $\hat{\theta}$ to obtain the estimation, via

$$\begin{bmatrix} \hat{X_B} \\ \hat{P_B} \end{bmatrix} = \sqrt{T_{eff}} \begin{bmatrix} \cos\hat{\theta} & -\sin\hat{\theta} \\ \sin\hat{\theta} & \cos\hat{\theta} \end{bmatrix} \begin{bmatrix} X_A \\ P_A \end{bmatrix}. \tag{6}$$

So far, Alice and Bob share a partially correlated Gaussian random variable. In our protocol, (5) can be rewritten as,

$$V_{est} = V_{error} + V_{drift}, \tag{7}$$

where V_{error} is the variance of φ expressed in (5) and V_{drift} corresponds to the variance of the relative phase drift $\Delta\varphi$. The detailed derivation of $\Delta\varphi$ is in Section 2.2.

2.2 The Influence of the Phase Drift

The phase drift may have an influence on the detection of the receiver. In order to analyze the influence of the phase drift in CVQKD, we assume that the X_{max} is the maxmal power of the signals, which means the x-quadrature and the p-quadrature of the transmitted signal follow Gaussian distribution on $(-X_{max}, X_{max})$. A quantum state $|\alpha\rangle = |X_A + iP_A\rangle$ rewritten as $|\alpha'\rangle = |X'_A + iP'_A\rangle$ because of the phase drift, where $X_A = R \cdot \cos(\theta)$ and $P_A = R \cdot \sin(\theta)$ are not linear with $X'_A = R \cdot \cos(\theta + \Delta\varphi)$ and $P'_A = R \cdot \sin(\theta + \Delta\varphi)$, respectively.

As for the quantum state $|\alpha\rangle$, we can derive the detective result in x to determine the effect of phase drift. For a random quantum state whose X axis's projection is X_A, P axis's projection follows the Gaussian distribution on $(-1, 1)$. We assume that a phase drift is introduced as $\Delta\varphi$ through the channel. All of the quantum states get $\Delta\varphi$ rotation as shown in Fig. 2. (X_L, X_H) represents the detective result from receiver. The new quantum states' detective results follow the Gaussian distribution in (X_L, X_H) and the $\bar{X}$ is the mean of (X_L, X_H). Due to that, we have $X_H - X_L = 2X_{max} \cdot \sin(\Delta\varphi)$ and $\bar{X} = X_A \cdot \cos(\Delta\varphi)$. Therefore, the influence from the phase drift on X axis can be approximately calculated as,

$$X_A \to X'_A \sim N(X_A \cdot \cos(\Delta\varphi), V_x \cdot \sin^2(\Delta\varphi)). \tag{8}$$

We find that the phase drift is not only an addictive process to the signal, but also a multiple process to the amplitude. Considering that the receiver will normalize this multiple coefficient to the channel transmission coefficient T during signal recovering and compensate T before data processing, the signal in actual postprocessing should be given by,

$$X''_A \sim N(X_A, V_x \cdot \tan^2(\Delta\varphi)). \tag{9}$$

According to above description, the phase drift can be approximately regarded as a noise whose variance is $V_x \cdot \tan^2(\Delta\varphi)$. If there is no phase drift, we have $\Delta\varphi = 0$ and $X''_A = X_A$. For the phase drift $\Delta\varphi = \pi/2$, we have $\tan^2(\Delta\varphi) \to \infty$. Thus the mutual information between transmitter and receiver reduces to 0, where x and p are independent from each other. It means that the choice of Bob is always different from Alice during quantum detection. In what follows, we will show how to estimate and compensate the phase drift.

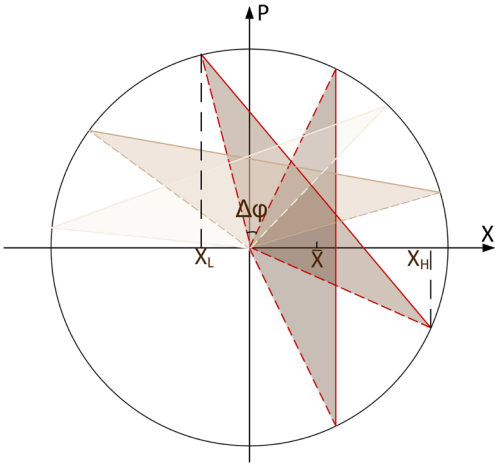

Fig. 2 Influence of the phase drift. Two dotted red triangles show the influence of the phase drift and the phase drift is $\Delta\varphi$. The other two triangle show different conditions with different value of $\Delta\varphi$. The detective result from receiver is (X_L, X_H). The new quantum state's detective result will be the Gaussian distribution in (X_L, X_H) and the mean is $\bar{X}$. Different color represents different value of $\Delta\varphi$

2.3 Phase Compensation Scheme

In order to estimate the phase drift under a lower SNR, we design a phase compensation scheme based on statistical characteristics of receiving data. By adding few testing frames in transmitting data, we can estimate the phase drift $\Delta\varphi$ in low SNR, and ensure the smooth in long-distance communications. In CVQKD, the quantum states transmitted by Alice follow the Gaussian distribution, as well as the location and the momentum. The transmitter generates signals follows the Gaussian distribution by loading signals follows the Rayleigh distribution in amplitude modulator (AM) and loading signals follows the uniform distribution in phase modulator (PM). We assume that $X \sim N(0, \sigma_A^2)$, and hence X can be described as $X = R \cdot \cos(\theta)$, where R follows the Rayleigh distribution, and θ follows the uniform distribution. Since the phase drift is $\Delta\varphi$ and the noise is $\epsilon \sim N(0, \sigma_\epsilon^2)$, the continuous variable X from Alice and Y from Bob can be given by,

$$X = R \cdot \cos(\theta)', \quad Y = (R \cdot \cos(\theta + \Delta\varphi) + \epsilon). \tag{10}$$

In subsequent data negotiation, the $\Delta\varphi$ prevents the process since the negotiation algorithm can only recover the the original signals from the additive white Gaussian noise (AWGN) signals, resulting in the obstacle of getting secure key in two group of continuous variables.

Let's take a method to estimate the phase drift $\Delta\varphi$. Alice sends one frame of testing data X_T in transmitting data, while the transmitter and the receiver both know the content in X_T and the testing frame won't be used to get the secure key. When Bob receive the data, we extract the testing frame Y_T and calculate the mathematical expectation of X_T and Y_T,

$$E\{X_T \cdot Y_T\} = E\{(R\cos(\theta)) \cdot (R\cos(\theta + \Delta\varphi) + \epsilon)\}, \tag{11}$$

where ϵ is the Gaussian white noise and θ is uniform distribution in $(0, 2\pi)$. Since θ, R, $\Delta\varphi$ and ϵ are independent variables from each other, we obtain,

$$E\{X_T \cdot Y_T\} = E\{R^2\} \cdot E\{\cos\theta \cdot \cos(\theta + \Delta\varphi)\} + E\{R \cdot \epsilon \cdot \cos\theta\}. \tag{12}$$

Due to the fact

$$E\{R \cdot \epsilon \cdot \cos\theta\} = E\{R\} \cdot E\{\epsilon\} \cdot E\{\cos\theta\} \approx 0, \tag{13}$$

we have

$$E\{X_T \cdot Y_T\} = E\{R^2\} \cdot E\{\cos\theta^2\} \cdot \cos\Delta\varphi = V_A \cdot \cos\Delta\varphi. \tag{14}$$

Therefore we could reduce the noise item and get the function of the phase drift by simple statistical analysis of the receiving data and the transmitting data. Since the variance of transmitting signal is a given system parameter, we can calculate the phase drift $\Delta\varphi$ in the channel in (11).

According to above-mentioned analysis, the calculation of the phase drift mostly relies on the relevance between receiving testing frame and original transmitting data. The maximum relevance is V_A, where the phase drift is 0, and the minimum relevance is $-V_A$, where the phase drift is π. However, the relevance is influenced by another parameter, named, the transmittance T. Therefore, we have,

$$Y = T\cot R \cdot \cos(\theta + \Delta\varphi) + \epsilon, \tag{15}$$

and then the (14) can be rewritten as,

$$E\{X_T \cdot Y_T\} = T \cdot E\{R^2\} \cdot E\{\cos\theta^2\} \cdot \cos\Delta\varphi = T \cdot V_A \cdot \cos\Delta\varphi. \tag{16}$$

Obviously, it's difficult to calculate the phase drift $\Delta\varphi$ when we don't know the transmitting parameter. To derive the transmitting parameter T and the phase drift, we introduce another group of X_T with the phase drift $\Delta\theta'$. Then we have

$$X'_T = R \cdot \cos(\theta + \Delta\theta'). \tag{17}$$

The mathematical expectation is given by,

$$E\{X_T \cdot Y_T\} = T \cdot V_A \cdot \cos(\theta + \Delta\theta'). \tag{18}$$

By combining (17) and (18), we can derive T and $\Delta\varphi$, which means the phase drift could be estimated under low SNR by a simple hardware design.

Note that the bandwidth will increase when we directly inserting testing frames in the time domain. Besides, the phase drift will also be changed drastically in the time domain. In the following, we use a phase modulator (PM) to implement the FDM and insert testing frames in the frequency domain.

3 The Phase Compensation Implementation in the FDM-based CVQKD System

There are two problems that need to be solved when inserting testing frames. Firstly, the spectral efficiency will be reduced if the testing frames are directly inserted into the time domain. Secondly, the phase drift will change with time. Once the phase drift is derived, the value of the phase drift may have changed again, making it difficult to achieve accurate phase compensation in real time. Due to these drawbacks, we adopt a FDM design and insert testing frames in the frequency domain. The FDM has higher frequency and power utilization, compared with the single frequency detection. Therefore, it has attracted much attention in the practical communication networks. There are several ways for the generation of multi-frequency light, where multiple lasers or optical frequency combs is usually applied. For example, phase-modulation FDM which works by periodically modulating the carrier phase to obtain multi-frequency light is currently used [27, 28].

In our scheme, we use a phase modulator to obtain FDM detection-light by phase-modulating the incident light, then the multiplexed detection frequency can be achieved by adjusting the modulation depth and modulation frequency of the phase modulator. The phase modulator in the phase compensation system can achieve frequency division multiplexing detection with the simple structure, as shown in Fig. 3. At Alice's side, we use an AM and a PM to perform the Gaussian modulation and frequency distribution multiplexing. Meanwhile, we insert the testing frames in the high frequency domain by the PM. The Att. is variable optical attenuator which is used for adjusting modulation variance and intensity. The pulses continue transmit through a single mode fiber (SMF). At Bob's side, the pulse is splitted into two parts to filter out useless information separately. One of the bundles passes through $filter1$ to obtain the testing frame for phase drift estimation, and the other bundle passes through $filter2$ to obtain the signal frame for heterodyne detection. At the same time, another frequency-stabilized laser generates an LO and then the LO is divided into two parts for heterodyne detection. Such arrangement has two advantages. Firstly, the locally generated LO waives the security loopholes associated with the transmitting LO and increases the secure key rate. Secondly, the FDM increases the spectral efficiency and enlarge the dynamic range of the phase compensation.

As for the compensation in a practical system, the conventional feedback phase tracking algorithm determines the phase drift angle by sampling the sweep signal of the frame header

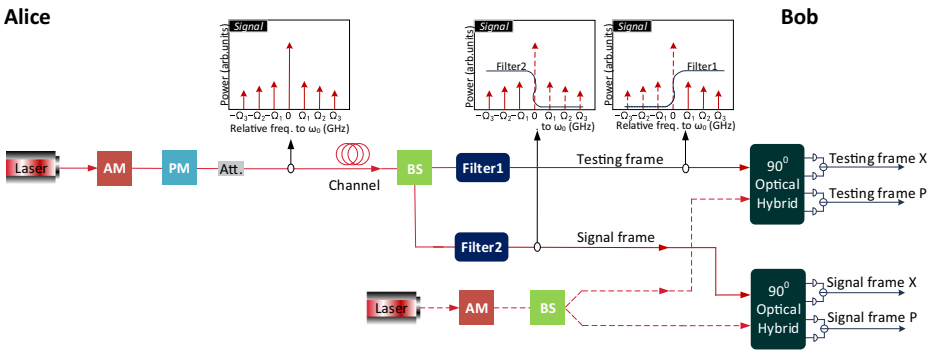

Fig. 3 The frequency division multiplexing design in CVQKD. We obtain FDM detection-light by phase-modulating the incident light and insert testing frames in frequency domain. Afterwards, we split signal frames and testing frames by two filters. And the testing frames are used to estimate phase drift. The AM is an amplitude modulator, PM is a phase modulator, the Att. is an attenuator, and the BS is a beam-splitter

when Bob receiving the data, and immediately loads a bias signal on the phase modulator after calculating the drift angle $\Delta\varphi$. Therefore, the output signals modulated by Bob's AM and PM eventually have similar phase information to the Alice. However, it is difficult to re-modify the phase information in the Gaussian variables superimposed with noise since the receiver has already completed the acquisition and storage of data. Therefore, we compensate the phase drift at Alice's side. The specific steps are as follows. After quantum channel communication, Alice and Bob have continuous variables X and Y, respectively. Through the phase estimation, we get the estimation of channel transmission coefficient T' and the estimation of channel phase drift $\Delta\varphi$. We send the value of $\Delta\varphi$ to Alice through the classic channel and then she recreates the data X'. The X' is information from R and θ originally loaded on the transmitters AM and PM, including the phase drift $\Delta\varphi$,

$$X' = R \cdot \cos(\theta + \Delta\varphi). \tag{19}$$

At the same time, Bob calculates T and then performs a linear operation on the receiving data to eliminate T and get Y',

$$Y' = \frac{1}{T'} \cdot T \cdot R \cdot \cos(\theta + \Delta\varphi) + \epsilon \approx R \cdot \cos(\theta + \Delta\varphi) + \epsilon. \tag{20}$$

From now on, the continuous variables shared by Alice and Bob will not have much difference in phase and linear proportions. The main difference between two sets of variables is that only the data owned by Bob adds additive Gaussian white noise, and this difference will be resolved by data negotiation. The detailed process of phase compensation is in Appendix.

Figure 4 shows the relations between the transmission distance and secure key rate when the estimation accuracy is decremented from 100% to 60%. The estimation accuracy is decremented by 5%. We find that the secret key rates and transmission distance decrease along with the decreased estimation accuracy. While Fig. 5 shows the estimation accuracy for different SNR and different signal length N. The estimation accuracy increases along with the increased SNR and the signal length N. Combined with these two cases, the estimation accuracy is close to 73% and the transmission distance is about 42 km when $SNR = 20$ and $N = 10$, while the estimation accuracy is close to 99.8% and the transmission distance is about 85 km when $SNR = 80$ and $N = 1000$.

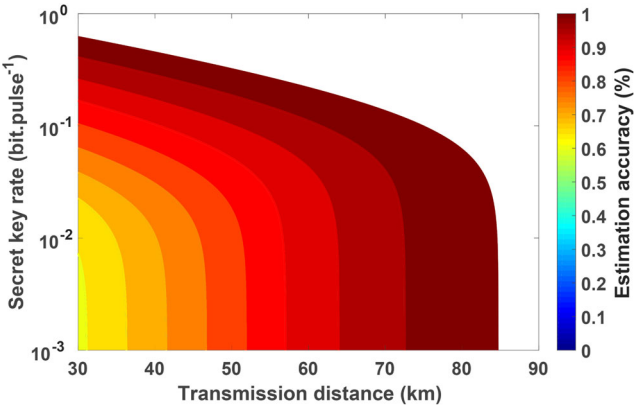

Fig. 4 The secret key rate as a function of transmission distance under different estimation accuracy. Different color correspond to different estimation accuracy. The estimation accuracy is the correct rate of phase estimation

4 Performance Analysis

The data from Alice and Bob are not only infected by additive Gaussian noise, but also phase drift $\Delta\varphi$. If we ignore the phase drift, the mutual information *I(x:y)* will reduce drastically. In the GMCS protocol, the channel module is addictive Gaussian white noise (AWGN) channel. The mutual information *I(x:y)* can be calculated using Shannon's equation,

$$I(x:y) = \frac{1}{2}\log_2\left(1+\frac{V_x}{V_N}\right) = \frac{1}{2}\log_2(1+SNR), \tag{21}$$

where V_x is signal's variance of transmitted signal, and V_N is the addictive Gaussian noise's variance of the channel. Therefore the received signal's variance satisfies $V_y = V_x + V_N$, and $SNR = V_x/V_N$ is the signal noise rate of the channel. According to the analysis in

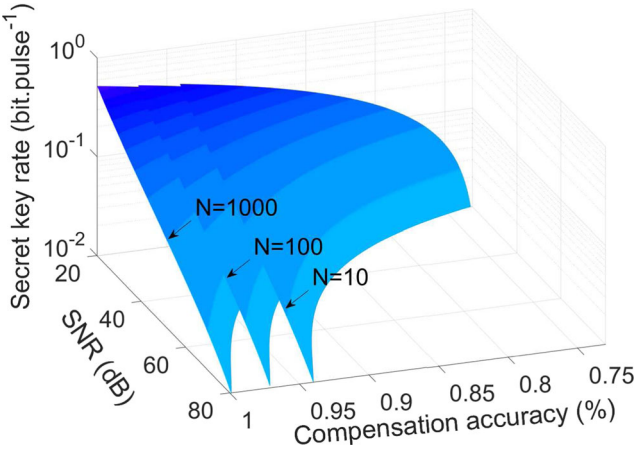

Fig. 5 The estimation accuracy for different SNR and different signal length N. The values of the N are $N = 10$, $N = 100$, and $N = 1000$ separately. The estimation accuracy is the correct rate of phase estimation

Section 2, we observe that the phase drift is approximately equivalent as bringing a noise whose variance is $V_x \cdot tan^2(\Delta\varphi)$. If there is no phase drift, then $\Delta\varphi = 0$, and $X''_A = X_A$. When the phase drift $\Delta\varphi$ equals to $\pi/2$, then $tan^2(\Delta\varphi) \to \infty$. The mutual information between Alice and Bob reduces to 0, corresponding to x and p that are independent to each other. Therefore, we obtain the expression of channel capacity on phase drift,

$$I(x:y) = \frac{1}{2}\log_2\left(1 + \frac{V_x}{V_N + V_x \cdot tan^2(\Delta\varphi)}\right). \tag{22}$$

With the phase compensation scheme introduced above, the post-processing stage will be insensitive to the phase of the input data. Compared with the existing hardware-based phase compensation scheme, our scheme not only reduces the hardware cost, simplifies the system design, but also has a simple algorithm structure and a software realization. More importantly, our scheme has greatly improved the accuracy of the phase estimation and can directly perform phase estimation and compensation for the quantum light. The simulation results of our algorithm under different phase drifts are shown in Fig. 6. Here we choose $V_{drift} = 0.001$, $V_{drift} = 0.1$, $V_{drift} = 0.2$, and $V_{drift} = 0.3$. In Fig. 6a and b, there are comparing between performance with phase compensation and performance without phase compensation. The secure key rate and the transmission distance are much better in the

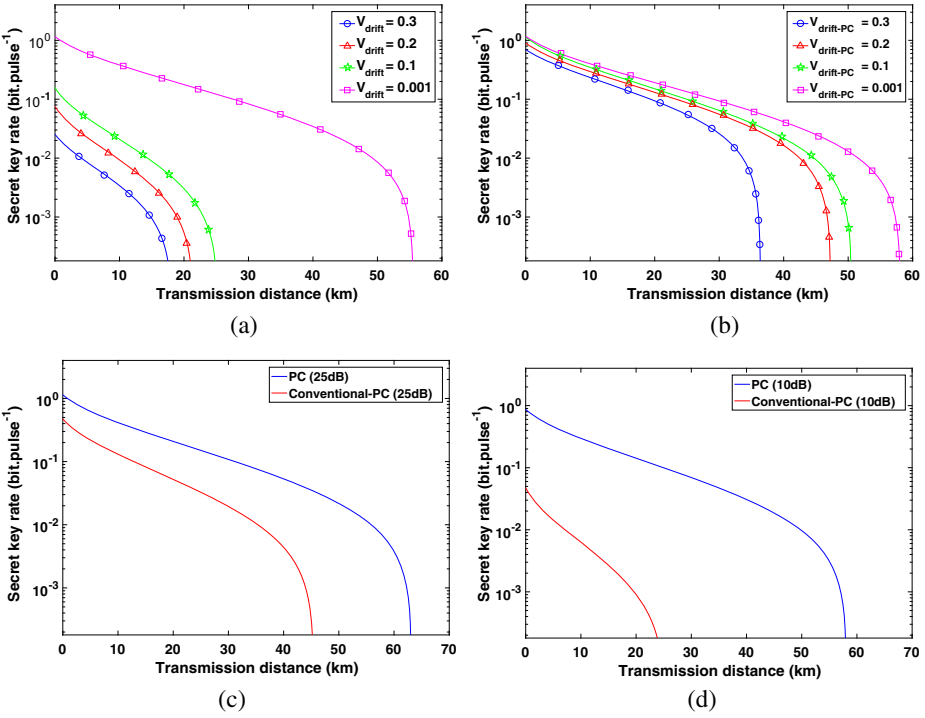

Fig. 6 The secret key rates as a function of transmission distance under different V_{drift} and SNR. The four lines in Fig. 6a of $V_{drift} = 0.3$, $V_{drift} = 0.2$, $V_{drift} = 0.1$, and $V_{drift} = 0.001$ show the conditions without phase compensation. The four lines in Fig. 6b of $V_{drift-PC} = 0.3$, $V_{drift-PC} = 0.2$, $V_{drift-PC} = 0.1$, and $V_{drift-PC} = 0.001$ show the conditions with phase compensation. V_{drift} represents the variance of phase drift. In Fig. 6c and d, the blue line represents our phase compensation scheme and the red line represents the conventional phase feedback compensation scheme. The full line represents $SNR = 10dB$ and the dotted line represents $SNR = 25dB$. $\beta = 0.95$, $N = 4000$, $V = 40$

scheme with phase compensation. As shown in Fig. 6a, when the phase drift $V_{drift} \geq 0.3$, the value of secret key rate is limited a lot. The secret key rates reduce to 0 when the transmission distance exceed 18 km. As shown in Fig. 6b, the transmission distance with phase compensation is over two times longer than those without phase compensation in each different V_{drift}.

Figure 6c and d show the secret key rate and transmission distance for our phase compensation scheme and the conventional phase compensation scheme with $SNR = 10dB$ and $SNR = 25dB$. We can observe that the proposed phase compensation scheme performs better than the conventional scheme, even in low SNR. Since the conventional scheme estimates the phase drift relying on receiver's well restoration to the signal's contour and can only estimate the phase drift when the SNR is much larger than 1, the conventional scheme is restricted under low SNR. According to above results, we can find that our scheme estimates the phase drift accurately and perform fine even under low SNR. Moreover, our phase compensation scheme has a straightforward mathematical form and simple system hardware design, contributing to practicality and security of the QKD networks.

5 Conclusion

In order to remove security loopholes associated with transmission of the LO, we have proposed a phase compensation scheme for the locally generated LO in the FDM-based CVQKD system to resist the phase drift between emitter laser and LO laser. By inserting few testing frames in the transmitting data and analyzing the corresponding segments in the receiving data, we can accurately estimate the phase drift under low SNR. Besides, we introduce the FDM based a PM in our locally generated LO scheme, increasing the dynamic compensative range and the spectral efficience.

Numerical simulation results show that the transmission distance and the secure key rate are improved with the achieved phase compensation. The proposed phase compensation scheme performs much better under low SNR compared with conventional scheme. It involves a simple experimental hardware requirements, paving the way to the practical application of the locally generated LO in CVQKD implementations. Comparing with previous one-way CVQKD system, this scheme could provide greater flexibility of high-speed shot-noise-limited measurement by controlling the optical power of the local LO, which might be suitable for further gigahertz CVQKD. It can be of interest in high rate and long distance communication networks.

Acknowledgments Thanks for the passionate help from Dakai Lin, Hai Zhong, Minglu Cai and other colleagues. Meanwhile, my parents have given me much encouragement and support. This work was supported by the National Natural Science Foundation of China (Grant Nos. 61379153, 61572529).

Appendix: Practical Application

As for the format of the compensatory frame, the compensatory frame's format is very important during phase estimation. The most crucial part is statistical characteristics which means the compensatory frame need to satisfy the Gaussian distribution. At the same time, we set the phase of compensatory frame as sweep signal, while the amplitude as the random frame follows rayleigh distribution. In this way, we can observe the sweep signal in Bob of

testing frame to ensure the channel and the system normal. From now on, the continuous variables shared by Alice and Bob will not have much difference in phase and linear proportions. The main difference between two sets of variables is that only the data at Bob adds additive Gaussian white noise, and this difference will be resolved by data negotiation. The process of phase compensation is in Fig. 7.

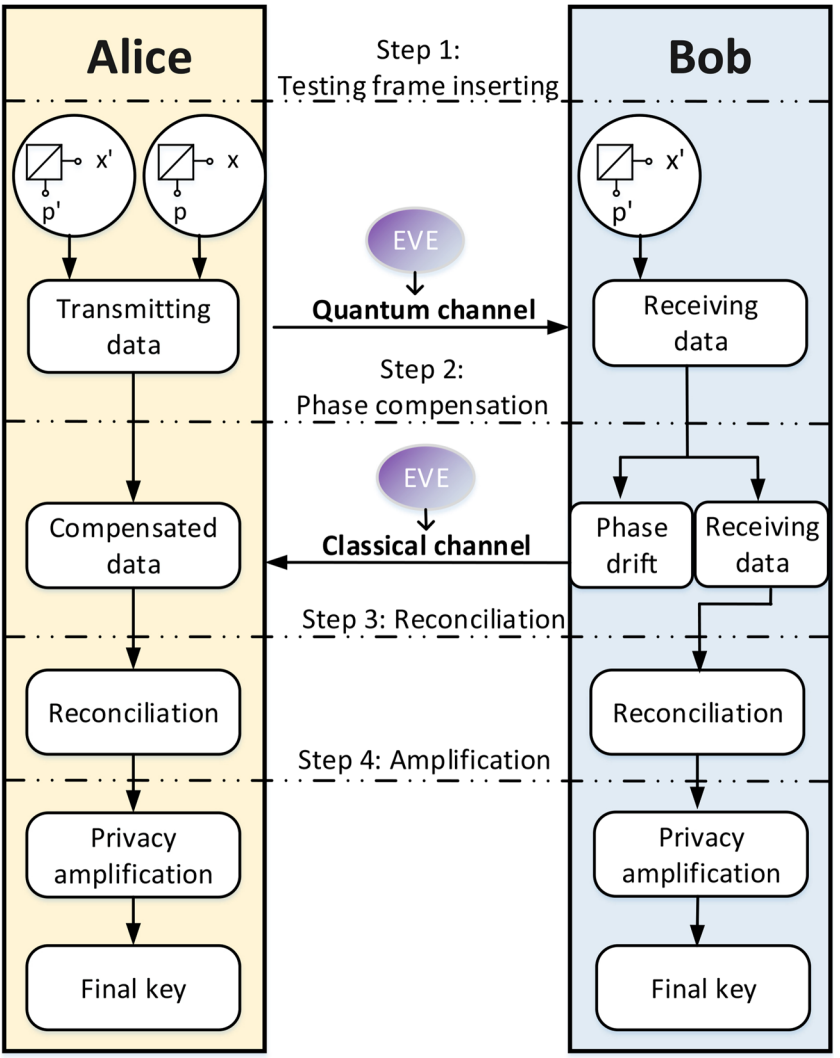

Fig. 7 Process of phase compensation

References

1. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: Rev. Mod. Phys. **81**, 1301 (2009)
2. Lo, H.K., Curty, M., Tamaki, K.: Nat. Photon. **8**, 595 (2014)
3. Samuel, L.B., Peter, V.L.: Rev. Mod. Phys. **77**, 513 (2005)
4. Diamanti, E., Lo, H.K., Qi, B., Yuan, Z.: Nat. Photon. **2**, 16025 (2016)
5. Lance, A.M., Symul, T., Sharma, V., Weedbrook, C., Ralph, T.C., Lam, P.K.: Phys. Rev. Lett. **95**, 180503 (2005)
6. Weedbrook, C., Lance, A.M., Bowen, W.P., Symul, T., Ralph, T.C., Lam, P.K.: Phys. Rev. Lett. **93**, 170504 (2004)
7. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: Rev. Mod. Phys. **84**, 621 (2012)
8. Diamanti, E., Leverrier, A.: Entropy **17**, 6072 (2015)
9. Kumar, R., Qin, H., Alléaume, R.: New J. Phys. **17**, 043027 (2015)
10. Grosshans, F., Assche, G.V., Wenger, J., Brouri, R., Cerf, N.J., Grangier, Ph.: Nature **421**, 238 (2003)
11. Biham, E., Boyer, M., Brassard, G., van de Graaf, J., Mor, T.: Algorithmica **34**, 372 (2002)
12. Kraus, B., Gisin, N., Renner, R.: Phys. Rev. Lett. **95**, 080501 (2005)
13. Scarani, V., Renner, R.: Phys. Rev. Lett. **100**, 200501 (2008)
14. Leverrier, A., García-Patrón, R., Renner, R., Cerf, N.J.: Phys. Rev. Lett. **110**, 030502 (2013)
15. Qi, B., Huang, L.L., Qian, L., Lo, H.-K.: Phys. Rev. A **76**, 053323 (2007)
16. Huang, D., Lin, D.K., Huang, P., Zeng, G.H.: Opt. Lett. **40**, 3695 (2015)
17. Huang, J.Z., Weedbrook, C., Yin, Z.-Q., Wang, S., Li, H.W., Chen, W., Guo, G.C., Han, Z.F.: Phys. Rev. A **87**, 062329 (2013)
18. Jouguet, P., Kunz-Jacques, S., Diamanti, E.: Phys. Rev. A **87**, 062313 (2013)
19. Ma, X.C., Sun, S.H., Jiang, M.S., Liang, L.M.: Phys. Rev. A **87**, 052309 (2013)
20. Soh, D.B.S., Brif, C., Coles, P.J., Lütkenhaus, N., Camacho, R.M., Urayama, J., Sarovar, M.: Phys. Rev. X **5**, 041010 (2015)
21. Qi, B., Lougovski, P., Pooser, R., Grice, W., Bobrek, M.: Phys. Rev. X **5**, 041009 (2015)
22. Corvaja, R.: Phys. Rev. A **95**, 022315 (2017)
23. Wang, T., Huang, P., Zhou, Y., Liu, W., Zeng, G.: Phys. Rev. A **97**, 012310 (2018)
24. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Rev. Mod. Phys. **74**, 145 (2002)
25. Huang, D., Huang, P., Wang, T., Li, H., Zhou, Y., Zeng, G.: Phys. Rev. A **95**, 022315 (2017)
26. Makarov, V., Brylevski, A., Hjelme, D.R.: Appl. Opt. **43**, 4385 (2004)
27. Zeng, F., Yao, J.: J. Lightwave Technol. **23**, 1721 (2005)
28. Zeng, F., Yao, J.: Opt. Express **12**, 3814 (2004)