


Article

Polarization Attack on Continuous-Variable Quantum Key Distribution with a Local Local Oscillator

Yun Shao¹, Yan Pan¹, Heng Wang¹, Yaodi Pi¹, Yang Li¹, Li Ma¹, Yichen Zhang² , Wei Huang^{1,*} and Bingjie Xu^{1,*}

¹ Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China; shaoyun@pku.edu.cn (Y.S.); py_swjtu@foxmail.com (Y.P.); wanghg1991@163.com (H.W.); jeremypipi@163.com (Y.P.); yishuihanly@pku.edu.cn (Y.L.); mali0878@163.com (L.M.)

² State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China; zhangyc@bupt.edu.cn

* Correspondence: huangwei096505@aliyun.com (W.H.); xbjpku@pku.edu.cn (B.X.)

Abstract: The estimation of phase noise of continuous-variable quantum key distribution protocol with a local local oscillator (LLO CVQKD), as a major process in quantifying the secret key rate, is closely relevant to the intensity of the phase reference. However, the transmission of the phase reference through the insecure quantum channel is prone to be exploited by the eavesdropper (Eve) to mount attacks. Here, we introduce a polarization attack scheme against the phase reference. Presently, in a practical LLO CVQKD system, only part of the phase reference pulses are measured to compensate for the polarization drift of the quantum signal pulses in a compensation cycle due to the limited polarization measurement rate, while the other part of the phase reference pulses are not measured. We show that Eve can control the phase noise by manipulating the polarization direction of the unmeasured phase reference to hide her attack on the quantum signal. Simulations show that Eve can obtain partial or total key rates information shared between Alice and Bob as the transmission distance increases. Improving the polarization measurement rate to 100% or monitoring the phase reference intensity in real-time is of great importance to protect the LLO CVQKD from polarization attack.

Keywords: continuous variable; quantum key distribution; local local oscillator; phase reference; polarization attack



Citation: Shao, Y.; Pan, Y.; Wang, H.; Pi, Y.; Li, Y.; Ma, L.; Zhang, Y.; Huang, W.; Xu, B. Polarization Attack on Continuous-Variable Quantum Key Distribution with a Local Local Oscillator. *Entropy* **2022**, *24*, 992.

<https://doi.org/10.3390/e24070992>

Academic Editors: Vladyslav Usenko, Stefano Olivares and Marcin Jarzyna

Received: 20 June 2022

Accepted: 14 July 2022

Published: 18 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In recent years, theoretical and experimental investigations of quantum key distribution for continuous variable (CVQKD) have increased tremendously [1,2]. CVQKD allows two legitimate communication parties, conventionally referred to as Alice and Bob, to share a common secret key encoded in continuous variables, for which the information-theoretical security is guaranteed by the laws of quantum mechanics. In particular, the Gaussian-modulated coherent-state (GMCS) protocol [3,4], as the most widely implemented CVQKD protocol, has the advantage of compatibility with classical coherent communication infrastructures. This protocol has demonstrated the secret key transmission up to over a 200-km optical fiber [5], and has achieved a field test over a 50-km commercial fiber [6]. At present, the GMCS CVQKD protocol is proved to be secure against the collective attacks and coherent attacks [7–12]. Moreover, the composable security proofs of the protocol have been proposed and improved [13–16]. However, theoretical description used for security proofs may not necessarily faithfully describe the actual setup. Therefore, bridging the gap between theoretical model and practical system is still required to build a robust implementation of quantum cryptography in practical use.

In fact, the practical security problem is a central challenge in all kinds of QKD protocols. Due to the technological imperfection in a QKD system, potential exploitable loopholes are opened for the eavesdropper Eve to launch attacks. In a practical transmission local oscillator (LO) CVQKD system, the LO is generated from Alice and transmitted to Bob through the insecure quantum channel for ease of coherent detection of the quantum signal. In this case, Eve can manipulate the LO to compromise the security of the system severely [17–21]. In order to avoid Eve’s access to the LO, an intriguing local LO protocol for CVQKD (LLO CVQKD) has been proposed and demonstrated [22–24], in which the LO is generated on Bob’s side. To date, considerable research have been conducted to improve the protocol [1,25], and a high-rate LLO CVQKD based on Gaussian modulation up to 7.04 Mbits/s over 25-km optical fiber in the asymptotic limit [26]. More recently, the key rate based on discrete modulation CVQKD (in comparison to Gaussian modulation) has been improved by an order of magnitude [27]. Despite the outstanding superiority of the LLO CVQKD in simplifying the hardware required and circumventing the LO attacks, its performance improvement is still severely retarded by the relatively high phase noise [28,29]. As a realistic option, one can use the trusted phase noise model to significantly improve the phase noise tolerance of the LLO CVQKD, in which part of the phase noise that can be locally calibrated by Bob is moved from the channel-added noise to the detector-added noise to get a better QKD performance [30]. For example, with some typical parameters, the transmission distance of the LLO CVQKD based on Gaussian modulation is limited to 40-km. Then, using the trusted phase noise model one can increase the corresponding maximum transmission distance by more than 65% and the secret key rate at the transmission distance of 25-km by more than 60% with the same simulation parameters [30]. Nevertheless, in a practical LLO CVQKD system, a relatively weak classical phase reference is generated from the signal laser and propagates along with the quantum signal from Alice to Bob to establish a reliable phase relationship between the quantum signal and the LO. This configuration will inevitably leave a security loophole for Eve to attack the phase reference [29,31]. Therefore, it is an ongoing task to search the security vulnerabilities and propose appropriate countermeasures.

Here, we introduce a polarization attack scheme against the LLO CVQKD protocol, inspired by the polarization attack on the transmission LO CVQKD [32]. This attack arises from the limited compensation rate in the polarization compensation process for the quantum signal. In a practical LLO CVQKD system, the phase reference is used to compensate for the polarization drift between the quantum signal and the LO. It is shown that Eve can use the system imperfection to hide her attack on the quantum signal by manipulating the polarization of the phase reference. The security of the LLO CVQKD system can be fully compromised without corresponding countermeasures.

This paper is organized as follows: in Section 2, we review the LLO CVQKD scheme and the trusted phase noise model, where the calculation formulas for secret key rate are presented. In Section 3, we discuss the polarization attack scheme against the phase reference as well as the countermeasures. Finally, the conclusion is given in Section 4.

2. Trusted Phase Noise Model for LLO CVQKD

In the following, we first review the trusted phase noise model for LLO CVQKD protocol, which will be essential for the analysis in the next section. We then present the calculations of the asymptotic secret key rate for CVQKD under the collective attack.

For simplicity, we assume the time-polarization multiplexing system for GMCS LLO CVQKD protocol based on heterodyne detection [33,34] are adopted, as illustrated in Figure 1. Alice prepares few-photon coherent state $|x + ip\rangle$ as quantum signal, in which the two orthogonal quadratures x and p are continuously modulated with Gaussian distribution centered on zero and with variance $V_A N_0$. Here, N_0 is the shot noise variance, and all noise variances in this paper are expressed in shot noise units (SNU). The coherent-state quantum signal is interleaved with the time-delayed phase reference and transmitted through an untrusted quantum channel that is characterized by transmittance T and excess

noise ζ . On the receiver side, Bob performs heterodyne detection using a locally generated LO pulses to measure both quadratures of the quantum signal simultaneously. He also performs heterodyne detection to measure both quadratures of the phase reference simultaneously so as to estimate the phase rotation of the quantum signal between Alice’s and Bob’s independent lasers frames. That is reasonable because the phase reference and the quantum signal are generated from the same laser and experience similar environmental effects. The coherent detector features an efficiency η and electronic noise v_{el} . After Alice and Bob obtain the correlated Gaussian variables as raw key, they can perform postprocessing, including parameter estimation, error correction, and privacy amplification, to get a secret key.

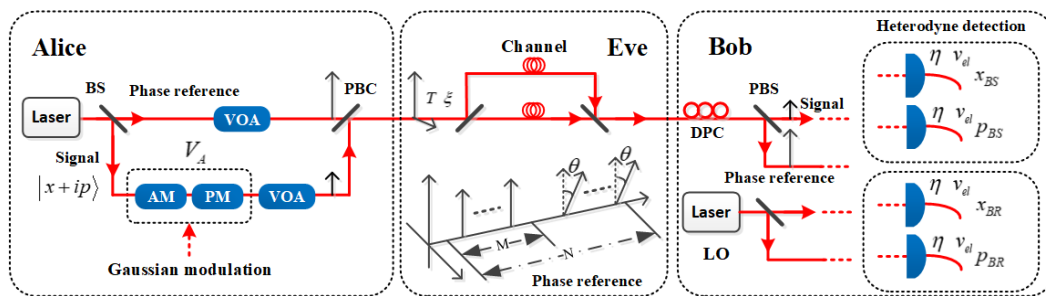


Figure 1. Schematic representation of the time-polarization multiplexing LLO CVQKD scheme. BS is the optical beam splitter, AM is the optical amplitude modulator, PM is the optical phase modulator, VOA is the variable optical attenuator, PBC is the optical polarization beam combiner, DPC is the dynamic polarization controller, and PBS is the optical polarization beam splitter.

Based on the scheme described above, the phase noise for the quantum signal can be estimated by [21,30,35]

$$\zeta_{\text{phase}} \approx \zeta_{\text{error}} = V_A \left(\frac{\chi + 1}{E_R^2} \right). \tag{1}$$

where the phase noise ζ_{phase} is dominated by the phase reference measurement noise ζ_{error} . Here, E_R is the amplitude of the phase reference on Bob’s side, χ is the total added noise imposed on the phase reference given by [30,31,35]

$$\chi = \frac{1 - T}{T} + \varepsilon_0 + \frac{2 - \eta + 2v_{el}}{T\eta} \tag{2}$$

where ε_0 is the excess noise of the phase reference with typical value $\varepsilon_0 = 0.002$ [36]. In the trusted phase noise model [30], part of the phase reference measurement noise associated with the detector efficiency η and the electronic noise v_{el} of Bob’s detector as well as the phase reference intensity on the receiver side that can be locally calibrated by Bob is considered to be trusted in order to get a higher secret key rate and longer transmission distance. Therefore, Equation (1) can be decomposed as:

$$\zeta_{\text{phase}} = \zeta_{\text{phase}}^U + \frac{\zeta_{\text{phase}}^T}{T}, \tag{3}$$

According to Equations (1)–(3), we have

$$\zeta_{\text{phase}}^U = \frac{V_A(1 + T\varepsilon_0)}{TE_R^2}, \tag{4}$$

$$\zeta_{\text{phase}}^T = \frac{V_A(2 - \eta + 2v_{el})}{\eta E_R^2} \tag{5}$$

In this regard, the added noises for the quantum signal can be modeled as follows [30]:

$$\chi_{\text{line}} = \frac{1}{T} - 1 + \zeta_{\text{tot}} - \frac{\zeta_{\text{phase}}^T}{T}, \tag{6}$$

$$\chi_{\text{het}} = \frac{2 - \eta + 2v_{el}}{\eta} + \zeta_{\text{phase}}^T, \tag{7}$$

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T}. \tag{8}$$

In Equation (6), χ_{line} represents the total channel added noise referred to the channel input, in which ζ_{tot} stands for the total excess noise obtained from the parameters estimation procedure, and mainly consists of the following parts [30]:

$$\zeta_{\text{tot}} = \zeta_0 + \zeta_{\text{AM}} + \zeta_{\text{LE}} + \zeta_{\text{ADC}} + \zeta_{\text{phase}}^U + \frac{\zeta_{\text{phase}}^T}{T}. \tag{9}$$

Here, ζ_0 is the system excess noise stemming from the unidentified or unprotected sources [28]. ζ_{AM} is the modulation noise that can be expressed as [35] $\zeta_{\text{AM}} = (E_{\text{Smax}}^A)^2 10^{-d_{dB}/10}$, where $E_{\text{Smax}}^A \approx \sqrt{10V_A}$ quantifies the maximal amplitude of the quantum signal. ζ_{ADC} is the analog-to-digital quantization noise which satisfies [34] $\zeta_{\text{ADC}} \geq (E_{\text{Smax}}^A)^2 / (12 \times 2^n)$, where E_{Smax}^A stands for the maximal amplitude of the quantum signal to be modulated. ζ_{phase}^U is the untrusted part of the phase noise referred to the channel input, and ζ_{phase}^T corresponds to the trusted part of the phase noise referred to Bob’s input. In Equation (7), χ_{het} represents the detection added noise referred to Bob’s input. Equation (8) represents the total added noise referred to the channel input.

It is known that the above prepare-and-measure CVQKD scheme is equivalent to the entanglement-based protocol, as outlined in Figure 2, for which the security against collective attacks has been strictly proved [37]. The asymptotic secret key rate of the LLO CVQKD in the context of reverse reconciliation can be expressed as [37]

$$K = \beta I_{\text{AB}} - \chi_{\text{BE}}, \tag{10}$$

where β is the reconciliation efficiency, I_{AB} is Shannon mutual information between Alice and Bob, and χ_{BE} is the Holevo information bound between Eve and Bob. The mutual information can be given by [37,38]

$$I_{\text{AB}} = \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \tag{11}$$

$$\chi_{\text{BE}} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right), \tag{12}$$

with $V = V_A + 1$ is the variance of the thermal state that Alice sent to Bob, and $G(x) = (x + 1) \log_2(x + 1) - \log_2 x$. The symplectic eigenvalues can be expressed as

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2} [A \pm \sqrt{A^2 - 4B}], \\ \lambda_{3,4}^2 &= \frac{1}{2} [C \pm \sqrt{C^2 - 4D}], \\ \lambda_5 &= 1. \end{aligned} \tag{13}$$

where

$$\begin{aligned} A &= V^2(1 - 2T) + 2T + T^2(V + \chi_{\text{line}})^2, \\ B &= T^2(V\chi_{\text{line}} + 1)^2, \end{aligned}$$

$$C = \frac{1}{[T(V + \chi_{\text{tot}})]^2} \left[A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}} \times (V\sqrt{B} + T(V + \chi_{\text{line}})) + 2T(V^2 - 1) \right],$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})} \right)^2. \tag{14}$$

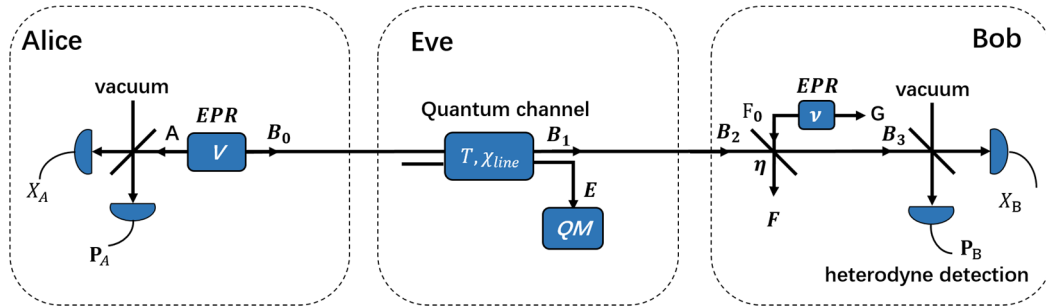


Figure 2. Schematic representation of the entanglement-based description of the CVQKD protocol. Alice’s Gaussian modulation of the coherent state is modelled by a heterodyne detection of one half of an EPR state with variance V . Bob’s detector noise is modelled by a beam splitter with transmission η , and the electronic v_{el} is modelled by an EPR state with variance v . The QM stands for Eve’s quantum memory.

3. Polarization Attack on the Phase Reference

In this section, we aim to discuss the security vulnerability and corresponding potential hack attack caused by technological imperfection of a practical LLO CVQKD system such as polarization turbulence of the quantum signal. Generally, the phase reference in LLO CVQKD system is required to transmit through the quantum channel to monitor and compensate for the phase and polarization drift of the quantum signal, which, however, could be used by Eve to mount attacks, such as the polarization attack.

In the previous study for the transmission LO CVQKD system, as the SNU plays an important role in CVQKD [39], a quantum hacking method was identified where Eve can attack the unmeasured LO pulses to control and tamper the practical SNU by using the limited compensation rate during the polarization compensation for the signal pulses [32]. Unlike the transmission LO CVQKD protocol, in the LLO CVQKD protocol, since the LO pulses are generated by Bob on the receiver side, potential attacks against the LO pulses will be ruled out. For a practical LLO CVQKD system, in order to establish a stable coherent detection for the quantum signal, aligned laser polarization directions between the quantum signal and the LO pulse are desired. However, the polarization drift of the quantum signal will reduce the efficiency of coherent detection owing to random perturbation in the quantum channel. Therefore, a polarization-drift compensation process is particularly necessary. From a practical point of view, in the LLO CVQKD system, since the quantum signal is too weak to identify its polarization direction on the receiver side, the weak classical phase reference is used to perform polarization measurement and compensation for the quantum signal. Ideally, a real-time polarization measurement and feedback control of each pulse for the phase reference and quantum signal would compensate for the polarization drift. More specially, as the polarization measurement rate of current commercial devices is much lower than the repetition frequency of the LLO CVQKD system [32], the polarization compensation in a practical system is performed by measuring part of the phase reference pulses in a compensation cycle. It is assumed that the polarization of the measured pulses is the same as that of the unmeasured pulses in a compensation cycle. Nevertheless, this approach will bring security risk, because Eve can manipulate the polarization direction of the unmeasured phase reference pulses, which would result in the discrepancy of polarization between the unmeasured pulses and the measured pulses. In the following discussion, we will show that in the context of LLO

CVQKD system, Eve has the ability to attack the unmeasured phase reference pulses to change the trusted part of the phase noise by manipulating the laser polarization of the unmeasured phase reference pulses in the quantum channel, which will make Alice and Bob overestimate the secret key rate.

As shown in Figure 1, in a time-polarization multiplexing LLO CVQKD system, on Alice's side, the parallel polarized signal pulse and phase reference pulse are recombined by a polarization beam combiner (PBC) to orthogonal polarization modes. After propagation through the lossy channel, a polarization-drift compensation process for the signal pulse and the phase reference pulse is implemented on the receiver side. First, in a polarization compensation cycle with N phase reference pulses, Bob selects M pulses to measure their polarization to determine the polarization drift from the target polarization. Second, a feedback signal based on the above measured results is generated to modulate the polarization controller to compensate for the polarization drift of the signal pulse and the phase reference pulse. Then the signal pulse and the phase reference pulse are demultiplexed and split into two paths by the polarization beam splitter (PBS), and made to interfere with the LO pulse separately on a balanced heterodyne detector.

In the trusted phase noise model for LLO CVQKD protocol, it is usually assumed that the phase reference intensity E_R^2 is measured and the trusted part of the phase noise ξ_{phase}^T is calibrated before the QKD run. In this case, Bob has no idea about ξ_{phase}^T when the intensity of the phase reference fluctuates during the QKD run. Consequently, Alice and Bob will get a false key rate if Eve can manipulate the intensity of the phase reference by changing its polarization direction during the key distribution process, while Bob still adopts the previously measured intensity to estimate the trusted part of the phase noise, as illustrated in Figure 1. To perform this attack, during the trusted phase noise calibration stage, Eve intercepts all the quantum signal and the phase reference sent by Alice at the channel input, and then separates them into her own two perfect quantum channel. For the phase reference pulse within one compensation cycle, Eve makes the polarization direction of the $N - M$ pulses deviate from the polarization direction of the M pulses whose polarization are measured for polarization drift compensation. Here, we use θ to represent the misalignment angle between them. After the polarization compensation, the intensity projection of the $N - M$ pulses in the main axis of the PBS at Bob's side thus becomes $E_R^2 \cos^2 \theta$. Following the scheme described above in Figure 1, according to Equation (5), the trusted part of the phase noise under the attack can be expressed as

$$\xi_{\text{phase}}^{T-\text{attack}} = V_A \left[\frac{2 - \eta + 2\nu_{el}}{\eta[kE_R^2 + (1 - k)E_R^2 \cos^2 \theta]} \right] = \tilde{\zeta}_{\text{phase}}^T \left[\frac{1}{k + (1 - k)\cos^2 \theta} \right]. \quad (15)$$

where $k = M/N$ is the ratio of the measured pulses to the compensation cycle pulses, which is named as polarization measurement rate (PMR).

Next, when Alice and Bob start the key distribution process, Eve can reduce θ to narrow the deviation of the polarization directions between the measured pulses (M) and the unmeasured pulses ($N - M$). This meant that the actual average intensity of the phase reference projected on the main axis of the PBS will be higher than its initial calibrated value. Note that the maximum change of the average intensity corresponds to the reduction of θ value to zero. In this case, one can apply Equation (15) to obtain the reduction of the trusted part of the phase noise, which can be written as

$$\Delta \tilde{\zeta}_{\text{phase}}^T = \xi_{\text{phase}}^{T-\text{attack}} \Big|_{\theta=\theta} - \xi_{\text{phase}}^{T-\text{attack}} \Big|_{\theta=0} = \tilde{\zeta}_{\text{phase}}^T \left[\frac{1}{k + (1 - k)\cos^2 \theta} \right] - \xi_{\text{phase}}^T. \quad (16)$$

One can find that the larger the misalignment angle θ controlled by Eve, the more the reduction of the trusted phase noise. It is worth noting that simply reducing the trusted phase noise does not necessarily imply that it will help Eve steal information about the quantum signal. This is because the total excess noise ζ_{tot} is estimated from the parameters estimation procedure. The reduction of the trusted phase noise will lead to the reduction

of the total excess noise, and the key rate information available to Eve can be estimated and discarded by Alice and Bob through the privacy amplification process [4]. Therefore, for purposes of getting the encoded information, Eve has to increase her attack on the quantum signal during the key distribution process, which will inevitably introduce excess noise ζ_{attack} . In this case, Eve can use the reduced part of the trusted phase noise to compensate for the introduced excess noise to hide her attack on the quantum signal, and gain information when the total excess noise is within the maximum tolerable excess noise. For simplicity of analysis, we assume that the reduction of the trusted phase noise is equal to excess noise introduced by Eve, i.e.,

$$\zeta_{\text{attack}} = \Delta\zeta_{\text{phase}}^T \tag{17}$$

Hence, when the phase reference is attacked, the added excess noise for the LLO CVQKD system under the trusted phase noise model can be expressed as

$$\lambda_{\text{line}}^{\text{attack}} = \frac{1}{T} - 1 + \zeta_{\text{tot}} - \frac{\zeta_{\text{phase}}^T}{T} + \frac{\zeta_{\text{attack}}}{T}, \tag{18}$$

$$\lambda_{\text{het}}^{\text{attack}} = \frac{2 - \eta + 2v_{el}}{\eta} + \zeta_{\text{phase}}^T - \Delta\zeta_{\text{phase}}^T, \tag{19}$$

$$\lambda_{\text{tot}}^{\text{attack}} = \lambda_{\text{line}}^{\text{attack}} + \frac{\lambda_{\text{het}}^{\text{attack}}}{T}. \tag{20}$$

Therefore, under the polarization attack, the total channel-added noise is increased while the detector-added noise is reduced, which will cause Alice and Bob to overestimate the secret key rate. Combining the above scheme with the calculations from Equations (10)–(14), we can get the key rate under the polarization attack.

In Figure 3, we simulate the secret key rate results for the LLO CVQKD system under the trusted phase noise model with a fixed PMR $k = 0.5$. The other typical parameters, as used in Refs. [28–31,34], are as follows: reconciliation efficiency $\beta = 0.95$, detector efficiency $\eta = 0.5$, modulation variance $V_A = 4$, electronic noise $v_{el} = 0.1$, attenuation coefficient $\alpha = 0.2$ dB/km, phase reference intensity $E_R^2 = 1000$, system excess noise $\zeta_0 = 0.01$, ADC quantization number $n = 10$, AM dynamics $d_{dB} = 40$, and finite extinction ratios $R_e = 40$ dB and $R_p = 30$ dB. The right solid red line represents the result without polarization attack, where the maximum transmission distance is larger than 60 km. Compared to the result without attack, the phase reference polarization attack can fully constitute threat to the security of the LLO CVQKD protocols. One can find that Eve’s intercepted information of the quantum signal is proportional to the misalignment angle θ of the unmeasured phase reference pulse. The left orange solid line represents the extreme polarization attack case where the misalignment angle is $\theta = \pi/2$. In this case, the real maximum transmission distance is dropped to less than 40 km, that is Eve can obtain partial or total key rate when the transmission distance is lower or higher than 40 km. We also calculate the secret key rate under different situations at the transmission distance of 30 km. It is shown that Eve can steal 8%, 32%, and 52% of the key information shared by Alice and Bob when the misalignment angles are $\theta = \pi/6$, $\theta = \pi/3$, and $\theta = \pi/2$, respectively. Moreover, the black dotted line shows that for small misalignment angle ($\theta = \pi/30$) the simulation approaches that of the case without polarization attack.

We further simulate the secret key rate at different PMR for a fixed misalignment angle $\theta = \pi/4$. The other simulation parameters are the same as that in Figure 3. One can see from Figure 4 that the larger the PMR, the more information about the quantum signal Eve stole. The left orange solid line represents the results with PMR = 0, where all the phase reference pulses can be manipulated by Eve to change the polarization to reduce the trusted phase noise. It can be speculated that the polarization attack can be prevented as the PMR increases to 100%. From the simulations one can find that Eve can steal 3%,

10%, 23%, and 52% of the quantum signal held by Alice and Bob when the PMR are $k = 0.9$, $k = 0.6$, $k = 0.3$, and $k = 0$, respectively.

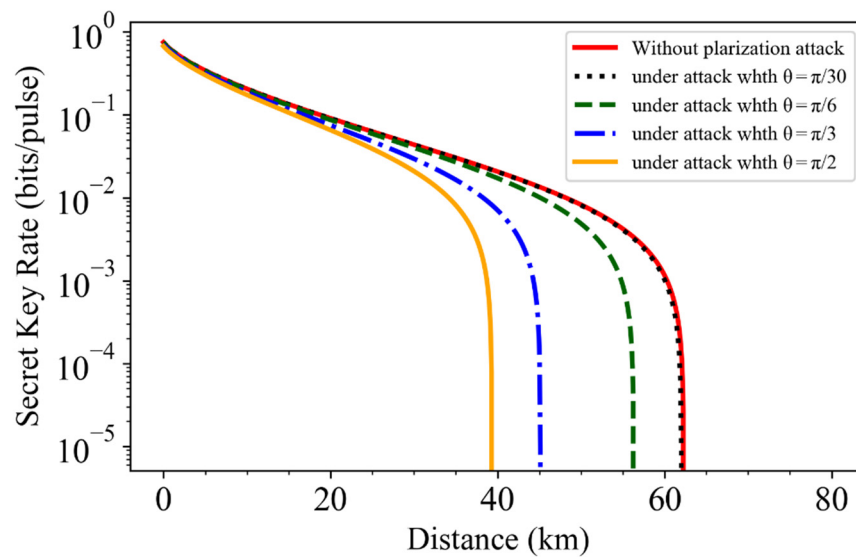


Figure 3. Simulations of secret key rate for the LLO CVQKD system under the trusted phase noise model. The right solid red line represents the result without attack. The black dotted line, green dashed line, blue dashed-dotted line, and left orange solid line represent the results under polarization attack when the misalignment angle θ is $\pi/20$, $\pi/6$, $\pi/3$, and $\pi/2$, respectively, where the PRM is fixed with $k = 0.5$.

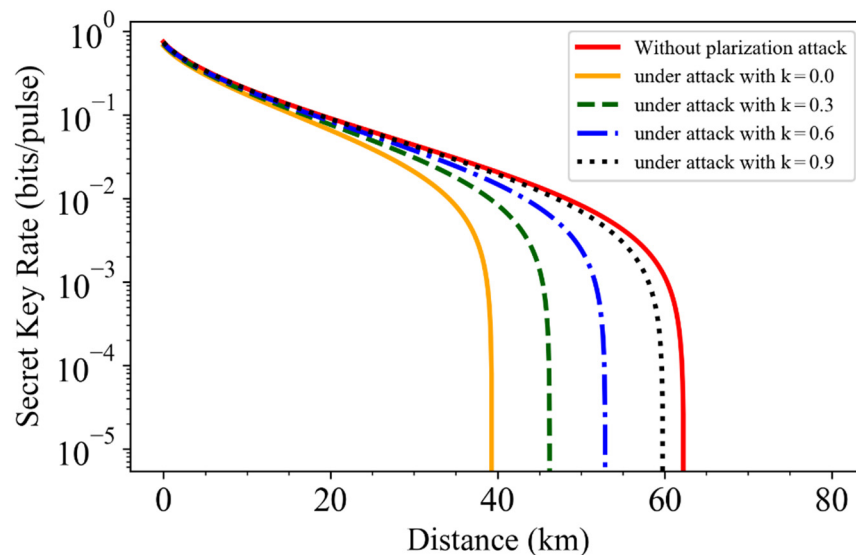


Figure 4. Simulations of secret key rate for the LLO CVQKD system under the trusted phase noise model. The right red solid line represents the result without attack. The black dotted line, blue dashed-dotted line, green dashed line and right orange solid line represent the results under polarization attack when the PMR k is 0, 0.3, 0.6 and 0.9, respectively, where the misalignment angle is fixed with $\theta = \pi/4$.

The above described attack scheme uncovers the importance of monitoring the intensity of the phase reference in real-time, which has been discussed in previous studies [31]. Mover, based on the analysis in Figure 4, one can find that improving the PMR of the phase reference pulse to 100% is also an effective way to protect the LLO CVQKD protocol from the polarization attack.

Next, let us look into the difference between the phase reference intensity attack [31] and the proposed phase reference polarization attack. Indeed, in the above two attack strategies, Eve essentially steals the quantum signal by manipulating the intensity of the phase reference. However, there are differences in both the attack schemes and the countermeasures. First, in the former attack scheme, Eve increases the intensity of the whole phase reference pulses directly using an intensity amplifier, while in the latter attack scheme, Eve does this by attacking the polarization compensation module to manipulate the polarization of the unmeasured phase reference pulses in a compensation cycle. Second, the countermeasures against the attacks are not exactly the same. For the latter attack scheme, in addition to monitoring the intensity of the phase reference in real time, one could improve the PMR to resist the attack.

4. Conclusions

In summary, we have studied the practical security of LLO CVQKD system related to phase reference. In a practical system, part of the phase reference pulses are used to measure and compensate for the polarization drift of the signal pulses. We have shown that the limited PMR for the phase reference will leave a security loophole, which can be exploited by Eve to mount attacks. We have proposed a polarization attack scheme, from which Eve can reduce the trusted phase noise to compensate for the introduced attack noise by manipulating the polarization of the unmeasured phase reference pulses. The simulations show that the larger the misalignment angle controlled by Eve and the smaller the PMR, the more information Eve can steal. To improve the practical security of the system, on the one hand, one can increase the PRM to 100%; on the other hand, one can monitor the intensity of the phase reference in real time.

Author Contributions: Y.S. conducted the simulations and the analysis. B.X. and W.H. supervised the research work. Y.S., Y.P. (Yan Pan), H.W. and B.X. wrote the original draft preparation. Y.P. (Yaodi Pi), Y.L., L.M., W.H. and Y.Z. discussed the results and reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China (Grant No. 2020YFA0309704), the National Natural Science Foundation of China (Grants No. U19A2076, No. 61901425, No. 62171418, and No. 62101516), the Sichuan Science and Technology Program (Grants No. 2019JDJQ0060, No. 2020YFG0289, and No. 2022YFG0330), the Chengdu Major Science and Technology Innovation Program (Grant No. 2021-YF08-00040-GX), the Chengdu Key Research and Development Support Program (Grants No. 2021-YF05-02430-GX, and No. 2021-YF09-00116-GX), the Sichuan Science and Technology Program (Grants No. 2022YFG0330, and No. 2021YJ0313), the Technology Innovation and Development Foundation of China Cyber Security (Grant No. JSCX2021JC001), and the Foundation of Science and Technology on Communication Security Laboratory (Grant No. 61421030402012111).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [[CrossRef](#)]
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012. [[CrossRef](#)]
3. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [[CrossRef](#)]
4. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [[CrossRef](#)]
5. Zhang, Y.C.; Chen, Z.Y.; Pirandola, S.; Wang, X.Y.; Zhou, C.; Chu, B.J.; Zhao, Y.J.; Xu, B.J.; Yu, S.; Guo, H. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **2020**, *125*, 010502. [[CrossRef](#)] [[PubMed](#)]

6. Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z.; et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006. [[CrossRef](#)]
7. Grosshans, F.; Cerf, N.J. Continuous-variable quantum cryptography is secure against non-Gaussian attacks. *Phys. Rev. Lett.* **2004**, *92*, 047905. [[CrossRef](#)] [[PubMed](#)]
8. García-Patrón, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [[CrossRef](#)]
9. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [[CrossRef](#)]
10. Pirandola, S.; Lloyd, S.; Braunstein, S.L. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504. [[CrossRef](#)]
11. Renner, R.; Cirac, J.I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504. [[CrossRef](#)] [[PubMed](#)]
12. Leverrier, A.; García-Patrón, R.; Renner, R.; Cerf, N.J. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502. [[CrossRef](#)] [[PubMed](#)]
13. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [[CrossRef](#)]
14. Leverrier, A. Security of Continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **2017**, *118*, 200501. [[CrossRef](#)] [[PubMed](#)]
15. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **2021**, *3*, 013279. [[CrossRef](#)]
16. Pirandola, S. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.* **2021**, *3*, 043014. [[CrossRef](#)]
17. Huang, J.-Z.; Weedbrook, C.; Yin, Z.-Q.; Wang, S.; Li, H.-W.; Chen, W.; Guo, G.-C.; Han, Z.-F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [[CrossRef](#)]
18. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309. [[CrossRef](#)]
19. Huang, J.Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **2014**, *89*, 032304. [[CrossRef](#)]
20. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339. [[CrossRef](#)]
21. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [[CrossRef](#)]
22. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the local oscillator “locally” in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **2015**, *5*, 041009. [[CrossRef](#)]
23. Soh, D.B.S.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **2015**, *5*, 041010. [[CrossRef](#)]
24. Huang, D.; Lin, D.K.; Huang, P.; Zeng, G.H. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **2015**, *40*, 3695. [[CrossRef](#)] [[PubMed](#)]
25. Guo, H.; Li, Z.; Yu, S.; Zhang, Y. Towards practical quantum key distribution using telecom components. *Fundam. Res.* **2021**, *1*, 96–98. [[CrossRef](#)]
26. Wang, H.; Pi, Y.D.; Huang, W.; Li, Y.; Shao, Y.; Yang, J.; Liu, J.L.; Zhang, C.L.; Zhang, Y.C.; Xu, B.J. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. *Opt. Express* **2020**, *28*, 32882. [[CrossRef](#)]
27. Wang, H.; Li, Y.; Pi, Y.D.; Pan, Y.; Shao, Y.; Ma, L.; Yang, J.; Zhang, Y.C.; Huang, W.; Xu, B.J. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. *Commun. Phys.* **2022**, *5*, 162. [[CrossRef](#)]
28. Qi, B.; Lim, C.C.W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator. *Phys. Rev. Appl.* **2018**, *9*, 054008. [[CrossRef](#)]
29. Ren, S.; Kumar, R.; Wonfor, A.; Tang, X.; Penty, R.; White, I. Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise. *J. Opt. Soc. Am. B* **2019**, *36*, B7–B15. [[CrossRef](#)]
30. Shao, Y.; Wang, H.; Pi, Y.D.; Huang, W.; Li, Y.; Liu, J.L.; Yang, J.; Zhang, Y.C.; Xu, B.J. Phase noise model for continuous-variable quantum key distribution with a local local oscillator. *Phys. Rev. A* **2021**, *104*, 032608. [[CrossRef](#)]
31. Shao, Y.; Li, Y.; Wang, H.; Pan, Y.; Pi, Y.D.; Zhang, Y.C.; Huang, W.; Xu, B.J. Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator. *Phys. Rev. A* **2022**, *105*, 032601. [[CrossRef](#)]
32. Zhao, Y.; Zhang, Y.; Huang, Y.; Xu, B.; Yu, S.; Guo, H. Polarization attack on continuous-variable quantum key distribution. *J. Phys. B At. Mol. Opt. Phys.* **2019**, *52*, 015501. [[CrossRef](#)]
33. Wang, T.; Huang, P.; Zhou, Y.; Liu, W.; Ma, H.; Wang, S.; Zeng, G. High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt. Express* **2018**, *26*, 2794. [[CrossRef](#)]
34. Wang, T.; Huang, P.; Zhou, Y.; Liu, W.; Zeng, G. Pilot-multiplexed continuous-variable quantum key distribution with a local local oscillator. *Phys. Rev. A* **2018**, *97*, 012310. [[CrossRef](#)]

35. Marie, A.; Alléaume, R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 012316. [[CrossRef](#)]
36. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381. [[CrossRef](#)]
37. Lodewyck, J.; Bloch, M.; Garía-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; Laughlin, S.W.M.; et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305. [[CrossRef](#)]
38. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B* **2009**, *42*, 114014. [[CrossRef](#)]
39. Zhang, Y.; Huang, Y.; Chen, Z.; Li, Z.; Yu, S.; Guo, H. One-time shot noise unit calibration method for continuous-variable quantum key distribution. *Phys. Rev. Appl.* **2020**, *13*, 024058. [[CrossRef](#)]