Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack

Jing-Zheng Huang,[1,*] Christian Weedbrook,[2] Zhen-Qiang Yin,[1,†] Shuang Wang,[1,‡] Hong-Wei Li,[1] Wei Chen,[1] Guang-Can Guo,[1] and Zheng-Fu Han[1]

[1]*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China*

[2]*Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada*

(Received 1 February 2013; published 24 June 2013)

The security proofs of continuous-variable quantum key distribution are based on the assumptions that the eavesdropper can neither act on the local oscillator nor control Bob's beam splitter. These assumptions may be invalid in practice due to potential imperfections in the implementations of such protocols. In this paper, we consider the problem of transmitting the local oscillator in a public channel and propose a wavelength attack which allows the eavesdropper to control the intensity transmission of Bob's beam splitter by switching the wavelength of the input light. Specifically we target continuous-variable quantum key distribution systems that use the heterodyne detection protocol using either direct or reverse reconciliation. Our attack is proved to be feasible and renders all of the final keys shared between the legitimate parties insecure, even if they have monitored the intensity of the local oscillator. To prevent our attack on commercial systems, a simple wavelength filter should be randomly added before performing monitoring detection.

DOI: 10.1103/PhysRevA.87.062329 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) enables two distant partners, Alice and Bob, to share common secret keys in the presence of an eavesdropper, Eve [1,2]. In theory, the unconditional security of the QKD protocol is guaranteed based on the laws of physics, in particular, the no-cloning theorem. But in practice, the key components of practical QKD systems have imperfections that do not fulfill the assumptions of ideal devices in theoretical security proofs. In discrete-variable QKD, imperfect devices such as single-photon detectors, phase modulators, Faraday mirrors, and fiber beam splitters open security loopholes to Eve and lead to various types of attacks [3–12].

Continuous-variable (CV) QKD [13] has developed immensely over the past decade [14], to the point that there are companies selling commercially available systems [15,16]. Even so, CV-QKD is potentially vulnerable to such idealization-to-practical problems that plague its discrete variable counterpart. In CV-QKD protocols, Alice encodes the key information onto the quadratures, $\hat{X}$ and $\hat{P}$, on a bunch of coherent states and sends them on to Bob. Bob measures one or both quadratures by performing homodyne [17] or heterodyne [18] detection on the signal with a relatively strong local oscillator (LO). Finally, they perform direct or reverse reconciliation and a privacy amplification process to distill a common secret key [1,13]. In practice, it is extremely difficult for Bob to generate an LO with the same initial polarization and phase as Alice's signal. Therefore, Alice prepares both the signal and the LO and sends them to Bob in the same optical fiber channel at the same time to avoid large drifts of the relative polarization and phase [19]. However, this implementation leaves a security loophole open for Eve.

In Ref. [20], the authors proposed an equal-amplitude attack. To perform this attack, Eve first intercepts the signal and LO and measures both of the quadratures by performing heterodyne detection on them. According to her measurement results, she reproduces two weak squeezed states which have the same intensity level as the signal and sends them onto Bob. Bob treats these two fake states as signal and LO and performs detections on them as usual. But now the detection is neither homodyne nor heterodyne detection, therefore Eve is able to make the extra noise of Bob's measurement much lower than the shot noise level. As a result, the total deviation between Bob's measurement and Alice's preparation is lower than the tolerable threshold derived from the theoretical security proofs [21,22]. Hence Alice and Bob cannot discover the presence of Eve.

In order to prevent this attack without modifying the original measurement setup, Bob needs to monitor the total intensity or the LO intensity [20]. We note that in this attack, Eve is assumed to be unable to control Bob's beam splitters. But in one of our recent studies [12], we found that it is possible for Eve to control the outputs of fiber beam splitters by utilizing their wavelength-dependent properties [23–25]. Importantly, such wavelength-dependent properties can be found in commercial CV-QKD systems [15,16]. Making use of this loophole, we propose a wavelength attack on a practical CV-QKD system using a heterodyne detection protocol [18]. Using this attack Eve can, in principle, achieve all of the secret keys without being discovered, even if Bob has monitored the total intensity or the LO intensity. Such an attack has practical and commercial consequences.

In the security analysis of CV-QKD protocols with direct (reverse) reconciliation, $V_{A|B}$ ($V_{B|A}$), Alice (Bob)'s conditional variance of Bob (Alice) has a status similar to that of the quantum bit error rate in discrete-variable QKD protocols. To

*jzhuang@mail.ustc.edu.cn
†yinzheqi@mail.ustc.edu.cn
‡wshuang@ustc.edu.cn

show that the hidden Eve would not be discovered in our attack, our method proves that the upper bound of $V_{A|B}$ ($V_{B|A}$) under our wavelength attack is always lower than the maximum value allowed by the secret key rate formula [18,22].

This paper is organized as follows. In Sec. II, we first review the heterodyne protocol and the wavelength-dependent properties of certain fiber beam splitters, then we propose a wavelength attack scheme on an all-fiber CV-QKD system using a heterodyne protocol in Sec. III. We prove the feasibility of this wavelength attack in Sec. IV and, finally conclude in Sec. V.

II. PRELIMINARY

A. Heterodyne detection protocol

In the heterodyne protocol [18], Alice first prepares a displaced vacuum state that will be sent to Bob. This is realized by choosing two real numbers X_A and P_A from a Gaussian distribution of variance V_A and zero mean. The whole ensemble of coherent states that Alice will send to Bob is given by the thermal state with variance $V = V_A + 1$. Bob receives this coherent state and simultaneously measures both the amplitude and the phase quadratures of the state using heterodyne detection. After repeating this process many times, they finally extract a binary secret key by using either a direct reconciliation [26] or a reverse reconciliation algorithm [18]. A typical CV-QKD system using a heterodyne protocol can be realized by the schematic shown in Fig. 1. In this scheme, time and polarization multiplexing are used so that the signal and LO can be transmitted in the same channel without interfering. To avoid the equal-amplitude attack [20], Bob uses a 10:90 beam splitter (not depicted in the figure) before the polarization beam splitter to monitor the LO intensity [14].

To perform the heterodyne detection, Bob uses the photodetector to convert the photons into a photocurrent $\hat{i}$. Here $\hat{i}$ and the photon number $\hat{n}$ are related by $\hat{i} = q\hat{n} = q\hat{a}^\dagger\hat{a}$, where $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators of the light state, and q is a suitable constant [27]. The extra quantum noise $\delta\hat{\alpha}_v$ is unavoidable in Bob's measurement results when he uses heterodyne detection due to the unused port of the 50:50 beam

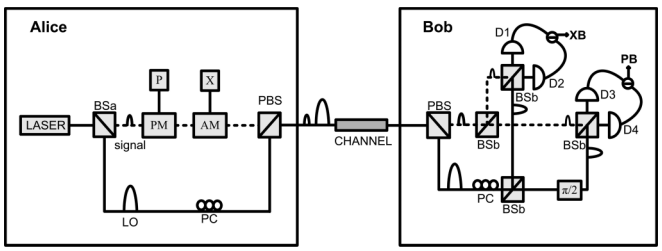

FIG. 1. Schematic of heterodyne detection protocol. BSa, 1:99 beam splitter; BSb, 50:50 beam splitter; PM, phase modulator; AM, amplitude modulator; PBS, polarization beam splitter; PC, polarization controller. Alice generates coherent light pulses with a 1550-nm laser diode, then separates them into a weak signal and a strong LO with the BSa. The signal is then modulated randomly following the centered Gaussian distribution in both quadratures, by using phase and AMs. The signal and LO are separated in time and modulated into orthogonal polarizations by the PBS before begin inserted into the channel.

splitter. To show this, let us first describe the signal and LO by operators $\hat{\alpha}_s$ and $\hat{\alpha}_{\rm LO}$, respectively. These operators can be broken up into two contributions [28]: the mean values of the amplitude α as well as the quantum noise fluctuations $\delta\alpha$. The operators can be written as

$$\hat{\alpha}_s = \alpha_s + \delta\hat{\alpha}_s, \quad \hat{\alpha}_{\rm LO} = \alpha_{\rm LO} + \delta\hat{\alpha}_{\rm LO}, \tag{1}$$

where α_s and $\alpha_{\rm LO}$ are complex numbers and we assume that the amplitude of the LO is much larger than the signal, i.e., $|\alpha_{\rm LO}| \gg |\alpha_s|$, and $\delta\hat{\alpha}_s$ and $\delta\hat{\alpha}_{\rm LO}$ are the fluctuations of the signal and LO, respectively.

The photocurrents read by the four photodetectors can be written as

$$\begin{aligned}
\hat{i}_1 &= q(\alpha^*_{\rm LO} + \delta\hat{\alpha}'^\dagger_{\rm LO} + \alpha^*_s + \delta\hat{\alpha}'^\dagger_s) \\
&\quad \times (\alpha_{\rm LO} + \delta\hat{\alpha}'_{\rm LO} + \alpha_s + \delta\hat{\alpha}'_s)/4, \\
\hat{i}_2 &= q(\alpha^*_{\rm LO} + \delta\hat{\alpha}'^\dagger_{\rm LO} - \alpha^*_s - \delta\hat{\alpha}'^\dagger_s) \\
&\quad \times (\alpha_{\rm LO} + \delta\hat{\alpha}'_{\rm LO} - \alpha_s - \delta\hat{\alpha}'_s)/4, \\
\hat{i}_3 &= q[e^{-i\frac{\pi}{2}}(\alpha^*_{\rm LO} + \delta\hat{\alpha}'^\dagger_{\rm LO}) + \alpha^*_s + \delta\hat{\alpha}'^\dagger_s] \\
&\quad \times [e^{i\frac{\pi}{2}}(\alpha_{\rm LO} + \delta\hat{\alpha}'_{\rm LO}) + \alpha_s + \delta\hat{\alpha}'_s]/4, \\
\hat{i}_4 &= q[e^{-i\frac{\pi}{2}}(\alpha^*_{\rm LO} + \delta\hat{\alpha}'^\dagger_{\rm LO}) - \alpha^*_s - \delta\hat{\alpha}'^\dagger_s] \\
&\quad \times [e^{i\frac{\pi}{2}}(\alpha_{\rm LO} + \delta\hat{\alpha}'_{\rm LO}) - \alpha_s - \delta\hat{\alpha}'_s]/4.
\end{aligned} \tag{2}$$

Here we have absorbed the vacuum noise terms $\delta\hat{\alpha}_v$ into the terms $\delta\hat{\alpha}'$. For simplicity, let us assume that $\alpha_{\rm LO}$ is a real number. To derive the quadratures $\hat{X}$ and $\hat{P}$, the difference between the two photocurrents should be measured,

$$\begin{aligned}
\delta\hat{i}_x &= i_1 - i_2 \\
&\approx q(\alpha_{\rm LO}\alpha^*_s + \alpha_{\rm LO}\alpha_s + \alpha_{\rm LO}\delta\hat{\alpha}'^\dagger_s + \alpha_{\rm LO}\delta\hat{\alpha}'_s)/2 \\
&= \frac{q\alpha_{\rm LO}}{2}(\alpha_s + \alpha^*_s + \delta\hat{\alpha}'_s + \delta\hat{\alpha}'^\dagger_s) \\
&= \frac{q\alpha_{\rm LO}}{2}(X + \delta\hat{X}') \\
&\to \hat{X}_B = \frac{2}{q\alpha_{\rm LO}}\delta\hat{i}_x = X + \delta\hat{X}', \\
\delta\hat{i}_p &= i_3 - i_4 \\
&\approx q(i\alpha_{\rm LO}\alpha^*_s - i\alpha_{\rm LO}\alpha_s + i\alpha_{\rm LO}\delta\hat{\alpha}'^\dagger_s - i\alpha_{\rm LO}\delta\hat{\alpha}'_s)/2 \\
&= \frac{q\alpha_{\rm LO}}{2}\left(\frac{\alpha_s - \alpha^*_s}{i} + \frac{\delta\hat{\alpha}'_s - \delta\hat{\alpha}'^\dagger_s}{i}\right) \\
&= \frac{q\alpha_{\rm LO}}{2}(P + \delta\hat{P}') \\
&\to \hat{P}_B = \frac{2}{q\alpha_{\rm LO}}\delta\hat{i}_p = P + \delta\hat{P}',
\end{aligned} \tag{3}$$

where $X \equiv \alpha_s + \alpha^*_s$ and $P \equiv -i(\alpha_s - \alpha^*_s)$ are the exact quadratures that Bob wants to measure, and $\delta\hat{X}' \equiv (\delta\hat{\alpha}_s + \delta\hat{\alpha}^\dagger_s) + (\delta\hat{\alpha}_v + \delta\hat{\alpha}^\dagger_v) = \delta\hat{X} + \delta\hat{X}_v$ and $\delta\hat{P}' \equiv -i(\delta\hat{\alpha}_s - \delta\hat{\alpha}^\dagger_s) - i(\delta\hat{\alpha}_v - \delta\hat{\alpha}^\dagger_v) = \delta P + \delta P_v$ are the quantum noises entering into Bob's measurement. Several terms have been neglected above according to the fact that $|\alpha_{\rm LO}| \gg |\alpha_s|$. $\delta\hat{X}$ and $\delta\hat{P}$ satisfy the canonical commutation relation $[\delta\hat{X}, \delta\hat{P}] = 2i$, therefore the Heisenberg uncertainty relation $\langle(\delta\hat{X})^2\rangle\langle(\delta\hat{P})^2\rangle = 1$ is derivable [27].

Under the condition that Eve cannot act on the LO (a common assumption in the security proofs [1]), only when

the excess noise reaches two times the shot-noise level can Eve perform an intercept-resend attack on the channel [29]. This is due to the fact that Eve will introduce vacuum noise by using heterodyne detection and, consequently, suffer quantum fluctuations when she reproduces the signal state in a simple intercept-resend attack.

B. Wavelength-dependent fiber beam splitter

In Ref. [12], we studied the wavelength-dependent property of the fiber beam splitter which is made by fused biconical taper technology [23]. The fused biconical taper beam splitter is made by closing two or more bare optical fibers, fusing them in a high-temperature environment, and drawing their two ends at the same time. Subsequently, a specific biconic tapered waveguide structure can be formed in the heating area. The fused biconical taper beam splitter is widely use in fiber QKD systems because of its features of low insertion loss, good directivity, and low cost. However, intensity transmission of the fused biconical taper beam splitter is wavelength dependent, and most types of fused biconical taper beam splitters work only in a limited range of wavelengths (limited bandwidths), where the intensity transmission of the beam splitter can be defined as $T \equiv I_{\text{port1}}/(I_{\text{port1}} + I_{\text{port2}})$, where I_{port1} (I_{port2}) is the output light intensity from beam splitter's output port 1 (port 2). A typical coupling ratio at the center wavelength provides optimal performance, but the intensity transmission varies periodically with wavelength changes. The relationship between the wavelength λ and the intensity transmission T using the coupling model is given in Refs. [24] and [25]:

$$T = F^2 \sin^2\left(\frac{C\lambda^{5/2}w}{F}\right) \equiv T(\lambda), \tag{4}$$

where F^2 is the fraction of power coupled, $C \cdot \lambda^{5/2}$ is the coupling coefficient, and w is the heat source width.

III. WAVELENGTH ATTACK ON A CV-QKD SYSTEM USING A HETERODYNE PROTOCOL

The basic idea of the wavelength attack is shown in Fig. 2. Eve intercepts the coherent states sent by Alice. She makes

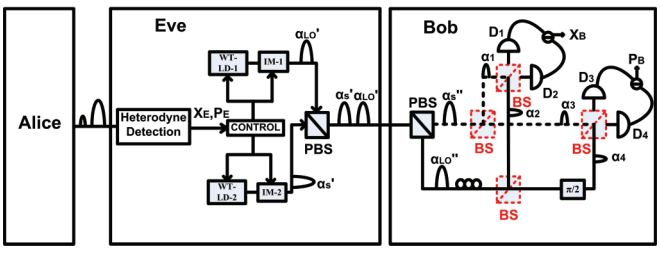

FIG. 2. (Color online) Schematic diagram of the wavelength attack scheme. WT-LD, wavelength tunable laser diode; IM, intensity modulator; BS, 50-50 beam splitter. The WT-LD and IM are used to produce fake coherent states, with the specific wavelength and amplitude set by the controller. Dotted (red) beam splitters are the ones controlled by Eve. The dottted beam splitter on the left has transmission T_1, while the dotted beam splitter at the bottom has transmission T_2. For simplicity, the 10:90 beam splitter and the generation of $|\alpha_3\rangle$ are not shown.

heterodyne measurement of the signal using the LO to achieve the quadrature values X_E and P_E. After that, Eve generates and resends three coherent states: a fake signal state $|\alpha_s'\rangle$, a fake LO state $|\alpha_{\text{LO}}'\rangle$, and an ancillary state $|\alpha_3\rangle$. Differently from the previous intercept-resend attack, these fake states have different wavelengthes, denoted λ_1 (for $|\alpha_s'\rangle$), λ_2 (for $|\alpha_{\text{LO}}'\rangle$), and λ_3 (for $|\alpha_3\rangle$). According to Eq. (4), the performance of Bob's beam splitter is dependent on the wavelength of the incoming light. Therefore for a fake signal with wavelength λ_1, the transmission of Bob's beam splitter is determined by the function $T(\lambda_1)$, which is defined in Eq. (4). Similarly, the intensity transmission of Bob's beam splitter to the fake LO state is determined by $T(\lambda_2)$. In other words, Eve can control Bob's beam splitter by tuning the wavelength of her fake states.

With the help of wavelength tunable laser diodes and intensity modulators, the wavelength and amplitude of these fake states are carefully chosen to satisfy the conditions

$$\begin{aligned}
&\text{(i)}\quad (1-T_3')|\alpha_3'|^2 + (1-T_1')|\alpha_s'|^2 + (1-T_2')|\alpha_{\text{LO}}'|^2 \\
&\qquad = 0.1|\alpha_{\text{LO}}|^2, \\
&\text{(ii)}\quad (1-T_1)(1-2T_1)T_1'|\alpha_s'|^2 + (1-T_2)(2T_2-1)T_2'|\alpha_{\text{LO}}'|^2 \\
&\qquad = \frac{\sqrt{\eta}X_E|\alpha_{\text{LO}}|}{2}, \\
&\text{(iii)}\quad T_1(1-2T_1)T_1'|\alpha_s'|^2 + T_2(2T_2-1)T_2'|\alpha_{\text{LO}}'|^2 \\
&\qquad = \frac{\sqrt{\eta}P_E|\alpha_{\text{LO}}|}{2},
\end{aligned} \tag{5}$$

where $T_i \equiv T(\lambda_i) \in [0,1] (i = 1,2)$, $T_j' \equiv T'(\lambda_j) \in [0,1]$ $(j = 1,2,3)$. Here η is the channel transmission efficiency, $|\alpha_s|$ and $|\alpha_{\text{LO}}|$ are the amplitudes of the original signal and the LO, respectively, $|\alpha_s'|$, $|\alpha_{\text{LO}}'|$, and α_3' are the amplitudes of the fake signal and the fake LO, and T_j' are the intensity transmissions of Bob's 10:90 beam splitter (for monitoring the LO light intensity).

Condition i ensures that the method of monitoring the LO intensity is invalid to Eve. Here we assume that Bob uses a 10:90 beam splitter to split the total light before being inserted into the PBS [31]. Because the 10:90 beam splitter is also wavelength dependent, its intensity transmission can be determined by a function similar to Eq. (4), which is denoted $T'(\lambda) \simeq F'^2 \sin^2(\frac{C'\lambda^{5/2}w'}{F'})$. Here $|\alpha_3\rangle$ is used to compensate the intensity when α_s' and α_{LO}' are both small. Eve selects an appropriate wavelength λ_3 such that $T_3 = 0$, therefore the intensity of $|\alpha_3\rangle$ is much lower than the shot-noise level and negligible.

As Bob measures the quadratures $\hat{X}_B$ and $\hat{P}_B$ by performing heterodyne detection on the fake signal and the fake LO, conditions ii and iii make Bob's measurement results coincide with those attained by Eve. To see explicitly where these relations come from, see Eqs. (B6) and (B7) in Appendix B. Note that the fake signal and the fake LO have different wavelengths, and hence, no interference occurs in this detection. The effect of this on measurement detection is that we no longer have heterodyne detection outputs but rather outputs that are proportional to Eve's measurements. Therefore, the photocurrents recorded by the photodetectors consist of parts from the signal and the LO. Eve should also make $T_1'|\alpha_s'|^2$ and $T_2'|\alpha_{\text{LO}}'|^2$ much smaller than $|\alpha_{\text{LO}}|^2$ in order to suppress the shot noise. We prove in Sec. IV that the extra noise introduced

by Bob's measurement is much lower than the shot-noise level, therefore the total noise can be kept under the alarm threshold. In other words, Eve can safely achieve the key information without being discovered by Alice or Bob.

Finally, we note that as there are limitations on the intensities, conditions ii and iii may not always be satisfied. However, in the analysis in Appendix A, we find that the probability of failing condition ii or iii is extremely close to 0.

IV. FEASIBILITY ANALYSIS

To analyze the feasibility of the wavelength attack, we first note that the following assumptions should be satisfied:

(i) This attack is restricted to an all-fiber coherent-state CV-QKD using the heterodyne protocol.

(ii) All of Bob's beam splitters have the same wavelength-dependent property; i.e., their intensity transmissions are all determined by Eq. (4) with the same parameters. This function and the detection efficiencies of Bob's detectors are both known by Eve. Here we assume that the detection efficiencies are wavelength independent, for simplicity. In practice, Eve can simply absorb the differences into the light amplitudes modulated by her and the final results are unchanged.

(iii) Eve has the ability to replace the quantum channel with a noiseless fiber, and her detectors have a high efficiency and negligible excess noise.

Before analyzing the feasibility of the wavelength attack, let us first rapidly review the security analysis of the Gaussian protocols based on coherent states and heterodyne detections under individual attacks. In what follows, we restrict ourselves to Gaussian attacks, which are proven optimal [30].

In the case of Gaussian attacks, the channel connecting Alice and Bob can be fully characterized by its transmission η and its excess noise ϵ above the shot-noise level, such that the total noise measured by Bob is $1+\eta\epsilon$ (in shot-noise units) [19]. Alternatively, one may use the total added noise defined as $\chi \equiv (1-\eta)/\eta + \epsilon$ for convenience. The secret key rates for Heisenberg-limited individual attack in direct reconciliation and reverse reconciliation are given, respectively, by [30]

$$K^{\mathrm{DR}} = \log_2 \frac{(1+\chi)[1+\eta(V+\chi)]}{(1+\chi V)[1+\eta(1+\chi)]}, \tag{6}$$

$$K^{\mathrm{RR}} = \log_2 \frac{V+\eta(1+\chi V)}{\eta(1+\chi V)[1+\eta(1+\chi)]}, \tag{7}$$

where $V = V_A + 1$ is the variance of Alice's modulated state as mentioned in Sec. II A. Note that we use the "Heisenberg-limited attack" rather than the optimal attack [22,30], as such an attack upper bounds Eve's information, thereby emphasizing our wavelength attack, which can beat even such a stringent attack. From the above formulas, we can see that when V and η are settled in practice, the secret key rate is fully determined by χ, which can be precisely estimated from the experimental data [19].

Another important parameter in the security proof is Alice's (Bob's) conditional variance of Bob's (Alice's) measurement $V_{A|B}$ ($V_{B|A}$) in direct reconciliation (reverse reconciliation),which can be thought of as the uncertainty in Alice's (Bob's) estimates of Bob's (Alice's) quadrature measurement result. In the CV-QKD, Alice and Bob use $V_{A|B}$ ($V_{B|A}$) to estimate the shot noise and modulation imperfections [19]. $V_{A|B}$ is defined (where both quadratures are symmetrized) as

$$V_{A|B} = \langle X_A^2 \rangle - \frac{\langle X_A \hat{X}_B \rangle^2}{\langle \hat{X}_B^2 \rangle}, \tag{8}$$

and similarly, we have $V_{B|A}$ defined as

$$V_{B|A} = \langle \hat{X}_B^2 \rangle - \frac{\langle X_A \hat{X}_B \rangle^2}{\langle X_A^2 \rangle}. \tag{9}$$

We note that $V_{A|B}$ ($V_{B|A}$) performs a role in CV-QKD protocols similarly to the quantum bit error rate in discrete-variable QKD protocols, which provide Alice and Bob an intuitive tool to detect the presence of Eve. To clarify this idea, let us first state the relation between $V_{A|B}$ ($V_{B|A}$) and χ. As the Gaussian character of the channel is maintained whether or not Eve performs Gaussian attacks, the conditional variance between Alice and Bob, which we denote $V_{A|B}^{\mathrm{normal}}$ and $V_{B|A}^{\mathrm{normal}}$, can be calculated as follows [30]:

$$V_{A|B}^{\mathrm{normal}} = \frac{(V-1)[\eta(\chi+1)+1]}{\eta(V+\chi)+1}, \tag{10}$$

$$V_{B|A}^{\mathrm{normal}} = \tfrac{1}{2}[\eta(1+\chi)+1]. \tag{11}$$

Note that there may be a little difference from the expressions in [30] due to the differences in the definitions of V.

On the other hand, to make the secret key rate positive, we require that [according to Eqs. (6) and (7)]

$$\chi < \chi_{\max}^{\mathrm{DR}} = \frac{\sqrt{4\eta^2+1}-1}{2\eta}, \tag{12}$$

with $\frac{2}{3} < \eta < 1$ for direct reconciliation, or

$$\chi < \chi_{\max}^{\mathrm{RR}} = \frac{\sqrt{\left(\frac{4}{\eta^2}+1\right)V^2 - 2V + 1} - V - 1}{2V}, \tag{13}$$

with $0 < \eta < 1$ for reverse reconciliation, should be satisfied.

Combining Eq. (10) with Eq. (12), we find that for the sake of deriving a positive secret key rate, the upper bound of $V_{A|B}^{\mathrm{normal}}$ yields

$$V_{A|B}^{\max} = \frac{(V-1)(\sqrt{4\eta^2+1}+2\eta+1)}{\sqrt{4\eta^2+1}+2\eta V+1}. \tag{14}$$

In other words, if $V_{A|B}$ is smaller than this threshold, the heterodyne protocol in direct reconciliation is considered to be secure. Similarly, the upper bound of $V_{B|A}^{\mathrm{normal}}$ is derived to be

$$V_{B|A}^{\max} = \frac{\sqrt{(4+\eta^2)V^2 - 2\eta^2 V + \eta^2} + (\eta+2)V - \eta}{4V}. \tag{15}$$

And the heterodyne protocol in reverse reconciliation is considered to be secure if $V_{B|A}$ is smaller than this threshold.

For these reasons, we can prove our attack feasible by showing that Eve can make $V_{A|B} < V_{A|B}^{\max}$ (in the direct reconciliation protocol) and $V_{B|A} < V_{B|A}^{\max}$ (in the reverse reconciliation protocol) when she is performing the wavelength attack.

A. Eve's wavelength attack

When Eve performs the wavelength attack, with channel noise, from a real value X_A chosen by Alice to the measurement result $\hat{X}_B$ achieved by Bob is written as (we write down the quadrature $\hat{X}$ only since the other quadrature $\hat{P}$ can be presented in a similar way)

$$\begin{aligned} X_A \to \hat{X}_A &= X_A + \hat{N}_A \\ \to \hat{X}_E &= \frac{1}{\sqrt{2}}(\hat{X}_A + \hat{N}_E) \\ \to \hat{X}_B &= \sqrt{\eta}\hat{X}_E + \hat{N}_B, \end{aligned} \tag{16}$$

where $\hat{N}_E$ represents the vacuum noise in Eve's heterodyne detection whose variance is normalized to 1, and $\hat{N}_B$ is the vacuum noise introduced by the heterodyne detection. The variance of each of the terms is given by $V_E = \frac{1}{2}(V+1)$ and $V_B = \eta V_E + V_{\mathrm{NB}}$. Here V_{NB} can then be considered as Eve's conditional variance of Bob's measurement result. In Appendix B, we derive the value of V_{NB} and show that it is smaller than 0.13. We are now ready to derive the conditional variances under Eve's attack, which are denoted $V_{A|B}^{\mathrm{attack}}$ and $V_{B|A}^{\mathrm{attack}}$.

1. $V_{A|B}^{\mathrm{attack}}$ *in direct reconciliation*

According to the definition of $V_{A|B}$ in Eq. (8), the value of $V_{A|B}^{\mathrm{attack}}$ can be computed as

$$V_{A|B}^{\mathrm{attack}} = \frac{2(V_{NB}+\eta)(V-1)}{2V_{NB}+\eta(V+1)}. \tag{17}$$

Combining Eqs. (B10) and (B11) and the discussion above, we can estimate that the value of $V_{A|B}^{\mathrm{attack}}$ is not larger than 1.9. As shown in Fig. 3 (where we set $V = 11$ and $\epsilon = 0.01$ [22]), $V_{A|B}^{\mathrm{attack}}$ is always lower than $V_{A|B}^{\max}$, so that Alice and Bob can never discover the eavesdropper under this attack. Besides, one should note that $V_{A|B}^{\mathrm{attack}}$ is always lower than the normal level when the channel loss is larger than 0.58 dB, therefore Eve should increase the deviations on purpose to make $V_{A|B}^{\mathrm{attack}}$ close to $V_{A|B}^{\mathrm{normal}}$ in order to avoid suspicion.

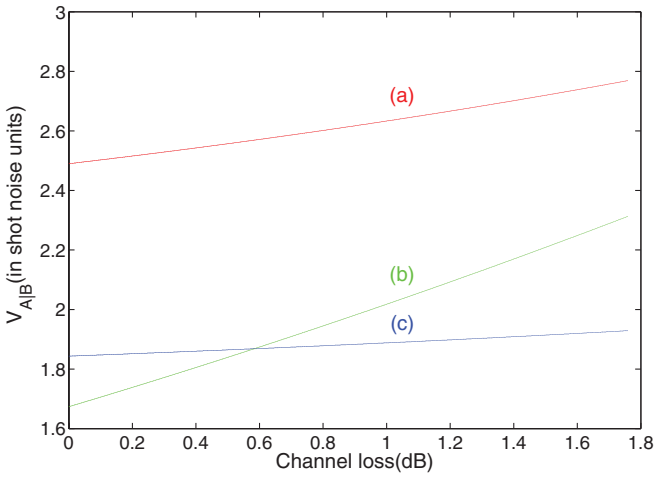

FIG. 3. (Color online) In direct reconciliation, the relation between the channel loss and the conditional variance $V_{A|B}$ in three cases: (a) the maximum tolerable value $V_{A|B}^{\max}$, (b) the value of $V_{A|B}^{\mathrm{normal}}$, and (c) the value of $V_{A|B}^{\mathrm{attack}}$. See text for details. Curves are plotted for experimentally realistic values, $V = 11$ and $\epsilon = 0.01$. We can see that $V_{A|B}^{\mathrm{attack}}$ is always lower than $V_{A|B}^{\max}$ and lower than $V_{A|B}^{\mathrm{normal}}$ when the channel loss is larger than 0.58 dB, at which point the key between Alice and Bob is no longer secure.

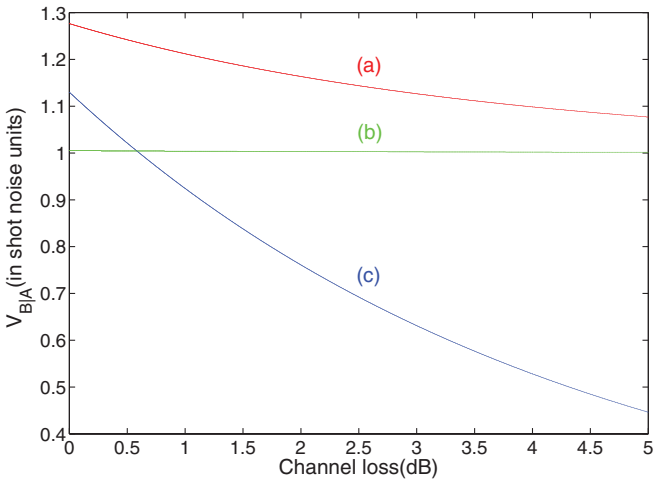

FIG. 4. (Color online) In reverse reconciliation, the relation between the channel loss and the conditional variance $V_{B|A}$ in three cases: (a) the maximum tolerable value $V_{B|A}^{\max}$, (b) the value of $V_{B|A}^{\mathrm{normal}}$, and (c) the value of $V_{B|A}^{\mathrm{attack}}$. See text for details. Curves are plotted for experimentally realistic values, $V = 11$ and $\epsilon = 0.01$. We can see that $V_{B|A}^{\mathrm{attack}}$ is always lower than $V_{B|A}^{\max}$ and lower than $V_{B|A}^{\mathrm{normal}}$ when the channel loss is greater than 0.58 dB, again leading to an insecure key.

2. $V_{B|A}^{\mathrm{attack}}$ *in reverse reconciliation*

In reverse reconciliation, using Eq. (9) with Eq. (16), the value of $V_{B|A}^{\mathrm{attack}}$ can be computed as

$$V_{B|A}^{\mathrm{attack}} = \eta + V_{NB}. \tag{18}$$

Combining Eqs. (B10) and (B11) and the discussion above, we can estimate that the value of $V_{B|A}^{\mathrm{attack}}$ is never larger than $\eta + 0.13$. As shown in Fig. 4 (where, again, we have set $V = 11$ and $\epsilon = 0.01$), it is always lower than the value of $V_{B|A}^{\max}$, so that Alice and Bob can never discover the eavesdropper under such an attack. Besides, one should note that $V_{B|A}^{\mathrm{attack}}$ is lower than $V_{B|A}^{\mathrm{normal}}$ when the channel loss is larger than 0.58 dB. Hence, Eve should increase the deviations to make $V_{A|B}^{\mathrm{attack}}$ close to $V_{A|B}^{\mathrm{normal}}$ in order to avoid suspicion.

V. DISCUSSION AND CONCLUSION

There are two points about the wavelength attack that should be made:

(1) As shown in Fig. 3 and Fig. 4, $V_{A|B}^{\mathrm{attack}}$ and $V_{B|A}^{\mathrm{attack}}$ are lower than $V_{A|B}^{\mathrm{normal}}$ and $V_{B|A}^{\mathrm{normal}}$, respectively, when $\eta < 0.88$. This is impossible when the protocol works normally, therefore Eve should add extra noise in her measurement result to increase $V_{A|B}^{\mathrm{attack}}$ and $V_{B|A}^{\mathrm{attack}}$. So perfect heterodyne detection is not necessary for Eve. In other words, assumption iii listed in Sec. IV can be compromised.

(2) In theory, the wavelength attack cannot be avoided by adding a wavelength filter before the monitoring detector,

because Eve can simply increase the input light intensity [12]. To make this method work, Bob should randomly choose to add or not to add a wavelength filter before the monitoring detector and observe the differences.

Finally, we note that a commercial CV-QKD system, as sold at [15], currently uses a wavelength-dependent beam splitter, although it does not fall into the regime studied in this paper because it uses homodyne detection rather than heterodyne detection. However, our results show that if one were going to use heterodyne detection with a commercial QKD unit, then the precautions mentioned here would need to be taken. Furthermore, possible quantum hacking opportunities with homodyne detection and wavelength-dependent beam splitters warrant further investigation.

In conclusion, we have proposed a realistic quantum hacking attack, namely, the wavelength attack, on continuous-variable QKD systems using heterodyne detection. If Alice and Bob do not take the necessary precautions for such an attack, the final secret key is, in principle, totally insecure, as Eve can obtain all the information about the final key. This is different from the equal-amplitude attack proposed in Ref. [20], as in the wavelength attack, Eve has the ability to control Bob's beam splitter, and therefore the suggestion of testing the total intensity in Ref. [20] would not prevent such an attack from occurring. To close such a loophole in practical CV-QKD systems, it is simply enough for Bob to randomly add a wavelength filter before his detection.

ACKNOWLEDGMENTS

This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200) and the National Natural Science Foundation of China (Grants No. 60921091 and No. 61101137). C.W. acknowledges support from the Ontario postdoctoral fellowship program, CQIQC postdoctoral fellowship program, CIFAR, Canada Research Chair program, NSERC, and QuantumWorks.

APPENDIX A: ACHIEVABLE X_E AND P_E

We estimate the achievable range of X_E and P_E in this Appendix. Before the analysis, let us first rewrite Eq. (4) as

$$T(\lambda) = F^2 \sin^2\left(\frac{Cw}{F}\lambda^{5/2}\right) = \sin^2(AX), \tag{A1}$$

where $A = \frac{Cw}{F}$ and $X = \lambda^{5/2}$; here we set $F = 1$ for simplicity. For the 50:50 BS, $T(\lambda_0) = \sin^2(AX_0) = 0.5$, where $\lambda_0 = 1550$ nm, hence $AX_0 = \arcsin(\sqrt{0.5})$. For other wavelengths, $AX = \arcsin(\sqrt{T(\lambda)})$ and we can get $X = \frac{\arcsin(\sqrt{T(\lambda)})}{\arcsin(0.5)} X_0$.

For the 10:90 BS, we similarly rewrite its transmission as $T'(\lambda) = \sin^2(BX)$ and easily derive that $BX_0 = \arcsin(\sqrt{0.9})$. Therefore,

$$T'(\lambda) = \sin^2\left(\frac{\arcsin\left(\sqrt{T(\lambda)}\right)}{\arcsin\sqrt{0.5}}\arcsin\sqrt{0.9}\right). \tag{A2}$$

Moreover, as mentioned in Sec. IV A, to suppress the shot noise we should make $|\alpha_s''| \equiv T_1'|\alpha_s'|^2$ and $|\alpha_{\mathrm{LO}}''| \equiv T_2'|\alpha_{\mathrm{LO}}'|^2$ much smaller than $|\alpha_{\mathrm{LO}}|^2$. In a practical CV-QKD system, the LO pulse arriving on Bob's side typically includes more than 10^8 photons [14]. For this reason, we constrain the maximum value of both $|\alpha_s''|^2$ and $|\alpha_{\mathrm{LO}}''|^2$ to be $10^6 \leqslant 10^{-2}|\alpha_{\mathrm{LO}}|^2$. On the other hand, to guarantee condition i, Eve should also make $(1 - T_1')|\alpha_s'|^2$ and $(1 - T_2')|\alpha_{\mathrm{LO}}'|^2$ not larger than 5×10^6. We then get the following maximum value constraints on the fake-state intensities:

$$\begin{aligned} |\alpha_s''|^2 &\leqslant \mathrm{Max}\left\{10^6, \frac{1 - T_1'}{T_1'}10^6\right\}, \\ |\alpha_{\mathrm{LO}}''|^2 &\leqslant \mathrm{Max}\left\{10^6, \frac{1 - T_2'}{T_2'}10^6\right\}. \end{aligned} \tag{A3}$$

From conditions ii and iii, we can get

$$\sqrt{\eta}X_E = \frac{2[(1 - T_1)(1 - 2T_1)|\alpha_s''|^2 + (1 - T_2)(2T_2 - 1)|\alpha_{\mathrm{LO}}''|^2]}{|\alpha_{\mathrm{LO}}|}, \quad \sqrt{\eta}P_E = \frac{2[T_1(1 - 2T_1)|\alpha_s''|^2 + T_2(2T_2 - 1)|\alpha_{\mathrm{LO}}''|^2]}{|\alpha_{\mathrm{LO}}|}. \tag{A4}$$

Combining Eqs. (A2), (A3) and (3), now we have enough information to derive the achievable value range of X_E and P_E by analytical calculations or numerical simulations. Either of these methods shows that $(\sqrt{\eta}X_E, \sqrt{\eta}P_E)$ satisfying $\eta|X_E|^2 + \eta|P_E|^2 < 20$ are always achievable. To see how high the probability of $|X_E|$(or $|P_E|$) > 20 is, we can apply the error integral function $\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-x^2}dx$ and get $P[|\sqrt{\eta}X_E| > 20 \text{ or } |\sqrt{\eta}P_E| > 20] = \mathrm{erfc}(\frac{20}{\sqrt{2V}})$, where V is the variance of X_E and P_E chosen by Gaussian distribution [32]. For the experimentally realistic value $V = 11$, we get $\mathrm{erfc}(\frac{20}{\sqrt{22}}) = 1.637 \times 10^{-9} \approx 0$, which concludes our claim in Sec. III. When X_E or P_E is out of reach, Eve can simply turn to performing the original intercept-resend strategy. The extra noise it involves is 1 (shot-noise unit) times this extremely low probability, which is negligible.

APPENDIX B: DERIVATION OF V_{NB}

To derive V_{NB}, let us start from the generation of Eve's fake states. As described in Sec. III, Eve generates the fake signal state and the fake LO state according to her measurement results and sends them to Bob. These fake states can be described by the operators

$$\hat{\alpha}_s' = \alpha_s' + \delta\hat{a}_s', \quad \hat{\alpha}_{\mathrm{LO}}' = \alpha_{\mathrm{LO}}' + \delta\hat{a}_{\mathrm{LO}}', \tag{B1}$$

where complex numbers α_s' and α_{LO}' are the amplitudes and $\delta\hat{a}_s'$ and $\delta\hat{a}_{\mathrm{LO}}'$ represent the fluctuations of the amplitudes as discussed in Sec. II A. Similarly, $\langle(\delta\hat{X}_k')^2\rangle = \langle(\delta\hat{P}_k')^2\rangle = 1$, where $\delta\hat{X}_k = \delta\hat{a}_k' + \delta\hat{a}_k'^\dagger$ and $\delta\hat{P}_k = -i(\delta\hat{a}_k' - \delta\hat{a}_k'^\dagger)$, $k = s$,

LO. After the (original) 10:90 beam splitter, they become

$$\hat{\alpha}_s'' = \sqrt{T_1'}\hat{\alpha}_s' + \sqrt{1-T_1'}\delta\hat{a}_{v1} = \alpha_s'' + \delta\hat{a}_s'', \quad \hat{\alpha}_{\mathrm{LO}}'' = \sqrt{T_2'}\hat{\alpha}_{\mathrm{LO}}' + \sqrt{1-T_2'}\delta\hat{a}_{v2}' = \alpha_{\mathrm{LO}}'' + \delta\hat{a}_{\mathrm{LO}}'', \tag{B2}$$

where $\delta\hat{a}_{v1}$ and $\delta\hat{a}_{v2}$ are the vacuum noises that interfere with the fake signal and the fake LO, respectively, at the beam splitter. $\alpha_s'' \equiv \sqrt{T_1'}\alpha_s'$, $\delta\hat{a}_s'' \equiv \sqrt{T_1'}\delta\hat{a}_s' + \sqrt{1-T_1'}\delta\hat{a}_{v1}'$, and similarly for the LO.

Bob performs heterodyne detection on these fake states. According to Eq. (4), Bob's beam splitter has different intensity transmissions for $\hat{\alpha}_s''$ and $\hat{\alpha}_{\mathrm{LO}}''$ because of their different wavelengths, denoted T_1 and T_2. After passing the first set of beam splitters, $\hat{\alpha}_s''$ is separated into $\hat{\alpha}_1$ and $\hat{\alpha}_3$, while $\hat{\alpha}_{\mathrm{LO}}''$ is separated into $\hat{\alpha}_2$ and $\hat{\alpha}_4$ (cf. Fig. 2), which can be expressed as follows:

$$\begin{aligned} \hat{\alpha}_1 &= \sqrt{1-T_1}\hat{\alpha}_s'' + \sqrt{T_1}\delta\hat{a}_{v1}', \quad \hat{\alpha}_2 = \sqrt{1-T_2}\hat{\alpha}_{\mathrm{LO}}'' + \sqrt{T_2}\delta\hat{a}_{v2}', \\ \hat{\alpha}_3 &= \sqrt{T_1}\hat{\alpha}_s'' - \sqrt{1-T_1}\delta\hat{a}_{v1}', \quad \hat{\alpha}_4 = e^{i\frac{\pi}{2}}(\sqrt{T_2}\hat{\alpha}_{\mathrm{LO}}'' - \sqrt{1-T_2}\delta\hat{a}_{v2}'). \end{aligned} \tag{B3}$$

To simplify the symbols, let us define $\delta\hat{\alpha}_1 \equiv \sqrt{1-T_1}\delta\hat{a}_s'' + \sqrt{T_1}\delta\hat{\alpha}_{v1}'$, $\delta\hat{\alpha}_2 \equiv \sqrt{1-T_2}\delta\hat{a}_{\mathrm{LO}}'' + \sqrt{T_2}\delta\hat{\alpha}_{v2}'$, $\delta\hat{\alpha}_3 \equiv \sqrt{T_1}\delta\hat{a}_s'' - \sqrt{1-T_1}\delta\hat{\alpha}_{v1}'$, and $\delta\hat{\alpha}_4 \equiv \sqrt{T_2}\delta\hat{a}_{\mathrm{LO}}'' - \sqrt{1-T_2}\delta\hat{\alpha}_{v2}'$. Furthermore, we define the quadratures of $\delta\hat{\alpha}_k$ by $\delta\hat{X}_k = \delta\hat{\alpha}_k + \delta\hat{\alpha}_k^\dagger$ and $\delta\hat{P}_k = -i(\delta\hat{\alpha}_k - \delta\hat{\alpha}_k^\dagger)$, where $k = 1,2,3,4$. Finally, after combining at the second set of beam splitters, the electromagnetic fields arriving at the four detectors can be written as

$$\begin{aligned} \hat{b}_1 &= \sqrt{1-T_1}\hat{\alpha}_1 + \sqrt{T_1}\delta\hat{\alpha}_{v1}'' + \sqrt{T_2}\hat{\alpha}_2 + \sqrt{1-T_2}\delta\hat{\alpha}_{v2}'', \quad \hat{b}_2 = \sqrt{T_1}\hat{\alpha}_1 - \sqrt{1-T_1}\delta\hat{\alpha}_{v1}'' - \sqrt{1-T_2}\hat{\alpha}_2 + \sqrt{T_2}\delta\hat{\alpha}_{v2}'', \\ \hat{b}_3 &= \sqrt{1-T_1}\hat{\alpha}_3 + \sqrt{T_1}\delta\hat{\alpha}_{v3}'' + \sqrt{T_2}\hat{\alpha}_4 + \sqrt{1-T_2}\delta\hat{\alpha}_{v4}'', \quad \hat{b}_4 = \sqrt{T_1}\hat{\alpha}_3 - \sqrt{1-T_1}\delta\hat{\alpha}_{v3}'' - \sqrt{1-T_2}\hat{\alpha}_4 + \sqrt{T_2}\delta\hat{\alpha}_{v4}'', \end{aligned} \tag{B4}$$

where the photocurrents are given by $\hat{i}_k = q\hat{b}_k^\dagger\hat{b}_k$. Bob's quadrature measurement results are then derived from the difference in photocurrents, using the method in Sec. II A. First, for detectors $D1$ and $D2$, we have

$$\begin{aligned} \hat{i}_x &= \hat{i}_1 - \hat{i}_2 \\ &= q(\hat{b}_1^\dagger\hat{b}_1 - \hat{b}_2^\dagger\hat{b}_2) \\ &= q\{(1-2T_1)[(1-T_1)|\alpha_s''|^2 + \sqrt{1-T_1}(\alpha_s''^*\delta\hat{\alpha}_1 + \alpha_s''\delta\hat{\alpha}_1^\dagger)] + (2T_2-1)[(1-T_2)|\alpha_{\mathrm{LO}}''|^2 + \sqrt{1-T_2}(\alpha_{\mathrm{LO}}''^*\delta\hat{\alpha}_2 + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_2^\dagger)] \\ &\quad + 2\sqrt{T_1}(1-T_1)(\alpha_s''^*\delta\hat{\alpha}_{v1}'' + \alpha_s''\delta\hat{\alpha}_{v1}''^\dagger) + 2\sqrt{T_2}(1-T_2)(\alpha_{\mathrm{LO}}''^*\delta\hat{\alpha}_{v2}'' + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_{v2}''^\dagger) + \sqrt{(1-T_1)T_2}[\sqrt{(1-T_1)(1-T_2)} \\ &\quad \times(\alpha_s''^*\alpha_{\mathrm{LO}}'' + \alpha_s''\alpha_{\mathrm{LO}}''^*) + \sqrt{1-T_1}(\alpha_s''^*\delta\hat{\alpha}_2 + \alpha_s''\delta\hat{\alpha}_2^\dagger) + \sqrt{1-T_2}(\alpha_{\mathrm{LO}}''\delta\hat{\alpha}_1^\dagger + \alpha_{\mathrm{LO}}''^*\hat{\alpha}_1)] - \sqrt{(1-T_2)T_1}[\sqrt{(1-T_1)(1-T_2)} \\ &\quad \times(\alpha_s''^*\alpha_{\mathrm{LO}}'' + \alpha_s''\alpha_{\mathrm{LO}}''^*) + \sqrt{1-T_1}(\alpha_s''^*\delta\hat{\alpha}_2 + \alpha_s''\delta\hat{\alpha}_2^\dagger) + \sqrt{1-T_2}(\alpha_{\mathrm{LO}}''\delta\hat{\alpha}_1^\dagger + \alpha_{\mathrm{LO}}''^*\hat{\alpha}_1)] \\ &\quad + (\sqrt{T_1T_2(1-T_2)} - \sqrt{(1-T_1)(1-T_2)^2})(\alpha_{\mathrm{LO}}''\delta\hat{\alpha}_{v1}''^\dagger + \alpha_{\mathrm{LO}}''^*\delta\hat{\alpha}_{v1}'') \\ &\quad + (\sqrt{(1-T_1)^2(1-T_2)} - \sqrt{T_1T_2(1-T_1)})(\alpha_s''\delta\hat{\alpha}_{v2}''^\dagger + \alpha_s''^*\delta\hat{\alpha}_{v2}'')\}, \end{aligned} \tag{B5}$$

where the terms $\delta\hat{\alpha}^\dagger\delta\hat{\alpha}$ are already neglected. Note that $\hat{\alpha}_{\mathrm{LO}}'$ and $\hat{\alpha}_s'$ have different frequencies, therefore any terms not containing the product of the same frequencies vanish during the measurement. The remaining terms compose the measurement result of $\hat{i}_x$:

$$\begin{aligned} \hat{i}_x &= q[(1-T_1)(1-2T_1)|\alpha_s''|^2 + (1-2T_1)\sqrt{1-T_1}(\alpha_s''^*\delta\hat{\alpha}_1 + \alpha_s''\delta\hat{\alpha}_1^\dagger) + (1-T_2)(2T_2-1)|\alpha_{\mathrm{LO}}''|^2 \\ &\quad + (2T_2-1)\sqrt{1-T_2}(\alpha_{\mathrm{LO}}''^*\delta\hat{\alpha}_2 + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_2^\dagger) + 2\sqrt{T_1}(1-T_1)(\alpha_s''^*\delta\hat{\alpha}_{v1}'' + \alpha_s''\delta\hat{\alpha}_{v1}''^\dagger) + 2\sqrt{T_2}(1-T_2)(\alpha_{\mathrm{LO}}''^*\delta\hat{\alpha}_{v2}' + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_{v2}''^\dagger)]. \end{aligned} \tag{B6}$$

Similarly, we get the measurement result of $\hat{i}_p$ as

$$\begin{aligned} \hat{i}_p &= \hat{i}_3 - \hat{i}_4 = q(\hat{b}_3^\dagger\hat{b}_3 - \hat{b}_4^\dagger\hat{b}_4) \\ &= q[T_1(1-2T_1)|\alpha_s''|^2 + (1-2T_1)\sqrt{T_1}(\alpha_s''^*\delta\hat{\alpha}_3 + \alpha_s''\delta\hat{\alpha}_3^\dagger) + T_2(2T_2-1)|\alpha_{\mathrm{LO}}''|^2 + (2T_2-1)\sqrt{T_2}(\alpha_{\mathrm{LO}}''^*\delta\hat{\alpha}_4 + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_4^\dagger) \\ &\quad + 2T_1\sqrt{1-T_1}(\alpha_s''^*\delta\alpha_{v3}'' + \alpha_s''\delta\alpha_{v3}''^\dagger) + i2T_2\sqrt{1-T_2}(\alpha_{\mathrm{LO}}''\delta\alpha_{v4}''^\dagger - \alpha_{\mathrm{LO}}''^*\delta\alpha_{v4}'')]. \end{aligned} \tag{B7}$$

Note that the squared modulus terms in the last two equations are what helped us derive the set of conditions in Eq. (5). The measurement results corresponding to Bob's quadratures $\hat{X}_B$ and $\hat{P}_B$ are then calculated

using Eq. (3):

$$\begin{aligned}
\hat{X}_B &= \frac{2\hat{i}_x}{q|\alpha_{\mathrm{LO}}|} = \frac{2[(1-T_1)(1-2T_1)|\alpha_s''|^2 + (1-T_2)(2T_2-1)|\alpha_{\mathrm{LO}}''|^2]}{|\alpha_{\mathrm{LO}}|} \\
&\quad + \frac{2[(1-2T_1)\sqrt{1-T_1}(\alpha_s''^{*}\delta\hat{\alpha}_1 + \alpha_s''\delta\hat{\alpha}_1^{\dagger}) + (2T_2-1)\sqrt{1-T_2}(\alpha_{\mathrm{LO}}''^{*}\delta\hat{\alpha}_2 + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_2^{\dagger})]}{|\alpha_{\mathrm{LO}}|} \\
&\quad + \frac{4[\sqrt{T_1}(1-T_1)(\alpha_s''^{*}\delta\hat{\alpha}_{v1}'' + \alpha_s''\delta\hat{\alpha}_{v1}''^{\dagger}) + \sqrt{T_2}(1-T_2)(\alpha_{\mathrm{LO}}''^{*}\delta\hat{\alpha}_{v2}'' + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_{v2}''^{\dagger})]}{|\alpha_{\mathrm{LO}}|} \\
&= \sqrt{\eta}X_E + \hat{X}_{\mathrm{NB}}, \\
\hat{P}_B &= \frac{2\hat{i}_x}{q|\alpha_{\mathrm{LO}}|} = \frac{2[T_1(1-2T_1)|\alpha_s''|^2 + T_2(2T_2-1)|\alpha_{\mathrm{LO}}''|^2]}{|\alpha_{\mathrm{LO}}|} \\
&\quad + \frac{2[(1-2T_1)\sqrt{T_1}(\alpha_s''^{*}\delta\hat{\alpha}_3 + \alpha_s''\delta\hat{\alpha}_3^{\dagger}) + (2T_2-1)\sqrt{T_2}(\alpha_{\mathrm{LO}}''^{*}\delta\hat{\alpha}_4 + \alpha_{\mathrm{LO}}''\delta\hat{\alpha}_4^{\dagger})]}{|\alpha_{\mathrm{LO}}|} \\
&\quad + \frac{4[T_1\sqrt{1-T_1}(\alpha_s''^{*}\delta\alpha_{v3}'' + \alpha_s''\delta\alpha_{v3}''^{\dagger}) + iT_2\sqrt{1-T_2}(\alpha_{\mathrm{LO}}''\delta\alpha_{v4}''^{\dagger} - \alpha_{\mathrm{LO}}''^{*}\delta\alpha_{v4}'')]}{|\alpha_{\mathrm{LO}}|} \\
&= \sqrt{\eta}P_E + \hat{P}_{\mathrm{NB}},
\end{aligned} \tag{B8}$$

where we have used conditions ii and iii from Eq. (5). Let α_{LO}'' and α_s'' be real; we then get the following inequalities:

$$\begin{aligned}
\hat{X}_{\mathrm{NB}} &= \frac{2[(1-2T_1)\sqrt{1-T_1}\alpha_s''(\delta\hat{\alpha}_1 + \delta\hat{\alpha}_1^{\dagger}) + (2T_2-1)\sqrt{1-T_2}\alpha_{\mathrm{LO}}''(\delta\hat{\alpha}_2 + \delta\hat{\alpha}_2^{\dagger})]}{|\alpha_{\mathrm{LO}}|} \\
&\quad + \frac{4[\sqrt{T_1}(1-T_1)\alpha_s''(\delta\hat{\alpha}_{v1}'' + \delta\hat{\alpha}_{v1}''^{\dagger}) + \sqrt{T_2}(1-T_2)\alpha_{\mathrm{LO}}''(\delta\hat{\alpha}_{v2}'' + \delta\hat{\alpha}_{v2}''^{\dagger})]}{|\alpha_{\mathrm{LO}}|}, \\
\hat{P}_{\mathrm{NB}} &= \frac{2[\sqrt{T_1}(1-2T_1)\alpha_s''(\delta\hat{\alpha}_3 + \delta\hat{\alpha}_3^{\dagger}) + \sqrt{T_2}(2T_2-1)\alpha_{\mathrm{LO}}''(\delta\hat{\alpha}_2 + \delta\hat{\alpha}_4^{\dagger})]}{|\alpha_{\mathrm{LO}}|} \\
&\quad + \frac{4[T_1\sqrt{1-T_1}\alpha_s''(\delta\alpha_{v3}'' + \delta\alpha_{v3}''^{\dagger}) + iT_2\sqrt{1-T_2}\alpha_{\mathrm{LO}}''(\delta\alpha_{v4}''^{\dagger} - \delta\alpha_{v4}'')]}{|\alpha_{\mathrm{LO}}|}.
\end{aligned} \tag{B9}$$

Therefore,

$$\begin{aligned}
V_{\mathrm{NB},x} &= \langle(\hat{X}_{\mathrm{NB}})^2\rangle = \frac{4\left[\left\langle(1-2T_1)^2(1-T_1)\alpha_s''^2\delta X_1^2\right\rangle + \left\langle(2T_2-1)^2(1-T_2)\alpha_{\mathrm{LO}}''^2\delta X_2^2\right\rangle\right]}{|\alpha_{\mathrm{LO}}|^2} \\
&\quad + \frac{16\left[\left\langle T_1(1-T_1)^2\alpha_s''^2\delta X_{v1}''^2\right\rangle + \left\langle T_2(1-T_2)^2\alpha_{\mathrm{LO}}''^2\delta X_{v2}''^2\right\rangle\right]}{|\alpha_{\mathrm{LO}}|^2} \\
&< 13 \times \frac{\max\{|\alpha_s''|^2, |\alpha_{\mathrm{LO}}''|^2\}}{|\alpha_{\mathrm{LO}}|^2} = 0.13,
\end{aligned} \tag{B10}$$

$$\begin{aligned}
V_{\mathrm{NB},p} &= \langle(\hat{P}_{\mathrm{NB}})^2\rangle = \frac{4\left[\left\langle(1-2T_1)^2T_1\alpha_s''^2\delta X_3^2\right\rangle + \left\langle(2T_2-1)^2T_2\alpha_{\mathrm{LO}}''^2\delta X_4^2\right\rangle\right]}{|\alpha_{\mathrm{LO}}|^2} \\
&\quad + \frac{16\left[\left\langle T_1^2(1-T_1)\alpha_s''^2\delta X_{v3}''^2\right\rangle + \left\langle T_2^2(1-T_2)\alpha_{\mathrm{LO}}''^2\delta X_{v4}''^2\right\rangle\right]}{|\alpha_{\mathrm{LO}}|^2} \\
&< 13 \times \frac{\max\{|\alpha_s''|^2, |\alpha_{\mathrm{LO}}''|^2\}}{|\alpha_{\mathrm{LO}}|^2} = 0.13.
\end{aligned} \tag{B11}$$

Here we use the facts that the maximum values of $(1-2T)^2(1-T)$, $(1-2T)^2T$, $T(1-T)^2$, and $T^2(1-T)$ are 1, 1, $\frac{4}{27}$, and $\frac{4}{27}$, respectively; $\langle\delta X^2\rangle = \langle\delta P^2\rangle = 1$; and the constraint of $\max\{|\alpha_s''|^2, |\alpha_{\mathrm{LO}}''|^2\} < 10^{-2}|\alpha_{\mathrm{LO}}|^2$ (see Appendix A).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 7382 (2007).

[4] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Phys. Rev. A **78**, 042333 (2008).

[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express. **8**, 27938 (2010).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photon. **4**, 686 (2010).
[7] F.-H. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[8] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Comm. **2**, 349 (2011).
[9] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).
[10] H. Weier, H. Krauss, M. Rau, M. Füerst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).
[11] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).
[12] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Phys. Rev. A. **84**, 062308 (2011).
[13] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[14] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nature Photon. **7**, 378 (2013).
[15] http://www.sequrenet.com/
[16] http://qlabsusa.com/
[17] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[18] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004); Phys. Rev. A. **73**, 022316 (2006).
[19] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A. **72**, 050303 (2005).
[20] H. Häseler, T. Moroder, and N. Lütkenhaus, Phy. Rev. A. **77**, 032303 (2008).
[21] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[22] J. Lodewyck and P. Grangier, Phys. Rev. A. **76**, 022332 (2007); J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, *ibid.* **76**, 052301 (2007).
[23] M. Eisenmann and E. Weidel, J. Lightwave Technol. **6**, 8588 (2010).
[24] A. Ankiewicz, A. Snyder, and X.-H. Zheng, J. Lightwave Technol. **4**, 1317 (1986).
[25] V. Tekippe, Fiber Integr. Opt. **9**, 97 (1990).
[26] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[27] S. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[28] H. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics*, 2nd ed. (Wiley-VCH Press, New York, 2003).
[29] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[30] R. García-Patrón, Ph.D. thesis, Université Libre de Bruxelles (2007).
[31] In a regular CV-QKD system, the LO intensity is approximately equal to the total intensity, therefore monitoring the total intensity is equivalent to monitoring the LO intensity. See also Ref. [14].
[32] G. B. Arfken and H. J. Weber, *Mathematical Methods for Physics* (Elsevier Academic Press, New York, 2006).