Robust continuous-variable quantum key distribution against practical attacks

Peng Huang,* Jingzheng Huang, Tao Wang, Huasheng Li, and Duan Huang
State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Quantum Sensing and Information Processing, Shanghai Jiaotong University, Shanghai 200240, China

Guihua Zeng†
State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China
and College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China
(Received 30 October 2016; published 1 May 2017)

Recently, several practical attacks on continuous-variable quantum key distribution (CVQKD) were proposed based on faking the estimated value of channel excess noise to hide the intercept-and-resend eavesdropping strategy, including the local oscillator (LO) fluctuation, calibration, wavelength, and saturation attacks. However, the known countermeasures against all these practical attacks will inevitably increase the complexity of the implementation of CVQKD and affect its performance. We develop here an asynchronous countermeasure strategy without structural modifications of the conventional CVQKD scheme. In particular, two robust countermeasures are proposed by adding peak-valley seeking and Gaussian postselection steps in conventional data postprocessing procedure. The analysis shows that the peak-valley seeking method naturally make the schemes immune to all known types of calibration attacks even when Eve simultaneously performs wavelength or LO fluctuation attacks and exhibit simpler implementation and better performance than the known countermeasures. Meanwhile, since the Gaussian postselection is able to resist the saturation attacks, the proposed schemes are secure against all known types of practical attacks.

DOI: 10.1103/PhysRevA.95.052302

I. INTRODUCTION

Continuous-variable quantum key distribution (CVQKD) [1–7] provides an alternative way for two distant parties, the sender Alice and receiver Bob, to share a string of secure secret keys through a quantum channel which is assumed to be controlled by the potential eavesdropper Eve. In CVQKD protocols, the secret key information is continuously modulated on the light field quadratures, which can be measured with coherent detection, such as homodyne or heterodyne detections. So CVQKD inherits the merits associated with the use of coherent detection, such as the high channel capacity and superior compatibility with intense classical channels [8]. So far, the Gaussian-modulated coherent-state (GMCS) CVQKD protocols have been proved theoretically secure against general collective attacks [9–11] and coherent attacks [12–15]. However, the practical implementation of GMCS CVQKD scheme inevitably deviates from the theoretical model, which may leave loopholes for an eavesdropper.

In a practical GMCS CVQKD system, the local oscillator (LO) signal is necessary to implement the coherent detection in Bob's side. In addition, the values of key parameters used to calculate the secret key rate are all expressed in shot-noise units, which are also related to the LO intensity [16]. However, the LO signal is not explicitly considered in the security proofs of theoretical CVQKD schemes [9,10,13] since it is not required to evaluate the secret key information at a theoretical level. In practice, the fluctuation of LO intensity will incur LO fluctuation attacks [17]. Moreover, Eve can tamper the LO intensity to mislead the estimation of shot noise so as to underestimate the channel excess noise to cover her intercept-and-resend attack. We denote these types of attacks here as LO-intensity calibration attacks. The efficient way to defeat these attacks is calibrating once-and-for-all the slope of the LO to shot-noise linear relation on homodyne detection, and then to monitor the LO intensity fluctuation and estimate the shot noise. Unfortunately, Eve can perform time-shift calibration attacks [18] even when LO intensity is monitored. The possible countermeasures are also suggested in [18] that one can use an amplitude modulator on Bob's signal path or a second homodyne detection on Bob's LO path to directly obtain the real-time shot noise. Unfortunately, these countermeasures cannot resist the time-shift calibration attacks when Eve simultaneously performs a wavelength attack [19], noted here as wavelength-calibration attacks.

Actually, the principle of all calibration attacks lies on misleading the legitimate parties to overestimate the shot noise so as to underestimate the channel excess noise. By exploiting the loophole of imperfect linearity of homodyne detection, Eve can also perform a saturation attack [20] to directly mislead the estimation of channel excess noise. Meanwhile, a simple countermeasure against saturation attack is also proposed in [20] that one can performing Gaussian postselection to defeat this attack without any modification of CVQKD hardware. However, to resist all of these practical attacks, the suggested countermeasure monitors the LO intensity and meanwhile inserts an amplitude modulator on Bob's signal path and randomly applies several attenuation ratios to check the noise linearity with respect to the attenuation ratio [19,21]. However, this method will inevitably increase the complexity of the implementation of CVQKD and lead to attenuation of the signal and thus reduction of secret key rate.

*huang.peng@sjtu.edu.cn
†ghzeng@sjtu.edu.cn

In this paper, we develop a countermeasure strategy relying on the improvement of data postprocessing procedure without any structural modification of the conventional GMCS CVQKD scheme [22]. In particular, two practical countermeasures are proposed by adding the peak-valley seeking and Gaussian postselection steps in conventional data postprocessing procedure. In these schemes, the regeneration of a synchronous trigger for homodyne detection is removed in Bob's side. Relying on the peak-valley seeking method, we show that the shot noise can be always well estimated in real time by using the calibrated linear relationship between the shot noise and LO intensity. So the peak-valley seeking method can make the schemes naturally immune to all known calibration attacks even when Eve simultaneously performs wavelength or LO fluctuation attacks. Since the using of Gaussian postselection is able to defeat the saturation attack, the proposed schemes will be secure against all known practical attacks. It should be mentioned that we do not introduce any structural modification in this countermeasure strategy, and we will show that the proposed countermeasures are more robust and efficient than the known ones.

This paper is organized as follows. In Sec. II, we first introduce the calibration technique in CVQKD system, and then take a review of the proposed calibration attacks and corresponding countermeasures, especially the LO-intensity and time-shift calibration attacks. In Sec. III, two CVQKD countermeasures based on peak-valley seeking and Gaussian postselection are proposed, and their performance to resist the current calibration attacks is analyzed. Finally, a conclusion and discussion are drawn in Sec. IV.

II. CALIBRATION ATTACKS AND KNOWN COUNTERMEASURES IN CVQKD SYSTEM

A. Calibration technique in CVQKD system

Before introducing the calibration attacks in CVQKD system, we first take a brief review of the GMCS CVQKD protocol. The conventional GMCS CVQKD protocol [22] can be roughly divided into two stages, i.e., the quantum communication and data postprocessing stages. In the former stage, Alice sends the prepared coherent states with Gaussian modulation through quantum channel, and Bob receives these states and measures one of the quadratures with a homodyne detector. It should be mentioned that the output result of the homodyne detector contains four parts, i.e., the modulated quadrature, the shot noise, the channel excess noise, and the electronic noise from homodyne detector. Then in the data postprocessing stage, Bob first accumulates the raw key data shared with Alice and they discard the uncorrected one to form the sifted key data by using public communication. After that, some of the sifted key data will be used to evaluate the parameters and practical secret key rate, then the left data will be further processed into a final secret key with error reconciliation and privacy amplification. It should be mentioned that the parameters used in the calculation of the secret key rate are quantified to shot-noise units, such as the modulation variance and excess noise. So it is necessary to know the shot noise around the distribution of the secret key.

In principle, the shot noise can be evaluated from results of the interference between the LO and vacuum mode in homodyne detection [18]. When the intensity of the LO is known, the shot noise can be also calculated by using the linear relationship between the variance of measurement results and the input intensity of the LO on the homodyne detection during CVQKD. In detail, a standard calibration technique was proposed by the authors of [18,23]. First, before quantum key distribution, Alice and Bob will establish the linear relationship between the shot noise and the LO intensity in a secure laboratory. Then, Bob measures the intensity of a fraction of LO with a power meter or a photodiode followed by an integration circuit. Finally, Alice and Bob deduce the shot noise with the previously established linear relationship, which can be used to further evaluate the secret key rate. So this calibration technique lies on two critical points, i.e, obtaining the real intensity of LO in Bob's homodyne detection and calibrating the real linear relationship between the shot noise and the LO intensity. However, these two points can be well exploited by Eve to perform calibration attacks. In the following, we will introduce the known calibration attacks in detail and the corresponding countermeasures.

B. Calibration attacks and known countermeasures

In the practical CVQKD scheme, a fraction of sifted key data will be randomly chosen to estimate the covariance matrix of the state shared by Alice and Bob to evaluate the secret key rate. Specifically, it involves estimations of the variance on Alice's and Bob's sites, $\langle x^2\rangle$ and $\langle y^2\rangle$, and the covariance between Alice and Bob, $\langle xy\rangle$ with the following expressions

$$\begin{aligned}\langle x^2\rangle &= V_x,\\ \langle y^2\rangle &= \eta T V_x + N_0 + \eta T\xi + V_{\mathrm{el}},\\ \langle xy\rangle &= \eta T V_x,\end{aligned} \tag{1}$$

where T is the transmission efficiency of quantum channel, $\xi = \epsilon N_0$ is the excess noise in quantum channel, $V_x = V_A N_0$ is the modulation variance, $V_{\mathrm{el}} = \upsilon_{\mathrm{el}} N_0$ is the electronic noise, and N_0 is the shot noise. Moreover, we can reasonably assume that the efficiency of homodyne detector and the electronic noise do not fluctuate during the QKD procedure.

To estimate these parameters from various measurements of Gaussian random correlated variables (x_i, y_i) centered on zero for $i = 1, \ldots, m$, the Gaussian linear model is justified in practice [13]

$$y = tx + z, \tag{2}$$

where $t = \sqrt{\eta T}$, and z follows a centered normal distribution with unknown variance $\sigma^2 = N_0 + \eta T\xi + V_{\mathrm{el}}$. One can finally estimate the true value of transmission efficiency and excess noise as $T = \hat{t}^2/\eta$ and $\xi = (\hat{\sigma}^2 - \hat{N}_0 - V_{\mathrm{el}})/\hat{t}^2$, where $\hat{N}_0$ is the calibrated shot noise, and $\hat{t}$ and $\hat{\sigma}^2$ are the maximum-likelihood estimators with the forms

$$\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} m x_i^2}, \quad \hat{\sigma}^2 = \frac{1}{m}\sum_{i=1}^{m}(y_i - \hat{t}x_i)^2. \tag{3}$$

If the calibrated shot noise $\hat{N}_0$ is not equal to the true value N_0 (usually $N_0 < \hat{N}_0$), the eavesdropper will underestimate

the excess noise, that is

$$\xi' = \xi - \frac{\hat{N}_0 - N_0}{\hat{t}^2}, \tag{4}$$

which can be expressed in the shot-noise units as

$$\epsilon' = \frac{N_0}{\hat{N}_0}\left[\epsilon - \frac{1}{\hat{t}^2}\left(\frac{\hat{N}_0}{N_0} - 1\right)\right]. \tag{5}$$

So in this circumstance, Eve can manipulate the calibration of shot noise to hide her intercept-and-resend eavesdropping strategy, and the communication is not secure anymore. We can see the aim of Eve's calibration attacks is to overestimate the shot noise. Then it will not match with the one in the output result of homodyne detection such that Alice and Bob will underestimate the large excess noise introduced by Eve's intercept-and-resend attack. To calibrate the true value of shot noise, the common way is to monitor the LO intensity and then using the previously established linear relationship between the shot noise and the LO intensity to deduce the shot noise.

Unfortunately, this method is not always feasible. As is known in the practical CVQKD system, Alice and Bob usually work synchronously and Bob needs to recover the electrical trigger from the transmitted classical optical signal, which can be one fraction of LO [18,22] or an extra classical optical signal [24,25]. The typical method is using a clock converting circuit to output a rising trigger signal when the intensity entering the photodiode is above a certain threshold. The trigger is adjusted such that the value of the signal at the output of homodyne detection is maximized or minimized. Jouguet *et al.* [18] proposed a typical calibration attack on the local oscillator, which was also used to generate the synchronous trigger.

This attack can be depicted in Fig. 1, which involves in attenuating the beginning of the LO pulses during QKD run to induce a delay of the trigger used for homodyne measurement, such that Alice and Bob cannot sample the real peak or valley value. It should be mentioned that monitoring the intensity of the local oscillator is invalid to defeat this attack, since Eve changed the linear relationship between the shot noise and LO intensity. To resist this attack, two countermeasures based on real-time shot-noise measurement techniques were also suggested by the authors of [18]. One method is by applying a strong attenuating on some randomly chosen pulse of Bob's signal path by using an amplitude modulator. The other one is by using a second homodyne detector on Bob's local oscillator path to obtain the real-time shot noise. The main intention is to calibrate the true value of shot noise and verify the equation $\hat{N}_0 = N_0$.

However, a practical attack strategy was proposed by the authors of [19], where the wavelength-dependent character of the fused biconical taper beam splitter can be utilized to nullify the real-time monitoring of shot noise. In this attack, Eve prepares and resends two extra coherent state pulses with wavelengths different from the one used by the legitimate parties in CVQKD scheme, where their polarizations are same with the signal and LO, respectively, such that they can successfully reach Bob's homodyne detection. Eve randomly chooses two selected wavelengths of signal and local oscillator pulses such that the transmittances of the 50:50 fused biconical taper beam splitter corresponding to the different wavelengths are deviated from 0.5.

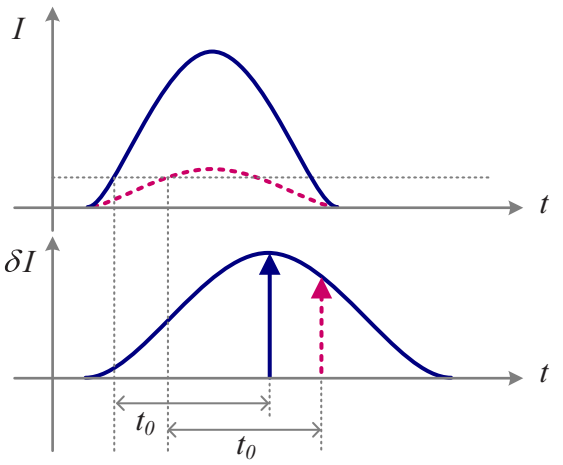

FIG. 1. The description of calibration attack by manipulating the classical synchronous pulse. The upper plot shows the profiles of the trigger signals generated at Bob's side depending on the shape of the classical synchronous pulse, the solid and dotted curves denote the original signal and the attenuated one by Eve. The lower plot shows the differential signal from homodyne detection, where the variance of the output value of the homodyne detection depending on the time of measurement. The trigger is delayed t_0 such that the value of the signal at the output of homodyne detection is maximized.

Consider the case that Bob uses strong attenuating on the signal path, the introduced LO pulses will contribute extra differential current, i.e., D_1^{LO} or D_2^{LO}, plus weak shot noise current for two different wavelengths. When Eve ensures that $D_1^{\mathrm{LO}} = -D_2^{\mathrm{LO}}$ and chooses the two wavelengths with equal probability, she can achieve zero statistical average and extra positive variance D_{LO} of shot noise. Thus, she can make the shot-noise-measurement results seem normal when she simultaneously performs calibration attack. For instance, when the realistic shot noise is reduced to 3/4 of the original level, Eve should make $D_{\mathrm{LO}} = 1/4N_0$. While for the case of no attenuation, the contribution of differential current introduced by the extra signal will be D_1^s or D_2^s for two different wavelengths, and she will ensure that $D_1^{\mathrm{LO}} = -D_2^{\mathrm{LO}} = -D_1^s = D_2^s$. Finally, the contribution of differential current from the extra signal will cancel the one from local oscillator, and these pulses with different wavelengths will almost introduce no extra influence on the measurement results. Thus, the methods to monitor the shot noise in real time are invalid for the joint attack of calibration and wavelength attacks.

The corresponding countermeasure is proposed based on the real-time shot-noise measurement technique. In particular, Bob can use a third attenuation ratio to obtain the polynomial function of the total noise to the attenuation ratio so as to avoid the all of the calibration attacks [19]. Moreover, the countermeasure is also showed to be useful to resist the saturation attack [19,21]. However, as referred above, these methods will inevitably increase the complexity and decrease the final secret key rate of CVQKD. In the following, we will introduce the proposed robust and efficient countermeasure strategy.

III. COUNTERMEASURE STRATEGY BASED ON IMPROVED DATA POSTPROCESSING

According to the principle of homodyne measurement, the encoded information in the quardratures of signal states, i.e., either the amplitude or phase quadrature is proportional to the measurement result of homodyne detection. Moreover, the measurement result naturally corresponds to the peak or valley photocurrent of the output electrical pulse, which comes from the differential photocurrent in homodyne detection. In practice, the analog output of homodyne detection will be sampled by an analog-to-digital convertor (ADC), and the sampled data will be processed in the postprocessing stage to generate the final secret key. So Alice and Bob will schedule the right trigger time so that the sampled values of ADC is the peak or valley values of the analog output. When Eve performs calibration attacks on the CVQKD schemes without any countermeasure, such as changing the LO intensity or shifting the trigger for homodyne detection, Alice and Bob will overestimate the shot noise and it will not match with the one in the output result of homodyne detection, this is actually a common characteristic for all known calibration attacks.

Fortunately, we find that the estimated shot noise can always match with the one in the output result of homodyne detection if one can simultaneously monitor the LO intensity and seek the peak or valley value of the analog output of homodyne detection. So this method of simultaneously monitoring the LO intensity and seeking the peak or valley value (noted as peak-valley seeking) can be used to resist all known calibration attacks. In the conventional GMCS CVQKD scheme, monitoring the LO intensity is a standard step, and peak-valley seeking can be implemented in the data postprocessing stage after Bob oversamples the output signal of homodyne detection. This method can be implemented without any modification on the structure of the conventional GMCS CVQKD scheme. Recently, it was shown that the saturation attack can be resisted by using Gaussian postselection without any modification of CVQKD hardware. Specifically, the Gaussian postselection consists in precalibrating the linearity domain of the homodyne detector, and then applying a Gaussian postselection filter to the quadrature measurements results of Bob so that the postselected measurement results fall within the linearity domain when the postselected input data are guaranteed to be Gaussian [20].

When we add both of the peak-valley seeking and Gaussian postselection steps into the conventional data postprocessing procedure, the GMCS CVQKD may be secure against all of the known practical attacks without any structural modification. This countermeasure strategy can be implemented more simply than the known ones. In the following, two exact countermeasures based on peak-valley seeking and Gaussian postselection are proposed and we will show their robustness and efficiency against the practical attacks.

A. Countermeasure with power meter based on peak-valley seeking and Gaussian postselection

The structure of the first countermeasure is the same as the conventional GMCS CVQKD scheme in [22], which is depicted in Fig. 2 (Alice's side is omitted). Instead of using a synchronous trigger to sample the peak or valley value of the analog output of homodyne detection, Bob oversamples the analog pulse with his own clock frequency f_{samp}, and the oversampled data are saved in Bob's side for further processing in the data postprocessing procedure. After the stage of transmission and detection of quantum states, Bob first picks the solitary peak or valley points with the largest absolute values in every period of the analog pulses with sorting algorithm. While in the conventional synchronous scheme, Bob samples the measurement results from the analog output of homodyne detection with frequency $f_s = 1/T_s$. The comparison of the performance of conventional synchronous and proposed countermeasures on the output pulses of homodyne detection is depicted in Fig. 3, where the positions of the peak and valley points in the conventional scheme are distorted by Eve's operations.

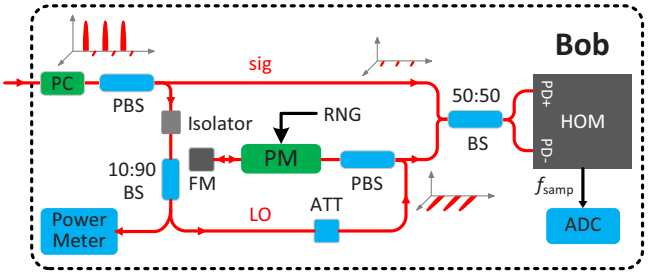

FIG. 2. Countermeasure against practical attacks with power meter based on peak-valley seeking and Gaussian postselection. PC is polarization controller, BS is beam splitter, PBS is polarization beam splitter, FM is faraday mirror, RNG is the random number generator, PM is phase modulator. The power meter is used to monitor the LO intensity in real time.

When Eve performs a time-shift calibration attack on the this scheme, Bob can always pick out the solitary peak or valley values in the positions A_7, B_7, C_7, D_7 for each analog signal period T_s after oversampling and sorting steps, where A, B, C, and D denote the four different pulses and the subscript number denotes the sampling position in each pulse. While for the

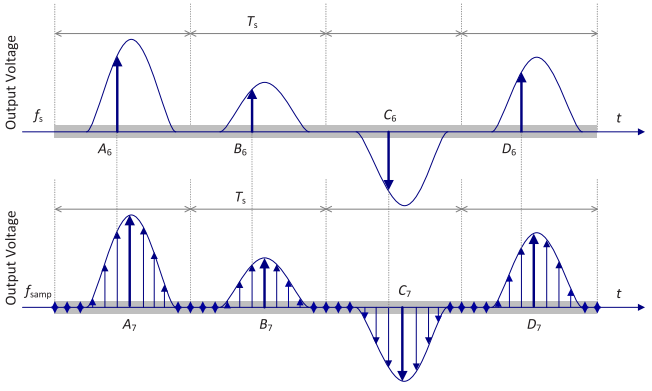

FIG. 3. Time-domain shapes of the output pulse from the homodyne detection for the conventional synchronous (upper) and peak-valley seeking (lower) schemes. The arrows denote the sampling positions in time flow.

conventional scheme, the output result of homodyne detection are changed to the values in the positions A_6, B_6, C_6, D_6 due to the time-shift calibration attack. After this step, Bob will obtain the real peak or valley values of the signals at the output of the homodyne detection. These data will be then processed by discarding the uncorrected one to form the sifted key data and further processed by Gaussian postselection. Finally, Alice and Bob perform parameter estimations, reconciliation, and privacy amplification to distill the secret key. Note here that the trigger clock regeneration part in Bob's side, for instance, using LO or other transmitted optical signals, is not needed in this scheme, since Bob can oversample the received signals with asynchronous clock and will always obtain the correct values of the encoded information. So any kind of time-shift calibration attacks are invalid.

Also, to evaluate the shot noise in real time, the previously established linear relationship between the shot noise and LO intensity is used and a small fraction of LO is used to monitor the LO intensity. Since the solitary peak or valley values of the output signal of homodyne detection can be always obtained, the established linear relationship between the shot noise and LO intensity will never be changed under Eve's time-shift calibration attacks. Thus the evaluated shot noise can be also correctly estimated according to the LO intensity and it will naturally match with the one in the result of homodyne detection. Naturally, the LO-intensity calibration attacks cannot work neither. Moreover, this scheme to some extent is more robust than the ones based on the fixed schedule trigger, i.e., the synchronous schemes since the trigger signal may be distorted in the transmission channel. However, the notable merit is that Eve has no chance to take any kind of known calibration attacks even when she simultaneously performs wavelength or LO fluctuation attacks. Since the added Gaussian postselection step can further resist the saturation attack, the proposed countermeasure will be secure against all known types of practical attacks.

In Fig. 4, we compare the theoretical secret key rates of the proposed countermeasure under collective attacks when taking into account finite-size effects [11] to the one of known countermeasure, i.e., the one by inserting an optical switch on Bobs signal path in the conventional synchronous scheme [18,19]. The secret key rate under the collective attacks for the nonasymptotic case is given by

$$K_{\text{finite}} = \frac{n}{N}\left[\beta I_{\text{AB}}^{\text{finite}} - \chi_{\text{BE}}^{\text{finite}} - \Delta(n)\right], \tag{6}$$

where I_{AB}^{finite} is the mutual information shared between Alice and Bob, $\chi_{\text{BE}}^{\text{finite}}$ is the Holevo bound on the information between Bob and Eve, $\Delta(n)$ is related to the security of the privacy amplification, N denotes the sampling block size, and n is the block size for final key generation.

In the data postprocessing procedure, the data with block size of $N-n$ are used for the parameters' estimation and phase compensation. We set $n/N = 1/2$ here in our scheme. The normalized modulation variance of Alice V_A is adjusted to maintain a signal-to-noise ratio of 0.75 on Bob's side, and the reconciliation efficiency is set as $\beta = 95\%$. The normalized excess noise on Bob's side is $\epsilon = 0.001$, and the normalized electronic noise of homodyne detection is $\nu_{\text{el}} = 0.01$. The original quantum efficiency of homodyne

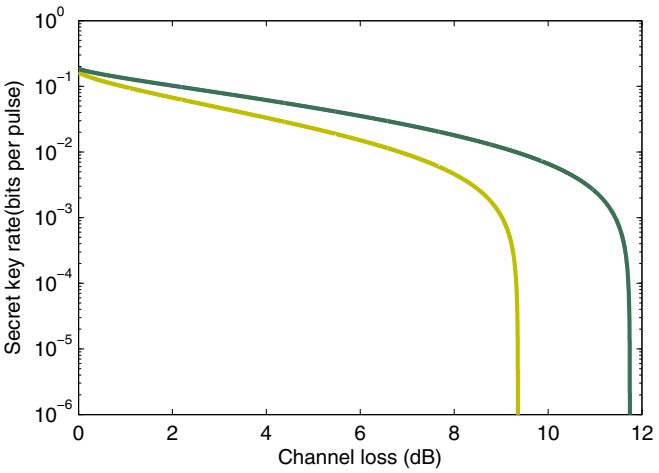

FIG. 4. Secret key rates under collective attacks with block size of 1×10^9 and security parameter 1×10^{-10}. The upper curve corresponds to the secret key rate of the proposed countermeasure with power meter based on peak-valley seeking and Gaussian postselection. The lower curve corresponds the countermeasure by inserting an optical switch on Bob's signal path to perform real-time shot-noise measurement.

detection, which corresponds to the upper curve for the proposed countermeasure, is assumed to be $\eta_{\text{pvs}} = 0.6$, while the lower curve corresponds to an equivalent efficiency $\eta_{\text{cali}} = 0.32$ for the known countermeasure by inserting an optical switch on Bob's signal path. It can be seen from Fig. 4 that the known countermeasure will decrease the secure transmission distance and secret key rate. The first reason is that a fraction of pulses are chosen at random to compute an estimation of the shot noise which will be discarded, and here we also set the fraction as 10% as in [18,19]. Second, the efficiency of Bob's homodyne detection η is reduced as shown above (the introduced losses by the optical switch or amplitude modulator is set as -2.7 dB as in [18,19]). Considering realistic values of all the parameters, we find in Fig. 4 that the maximum channel loss increases from 9.35 to 11.75 dB when implementing this countermeasure. Actually, improving the data postprocessing procedure of the CVQKD scheme by adding peak-valley seeking and Gaussian postselection does not affect the theoretical secure transmission loss and the secret key rate.

It should be mentioned that when Eve performs calibration or saturation attacks in the known countermeasure, Alice and Bob will find her eavesdropping and may discard all of the shared data due to Eve's intercept-and-resend attack. Here the use of monitoring of the LO intensity and peak-valley seeking method naturally defeat all of the known calibration attacks in an active way. So Eve's calibration attacks are all invalid, and Alice and Bob can always obtain the secret key under these practical attacks. Also, the Gaussian postselection may allow one to distill the secret key even in the presence of moderate saturation, i.e., the raw key data are partly saturated [20]. So we can see the proposed countermeasure is more robust and efficient than the known one. Nevertheless, we should note that the using of peak-valley seeking and Gaussian postselection will to some extent increase the computational

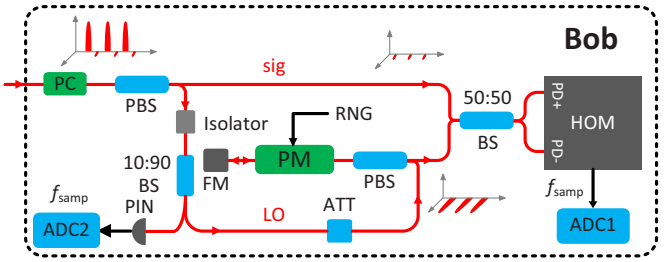

FIG. 5. Countermeasure against practical attacks with dual-sampling measurement based on peak-valley seeking and Gaussian postselection. PC is polarization controller, BS is beam splitter, PBS is polarization beam splitter, FM is faraday mirror, RNG is the random number generator, PM is phase modulator. ADC2 is used to monitor the corresponding intensity of LO signal in homodyne detection.

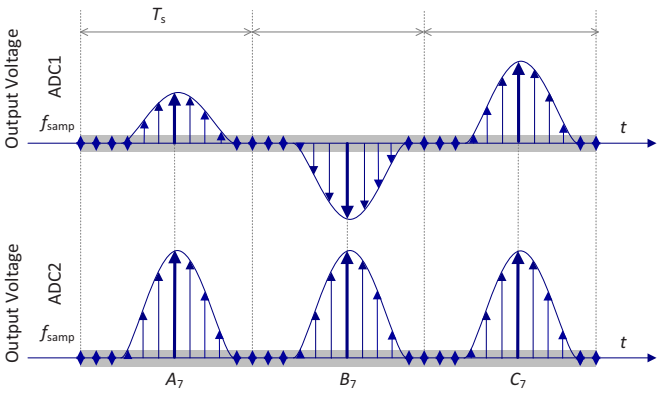

FIG. 6. Time-domain shapes of the output pulse from the homodyne detection and PIN detector for the dual-sampling measurement. The arrows denote the sampling positions in time flow.

complexity in Bob's side. Since Gaussian postselection can be implemented by classical postprocessing, we can use the high-speed graphics processing unit (GPU) device [26] or field program gate array (FPGA) in the reconciliation step to release the increased computational complexity. Actually, comparing to the continuous-variable reconciliation and privacy amplification, the computational complexity of peak-valley seeking and Gaussian postselection is still limited.

However, there exists the case that the output values from the peak-valley seeking step are not the real peak or valley values of the analog output of homodyne detector due to limited sampling points, which is known as finite sampling bandwidth effects [27]. We can expand the duration of the analog pulse and increase sampling frequency f_{samp} to compromise the finite sampling bandwidth effects and improve the accuracy of the peak-valley seeking method. Moreover, the analysis in [27] also reveals that when the sampling frequency is fixed to 1 GHz, the inaccuracy can be negligible if the CVQKD system repetition rate is below 2 MHz for proper parameters. So the proposed countermeasure above is more suitable for CVQKD schemes with relatively low repetition rate. While for the case of the higher one, a method is proposed to rectify the corresponding intensity of LO based on the dual-sampling measurement [27], such that the shot noise will always precisely matche with the one in the output result of homodyne detection, even when the solitary peak or valley values are not precisely located.

Actually, the finite sampling bandwidth effects will lead to LO calibration attacks since the shot noise is overestimated and then deduces incorrect estimations of transmission efficiency and excess noise. Fortunately, the dual-sampling method can be also used in peak-valley seeking step to further resist this LO calibration attacks arising from the finite bandwidth effects, which will be introduced in the following.

B. Countermeasure with dual-sampling measurement based on peak-valley seeking and Gaussian postselection

The second countermeasure CVQKD scheme has the same structure as the first one, which is shown in Fig. 5 (Alice's side is omitted). However, instead of using a power meter to monitor the real-time intensity of LO, a positive intrinsic-negative (PIN) detector and another ADC (called ADC2 in Fig. 5 with the same type of ADC1) are used to sample the output of LO with frequency f_{samp}. To ensure their synchronization, both of these ADCs are triggered by the same electronic circuit. So in this scheme, the real-time intensity of LO, which corresponds to the one interfered in homodyne detection, will be obtained precisely. Thus the evaluated shot noise will precisely match with the one in the real-time output result of homodyne detection, i.e., the sampled values of ADC1 at the same time slot.

Also, Bob oversamples the analog pulse with frequency f_{samp} and saves the sampled data in Bob's side for further processing. After the stage of transmission and detection of quantum states, Bob first performs a sorting algorithm to pick the solitary peak or valley points with the largest absolute values in every period of the analog pulses and saves their positions. Meanwhile, Bob oversamples the output of the PIN detector with sampling frequency f_{samp} and saves the corresponding values of the real-time intensity of LO in the same positions for each pulses. The dual-sampling measurement on the output electrical pulses of homodyne detection and PIN detector can be depicted in Fig. 6. In the upper plot, Bob picks out the solitary peak or valley values in the positions A_7, B_7, C_7 from the output of homodyne detection for each analog signal period T_s with sorting algorithm. In the lower plot, Bob saves the corresponding intensity of LO in the same positions to estimate the shot noise by using the relationship between the one and shot noise. After this step, these data will be then processed by discarding the uncorrected one to form the sifted key data and further processed by Gaussian postselection. Finally, Alice and Bob perform parameter estimations, reconciliation, and privacy amplification to distill the final secret key.

In the practical CVQKD scheme, the LO pulse will be delayed in Bob's station to implement the interference of LO and signal pulse in homodyne detection. So the corresponding LO pulse for intensity sampling will be delayed for a constant period. Without loss of generality, we do not consider here the duty cycle of LO and signal pulses either. Therefore, even when the real peak or valley values of the analog output of homodyne detection are not precisely oversampled, Alice and Bob will obtain the corresponding intensity of LO, and thus remove the

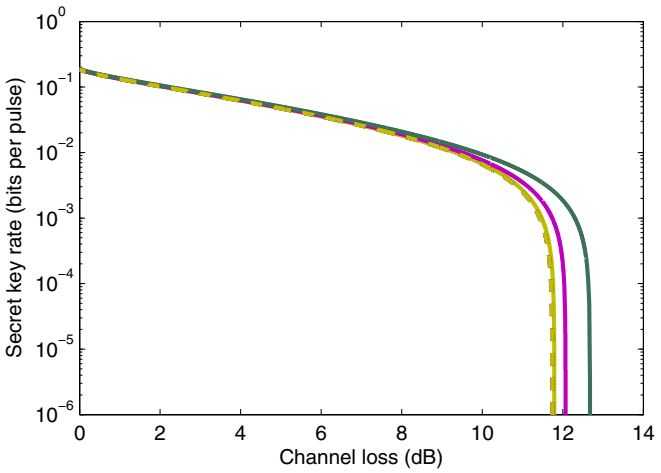

FIG. 7. The secret key rates under collective attacks with (the dashed curves, the three curves are almost overlapped) and without (the solid curves) dual-sampling measurement, when considering the finite sampling bandwidth effects. Curves from top to bottom represent $f_{\mathrm{rep}} = 10$, 5, and 2 MHz.

finite sampling bandwidth effects and correctly perform the parameter estimation as

$$\hat{N}_0 = k^2 N_0, \quad \hat{V}_A = V_A, \quad \hat{T} = T,$$
$$\hat{\epsilon} = \epsilon, \quad \hat{\nu_{\mathrm{el}}} = \frac{1}{k^2}\nu_{\mathrm{el}}, \tag{7}$$

where $k = \exp(-\frac{8 f_{\mathrm{rep}}^2}{f_{\mathrm{samp}}^2})$ is the ratio between the real peak or valley value and the oversampled one [27]. While existing the finite sampling bandwidth effects, these parameters become

$$\hat{N}_0 = N_0, \quad \hat{V}_A = V_A, \quad \hat{T} = k^2 T,$$
$$\hat{\epsilon} = \epsilon - \frac{1-k^2}{k^2 \eta T}, \quad \hat{\nu_{\mathrm{el}}} = \nu_{\mathrm{el}}, \tag{8}$$

where both of the practical transmission efficiency and excess noise are underestimated.

The secret key rates of the countermeasures based on improved data postprocessing under collective attacks with or without the dual-sampling measurement when considering the finite sampling bandwidth effects are shown in Fig. 7, where the block size and security parameter are 1×10^9 and 1×10^{-10}, respectively. The oversampling bandwidth is fixed to 1 GHz, and the normalized modulation variance of Alice V_A is adjusted to maintain a signal-to-noise ratio of 0.75 on Bob's side, and the reconciliation efficiency is $\beta = 95\%$. The normalized excess noise on Bob's side is $\nu_{\mathrm{el}} = 0.01$, and the quantum efficiency and normalized electronic noise of homodyne detection are assumed to be $\eta_{\mathrm{pvs}} = 0.6$ and $\nu_{\mathrm{el}} = 0.01$, respectively. We can find that the finite sampling bandwidth can be effectively removed by introducing the dual-sampling measurement, and thus the parameters can be always correctly estimated to resist the LO calibration attacks arising from finite sampling bandwidth effects.

Note that in [27], Alice and Bob do not use the sorting algorithm to seek precisely the peak or valley values, but just appoint a fixed position with the synchronous trigger. So the previously established linear relationship between the shot noise and the LO intensity can be also changed under Eve's time-shift calibration attacks. Thus even when using the dual-sampling measurement, the shot noise estimated according to the real-time intensity of LO will not match with the one in the output result of homodyne detection, and the communication will not be secure anymore under the time-shift calibration attacks. In addition, the transmission of the classical trigger signal may incur other potential attacks. Therefore, comparing to the original CVQKD scheme with dual-sampling measurement [27], the proposed countermeasure, i.e, the asynchronous CVQKD scheme with dual-sampling measurement based on the peak-valley seeking method is more robust in practical application. Also, since the Gaussian postselection step is added in the data postprocessing procedure, this countermeasure can further resist the saturation attack.

IV. CONCLUSION AND DISCUSSION

We investigate the principle of the known calibration attacks on the practical CVQKD schemes and develop a countermeasure strategy relying on the improvement of data postprocessing without structural modifications of the conventional CVQKD scheme. In particular, we propose two robust countermeasures by introducing peak-valley seeking and Gaussian postselection methods in conventional data postprocessing procedure. While for the case of low repetition rate of CVQKD scheme, a robust countermeasure with power meter based on peak-valley seeking and Gaussian postselection is proposed, where the transmission and regeneration of synchronous signal are not needed. In this scheme, the peak-valley seeking method is used to sample the real peak or valley value of the signal at the output of the homodyne detection. Simultaneously, a power meter is used to achieve real-time shot-noise estimation, such that the estimated shot noise can always match with the one in the output result of homodyne detection. So this characteristic makes the proposed countermeasure naturally immune to all of the currently known calibration attacks even when Eve simultaneously performing wavelength and LO fluctuation attacks. Moreover, this countermeasure can further resist the saturation attack due to the Gaussian postselection step in the data postprocessing procedure. Since the proposed countermeasure can defeat all the known practical attacks in an active way without modifying the structure of the conventional CVQKD scheme, it is more robust and efficient than the known countermeasures. While for the case of high repetition rate, the finite sampling bandwidth effects should be considered and an enhanced countermeasure is developed by introducing the dual-sampling measurement, i.e., using another ADC instead of power meter to perform precise shot-noise estimation in real time. The analysis shows that the finite bandwidth effects can be well removed and the robustness is kept against the practical attacks. It should be mentioned that the peak-valley seeking and Gaussian postselection methods can be integrated in data postprocessing procedure, where the using of high-speed GPU and FPGA will quite release the increased computational complexity.

As summarized above, the proposed two practical asynchronous countermeasures are also immune to wavelength attacks, it is because for the CVQKD scheme with homodyne detection, the successful wavelength attacks relies on the

simultaneous implementation of LO-intensity or time-shift calibration attacks. Moreover, Eve's attack by manipulating the LO by adding another classical signal with different wavelength will be invalid since the estimated shot noise in the two proposed countermeasures will always match with the one in the output result of homodyne detection. Also, the trojan-horse attack [28,29] is invalid since the using of isolators in Alice and Bobs's stations will completely prevent the transmission of the eavesdropping signal.

ACKNOWLEDGMENTS

We thank C. Wang and H. Qin for their fruitful discussions about sampling technique and countermeasures against the saturation attack. This work was supported by the National Natural Science Foundation of China (Grants No. 61332019, No. 61471239, No. 61501290, and No. 61671287), and the National key research and development program (Grant No. 2016YFA0302600).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[3] F. Grosshan, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[4] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[5] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[6] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).
[7] 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).
[8] R. Kumar, H. Qin, and R. Alléaume,, New J. Phys. **17**, 043027 (2015).
[9] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[10] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[11] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[12] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[13] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[14] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[15] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[16] M. G. Raymer, J. Cooper, H. J. Carmichael, M. Beck, and D. T. Smithey, J. Opt. Soc. Am. B **12**, 1801 (1995).
[17] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **88**, 022339 (2013).
[18] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[19] J. Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Phys. Rev. A **89**, 032304 (2014).
[20] H. Qin, R. Kumar, and R. Alléaume, Phys. Rev. A **94**, 012325 (2016).
[21] S. Kunz-Jacques and P. Jouguet, Phys. Rev. A **91**, 022307 (2015).
[22] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[23] P. Jouguet *et al.*, Opt. Express **20**, 14030 (2012).
[24] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, Sci. Rep. **5**, 14607 (2015).
[25] D. Huang *et al.*, Opt. Express **23**, 17511 (2015).
[26] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, Int. J. Quantum. Inform. **13**, 1550010 (2015).
[27] C. Wang, P. Huang, D. Huang, D. Lin, and G. Zeng, Phys. Rev. A **93**, 022315 (2016).
[28] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).
[29] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, IEEE J. Sel. Top. Quantum Electron. **21**, 6600710 (2015).