Quantum Inf Process (2018) 17:11
https://doi.org/10.1007/s11128-017-1783-8

Practical performance of real-time shot-noise measurement in continuous-variable quantum key distribution

Tao Wang[1] · Peng Huang[1] · Yingming Zhou[1] · Weiqi Liu[2] · Guihua Zeng[1,2]

Received: 19 June 2017 / Accepted: 1 December 2017

Abstract In a practical continuous-variable quantum key distribution (CVQKD) system, real-time shot-noise measurement (RTSNM) is an essential procedure for preventing the eavesdropper exploiting the practical security loopholes. However, the performance of this procedure itself is not analyzed under the real-world condition. Therefore, we indicate the RTSNM practical performance and investigate its effects on the CVQKD system. In particular, due to the finite-size effect, the shot-noise measurement at the receiver's side may decrease the precision of parameter estimation and consequently result in a tight security bound. To mitigate that, we optimize the block size for RTSNM under the ensemble size limitation to maximize the secure key rate. Moreover, the effect of finite dynamics of amplitude modulator in this scheme is studied and its mitigation method is also proposed. Our work indicates the practical performance of RTSNM and provides the real secret key rate under it.

Keywords Continuous-variable · Quantum key distribution · Shot-noise measurement · Practical performance

✉ Peng Huang
huang.peng@sjtu.edu.cn

✉ Guihua Zeng
ghzeng@sjtu.edu.cn

[1] State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Laboratory on Navigation and Location-Based Service, and Center of Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China

[2] College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China

Published online: 08 December 2017

1 Introduction

Continuous-variable quantum key distribution (CVQKD) provides a secure way to allow two remote participants, the sender Alice and the receiver Bob, to establish a secret key through an insecure quantum channel [1–3]. One well-known CVQKD scheme is the Gaussian modulated coherent state (GMCS) scheme [2–5], which has been proven on being secure against general collective attacks, which are optimal both in the asymptotic case [6–8] and in the finite-size regime [9–11]. Besides the theoretical security demonstrated, GMCS CVQKD has been experimentally demonstrated over long secure distance [12,13] and at high speed [14,15] by using commercial components. Especially, field tests of the GMCS CVQKD protocol have also been performed for point-to-point distribution [16,17] and for network distribution [18]. It is foreseeable that this scheme will be an appealing solution for future secure quantum communication.

However, there are deviations between the theoretical GMCS CVQKD protocol and its practical system, such as the untrusted local oscillator (LO), wavelength-dependent coupling ratio of the beam splitter and electronics saturation of detector. Actually, these deviations will incur loopholes to potential eavesdropper Eve. By far, several practical security attacks, such as the LO fluctuation attack [19], the LO calibration attack [20], the wavelength attack [21,22] and the saturation attack [23], have been reported and corresponding countermeasures have also been proposed. In order to defend practical attacks, real-time monitoring technologies are extensively adopted to prevent both attacks and signal disturbance [24–26]. In CVQKD regime, it is noteworthy that a real-time shot-noise measurement (RTSNM) scheme is proposed in Ref. [20] to resist the LO fluctuation attack and the calibration attack. Moreover, this scheme is also shown to be effective to avoid the wavelength attack [22] and the saturation attack [27]. Besides the security improvements, the stability of the CVQKD system is also improved. Since the secret key rate is very sensitive to the value of shot-noise variance, real-time monitoring of it greatly reduces the error introduced by the fluctuation of the LO intensity.

We should note that a novel implementation of CVQKD is also proposed, in which the LO is generated at Bob's side, therefore called as local LO (LLO) scheme [28–30]. Without transmitting LO, the security loopholes of LO can be fundamentally solved. However, the LLO scheme has its intrinsic drawbacks: Firstly, since two lasers employed in each side are independent, the laser frequency instability and the fluctuation of the relative phase will lead to an intolerable phase noise. Although the pilot is adopted to compensate the phase drift, the phase noise is still larger than the conventional CVQKD [29]. Moreover, the pilot, which is the classical signal like the LO, may also has the loophole. By contrast, the RTSNM scheme is a viable option exploiting monitoring techniques to fill the loopholes as mentioned above. Besides, it is established on the conventional CVQKD, which has relatively low phase noise and smaller change in the structure. However, to date, the practical performance of the RTSNM implementation is ignored. Since this procedure is also a major part of the practical CVQKD system, it is necessary to analyze the practical performance of itself.

In this paper, we indicate the RTSNM practical performance and investigate their effects on the CVQKD system for the first time. More specifically, we firstly consider the effect of the block size for RTSNM. Result shows that finite-size effect in shot-noise measurement may decrease the precision of parameter estimation and eventually cause a tight security bound. To mitigate that, we explore the optimal block size for RTSNM under the ensemble size limitation to maximize the secure key rate. Besides, the effect of finite dynamics of amplitude modulator (AM) in the RTSNM scheme is also studied and relieved, which becomes a guideline for the actual device choice.

The remainder is organized as follows. In Sect. 2, we illustrate this RTSNM scheme in detail and explain how it protects from practical attacks. In Sect. 3, we emphasize the finite-size effect in shot-noise measurement. On this basis, the optimal block size for it under ensemble size limitation is explored. Besides, the influence of amplitude modulator finite dynamics is discussed in Sect. 4. Finally, conclusions are drawn in Sect. 5.

2 Real-time shot-noise measurement description

As is well known, in the GMCS CVQKD protocol, Alice encodes the key information X_A and P_A from a set of Gaussian random numbers with variance V_A and zero mean, prepares a coherent state $|X_A + iP_A\rangle$ and sends it to bob. To obtain the secret key, Bob uses a homodyne detector to perform interferometric measurement. For the shot-noise measurement, Bob's apparatus has been improved, which is illustrated in Fig. 1. The polarization-multiplexing LO pulse and signal pulse are splitted by a polarizing beam splitter. A phase modulator randomly generates a ψ (0 or $\pi/2$) phase shift to measure either x or p. Then, the demultiplexed LO pulse and signal pulse interfere in a homodyne detector. The output intensity is proportional to the modulated quadratures.

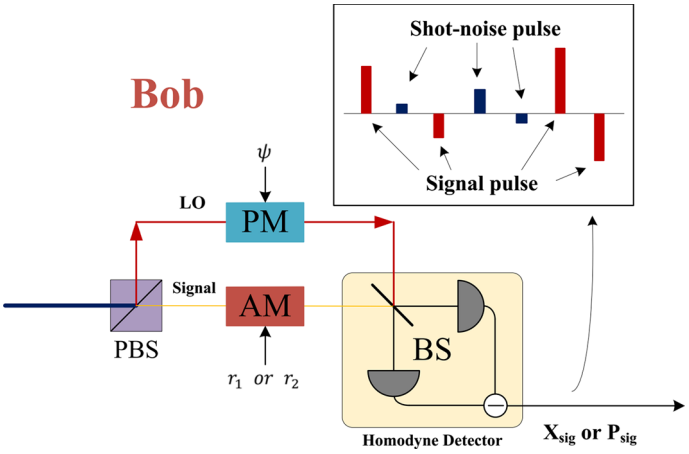

Fig. 1 The structure of Bob's apparatus in the RTSNM scheme. *PBS* polarizing beam splitter, *LO* local oscillator, *AM* amplitude modulator, r_1, r_2 extinction ratio, *PM* phase modulator, ψ phase shift 0 or $\pi/2$, *BS* beam splitter

Moreover, a data acquisition module is used to obtain the transmitted key information. Compared with the conventional CVQKD structure, the RTSNM scheme has a slight change at Bob's side: A second AM is inserted at Bob's signal path. Therefore, Bob can randomly choose from two extinction ratios (r_1 or r_2) of the AM to measure the signal pulse or the shot-noise pulse. Particularly, r_1 ($r_1 \approx 0\,\mathrm{dB}$) is chosen for quadrature signal measurement, while r_2 ($r_2 \approx \infty\,\mathrm{dB}$) is for shot-noise measurement.

This appended structure can protect CVQKD system against practical attacks. Firstly, in Ref. [19], author pointed out that the LO fluctuation opened a loophole for Eve and suggested receivers must monitor the LO fluctuation carefully. However, this monitoring countermeasure had been broken by the calibration attack, which modified the linear relationship between the variance of the homodyne detection measurements and the local oscillator power [20]. Fortunately, author proposed the real-time shot-noise measurement, which avoided the linear relationship and directly measured the shot noise. Besides, the wavelength attack referred in [22] exploited the loophole of the wavelength-dependent coupling ratio of the beam splitter. It was demonstrated that this attack could be defeated by applying three different extinction ratios of AM to check the transmittance linearity. Moreover, the saturation attack [23] could be defeated similarly by using more different extinction ratios [27]. On the other hand, real-time measurement continuously updates the real value of shot-noise variance, which ensures the system can run for longtime under the LO fluctuation and slight environmental change. The experiment result in [27] shows that it can work well incorporated with the practical CVQKD system. So far, due to the high efficiency of this scheme, it is a promising candidate to be integrated in CVQKD.

3 Practical performance: limited block size for RTSNM

After quantum signal transmission and detection, it is essential to perform the system calibration which determines the secret key rate. This procedure is called parameter estimation. After parameter estimation, Alice and Bob could know the maximal information leaked to Eve. As mentioned in [9], the finite-size effect will change the estimation procedure and lead to a lower key rate. Similarly, because the block size (times to choose r_2) for shot-noise measurement is also limited in the real-world scenario, the evaluation of shot noise is also suffered from the finite-size effect. Therefore, we explore the severity of this effect on the secret key rate and propose its mitigation scheme. We should note that Ref. [31] also emphasizes the accuracy of the shot noise, but our practical performance analysis concerns about the practical implementation of RTSNM, which focuses more on its application.

3.1 Parameter estimation pertaining to RTSNM

Due to the appended RTSNM, the parameter estimation procedure has some changes compared with the conventional one. After quantum transmission, Alice and Bob share two correlated vectors $P = \{(x_i, y_i)|i = 1, 2, \ldots, N\}$, where N is the total number of received data when the extinction ratio is r_1. Meanwhile, Bob also acquires a single vector $Q = \{(y_{0i})|i = 1, 2, \ldots, N'\}$, where N' is the total number when the ratio

is r_2. The involved quantum channel of CVQKD is a normal linear model with the following relations between Alice and Bob:

$$y = tx + z, \quad y_0 = z_0, \tag{1}$$

where $t = \sqrt{\eta T}$, z denotes the total noise term following a centered normal distribution with variance $\sigma^2 = \eta T \varepsilon N_0 + N_0 + V_{\mathrm{el}}$ and z_0 denotes the partial noise term following a centered normal distribution with variance $\sigma_0^2 = N_0 + V_{\mathrm{el}}$. The involved parameter η denotes the efficiency of the homodyne detectors, T denotes the transmittance of the quantum channel, N_0 is the variance of shot noise, ε is the excess noise in shot-noise units, and V_{el} is the detector's electronic noise. Therefore, x, y and y_0 satisfy the following relations:

$$\langle x^2 \rangle = V_{\mathrm{A}}, \langle xy \rangle = \sqrt{\eta T} V_{\mathrm{A}}, \tag{2}$$

$$\langle y^2 \rangle = \eta T V_{\mathrm{A}} + \eta T \varepsilon N_0 + N_0 + V_{\mathrm{el}}, \tag{3}$$

$$\langle y_0^2 \rangle = N_0 + V_{\mathrm{el}}, \tag{4}$$

where V_{A} is the modulation variance. Here we should make clear that all the parameters, such as T, N_0 and V_{el}, are assumed constant in one block for simplicity. In order to evaluate these relative parameters, Alice and Bob randomly select m pairs of correlated data ($m < N$) from P vectors to perform the conventional parameter estimation; meanwhile, Bob also uses m' ($m' = N'$) individual data from Q vector to perform the shot-noise estimation procedure. The maximum-likelihood estimators $\hat{t}$, $\hat{\sigma}^2$ and ${\hat{\sigma_0}}^2$ are known for the normal linear model [31]:

$$\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2}, \tag{5}$$

$$\hat{\sigma}^2 = \frac{1}{m} \sum_{i=1}^{m} (y_i - \hat{t} x_i)^2, \quad {\hat{\sigma_0}}^2 = \frac{1}{m'} \sum_{i=1}^{m'} (y_{0i})^2, \tag{6}$$

where the parameter $\hat{t}$ and $\hat{\sigma}^2$ and ${\hat{\sigma_0}}^2$ are independent estimators with the following distribution:

$$\hat{t} \sim N\left(t, \frac{\sigma^2}{\sum_{i=1}^{m} x_i^2}\right), \tag{7}$$

$$\frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1), \quad \frac{m'{\hat{\sigma_0}}^2}{{\sigma_0}^2} \sim \chi^2(m'-1), \tag{8}$$

where t, ${\sigma}^2$ and ${\sigma_0}^2$ are the true values of the parameters. In the limit of large m and m' (e.g., $m, m' > 10^6$), the χ^2 distribution converges to a normal distribution. Therefore, the confidence intervals for these estimators are

$$t \in [\hat{t} - \Delta t, \hat{t} + \Delta t], \tag{9}$$

$$\sigma^2 \in [\hat{\sigma}^2 - \Delta\sigma^2, \hat{\sigma}^2 + \Delta\sigma^2], \tag{10}$$

$$\sigma_0{}^2 \in \left[\hat{\sigma_0}^2 - \Delta\sigma_0{}^2, \hat{\sigma_0}^2 + \Delta\sigma_0{}^2\right], \tag{11}$$

where $\Delta t = z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{\hat{\sigma}^2}{mV_{\mathrm{A}}}}$, $\Delta\sigma^2 = z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}$ and $\Delta\sigma_0{}^2 = z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{\sigma_0}^2\sqrt{2}}{\sqrt{m'}}$. ϵ_{PE} denotes the probability that the estimated parameter does not belong to the confidence region and $z_{\epsilon_{\mathrm{PE}}/2}$ is a coefficient satisfying $1 - \mathrm{erf}(z_{\epsilon_{\mathrm{PE}}/2}/\sqrt{2}) = \epsilon_{\mathrm{PE}}/2$, where $\mathrm{erf}(x)$ is the error function defined as

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\mathrm{d}t. \tag{12}$$

Using the previous estimators, the channel transmission T and excess noise ε could be estimated with the following relation:

$$T = \hat{t}^2/\eta, \tag{13}$$

$$\varepsilon = \frac{\hat{\sigma}^2 - \hat{\sigma_0}^2}{\hat{t}^2\left(\hat{\sigma_0}^2 - V_{\mathrm{el}}\right)}. \tag{14}$$

The detector's electronic noise V_{el} is assumed constant, which applies to the situation that V_{el} only has a slight variation in one block. However, since σ_0^2 is calibrated and estimated during the QKD process, the statistical noise cannot be ignored. At this point, it is worth considering the relationship between the information acquired by Eve S_{BE} and $\hat{\sigma_0}^2$. As is well known, S_{BE} will increase with the increase of ε. Besides, according to Eq. (14), it is clear that increasing $\hat{\sigma_0}^2$ will decrease ε. Therefore, one can derive

$$\frac{\partial S_{\mathrm{BE}}}{\partial\hat{\sigma_0}^2} < 0. \tag{15}$$

That is to say, the mutual information acquired by Eve is decreased with $\hat{\sigma_0}^2$. In order to ensure the security of RTSNM, one should consider the most pessimistic case that Eve's information may be underestimated. Therefore, we need to make sure the probability that the true value of σ_0^2 is overestimated by the estimator is less than ϵ_{PE}. On this basis, T_{min} and $\varepsilon_{\mathrm{max}}$ corresponding to the lower bound of T and the upper bound of ε, respectively, can be calculated:

$$T_{\mathrm{min}} = (\hat{t} - \Delta t)^2/\eta, \tag{16}$$

$$\varepsilon_{\mathrm{max}} = \frac{\left(\hat{\sigma}^2 + \Delta\sigma^2 - \left(\hat{\sigma_0}^2 - \Delta\sigma_0{}^2\right)\right)}{\hat{t}^2\left(\left(\hat{\sigma_0}^2 - \Delta\sigma_0{}^2\right) - V_{\mathrm{el}}\right)}. \tag{17}$$

In contrast, in the conventional parameter estimation, because of the ignorance of $\Delta\sigma_0{}^2$, $\varepsilon'_{\mathrm{max}}$ will be relatively small:

$$\varepsilon'_{\mathrm{max}} = \frac{\left(\hat{\sigma}^2 + \Delta\sigma^2 - \hat{\sigma_0}^2\right)}{\hat{t}^2\left(\hat{\sigma_0}^2 - V_{\mathrm{el}}\right)}. \tag{18}$$

Therefore, the added noise due to finite size for RTSNM $\Delta\varepsilon_{\mathrm{fs}}$ is

$$\begin{aligned}\Delta\varepsilon_{\mathrm{fs}} &= \varepsilon_{\max} - \varepsilon'_{\max} \\ &\approx \frac{\Delta{\sigma_0}^2}{\hat{t}^2({\hat{\sigma_0}}^2 - V_{\mathrm{el}})} \approx z_{\epsilon_{\mathrm{PE}}/2}\frac{\sqrt{2}}{\eta T\sqrt{m'}},\end{aligned} \tag{19}$$

where $V_{\mathrm{el}} \ll {\hat{\sigma}_0}^2$. As shown in Fig. 2a, it is obvious that the size of m' has a major impact on the added noise $\Delta\varepsilon_{\mathrm{fs}}$. We note that the added noise induced by the finite block size for RTSNM is similar to the conventional finite-size effect in CVQKD, which means larger block size for RTSNM will decrease the added noise. In order to guarantee secure key being generated, the excess noise has to be decreased to one or two orders of magnitude lower than shot noise. Therefore, we need not only a sufficient number of pairs of correlated data to mitigate the finite-size effect in conventional parameter estimation, but also a large block size for RTSNM to reduce the added noise.

Given the parameters $T_{\min}$ and $\varepsilon_{\max}$, Alice and Bob can calculate the information they shared. According to Ref. [9], the secret key rate K with n received pulses used for key establishment is expressed as

$$K = \frac{n}{N}\left[\beta I_{\mathrm{AB}} - S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}} - \Delta(n)\right], \tag{20}$$

where $n = N - m$, $\beta \in (0, 1)$ is the efficiency of reverse reconciliation. $S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}}$ represents the maximal value of the Holevo information compatible with the statistics except with

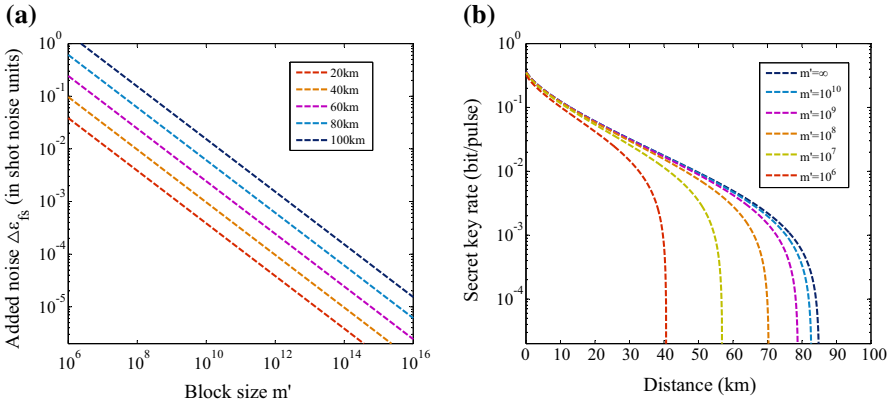

Fig. 2 **a** The added noise introduced by the finite block size m' for RTSNM. The security parameter ϵ_{PE} is 10^{-10}, and the quantum efficiency η is 0.6. From bottom to top, curves, respectively, correspond to the channel distances of 20, 40, 60, 80 and 100 km, where the loss rate of fiber is assumed as 0.2 dB/km. **b** Secret key rate in the finite block size for RTSNM. From left to right, curves correspond, respectively, to block size $m' = 10^6, 10^7, 10^8, 10^9, 10^{10}$ and infinite for RTSNM. Parameters are typically set as: the modulation variance $V_{\mathrm{A}} = 4$, the quantum efficiency $\eta = 0.6$, the electronic noise $v_{\mathrm{el}} = 0.01$, the excess noise $\varepsilon = 0.01$, the practical reconciliation efficiency $\beta = 95\%$, the security parameter $\epsilon_{\mathrm{PE}} = 10^{-10}$, the sampling length $N = 10^9$ and the block length for parameter estimation $m = 0.5 \times N$

probability ϵ_{PE} and I_{AB} represents the Shannon mutual information between Alice and Bob, which can be derived from Bob's measured variance V_Y and the conditional variance $V_{Y|X}$ as

$$I_{\mathrm{AB}} = \frac{1}{2}\log_2 \frac{V_Y}{V_{Y|X}} = \frac{1}{2}\log_2 \frac{V_Y}{\hat{\sigma}^2}, \tag{21}$$

while $S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}}$ is determined by the following covariance matrix between Alice and Bob:

$$\Gamma_{\mathrm{AB}} = \begin{bmatrix} (V_{\mathrm{A}}+1)\mathbb{I}_2 & \sqrt{T_{\min}\left(V_{\mathrm{A}}^2+2V_{\mathrm{A}}\right)}\sigma_z \\ \sqrt{T_{\min}\left(V_{\mathrm{A}}^2+2V_{\mathrm{A}}\right)}\sigma_z & [T_{\min}(V_{\mathrm{A}}+\varepsilon_{\max})+1]\mathbb{I}_2 \end{bmatrix}, \tag{22}$$

where the matrices $\mathbb{I}_2 = \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$, $\sigma_z = \left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]$. According to this covariance matrix, $S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}}$ can be calculated using

$$S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{23}$$

where $G(x) = (x+1)\log_2(x+1) - xlog_2x$, $\lambda_i \geq 1$ are symplectic eigenvalues derived from covariance matrices.

Besides, $\Delta(n)$ is a linear function of n and related to the security of the privacy amplification, which can be expressed as

$$\Delta(n) = 7\sqrt{\frac{\log_2(1/\overline{\epsilon})}{n}} + \frac{2}{n}\log_2\frac{1}{\epsilon_{\mathrm{PA}}}, \tag{24}$$

where $\overline{\epsilon}$ and ϵ_{PA}, which are virtual parameters and can be optimized in the computation, denote the smoothing parameter and the failure probability of the privacy amplification, respectively. For calculation, $\overline{\epsilon}$ and ϵ_{PA} are usually set to be equal to ϵ_{PE}. Based on Eqs. (21), (23) and (24), we use $T_{\min}$ and $\varepsilon_{\max}$ from Eqs. (16) and (17) to calculate the secret key rate. Figure 2b shows the security bound of CVQKD system with finite block size for RTSNM. The modulation variance V_{A} is optimized to 4. The rate is calculated under collective attacks with finite-size effect. We note that the security bound descends with the decrease in the block size m'. For example, even if we use enough block of size m for the conventional parameter estimation, no secret key could be extracted at 50 km with a shot-noise measurement on blocks of size 10^6. In other words, the parameter m' will sharply shorten the maximal transmission distance and lead to a lower curve of secret key rate.

In theory, this remarkable decrease in distance range is fundamentally caused by the added noise introduced by RTSNM. Therefore, according to Eq. (19), we need a large block size m' for RTSNM to decrease the value of the added noise. However, obtaining an infinite precision in shot-noise estimation as required in the theoretic case is impossible. Furthermore, since the value of shot noise is one or two order of magnitude larger than excess noise, the accuracy of estimation of the shot noise will significantly influence excess noise in CVQKD. In short, using this RTSNM

scheme, although the practical security and stability of the system are improved, we may sacrifice the transmission distance and the final key rate. Here one should note that the main idea of this section is not on the fluctuation of the parameter but on the influence of the estimation fluctuation. However, from a practical perspective, the real value of parameters is variable even in one block, which makes the analysis model more complicated. Therefore, we should clarify that our model is a simplified model and applies to the typical parameters with a slight variation.

3.2 Optimal block size for RTSNM

In order to mitigate this practical effect, we interest in the optimal block size for RTSNM, namely the optimal times to choose the extinction ratio r_2. Reference [32] studied the optimal ratio between the information carrier length and the estimation data length to maximize the secret key rate, which aimed at the conventional CVQKD. In RTSNM scenario, the length optimization will be more complicated. Based on the above analysis, it is clear that larger block size m' used to measure the shot noise will decrease the added noise and ultimately increase the final key rate. Besides, larger block size m used for the conventional parameter estimation will also result in less excess noise introduced by the finite-size effect. Therefore, due to the limited ensemble size in a communication, we need to make a trade-off between the block size m' to measure the shot noise and block size m for the conventional parameter estimation. In order to discuss both finite-size effects, we clarify the relationship between m, m' and $\varepsilon_{\max}$. Assuming $\hat{\sigma}^2 \approx \sigma^2$, $\hat{\sigma_0}^2 \approx {\sigma_0}^2$ and $\hat{t}^2 \approx \eta T$, Eq. (17) can be simplified as

$$\varepsilon_{\max} \approx \frac{\eta T\varepsilon + z_{\epsilon_{\mathrm{PE}}/2}\frac{\sqrt{2}}{\sqrt{m}}(\eta T\varepsilon + 1 + v_{\mathrm{el}}) + z_{\epsilon_{\mathrm{PE}}/2}\frac{\sqrt{2}}{\sqrt{m'}}(1 + v_{\mathrm{el}})}{\eta T}, \tag{25}$$

where the first term is the conventional excess noise ε, the second term is the added noise due to the finite size m and the third term is the added noise due to the finite size m'. According to this equality, the change of the excess noise $\varepsilon_{\max}$ in terms of the block size ratio m/m' can be analyzed. As shown in Fig. 3a, we note that when two block sizes close to equal, the excess noise $\varepsilon_{\max}$ decrease to the minimum. On the contrary, either smaller size for shot-noise measurement or smaller size for the conventional parameter estimation will similarly cause more excess noise. This appearance is fundamentally derived from the fact that the second term in Eq. (25) is quite close to the third term, since ε in the practical scenario is much less than 1. Therefore, these two terms due to the limited size are approximate under $m = m'$. This result is based on the most pessimistic case that both statistical biases are considered, which can guarantee the security in the estimation procedure.

In the practical scenario, the whole frame size of a communication is always finite. Therefore, reasonable arrangement of the whole frame will help us acquire the maximal secure key rate in a communication. The block size m for the conventional parameter estimation, the block size m' for shot-noise measurement and the block size n for key distillation are the three major components of the whole frame. Although the length cost for frame synchronization [33] and phase compensation [34] is essential, these

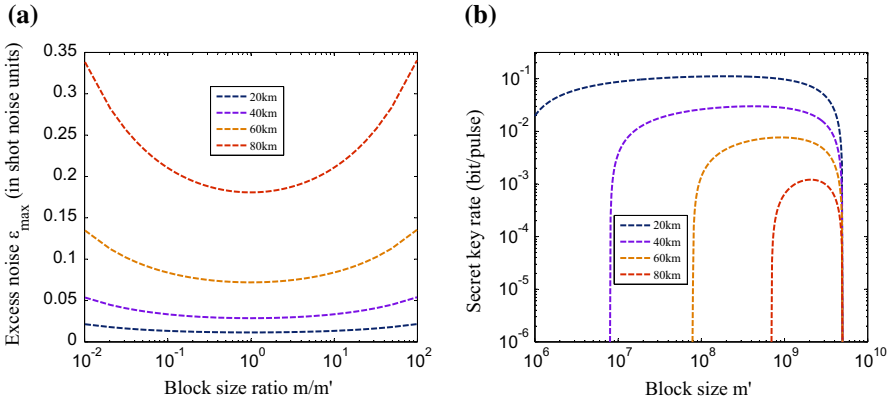

Fig. 3 **a** The excess noise $\varepsilon_{\max}$ as a function of the block size ratio m/m'. From bottom to top, curves correspond, respectively, to the channel distances 20, 30, 40, 50 km. The total block size for estimation parameter $m + m'$ is assumed as 10^9, the modulation variance V_A is 4, the excess noise $\varepsilon = 0.01$, the electronic noise $v_{el} = 0.01$, the security parameter ϵ_{PE} is 10^{-10}, and the quantum efficiency η is 0.6. **b** The secure key rate as a function of the block size m'. From the inside out, curves correspond to the channel distances 80, 60, 40, 20 km. The whole frame size is set as $N + N' = 10^{10}$, which is total amount of these three major components. The modulation variance V_A is 4, the electronic noise v_{el} is 0.01, the excess noise ε is 0.01, the security parameter ϵ_{PE} is 10^{-10}, and the quantum efficiency η is 0.6. With the increase in m, all the curves present earlier increase and later decrease trend

blocks can be ignored because they are not the same order of aforementioned three components. According to above analysis, excess noise will decrease to the minimum when m is close to m'. Thus, the secure key rate in a communication is investigated under the assumption that $m = m'$. Therefore, Eq. (20) is modified as

$$K = \frac{n}{n + m + m'} \left[\beta I_{AB} - S_{BE}^{\epsilon_{PE}} - \Delta(n) \right]. \tag{26}$$

As shown in Fig. 3b, because of the finite-size effect in CVQKD, the secret key rate rises with the increase in m' when it is relatively small. However, when it costs too large size to estimate parameter, the secret key rate will decrease due to the reduced size for key distillation. We also note that under the condition of long-distance distribution, larger block size for estimation is demanded to maximize the secure key rate in a communication.

Results in this section show the block size for RTSNM has a big impact on secure key rate, so the practical performance with the limited block size needs to be emphasized in the practical implementation. In order to mitigate this effect, we discuss the optimal block size for RTSNM. Simulation results show reasonable arrangement is essential for obtaining the maximal secret key rate. Meanwhile, arrangement of the whole frame is vital because of its relevance to practical application.

4 Practical performance: finite dynamics of amplitude modulator in RTSNM

Except for the practical performance with the limited block size, it is noteworthy that in the practical scenario, the actual device in RTSNM also has imperfect performance. Although the device is equipped in Bob and cannot be controlled by Eve, this practical effect will deteriorate the system performance. For example, the AM in Fig. 1 has finite dynamics, which is different with the ideal model. In other words, the extinction ratio of AM can neither reach 0 dB nor increase to ∞ dB. Therefore, in the real-world conditions, the effect of finite dynamics should be considered. And because the minimal extinction ratio r_1 and maximal extinction ratio r_2 have different impact on the secure key rate, we analysis them separately.

4.1 The effect of the minimal extinction ratio

The minimal extinction ratio r_1 cannot be ignored in the practical implementation. The commercial amplitude modulator of Thorlabs has a typical r_1 value with 3–5 dB [35]. Because this component is equipped in the signal path, the minimal extinction ratio will fully contribute to the quantum efficiency of Bob's side; thus, one can modify the quantum efficiency formula as

$$\eta_{\mathrm{Bob}} = \eta_{\mathrm{Det}}\eta_{\mathrm{AM}}, \tag{27}$$

where η_{Det} denotes the quantum efficiency of detector and $\eta_{\mathrm{AM}} = 10^{\frac{-r_1}{10}}$ denotes the contribution of r_1, which deteriorates the quantum efficiency. In Fig. 4, we separately use different minimal extinction ratio r_1 to simulate the key rate. Result shows that r_1 has a big effect on the key rate. In order to relieve this practical effect, we need to choose the AM with relatively small r_1 so that the transmission distance increases.

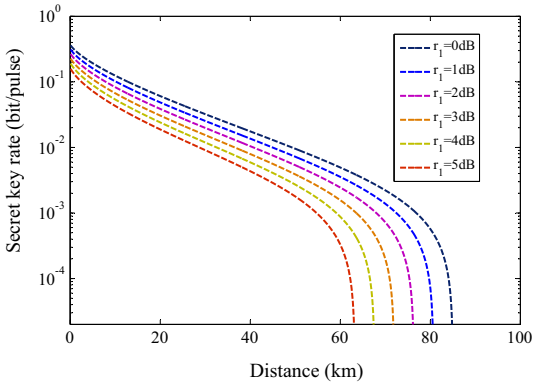

Fig. 4 The effect of the minimal extinction ratio. Parameters are set as: the modulation variance $V_{\mathrm{A}} = 4$, the quantum efficiency of detector $\eta = 0.6$, the electronic noise $v_{\mathrm{el}} = 0.01$, the excess noise $\varepsilon = 0.01$, the practical reconciliation efficiency $\beta = 95\%$, the security parameter $\epsilon_{\mathrm{PE}} = 10^{-10}$, the sampling length $N = 10^9$ and the block length for parameters estimation $m = 0.5 \times N$. From top to bottom, curves correspond to the minimal extinction ratio $r_1 = 0$–6 dB

4.2 The effect of the maximal extinction ratio

Here we discuss the effect of the r_2, namely the maximal extinction ratio. Because the r_2 cannot reach to ∞ dB, a fraction of signal and excess noise will go through the AM. Therefore, we cannot estimate the shot-noise value straightly. However, in Ref. [22], a modified parameter estimation method is proposed: based on Eqs. (3) and (4), two extinction ratio parameters r_1 and r_2 are introduced. Therefore, the variances of y and y_0 are expressed as

$$\left\langle y^2 \right\rangle \equiv V_{s1} = 10^{\frac{-r_1}{10}} \eta T (v_{\mathrm{A}} + \varepsilon) N_0 + N_0 + V_{\mathrm{el}}, \tag{28}$$

$$\left\langle {y_0}^2 \right\rangle \equiv V_{s2} = 10^{\frac{-r_2}{10}} \eta T (v_{\mathrm{A}} + \varepsilon) N_0 + N_0 + V_{\mathrm{el}}, \tag{29}$$

where $v_{\mathrm{A}} = V_{\mathrm{A}}/N_0$. Utilizing the difference between these two equations, the shot noise $\hat{N}_0$ and the excess noise $\hat{\varepsilon}$ could be estimated with the following relation:

$$\hat{N}_0 = \frac{10^{\frac{-r_1}{10}} V_{s2} - 10^{\frac{-r_2}{10}} V_{s1}}{10^{\frac{-r_1}{10}} - 10^{\frac{-r_2}{10}}} - V_{\mathrm{el}}, \tag{30}$$

$$\hat{\varepsilon} = \left[\frac{V_{s1} - V_{s2}}{\left(10^{\frac{-r_1}{10}} - 10^{\frac{-r_2}{10}}\right) \eta T} - V_{\mathrm{A}} \hat{N}_0 \right] \Big/ \hat{N}_0. \tag{31}$$

Certainly, the finite-size effect has to be considered. When m, m' is large enough ($m, m' > 10^6$), y and y_0 distribution converges to a normal distribution:

$$y^2 \sim N\left(V_{s1}, \frac{2V_{s1}^2}{m}\right), \tag{32}$$

$$y_0^2 \sim N\left(V_{s2}, \frac{2V_{s2}^2}{m'}\right). \tag{33}$$

For simplicity, we assume $m = m'$. According to Eq. (31), the distribution of $\hat{\varepsilon}$ is

$$\hat{\varepsilon} \sim N\left(\varepsilon, \frac{2V_{s1}^2 + 2V_{s2}^2}{m\eta^2 T^2 N_0^2 \left(10^{\frac{-r_1}{10}} - 10^{\frac{-r_2}{10}}\right)^2}\right). \tag{34}$$

In the real-world scenario, $r_1 \ll r_2$ and $r_2 \approx \infty$ dB are assumed to simplify Eq. (34) as

$$\hat{\varepsilon} \sim N\left(\varepsilon, \frac{2\left((\eta T V_{\mathrm{A}} + 1)^2 + 1\right)}{m\eta^2 T^2 \left(10^{\frac{-r_1}{10}} - 10^{\frac{-r_2}{10}}\right)^2}\right). \tag{35}$$

Considering the pessimistic situation, the maximal excess noise $\varepsilon_{\max}$ is counted; thus, the added noise introduced by finite dynamics $\Delta\varepsilon_{\mathrm{fd}}$ is

$$\Delta\varepsilon_{\mathrm{fd}} = z_{\epsilon_{\mathrm{PE}}/2}\frac{\sqrt{2\left((\eta T V_{\mathrm{A}}+1)^2+1\right)}}{\sqrt{m}\eta T\left(10^{\frac{-r_1}{10}}-10^{\frac{-r_2}{10}}\right)}, \tag{36}$$

where $z_{\epsilon_{\mathrm{PE}}/2}$ is also the confidence coefficient. The following reasons can account for the difference between this added noise and Eq. (11): Firstly, due to the finite dynamics of AM, the estimation procedure is modified, which takes the finite dynamics (r_1, r_2) into consideration. Besides, because we utilize the difference of the signal y and the signal y_0 to estimate parameters, the fluctuation of the signal y will decrease the accuracy of the parameter estimation. The added noise will increase with the modulation variance V_{A}. Therefore, this estimation method has the larger deviation compared with conventional one. The added noise as a function of the extinction ratio r_2 is shown in Fig. 5a. Because this added noise is relevant to the modulation variance, different V_{A} is adopted to compare. One can note that the added noise $\triangle\varepsilon_{\mathrm{fd}}$ decreases with r_2. However, the decrement induced by the growth of r_2 is small when $r_2 > 20$ dB. Not surprisingly, the modulation variance in this estimation scheme has significant influence on the added noise $\triangle\varepsilon_{\mathrm{fd}}$. As we mentioned above, larger modulation variance may induce a relatively larger statistical noise, which may deteriorate the final excess noise. We should note that the extinction ratio parameters are calibrated in a secure laboratory; therefore, the estimation errors can be made arbitrarily small.

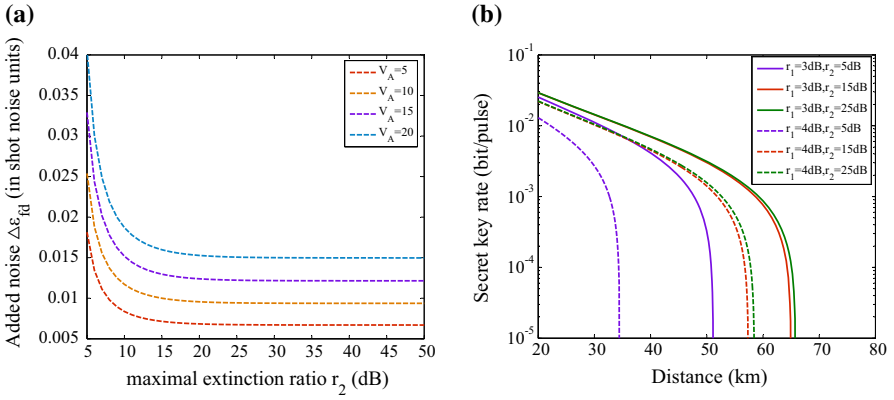

Fig. 5 **a** The added noise due to the finite r_2. Parameters are set as: the extinction ratio $r_1 = 3$ dB, the security parameter $\epsilon_{\mathrm{PE}} = 10^{-10}$, the block size for parameter estimation $m = 10^9$, the channel distance 25 km, the quantum efficiency $\eta = 0.6$. From bottom to top, curves correspond to the modulation variance $V_{\mathrm{A}} = 5, 10, 15, 20$. **b** The key rate with different dynamics. The group of solid lines represents the key rate with $r_1 = 3$ dB, while the group of dash lines corresponds to $r_1 = 4$ dB. Parameters are set as: the modulation variance $V_{\mathrm{A}} = 4$, the quantum efficiency $\eta = 0.6$, the electronic noise $v_{\mathrm{el}} = 0.01$, the excess noise $\varepsilon = 0.01$, the practical reconciliation efficiency $\beta = 95\%$, the security parameter $\epsilon_{\mathrm{PE}} = 10^{-10}$, the block size $m = m' = 10^9$

According to Eq. (20), the final key rate with finite dynamics of AM is shown in Fig. 5b. Both r_1 and r_2 are varied to show the influence of different dynamics. The lines with the same color represent the key rate with different r_1, indicating that smaller r_1 will increase the distance as we discussed in Sect. 4.1. The group of solid lines as well as the group of dash lines corresponds to the key rate with different r_2. One can find that the key rate will increase with the parameter r_2. Not surprisingly, the security bound ascends slightly with $r_2 > 20\,\mathrm{dB}$, which conforms to Fig. 5a. That is to say, the maximal extinction ratio just needs to be greater than 20 dB and higher extinction ratio has a little influence on the transmission distance and final key rate. Therefore, in the practical system $r_2 \approx 20\,\mathrm{dB}$ is enough. More importantly, the minimal extinction ratio r_1, which fully contributes to the quantum efficiency, has a big impact on the performance of the system. Therefore, choosing a AM with low r_1 is a better choice for RTSNM.

5 Conclusion

In summary, we have investigated the practical performance of RTSNM and mitigated its effects. Although RTSNM is used to improve the practical security of CVQKD, this monitoring procedure is also a major component of the whole CVQKD system. Therefore, the practical performance of itself should be considered. In particular, we find that the parameter estimation pertaining to the RTSNM scheme is changed and finite block size for RTSNM causes the added noise. And this imperfection reduces the bound of secure key rate and shortens the transmission distance. To relieve such effect, we indicate that when the block size to measure the shot noise is close to the block size for the conventional parameter estimation, the total excess noise reaches the minimum. On this basis, the optimal arrangement of the whole frame is investigated and we finally obtain the maximal secure key rate in one block. Moreover, the practical performance with finite AM dynamics is also studied. Results show that the minimal extinction ratio of AM fully contributes to the quantum efficiency, while the maximal extinction ratio slightly influences the secure key rate when it is greater than 20 dB. Therefore, AM with high dynamics will improve the performance of RTSNM. To conclude, in the practical implementation of RTSNM, its practical performance needs to be considered and optimized so that the final secret key rate could be trustworthy and improved.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grants Nos. 61332019, 61671287, 61631014) and the National Key Research and Development Program (Grant No. 2016YFA0302600).

References

1. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: Gaussian quantum information. Rev. Mod. Phys. **84**(2), 621 (2012)
2. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**(5), 057902 (2002)

3. Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N.J., Grangier, P.: Quantum key distribution using Gaussian-modulated coherent states. Nature **421**(6920), 238–241 (2003)
4. Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N.J., Tuallebrouri, R., McLaughlin, S.W., Grangier, P.: Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys. Rev. A **76**(4), 042305 (2007)
5. Qi, B., Huang, L.L., Qian, L., Lo, H.K.: Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. Phys. Rev. A **76**(5), 052323 (2007)
6. García-Patrón, R., Cerf, N.J.: Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys. Rev. Lett. **97**(19), 190503 (2006)
7. Navascués, M., Grosshans, F., Acín, A.: Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys. Rev. Lett. **97**(19), 190502 (2006)
8. Renner, R., Cirac, J.I.: de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys. Rev. Lett. **102**(11), 110504 (2009)
9. Leverrier, A., Grosshans, F., Grangier, P.: Finite-size analysis of a continuous-variable quantum key distribution. Phys. Rev. A **81**(6), 062343 (2010)
10. Furrer, F., Franz, T., Berta, M., Leverrier, A., Scholz, V.B., Tomamichel, M., Werner, R.F.: Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. Phys. Rev. Lett. **109**(10), 100502 (2012)
11. Leverrier, A.: Composable security proof for continuous-variable quantum key distribution with coherent states. Phys. Rev. Lett. **114**(7), 070501 (2015)
12. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., Diamanti, E.: Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat. Photon. **7**(5), 378–381 (2013)
13. Huang, D., Huang, P., Lin, D., Zeng, G.: Long-distance continuous-variable quantum key distribution by controlling excess noise. Sci. Rep. **6**, 19201 (2016)
14. Wang, C., Huang, D., Huang, P., Lin, D., Peng, J., Zeng, G.: 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel. Sci. Rep. **5**, 14607 (2015)
15. Huang, D., Lin, D., Wang, C., Liu, W., Fang, S., Peng, J., Zeng, G.: Continuous-variable quantum key distribution with 1 Mbps secure key rate. Opt. Express **23**(13), 17511–17519 (2015)
16. Fossier, S., Diamanti, E., Debuisschert, T., Villing, A., Tualle-Brouri, R., Grangier, P.: Field test of a continuous-variable quantum key distribution prototype. New J. Phys. **11**(4), 045023 (2009)
17. Jouguet, P., Kunz-Jacques, S., Debuisschert, T., Fossier, S., Diamanti, E., Alléaume, R., Tualle-Brouri, R., Grangier, P., Leverrier, A., Pache, P., Painchault, P.: Field test of classical symmetric encryption with continuous variables quantum key distribution. Opt. Express **20**(13), 14030–14041 (2012)
18. Huang, D., Huang, P., Li, H., Wang, T., Zhou, Y., Zeng, G.: Field demonstration of a continuous-variable quantum key distribution network. Opt. Lett. **41**(15), 3511–3514 (2016)
19. Ma, X.C., Sun, S.H., Jiang, M.S., Liang, L.M.: Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. Phys. Rev. A **88**(2), 022339 (2013)
20. Jouguet, P., Kunz-Jacques, S., Diamanti, E.: Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys. Rev. A **87**(6), 062313 (2013)
21. Huang, J.Z., Weedbrook, C., Yin, Z.Q., Wang, S., Li, H.W., Chen, W., Guo, G.C., Han, Z.F.: Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. Phys. Rev. A **87**(6), 062329 (2013)
22. Huang, J.Z., Kunz-Jacques, S., Jouguet, P., Weedbrook, C., Yin, Z.Q., Wang, S., Chen, W., Guo, G.C., Han, Z.F.: Quantum hacking on quantum key distribution using homodyne detection. Phys. Rev. A **89**(3), 032304 (2014)
23. Qin, H., Kumar, R., Alléaume, R.: Quantum hacking: saturation attack on practical continuous-variable quantum key distribution. Phys. Rev. A **94**(1), 012325 (2016)
24. Wang, S., Chen, W., Guo, J.F., Yin, Z.Q., Li, H.W., Zhou, Z., Guo, G.C., Han, Z.F.: 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. Opt. Lett. **37**(6), 1008–1010 (2012)
25. Wang, S., Chen, W., Yin, Z.Q., et al.: Field and long-term demonstration of a wide area quantum key distribution network. Opt. Express **22**(18), 21739–21756 (2014)
26. Wang, S., Yin, Z.Q., Chen, W., et al.: Experimental demonstration of a quantum key distribution without signal disturbance monitoring. Nat. Photon. **9**(12), 832–836 (2015)
27. Kunz-Jacques, S., Jouguet, P.: Robust shot-noise measurement for continuous-variable quantum key distribution. Phys. Rev. A **91**(2), 022307 (2015)
28. Huang, D., Huang, P., Lin, D., Wang, C., Zeng, G.: High-speed continuous-variable quantum key distribution without sending a local oscillator. Opt. Lett. **40**(16), 3695–3698 (2015)

29. Qi, B., Lougovski, P., Pooser, R., Grice, W., Bobrek, M.: Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. Phys. Rev. X **5**(4), 041009 (2015)
30. Soh, D.B.S., Brif, C., Coles, P.J., Lütkenhaus, N., Camacho, R.M., Urayama, J., Sarovar, M.: Self-referenced continuous-variable quantum key distribution protocol. Phys. Rev. X **5**(4), 041010 (2015)
31. Jouguet, P., Kunz-Jacques, S., Diamanti, E., Leverrier, A.: Analysis of imperfections in practical continuous-variable quantum key distribution. Phys. Rev. A **86**(3), 032309 (2012)
32. Ruppert, L., Usenko, V.C., Filip, R.: Long-distance continuous-variable quantum key distribution with efficient channel estimation. Phys. Rev. A **90**(6), 062310 (2014)
33. Lin, D., Huang, P., Huang, D., Wang, C., Peng, J., Zeng, G.: High performance frame synchronization for continuous variable quantum key distribution systems. Opt. Express **23**(17), 22190–22198 (2015)
34. Huang, P., Lin, D.K., Huang, D., Zeng, G.H.: Security of continuous-variable quantum key distribution with imperfect phase compensation Int. J. Theor. Phys. **54**(8), 2613–2622 (2015)
35. www.thorlabs.com