CHIN. PHYS. LETT. Vol. 38, No. 4 (2021) 040301

Continuous-Variable Measurement-Device-Independent Quantum Key Distribution with One-Time Shot-Noise Unit Calibration

Luyu Huang(黄露雨), Yichen Zhang(张一辰)*, and Song Yu(喻松)

State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

(Received 22 October 2020; accepted 2 February 2021; published online 6 April 2021)

Imperfections in practical detectors, including limited detection efficiency, and inherent electronic noise, can seriously decrease the transmission distance of continuous-variable measurement-device-independent quantum key distribution systems. Owing to the difficulties inherent in realizing a high-efficiency fiber homodyne detector, challenges still exist in continuous-variable measurement-device-independent quantum key distribution system implementation. We offer an alternative approach in an attempt to solve these difficulties and improve the potential for system implementation. Here, a novel practical detector modeling method is utilized, which is combined with a one-time shot-noise-unit calibration method for the purpose of system realization. The new modeling method benefits greatly from taking advantage of one-time shot-noise-unit calibration methods, such as measuring electronic noise and shot noise directly to a novel shot-noise unit, so as to eliminate the statistical fluctuations found in previous methods; this makes the implementation of such systems simpler, and the calibration progress more accurate. We provide a simulation of the secret key rate versus distance with different parameters. In addition, the minimal detection efficiency required at each distance, as well as the contrast between the two methods, are also shown, so as to provide a reference in terms of system realization.

DOI: 10.1088/0256-307X/38/4/040301

As a realistic application in the quantum information field, quantum key distribution (QKD)[1,2] allows us to establish a secure key between two legitimate parties, called Alice and Bob, with information-theoretical security based on the principles of quantum mechanics. In the past few decades, developments in QKD have facilitated expansion from the discrete-variable domain to the continuous-variable (CV)[3–5] domain. Owing to its ease of integration[6] and the fact that only traditional telecommunication equipment is required, great progress has been made in the field of CV-QKD, both theoretically[7–15] and experimentally.[16–23] The experimental transmission distances have been extended to 202 km using laboratory fiber links,[17] and to 50 km using commercial fibers.[19] Moreover, quantum networks have also become a fertile area of research in recent years.[24]

Although CV-QKD is theoretically secure, the security of practical systems is still worth considering, due to the gap between theoretical assumptions and practical implementation. On the one hand, a practical device may contain loopholes, allowing an eavesdropper to take advantage of the resulting information leakage, and thereby undermining the security of the entire system.[25–27] To resolve this issue, many semi-device-independent CV-QKD protocols have been proposed to close such loopholes, including the source-device-independent protocol[28,29] and the measurement-device-independent (MDI) protocol.[30,31] Owing to its ability to withstand attacks against the detectors on the receiver side, studies related to CV-MDI QKD protocols have proliferated in recent years, including in areas such as system performance improvement with post-selection,[32] photon subtraction,[33,34] and simplification via unidimensional modulated coherent states.[35,36]

Defects in practical detectors, including limited detection efficiency and inherent electronic noise, seriously decrease the transmission distance of the CV-MDI QKD system. Owing to difficulties in realizing a high-efficiency fiber homodyne detector, challenges still exist in CV-MDI QKD system implementation. At present, compensation for the defects in practical detectors is based on studies modeling the flaws of the practical components, where a beamsplitter and an Einstein–Podolsky–Rosen (EPR) state are used to model the limited detection efficiency and inherent electronic noise, respectively. Correspondingly, two-time calibration (TTC) procedure is applied for shot-noise-unit (SNU) calibration, whereby the electronic noise of a practical detector is measured first, and the output of the detector, with the local oscillator path included, is measured subsequently. The difference between the second measurement results and the first measurement results is regarded as the SNU.

Supported by the National Natural Science Foundation of China (Grant Nos. 61531003 and 62001044), and the Fundamental Research Funds for the Central Universities of China.

*Corresponding author. Email: zhangyc@bupt.edu.cn

© 2021 Chinese Physical Society and IOP Publishing Ltd

Since the SNU is not measured directly, the method not only introduces inaccuracies, but also opens loopholes and leaks information to Eve. To resolve this issue, another method, known as the one-time shot-noise-unit calibration (OTC) method[37] has been reported, in combination with a proposed new modeling method, whereby two beamsplitters are used to model the detection efficiency and electronic noise. The method can utilize the OTC, rather than the TTC strategy, in which SNU is measured directly, rendering the SNU calibration more accurate, and the experimental implementation simpler. Therefore, although the conventional modeling method has been studied in depth,[38,39] the new approach offers powerful advantages in terms of experimental implementation.

In this work, we therefore utilize the new modeling method, corresponding to the OTC method, to model the imperfections of practical detectors, in place of the conventional modeling method, with the aim of helping to resolve these difficulties and enhance potential system implementations. The new practical CV-MDI QKD scheme proposed in this Letter not only takes advantage of the OTC scheme, but also performs as well as the conventional method. The rest of the letter is organized as follows: Firstly, we review the entanglement-based (EB) scheme of CV-MDI QKD. Next, we examine the schemes of the two modeling methods, for which we derive the relationship of the quadratures and covariance matrices. We then calculate the secret key rate, and show the numerical simulation results, based on various simulation parameters. In addition, the minimal detection efficiency required at each distance and the contrast between the two modeling method are reported, so as to provide a reference in terms of system realization. Finally, we provide an analysis and summary of our work.

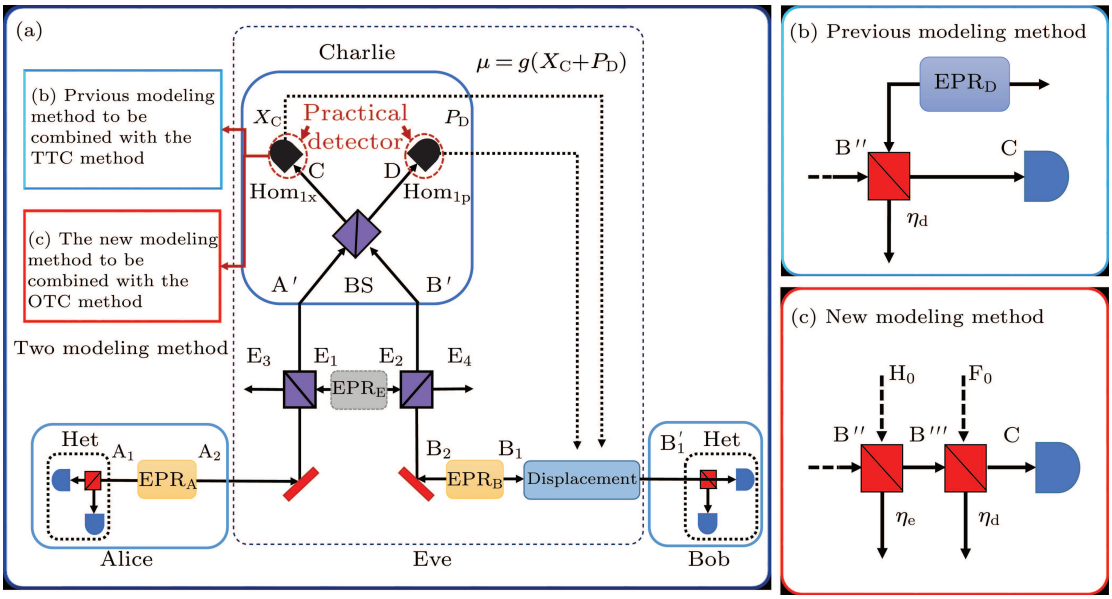

Fig. 1. (a) The entanglement-based (EB) scheme of the practical CV-MDI QKD system. Alice and Bob are both sender, and the receiver is the untrusted party, Charlie. In particular, the eavesdropper Eve can perform attacks with an EPR state $\Phi_{E_1E_2}$ and two beamsplitters to reflect with the transmitted states in the channels. The modes at the output ports of the two beamsplitters collected by Eve are E_3 and E_4. After receiving the modes transmitting through the channels, Charlie performs Bell-state measurement and the measurement results are announced to the public subsequently. Next, Bob modifies his data with a displacement D_μ according to the results while Alice keeps her data unchanged. (b) The conventional modeling method that is combined with TTC method, where a beamsplitter and an Einstein–Podolsky–Rosen (EPR) state are used to model the limited detection efficiency and inherent electronic noise respectively. (c) The new modeling method corresponding to the OTC method, where two beamsplitters are used for modeling the detection efficiency and electronic noise. Modes H_0 and F_0 both represent vacuum states.

For ease of calculation, the EB scheme is used for our theoretical security analysis, while its prepare-and-measurement (PM) scheme equivalent is used for the experimental implementation. It is worth noting that our work offers great advantages in terms of the PM scheme, but the security analysis is still based on the EB scheme. We begin by reviewing the EB scheme of CV-MDI QKD protocol, as shown in Fig. 1(a). Firstly, Alice and Bob independently generate EPR states, $|\Phi_{A_1A_2}\rangle$, and $|\Phi_{B_1B_2}\rangle$, with the same variance, $V_A = V_B$. Next, Alice and Bob keep the mode A_1 and the mode B_1 and perform heterodyne detection on them for each side, while sending the other two modes to the untrusted party, Charlie, through two different channels, whose lengths are L_{AC}, and L_{BC}, respectively. Having received the modes, Charlie performs a Bell-state measurement. The measurement results are regarded as $\{X_C, P_D\}$, and are subsequently

announced to the public. Bob then modifies his data via a displacement, D_μ, of gain g, based on the results, while Alice keeps her data unchanged. Finally, the two legitimate parties perform classical post-processing as usual.

In the realistic CV-MDI QKD system, defects in practical detectors decrease their performance. As such, modeling the practical detector is a requirement for any theoretical analysis. The conventional method has been studied in detail in Refs. [38,39], where a beamsplitter and an EPR state are used to model the two imperfections, as illustrated in Fig. 1(b). Supposing that the efficiency of the beamsplitter is $\eta_{\rm d}$, the variance of the $\rm EPR_D$ state becomes $v = 1 + v_{\rm el}/(1-\eta_{\rm d})$, where $v_{\rm el}$ denotes the variance in the electronic noise. When considering the worst case scenario, whereby Charlie is absolutely controlled by Eve, the scheme is equal to the one-way CV-QKD protocol with coherent states and heterodyne detection.[31] The 'transmission efficiency' of the 'equivalent channel' is $T = \frac{g^2}{2}\eta_{\rm d}\eta_{\rm A}$, where g is the gain of displacement, and $\eta_{\rm A}$ is the transmission efficiency of the channel between Alice and Charlie. When $g = \sqrt{2/(\eta_{\rm B}\eta_{\rm d})}\sqrt{(V_{\rm B}-1)/(V_{\rm B}+1)}$, the equivalent excess noise has the minimum value

$$\varepsilon' = \varepsilon_{\rm A} + \frac{1}{\eta_{\rm A}}[\eta_{\rm B}(\varepsilon_{\rm B}-2) + 2 + 2\chi_{\rm C}], \tag{1}$$

where $\chi_{\rm C} = (1-\eta_{\rm d})/\eta_{\rm d} + v_{\rm el}/\eta_{\rm d}$.

However, the conventional modeling method is combined with TTC strategy, where the electronic noise of a practical detector is measured first, and the output of the detector, with the local oscillator path included, is measured subsequently, and the difference between the second measurement results and the first measurement results is regarded as the SNU. Since SNU is measured indirectly, the method introduces inaccuracies into the experimental results. To counter this, we use a new modeling method, corresponding to the OTC scheme, as shown in Fig. 1(c), to model the flaws, in which two beamsplitters, with efficiencies $\eta_{\rm e}$ and $\eta_{\rm d}$, are used to model the electronic noise and the limited detection efficiency, respectively. The method can be combined with the OTC strategy, where SNU is measured directly, thereby not only simplifying the experimental implementation but also closing any loopholes that may occur during the calibration progress. In the following, we investigate the detailed relationship of the quadratures, and the calculation of the secret key rate. Firstly, Alice and Bob independently generate $\rm EPR_A$ and $\rm EPR_B$ states, $|\Phi_{\rm A_1A_2}\rangle$ and $|\Phi_{\rm B_1B_2}\rangle$, with the same variance, $V_{\rm A} = V_{\rm B} = V$. Next, Alice and Bob keep mode A_1 and mode B_1, while sending the other two modes, A_2 and B_2, to the untrusted party, Charlie, through two different channels. Having received the two modes, Charlie then mixes them into a 50 : 50 beamsplitter, and performs a Bell-state measurement on the two outputs, using two practical detectors, modeled via the OTC scheme. The relationship of the quadratures can be written as

$$\begin{aligned}
\hat{A}' &= \sqrt{\eta_{\rm A}}\hat{A}_2 + \sqrt{1-\eta_{\rm A}}\hat{E}_1,\\
\hat{B}' &= \sqrt{\eta_{\rm B}}\hat{B}_2 + \sqrt{1-\eta_{\rm B}}\hat{E}_2,\\
\hat{A}'' &= \frac{1}{\sqrt{2}}(\hat{A}' - \hat{B}'),\\
\hat{B}'' &= \frac{1}{\sqrt{2}}(\hat{A}' + \hat{B}'),\\
\hat{A}''' &= \sqrt{\eta_{\rm e}}\hat{A}'' + \sqrt{1-\eta_{\rm e}}\hat{H}_0,\\
\hat{B}''' &= \sqrt{\eta_{\rm e}}\hat{B}'' + \sqrt{1-\eta_{\rm e}}\hat{H}_0',\\
\hat{C} &= \sqrt{\eta_{\rm d}}\hat{A}''' + \sqrt{1-\eta_{\rm d}}\hat{F}_0,\\
\hat{D} &= \sqrt{\eta_{\rm d}}\hat{B}''' + \sqrt{1-\eta_{\rm d}}\hat{F}_0',\\
\hat{B}'_{1x} &= \hat{B}_{1x} + g\hat{C}_x,\\
\hat{B}'_{1p} &= \hat{B}_{1p} + g\hat{D}_p,
\end{aligned} \tag{2}$$

where $\eta_{\rm A} = 10^{-\alpha L_{\rm AC}/10}$, $\eta_{\rm B} = 10^{-\alpha L_{\rm BC}/10}$, and $\alpha = 0.2\,{\rm dB/km}$ is the loss of the fiber. Note that the modes above are all presented in Fig. 1, except $\hat{A}''$, $\hat{A}'''$, $\hat{H}_0'$, and $\hat{F}_0'$, which are symmetric to the modes through the channel between Bob and Charlie shown in Fig. 1(c). Here, we can obtain the covariance matrix $\gamma_{\rm A_1B_1'}$ of the tripartite quantum state $\rho_{\rm A_1B_1'}$ as

$$\begin{aligned}
\gamma_{\rm A_1B_1'} &= \begin{pmatrix} V_{\rm A}\mathbb{I} & \sqrt{T'(V_{\rm A}^2-1)}\sigma_z \\ \sqrt{T'(V_{\rm A}^2-1)}\sigma_z & [T'(V_{\rm A}-1)+1+T'\varepsilon'']\mathbb{I} \end{pmatrix}\\
&= \begin{pmatrix} \gamma_{\rm A_1} & \sigma_{\rm A_1B_1'}^{\rm T} \\ \sigma_{\rm A_1B_1'} & \gamma_{\rm B_1'} \end{pmatrix},
\end{aligned} \tag{3}$$

where $T' = g^2/2\eta_{\rm e}\eta_{\rm d}\eta_{\rm A}$, and $\varepsilon'' = \chi_{\rm A} + 1 - 2(\eta_{\rm e}\eta_{\rm d}-1)/(\eta_{\rm e}\eta_{\rm d}\eta_{\rm A}) + \eta_{\rm B}(V_{\rm B}+\chi_{\rm B})/\eta_{\rm A} + 2[V_{\rm B} - 1 - g\sqrt{2\eta_{\rm d}\eta_{\rm e}\eta_{\rm B}(V_{\rm B}^2-1)}]/(g^2\eta_{\rm d}\eta_{\rm e}\eta_{\rm A})$. Here $\chi_{\rm A} = 1/\eta_{\rm A} - 1 + \varepsilon_{\rm A}$, and $\chi_{\rm B} = 1/\eta_{\rm B} - 1 + \varepsilon_{\rm B}$. When $g = \sqrt{2/(\eta_{\rm B}\eta_{\rm d}\eta_{\rm e})}\sqrt{(V_{\rm B}-1)/(V_{\rm B}+1)}$, the minimum value of ε'' is attained, which is

$$\begin{aligned}
\varepsilon'' &= \chi_{\rm A} + 1 - \frac{2(\eta_{\rm e}\eta_{\rm d}-1)}{\eta_{\rm e}\eta_{\rm d}\eta_{\rm A}} + \frac{\eta_{\rm B}}{\eta_{\rm A}}(V_{\rm B}+\chi_{\rm B})\\
&\quad + \frac{2[V_{\rm B} - 1 - g\sqrt{2\eta_{\rm d}\eta_{\rm e}\eta_{\rm B}(V_{\rm B}^2-1)}]}{g^2\eta_{\rm d}\eta_{\rm e}\eta_{\rm A}}\\
&= \frac{1}{\eta_{\rm A}} + \varepsilon_{\rm A} - \frac{2(\eta_{\rm e}\eta_{\rm d}-1)}{\eta_{\rm e}\eta_{\rm d}\eta_{\rm A}} + \frac{\eta_{\rm B}}{\eta_{\rm A}}\left(V_{\rm B} + \frac{1}{\eta_{\rm B}} - 1 + \varepsilon_{\rm B}\right)\\
&\quad + \frac{[V_{\rm B} - 1 - \sqrt{\frac{2}{\eta_{\rm B}\eta_{\rm d}\eta_{\rm e}}}\sqrt{\frac{V_{\rm B}-1}{V_{\rm B}+1}}\sqrt{2\eta_{\rm d}\eta_{\rm e}\eta_{\rm B}(V_{\rm B}^2-1)}]}{\frac{\eta_{\rm A}\eta_{\rm e}\eta_{\rm d}}{\eta_{\rm B}\eta_{\rm e}\eta_{\rm d}}}\\
&= -\frac{1}{\eta_{\rm A}} + \varepsilon_{\rm A} + \frac{2}{\eta_{\rm e}\eta_{\rm d}\eta_{\rm A}} + \frac{\eta_{\rm B}}{\eta_{\rm A}}\left(V_{\rm B} + \frac{1}{\eta_{\rm B}} - 1 + \varepsilon_{\rm B}\right)\\
&\quad + \frac{V_{\rm B} - 1 - 2(V_{\rm B}-1)}{\frac{\eta_{\rm A}(V_{\rm B}-1)}{\eta_{\rm B}(V_{\rm B}+1)}}\\
&= \varepsilon_{\rm A} + \frac{1}{\eta_{\rm A}}\left[\eta_{\rm B}(\varepsilon_{\rm B}-2) + \frac{2}{\eta_{\rm d}\eta_{\rm e}}\right].
\end{aligned} \tag{4}$$

Note that when $\eta_{\rm d} = \eta_{\rm e} = 1$, the value of ε'' is equal to that of the ideal CV-MDI QKD protocol, i.e., the condition in which two beamsplitters are not set to the system. Furthermore, we set $\eta_{\rm e} = 1/(1+v_{\rm el})$[28] to facilitate the PM scheme and the EB scheme equivalence, and compare the results of Eqs. (1) and (4). Interestingly, these are proved to be absolutely equal if the optimal g is selected for the equivalent excess noise minimum. This demonstrates that the CV-MDI QKD system with the new modeling method corresponding to the OTC scheme, as discussed in this study, simplifies the calibration procedure of the protocol, and renders the calibration results more accurate in terms of practical implementation, without detriment to the system performance as a whole. As such, it offers great potential for future experimental implementation.

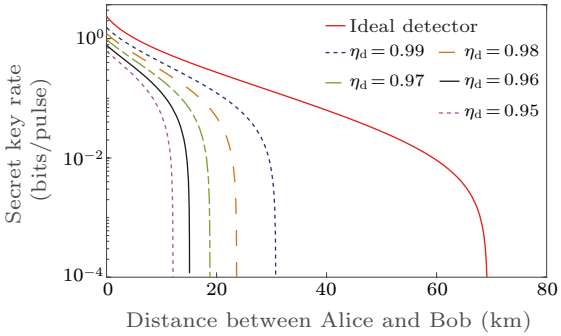

Fig. 2. Secret key rate versus distance between Alice and Bob, for different detection efficiencies $\eta_{\rm d}$. In particular, we set $L_{\rm BC} = 0$ for maximal performance. Here $\eta_{\rm d} = 1$, and $v_{\rm el} = 0$ represent the ideal detector case, and $v_{\rm el} = 0.005$ denotes other cases.

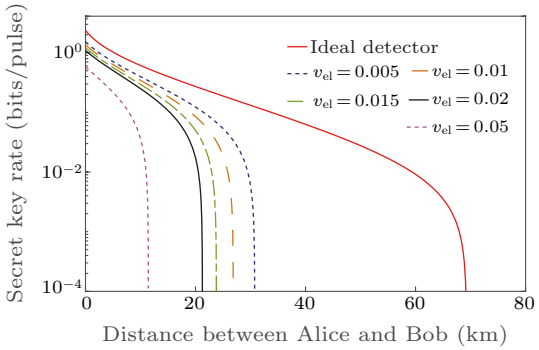

Fig. 3. Secret key rate versus distance between Alice and Bob with different electronic noise, $v_{\rm el}$. Here, we set $L_{\rm BC} = 0$ for maximal performance; $\eta_{\rm d} = 1$, and $v_{\rm el} = 0$ represent the ideal detector case, and $\eta_{\rm d} = 0.99$ denotes other cases.

Now, the secret key rate with reverse reconciliation can be calculated from the covariance matrix $\gamma_{\rm A_1B_1'}$, which can be given by

$$R = \beta I_{\rm AB} - \chi_{\rm BE}, \tag{5}$$

where $I_{\rm AB}$ denotes the mutual Shannon entropy between Alice and Bob, $\chi_{\rm BE}$ is the von Neumann entropy between Bob and Eve, and β represents the efficiency of the reverse reconciliation.[40] The former can be calculated by $I_{\rm AB} = 1/2(\log_2 V_{\rm A} - \log_2 V_{\rm A|B})$, while the latter can be calculated by

$$\chi_{\rm BE} = \sum_{i=1}^{2} G\Big(\frac{\lambda_i - 1}{2}\Big) - G\Big(\frac{\lambda_3 - 1}{2}\Big), \tag{6}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, and $\lambda_{1,2}$ are the symplectic eigenvalues of $\gamma_{\rm A_1B_1'}$, and λ_3 is the symplectic eigenvalue of $\gamma_{\rm A_1|B_1'}$, which can be calculated from

$$\gamma_{\rm A_1|B_1'} = \gamma_{\rm A_1} - \sigma^{\rm T}_{\rm A_1B_1'}(\gamma_{\rm B_1'} + \mathbb{I})^{-1}\sigma_{\rm A_1B_1'}. \tag{7}$$

We began by providing a simulation and discussion of the secret key rate, and the effect of system defects. For our numerical simulation, we assume the variance $V_{\rm A} = V_{\rm B} = 40$, the excess noise of the channels are $\varepsilon_{\rm A} = \varepsilon_{\rm B} = 0.002$, and the reconciliation efficiency is $\beta = 0.98$.[19] As illustrated by Eq. (4), both the electronic noise and the detection efficiency can greatly influence the equivalent excess noise ε'', which has directly relevance to protocol performance. The effects of the two parameters are considered separately, and the ideal detector case is also concluded. Specifically, we fix $v_{\rm el} = 0.005$ to reveal the changes in system performance with different $\eta_{\rm d}$, as shown in Fig. 2, $\eta_{\rm d} = 0.99$ to illustrate changes in system performance with different $v_{\rm el}$, as shown in Fig. 3. In particular, $\eta_{\rm d} = 1$ and $v_{\rm el} = 0$ are set for the ideal detector case, and $L_{\rm BC} = 0$ is used for all simulations. Firstly, as shown in Fig. 2, the performance of the protocol deteriorates sharply when the detection efficiency decreases. Although Charlie is set on Bob's side, which is proven to achieve the optimal performance, the transmission distance drops below 20 km when the detection efficiency decreases to 0.97. Given that $\eta_{\rm d}$ is on the denominator, with an increase in distance, the smaller the $\eta_{\rm d}$ is, the faster the excess noise, ε'', increases. In other words, $\eta_{\rm d}$ has a great influence on the farthest transmission distance. As shown in Fig. 2, a decrease of 0.01 will cause a significant change in the transmission distance. This is part of reason why the difference between the ideal detector and the detector with an efficiency of 0.99 is so obvious. In practice, the difference is influenced not only by $\eta_{\rm d}$, but also by the electronic noise, $v_{\rm el}$. Specifically, the ideal case corresponds to $\eta_{\rm d} = 1$ and $v_{\rm el} = 0$, which represents a perfect detector, and the $v_{\rm el}$ is fixed to be 0.005 for other cases with different $\eta_{\rm d}$. Thus, due to the increase in the numerator, $v_{\rm el}$, the denominator $\eta_{\rm d}$ decreases, and the difference between the case of $\eta_{\rm d} = 0.99$ and the ideal case is obvious. We then choose $\eta_{\rm d} = 0.99$ for the simulation, in order to examine the effects of electronic noise on performance, as shown in Fig. 3. As we can see, changes in the level of electronic noise will also have a serious impact on system performance. Even though a small value, $v_{\rm el} = 0.005$, is used in our simulation, there is still a severe performance degradation. It is evident

that imperfections in practical detectors do make a difference in realistic CV-MDI QKD systems, and as such, it is highly relevant to model these in any theoretical analysis. In addition, as we can see from the evidence in Figs. 2 and 3, these effects, i.e., that $v_{\rm el}$ is 10 times greater than the original value, and $\eta_{\rm d}$ is reduced by 0.04 in terms of system performance, are similar. Comparatively speaking, the change in $v_{\rm el}$ has less effect with respect to performance degradation than the value of $\eta_{\rm d}$. It is therefore a matter of some urgency to eliminate the bad influence of detection efficiency reduction on system performance; this constitutes the essence of our work here, which may help to resolve these difficulties, and improve practical system implementation. Finally, the simulation of minimal detection efficiency, $\eta_{\rm d}$, at each distance is given in Fig. 4, which highlights the requirement for detection efficiency in practical detectors under conditions in which $v_{\rm el} = 0.01$, 0.02, 0.05, respectively in our experiment.

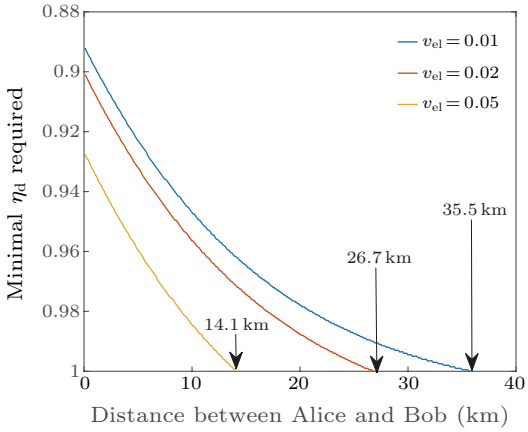

Fig. 4. The minimal $\eta_{\rm d}$ required for experimental implementation with different electronic noise. Here $\eta_{\rm d}$ reaches 1 at 14.1 km for $v_{\rm el} = 0.01$, 26.7 km for $v_{\rm el} = 0.02$, 35.5 km for $v_{\rm el} = 0.05$, respectively.

Table 1. Main parameters and contrast of CV-MDI QKD system with conventional method and OTC method.

	TTC method	OTC method
Transmission efficiency	Equal $\left(\frac{\eta_{\rm A}(V_{\rm B}-1)}{\eta_{\rm B}(V_{\rm B}+1)}\right)$	
Equivalent excess noise	Equal $\left(\varepsilon'' = \varepsilon_{\rm A} + \frac{1}{\eta_{\rm A}}\left[\eta_{\rm B}(\varepsilon_{\rm B} - 2) + 2\frac{1+v_{\rm el}}{\eta_{\rm d}}\right]\right)$	
Displacement gain	$\sqrt{\frac{2}{\eta_{\rm B}\eta_{\rm d}}}\sqrt{\frac{V_{\rm B}-1}{V_{\rm B}+1}}$	$\sqrt{\frac{2}{\eta_{\rm B}\eta_{\rm d}\eta_e}}\sqrt{\frac{V_{\rm B}-1}{V_{\rm B}+1}}$
Characteristic and comparison	1. Unable to monitor shot-noise directly 2. Existing big fluctuation in statistics	1. Monitor shot-noise in real-time 2. Reducing statistical volatility 3. Performing as well as the previous method*.

*NB: The outputs with the two methods are not equal in a one-way CV-QKD system, which differs from the CV-MDI QKD system discussed in this Letter.

To conclude, defects in practical detectors have a deleterious effect on CV-MDI QKD protocol performance. As such, it is important to model them for the purpose of future optimization and compensation projects. In this study, we have utilized a new modeling method in combination with the OTC method, replacing the previous modeling method for the CV-MDI QKD protocol, and the core parameters of the two methods are demonstrated to be identical in terms of the relationship of the quadratures. In other words, using the new method will not make the system worse, in contrast to the results for the one-way CV-QKD system. Moreover, the new method has the great advantage that the SNU is measured directly, thereby reducing statistical volatility, and rendering the results more accurate. By eliminating the adverse effects of this statistical volatility, the new modeling method is of greater benefit with respect to experimental implementation. Note that in the CV-MDI QKD protocol, all of the security loopholes caused by detection errors are closed. As such, there is no difference in terms of security between the two modeling methods, or the two corresponding calibration methods in the CV-MDI QKD system. Evidence for the contrast between the modeling method corresponding to the OTC method, and the modeling method corresponding to the TTC method, is given in Table 1. We also detail the minimal detection efficiency required for each distance, which acts as a reference point for future experiments. Therefore, our work lays the foundation for future research into compensation, performance improvement, and experimental implementation, based on the OTC method in CV-MDI QKD system.

References

[1] Pirandola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J, Razavi M, Shaari J S, Tomamichel M, Usenko V C, Vallone G, Villoresi P and Wallden P 2020 *Adv. Opt. Photon.* **12** 1012
[2] Xu F, Ma X, Zhang Q, Lo H K and Pan J 2020 *Rev. Mod. Phys.* **92** 025002
[3] Weedbrook C, Pirandola S, Garcia-Patron R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[4] Diamanti E and Leverrier A 2015 *Entropy* **17** 6072
[5] Li Y, Wang X, Bai Z, Liu W, Yang S and Peng K 2017 *Chin. Phys. B* **26** 040303
[6] Zhang G, Haw J Y, Cai H, Xu F, Assad S M, Fitzsimons J

F, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek L C and Liu A Q 2019 *Nat. Photon.* **13** 839
[7] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[8] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[9] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
[10] Leverrier A and Grangier P 2015 *Phys. Rev. Lett.* **114** 070501
[11] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501
[12] Li Z, Zhang Y and Guo H 2018 arXiv:1805.04249 [quant-ph]
[13] Ghorai S, Grangier P, Diamanti E and Leverrier A 2019 *Phys. Rev. X* **9** 021059
[14] Lin J, Upadhyaya T, Lutkenhaus N 2019 *Phys. Rev. X* **9** 041064
[15] Ottaviani C, Woolley M J, Erementchouk M, Federici J F, Mazumder P, Pirandola S and Weedbrook C 2020 *IEEE J. Sel. Areas Commun.* **38** 483
[16] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photon.* **7** 378
[17] Zhang Y, Li Z, Chen Z, Weedbrook C, Zhao Y, Wang X, Huang Y, Xu C, Zhang X, Wang Z, Li M, Zhang X, Zheng Z, Chu B, Gao X, Meng N, Cai W, Wang Z, Wang G, Yu S and Guo H 2019 *Quantum Sci. Technol.* **4** 065006
[18] Aguado A, Lopez V, Lopez D, Peev M, Poppe A, Pastor A, Folgueira J and Martin V 2019 *IEEE Commun. Mag.* **57** 20
[19] Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S and Guo H 2020 *Phys. Rev. Lett.* **125** 010502
[20] Eriksson T A, Luis R S, Puttnam B J, Rademacher G, Fujiwara M, Awaji Y, Furukawa H, Wada N, Takeoka M and Sasaki M 2020 *J. Lightwave Technol.* **38** 2214
[21] Qi B, Gunther H, Evans P G, Williams B P, Camacho R M and Peters N A 2020 *Phys. Rev. Appl.* **13** 054065
[22] Wang H, Pi I, Huang W, Li Y, Shao Y, Yang J, Liu J, Zhang C, Zhang Y and Xu B 2020 *Opt. Express* **28** 32882
[23] Su X, Wang W, Wang Y, Jia X, Xie C and Peng K 2009 *Europhys. Lett.* **87** 20005
[24] Su X, Wang M, Yan Z, Jia X, Xie C and Peng K 2020 *Sci. Chin. Inf. Sci.* **63** 180503
[25] Ma X, Sun S, Jiang M and Liang L 2013 *Phys. Rev. A* **87** 52309
[26] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev. A* **87** 062313
[27] Zhao Y, Zhang Y, Huang Y, Xu B, Yu S and Guo H 2018 *J. Phys. B* **52** 015501
[28] Weedbrook C 2013 *Phys. Rev. A* **87** 022308
[29] Zhang Y, Chen Z, Weedbrook C, Yu S and Guo H 2020 *Sci. Rep.* **10** 6673
[30] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 *Nat. Photon.* **9** 397
[31] Li Z, Zhang Y, Xu F, Peng X and Guo H 2014 *Phys. Rev. A* **89** 052301
[32] Wilkinson K N, Papanastasiou P, Ottaviani C, Gehring T and Pirandola S 2020 *Phys. Rev. Res.* **2** 033424
[33] Zhao Y, Zhang Y, Xu B, Yu S and Guo H 2018 *Phys. Rev. A* **97** 042328
[34] Ma H, Huang P, Bai D, Wang S, Bao W and Zeng G 2018 *Phys. Rev. A* **97** 042329
[35] Huang L, Zhang Y, Chen Z and Yu S 2019 *Entropy* **21** 1100
[36] Bai D, Huang P, Zhu Y, Ma H, Xiao T, Wang T and Zeng G 2020 *Quantum Inf. Process.* **19** 53
[37] Zhang Y, Huang Y, Chen Z, Li Z, Yu S and Guo H 2020 *Phys. Rev. Appl.* **13** 024058
[38] Lodewyck J, Bloch M, Garcia-Patron R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W and Grangier P 2007 *Phys. Rev. A* **76** 042305
[39] Usenko V C and Filip R 2016 *Entropy* **18** 20
[40] Zhou C, Wang X Y, Zhang Y C, Zhang Z G, Yu S and Guo H 2019 *Phys. Rev. Appl.* **12** 054013