Frontiers of Physics
https://doi.org/10.1007/s11467-020-0954-8
Front. Phys.
15(3), 31601 (2020)

RESEARCH ARTICLE

Simultaneous measurement-device-independent continuous variable quantum key distribution with realistic detector compensation

Xiao-Dong Wu[1], Yi-Jun Wang[1], Duan Huang[2,†], Ying Guo[1,‡]

[1] *School of Automation, Central South University, Changsha 410083, China*
[2] *School of Computer Science and Engineering, Central South University, Changsha 410083, China*
Corresponding author. E-mail: [†] duan.huang@foxmail.com, [‡] yingguo@csu.edu.cn

Received October 7, 2019; accepted January 8, 2020

We propose a novel scheme for measurement-device-independent (MDI) continuous-variable quantum key distribution (CVQKD) by simultaneously conducting classical communication and QKD, which is called "simultaneous MDI-CVQKD" protocol. In such protocol, each sender (Alice, Bob) can superimpose random numbers for QKD on classical information by taking advantage of the same weak coherent pulse and an untrusted third party (Charlie) decodes it by using the same coherent detectors, which could be appealing in practice due to that multiple purposes can be realized by employing only single communication system. What is more, the proposed protocol is MDI, which is immune to all possible side-channel attacks on practical detectors. Security results illustrate that the simultaneous MDI-CVQKD protocol can secure against arbitrary collective attacks. In addition, we employ phase-sensitive optical amplifiers to compensate the imperfection existing in practical detectors. With this technology, even common practical detectors can be used for detection through choosing a suitable optical amplifier gain. Furthermore, we also take the finite-size effect into consideration and show that the whole raw keys can be taken advantage of to generate the final secret key instead of sacrificing part of them for parameter estimation. Therefore, an enhanced performance of the simultaneous MDI-CVQKD protocol can be obtained in finite-size regime.

Keywords measurement-device-independent, continuous-variable quantum key distribution, simultaneous, realistic detector compensation

1 Introduction

Quantum key distribution (QKD), which utilizes quantum physics to enable the generation of secret keys between two remote users (Alice and Bob) by employing untrusted quantum and classical channels [1–7]. Two main categories of QKD protocols have been analyzed: discrete-variable (DV) QKD protocols [8–12] and continuous-variable (CV) QKD protocols [13–16]. Unlike the DVQKD which in view of single photon detection, the CVQKD employs the quadrature components of the optical field to transmit the signals which constitute the shared randomness [17–24]. The receiver, Bob, measures the quadratures by utilizing high-speed and high-efficiency coherent detection (i.e., homodyne or heterodyne detection) techniques [13].

The Gaussian-modulated coherent state (GMCS) protocol is the one well-known CVQKD scheme mainly because of its theoretical security [21, 25–30] and its practicality [31–34]. However, the security analysis of GMCS protocol is usually based on the ideal assumption that the devices are perfect and cannot be eavesdropped, which is difficult to realize in the experimental implementation [35–37]. From a practical point of view, the security loopholes caused by the imperfect devices can possibly be exploited by eavesdroppers to adopt quantum attack strategies, such as calibration attacks [38], local oscillator (LO) fluctuation attack [39], wavelength attacks [37, 40], the homodyne-detector-blinding attack [41] and the saturation attack [42]. These attacks aimed to practical devices have a serious effect on the practical security of the CVQKD system.

To effectively eliminate all the existing and potential attacks focused on practical detectors, measurement-device independent (MDI) QKD protocols were proposed, which guarantees to be secure against all possible detection attacks [43, 44]. Soon afterwards, the MDI-QKD was well-analyzed not only in theory [45–49] but also demonstrated successfully in experiments [50–52]. At present, MDI-DVQKD [44, 53, 54] and MDI-CVQKD [55–57] are two main practical implementation ways for MDI-QKD. In the framework of MDI-CVQKD, Alice and Bob are deemed as senders. While, an untrusted third party, Charlie, is introduced to perform Bell-state measurement (BSM) when he receives the quantum states sent by Alice and Bob. Such measurement results can be taken advantage of by

© Higher Education Press and Springer-Verlag GmbH Germany, part of Springer Nature 2020

Alice and Bob for secure keys generation in the postprocessing. The MDI-CVQKD can remove all the known and unknown side-channel attacks due to that the untrusted third party Charlie is in charge of performing measurement, there is no correlation between the security of the protocol and the detectors.

Up to now, most of the MDI-CVQKD protocols are based on Gaussian modulation, namely, the senders Alice and Bob employ amplitude and phase modulators to encode the information on coherent states, respectively. It is interesting that the infrastructure needed for CVQKD implementation is amazingly similar to that for classical coherent optical communication. Recently, the one-way simultaneous classical communication and quantum (SCCQ) protocol [58] and its improvement schemes [59–61] were proposed in view of this similarity, where the quantum information for CVQKD combined with bits for classical communication are encoded on the same coherent state. This is an attractive scheme in practice due to that only one set of transceivers can be employed to realize multiple purposes, which effectively reduces the cost of CVQKD itself.

In this paper, we develop the MDI-CVQKD protocol by simultaneously conducting classical communication and QKD, which is called "simultaneous MDI-CVQKD" protocol. In our scheme, each sender can superimpose random numbers for QKD on classical information by taking advantage of the same weak coherent pulse. At Charlie's side, the same coherent receiver is used to decode this pulse. The motivation of our scheme is to realize the secret key distribution based on the background of classical communication at a minimal cost in MDI framework. Such arrangement has the following advantages: on the one hand, a single communication infrastructure (MDI) can be taken advantage of for both classical communication and QKD, and it waives the necessity of reservation of a separate channel for QKD, which can effectively reduce the cost of the implementation of quantum key distribution; on the other hand, the proposed scheme is MDI, thus it can be immune to all possible side-channel attacks on practical detectors. What is more, the imperfections of the practical detectors owned by Charlie have significant impact on the performance of the proposed protocol. To overcome the limitation, we insert two optical phase-sensitive amplifiers at the output ports of the quantum channel to make compensation for the practical detectors. In addition, the security bounds of the simultaneous MDI-CVQKD protocol are derived to against Gaussian collective attacks. Furthermore, the finite-size effect is taken into consideration. We show the whole raw keys can be utilized to generate the final secret key instead of sacrificing part of them for parameter estimation. Consequently, the performance improvement of the simultaneous MDI-CVQKD protocol can be achieved in finite-size regime.

This paper is structured as follows. In Section 2, we first introduce the original MDI-CVQKD protocol, then present the details of the simultaneous MDI-CVQKD protocol. In Section 3, we show numeric simulation and performance analysis based on the asymptotic limit. A way taken advantage of for compensating the imperfection of the realistic detectors is introduced in Section 4. In Section 5, we perform the security analysis of the simultaneous MDI-CVQKD protocol with numerical simulation in finite-size regime. Finally, conclusion and discussions are drawn in Section 6.

2 Simultaneous MDI-CVQKD protocol

In this section, we first review the original MDI-CVQKD scheme. After that, we extend it to simultaneous MDI-CVQKD protocol. Note that the entanglement-based (EB) MDI-CVQKD protocol can be regarded as equivalent one-way model of the EB scheme where Bob performs heterodyne detection. That is to say both the X quadrature and the P quadrature can be simultaneously measured by Bob. Consequently, in this paper, we adopt the quadrature phase-shift keying (QPSK) scheme for classical communication and GMCS protocol for QKD protocol.

2.1 Description of MDI-CVQKD protocol

As shown in Figs. 1(a) and (b), Alice and Bob utilize lasers to generate light sources, then they randomly prepare a coherent state at each side by employing Gaussian modulation scheme. After that, Alice and Bob send their coherent states to Charlie. When Charlie receives the transmitted coherent states, he combines them and then detects the coherent states by performing Bell state measurement (BSM). Since Charlie announces the measurement results publicly, the corrected data can be utilized for parameter estimation by Alice and Bob. Finally, by using an authenticated public channel, Alice and Bob obtain the identical secret key through finishing the information reconciliation and privacy amplification.

In practice, the prepare-and-measurement (PM) version is usually applied due to its easiness and simplicity. However, in order to simplify the security analysis, the equivalent EB scheme is usually adopted. As shown in Fig. 1, Alice and Bob generate Einstein–Podolsky–Rosen (EPR) state [62] respectively. In each side, one mode A_1 (B_1) is kept and the other mode A_2 (B_2) is sent to Charlie through the untrusted quantum channel. After Charlie receiving the incoming modes A_3 and B_3, he performs BSM-based detection to measure two output modes A_4 and B_4, namely, measure the x-quadrature of A_4 and p-quadrature of B_4. Then Charlie announces the measurement result $\theta = (x_C + \mathrm{i}p_C)/2$. According to this measurement result, Bob uses operation $D(\theta)$ to displace his own mode B_1 and thus achieves mode B_0. Finally, Alice and Bob can obtain the raw data by performing heterodyne detection to measure modes A_1 and B_0.

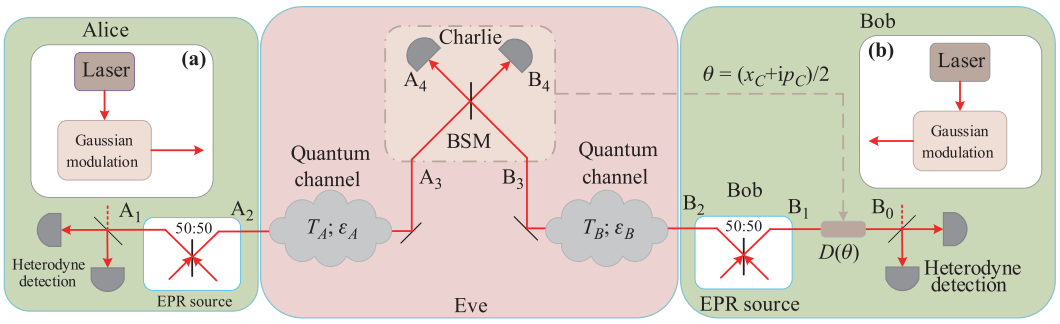


Fig. 1 Entanglement-based (EB) model of the traditional MDI-CVQKD protocol. The two-mode squeezed states (EPR) are generated respectively by Alice and Bob and sent to Charlie who performs BSM-based detection. T_A (T_B) represents the transmittance of the quantum channel for Alice to Charlie (Bob to Charlie), ε_A (ε_B) represents the channel excess noise for Alice to Charlie (Bob to Charlie), $D(\theta)$ represents displacement operation. **(a)** The equivalent prepare-and-measurement (PM) scheme at Alice's side. **(b)** The equivalent PM scheme at Bob's side.

2.2 The simultaneous MDI-CVQKD protocol

In QPSK modulation scheme, two classical bits, denoted as s and t, are encoded into the X quadrature and the P quadrature of a coherent state, which is expressed as

$$|\phi\rangle = |(\mathrm{e}^{-\mathrm{i}s\pi} + \mathrm{i}\mathrm{e}^{-\mathrm{i}t\pi})\alpha\rangle, \tag{1}$$

where α stands for a real number. While, in GMCS QKD protocol, a coherent state $|x + \mathrm{i}p\rangle$ is prepared randomly, where x and p represent Gaussian random numbers with zero mean and a variance of VN_0. Note that $N_0 = 0.25$ stands for the shot-noise variance and V represents the modulation variance. As shown in Fig. 2, we depict the implementation of simultaneous MDI-CVQKD protocol, which can be described as follows.

Step 1: At Alice's side (at Bob's side), classical bits $\{s_A, t_A\}$ ($\{s_B, t_B\}$) and Gaussian random numbers $\{x'_A, p'_A\}$ ($\{x'_B, p'_B\}$) are encoded on a coherent state $|(x'_A+\mathrm{e}^{-\mathrm{i}s_A\pi}\alpha)+\mathrm{i}(p'_A+\mathrm{e}^{-\mathrm{i}t_A\pi}\alpha)\rangle$ ($|(x'_B+\mathrm{e}^{-\mathrm{i}s_B\pi}\alpha)+\mathrm{i}(p'_B+\mathrm{e}^{-\mathrm{i}t_B\pi}\alpha)\rangle$). After that, Alice and Bob transmit their coherent states to Charlie through untrusted quantum channel.

Step 2: When Charlie receives the transmitted coherent states, he performs BSM-based detection to obtain the measurement results $\{x_R, p_R\}$ and determines the classical bits $\{s_R, t_R\}$ according to the signs of his measurement results. Namely, the bit value of s_R (t_R) is set to be 0 if x_R (p_R)>0. Otherwise, the bit value is set to be 1. Then Charlie processes his measurement results, which are given by

$$\begin{aligned} x_C &= \sqrt{\frac{2}{T\eta}}x_R + (2s_R - 1)\alpha, \\ p_C &= \sqrt{\frac{2}{T\eta}}p_R + (2t_R - 1)\alpha, \end{aligned} \tag{2}$$

where T represents the normalized parameter which is related with channel transmittance (its expression is shown in Section 3), η represents the Charlie's detector efficiency, and since Charlie performs conjugate homodyne detection, the factor is $\sqrt{2}$. Then he publicly announces the measurement result, which is denoted as variable C with complex value $\theta = (x_C + \mathrm{i}p_C)/2$.

Step 3: When Alice and Bob receive Charlie's measurement results, Bob's data is modified to $x_B = x'_B - k_{x'_B}(\theta)$ and $p_B = p'_B - k_{p'_B}(\theta)$. While Alice's data is kept unchanged, namely, $x_A = x'_A$ and $p_A = p'_A$. Here k stands for the amplification coefficient related to channel loss. Here we use variables X and Y to describe the local raw data owned by Alice and Bob, respectively. Namely, $X = (x_A, p_A)$ and $Y = (x_B, p_B)$.

Step 4: Alice and Bob perform parameter estimation from a randomly chosen sample of data X and Y by utilizing an authenticated public channel. Then they finish the information reconciliation and privacy amplification to achieve the identical secret key as in the case of traditional MDI-CVQKD protocol.

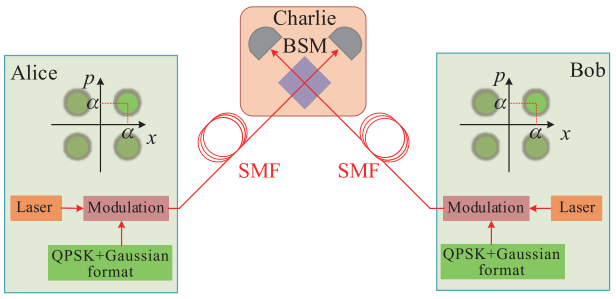


Fig. 2 Implementation of the simultaneous MDI-CVQKD protocol with phase-space representations of simultaneous QPSK and Gaussian modulation. SMF: Single mode fiber.

3 Asymptotic security of simultaneous MDI-CVQKD protocol

In this section, the security of simultaneous MDI-CVQKD protocol is analyzed by considering asymptotic case. To simplify the security analysis, we focus on the EB scheme

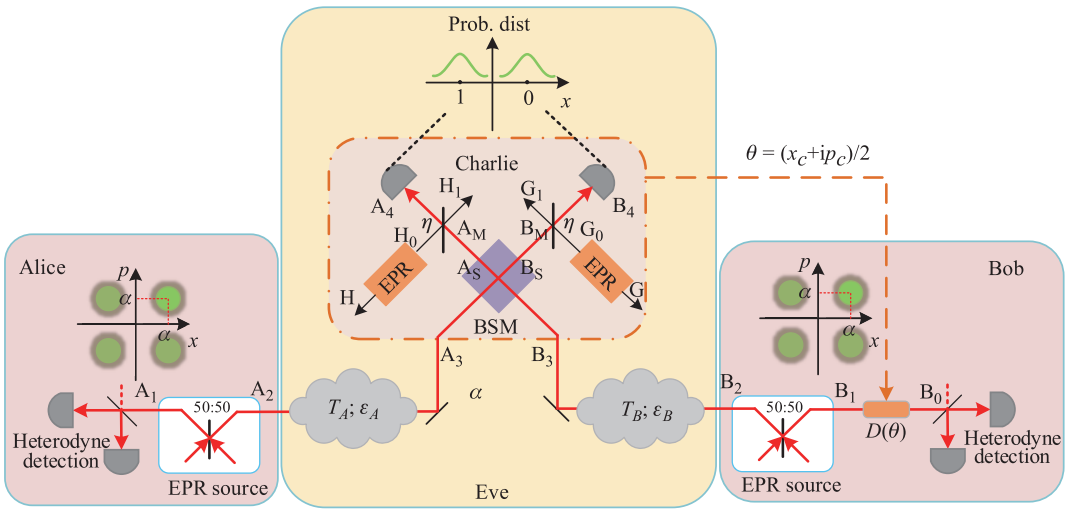


Fig. 3 The equivalent EB model of simultaneous MDI-CVQKD protocol with phase-space representations of simultaneous QPSK and Gaussian modulation.

of the simultaneous MDI-CVQKD protocol, as illustrated in Fig. 3. Alice (Bob) generates an EPR state with variance V_A (V_B), one mode A_1 (B_1) is kept while the other mode A_2 (B_2) is sent to Charlie through the untrusted quantum channel. The two-mode attack has been proven to be the optimal attack strategy against the MDI-CVQKD protocol [48, 56]. However, in practice, the correlation between the ambient noise of the two quantum channels becomes very weak when the two quantum channels (from Alice to Charlie and Bob to Charlie) are from different directions. What is more, the successful implementation of quantum correlations in both quantum channels requires Eve to overcome some technical difficulties. Therefore, we adopt two Markovian memoryless Gaussian quantum channels to reduce the quantum channel of the proposed protocol into a one-mode channel. Based on this, we can degenerate the two-mode attack into a one-mode attack. Consequently, the entangling cloner attack, which is the optimal one-mode collective Gaussian attack, is used to model Gaussian channels between Alice to Charlie and Bob to Charlie, respectively [25, 63]. When Charlie receives the incoming modes A_3 and B_3, he interferes at a 50:50 beam splitter (BS) with two output modes A_s and B_s. These two output modes are, then further transformed into the modes A_4 and B_4 to model the practical homodyne detector characterized by efficiency η and electronic noise ν_{el}. After that both the x-quadrature of A_4 and p-quadrature of B_4 are measured through homodyne detections. After homodyne detections, Charlie obtains measurement results $\{x_R, p_R\}$ whose signs are important to determine the classical bits $\{s_R, t_R\}$. That is to say the bit value of s_R (t_R) is set to be 0 if x_R (p_R)>0; otherwise, the bit value is set to be 1. Then the measurement results are processed, which are given by

$$x_C = \sqrt{\frac{2}{T\eta}}x_R + (2s_R - 1)\alpha,$$

$$p_C = \sqrt{\frac{2}{T\eta}}p_R + (2t_R - 1)\alpha, \tag{3}$$

where T and η are as the same as the afore-mentioned definitions. The measurement results processed by Bob can be described as C with complex value $\theta = (x_C + \mathrm{i}p_C)/2$ and be announced publicly. After receiving Charlie's measurement results, Bob displaces his own mode B_1 by operations $D(\theta)$ while Alice keeps her mode unchanged. Then Alice and Bob perform heterodyne detections to measure the yielded modes A_1 and B_0 to achieve the raw data $X = (x_A, p_A)$ and $Y = (x_B, p_B)$, respectively.

We suppose both communication channel losses are γ. Therefore, the channel transmittances can be expressed as $T_A = 10^{\frac{-\gamma L_{AC}}{10}}$ and $T_B = 10^{\frac{-\gamma L_{BC}}{10}}$, where L_{AC} and L_{BC} represent the fiber length from Alice to Charlie and Bob to Charlie, respectively. And the corresponding thermal excess noises are, respectively, denoted as ε_A and ε_B. Here we set parameter $T = \frac{T_A g^2}{2}$ which is related with transmittance of the quantum channel; g stands for the gain of displacement. Note that the equivalent excess noise of the equivalent one-way scheme can be expressed as [57]

$$\xi_{th} = 1 + \chi_A + \frac{1}{T_A}[T_B(\chi_B - 1)] + \frac{1}{T_A}\left(\frac{\sqrt{2(V_B - 1)}}{g} - \sqrt{T_B(V_B + 1)}\right)^2, \tag{4}$$

where $\chi_A = \frac{1-T_A}{T_A} + \varepsilon_A$ and $\chi_B = \frac{1-T_B}{T_B} + \varepsilon_B$. It is remarkable that the equivalent excess noise can be minimized when parameter $g = \sqrt{\frac{2(V_B-1)}{T_B(V_B+1)}}$, thus we have

$$\xi_{th} = \frac{T_B}{T_A}(\varepsilon_B - 2) + \frac{2}{T_A} + \varepsilon_A. \tag{5}$$

In practice, the homodyne detectors owned by Charlie are not the ideal devices. Therefore, it exists detection-added noise χ_h, which is given by $\chi_h = [(1 - \eta) + \nu_{el}]/\eta$.

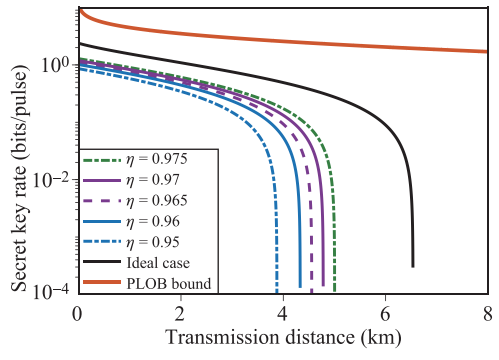


Fig. 4 The relationship between the secret key rate and the transmission distance in the symmetric case ($L_{AC} = L_{BC}$). Here we set the reconciliation efficiency $\beta = 0.98$, the channel excess noise $\varepsilon_A = \varepsilon_B = 0.002$, electronic noise of homodyne detector $\nu_{el} = 0.01$, the variance $V_A = V_B = 40$, the real parameter $\alpha = 100$.

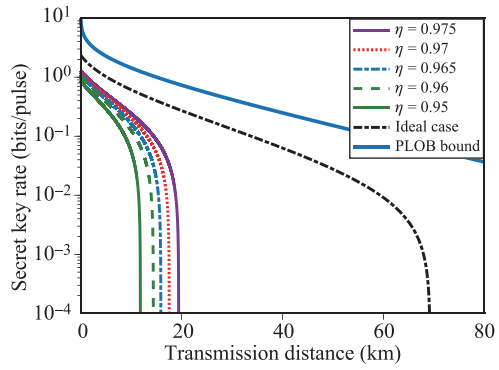


Fig. 5 The relationship between the secret key rate and the transmission distance in the most asymmetric case ($L_{BC} = 0$). Other parameters are set the same as Fig. 4.

Now let's calculate the BER of the classical QPSK modulation. Based on Eq. (1), we have

$$Q_{BER} = \frac{1}{2} erfc\left(\frac{\sqrt{T\eta}\alpha}{\sqrt{4N_t N_0}}\right), \tag{6}$$

where $erfc$ is the complementary error function, N_t is the overall noise variance at Charlie's side, which is given by

$$N_t = \frac{1}{2} T\eta(V + \xi_{th}) + 1 + \nu_{el}. \tag{7}$$

It has been shown that the security proofs of the standard GMCS QKD can be taken advantage of to the one-way SCCQ protocol [58]. Besides, considering the fact that device-dependent one-way QKD can be simulated with arbitrarily high precision by MDI schemes. Therefore, the security proofs of the conventional MDI-CVQKD protocol applies equally to the proposed protocol. Detailed calculation of the asymptotic secret key rate is shown in Appendix A.

In the following, we illustrate the performance of the proposed protocol in the symmetric case ($L_{AC} = L_{BC}$) and the most asymmetric case ($L_{BC} = 0$), as shown in Fig. 4 and Fig. 5 respectively. It is noteworthy that we make comparisons between the ideal condition (ideal homodyne detectors with $\eta = 1$, $\nu_{el} = 0$) and the practical condition (imperfect detectors) in both simulation figures. We observe that the detection efficiency of the imperfect detector owned by Charlie has an important effect on the performance of the proposed protocol in both cases. For example, in the symmetric case, the transmission distance of the simultaneous MDI-CVQKD protocol can reach 6.18 km when Charlie uses the ideal detectors with $\eta = 1$ and $\nu_{el} = 0$. However, the transmission distance reduced to 4.61 km when the detection efficiency $\eta = 0.975$. While, in the asymmetric case, we can obtain the 69.14 km transmission distance when the detector is ideal and the 19.42 km transmission distance when $\eta = 0.975$, which the distance gap between the ideal condition and the practical condition has increased to 49.72 km. In addition, for the practical condition, even slightly reduce the detection efficiency can cause the performance of the proposed protocol worse. Note that we also plot the PLOB bound in both Fig. 4 and Fig. 5, which illustrates the ultimate limit of repeaterless communication [64].

4 Compensation for detector imperfection using optical amplifier

As above analysis, the imperfection of the practical detectors owned by Charlie has a significant effect on the performance of the simultaneous MDI-CVQKD protocol. Therefore, it is necessary to consider methods of surmounting this limitation. As shown in Fig. 6, we employ the phase-sensitive amplifiers (PSAs) to compensate for the detectors' imperfections. The PSA can be deemed as a degenerate optical parametric amplifier which ideally allows noiseless amplification of a chosen quadrature [65]. We describe it by the transformations

$$\begin{pmatrix} x_{A_M} \\ p_{A_M} \end{pmatrix} = \Theta_{PSA_1} \begin{pmatrix} x_{A_S} \\ p_{A_S} \end{pmatrix} = \begin{pmatrix} \sqrt{G} & 0 \\ 0 & \dfrac{1}{\sqrt{G}} \end{pmatrix} \begin{pmatrix} x_{A_S} \\ p_{A_S} \end{pmatrix} \tag{8}$$

and

$$\begin{pmatrix} x_{B_M} \\ p_{B_M} \end{pmatrix} = \Theta_{PSA_2} \begin{pmatrix} x_{B_S} \\ p_{B_S} \end{pmatrix} = \begin{pmatrix} \dfrac{1}{\sqrt{G}} & 0 \\ 0 & \sqrt{G} \end{pmatrix} \begin{pmatrix} x_{B_S} \\ p_{B_S} \end{pmatrix}, \tag{9}$$

where G represents the gain of the amplification. Based on the calculations shown in Section 3, the usage of PSA can be equivalent to modifying χ_h into χ_h^{PSA}, which is given by

$$\chi_h^{PSA} = \frac{(1-\eta) + \nu_{el}}{G\eta}. \tag{10}$$

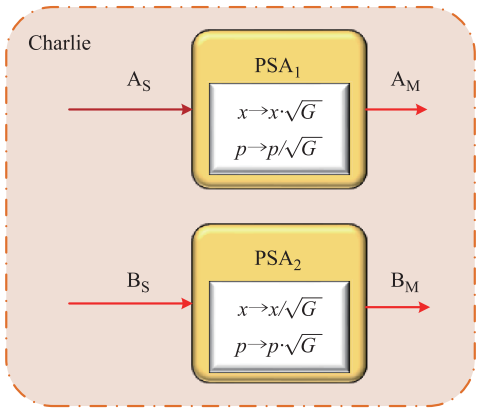


Fig. 6 Model for phase-sensitive amplifier placed at front of Charlie's homodyne detectors.

Then the secret key rate shown in Appendix A can be modified into K_{asy}^{PSA}.

We plot the three-dimension figure to show the relationship between the secret key rate and the gain of PSA, transmission distance under the most asymmetric case, as illustrated in Fig. 7. It is remarkable that the detection efficiencies we use to describe the practical detectors in Fig. 4 and Fig. 5 are high ($> 90\%$), which is hard to realize in view of current fiber-based optical detection technology. The standard values of parameters η and ν_{el} in experiments are, respectively, $\eta = 0.6$ and $\nu_{el} = 0.05$. Consequently, in Fig. 7, we adopt $\eta = 0.6$ and $\nu_{el} = 0.05$ to describe the practical detectors. What is more, the performance of the ideal homodyne detectors ($\eta = 1$, $\nu_{el} = 0$) is also plotted to make comparison. We find that the secret key rate of the proposed simultaneous MDI-CVQKD protocol rises steadily with the increased gain of PSA and becomes closer to the ideal case.

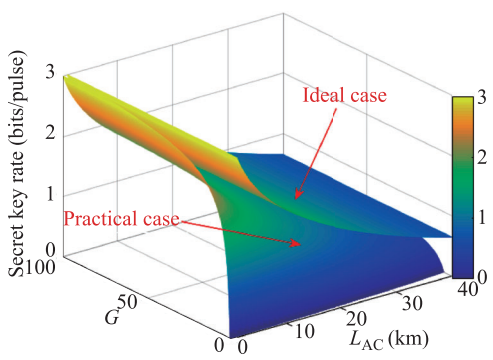


Fig. 7 The relationship between the secret key rate and the gain of PSA, transmission distance under the most asymmetric case by using the practical homodyne detector with $\eta = 0.6$ and $\nu_{el} = 0.05$. The performance of the case using ideal homodyne detectors is also plotted to make comparison. Here the reconciliation efficiency $\beta = 0.98$, the channel excess noise $\varepsilon_A = \varepsilon_B = 0.002$, the variance $V_A = V_B = 40$ and the real parameter $\alpha = 100$.

The relationship between the secret key rate and the transmission distance under different gain factors G is shown in Fig. 8. It is noteworthy that we adopt $\eta = 0.6$ and $\nu_{el} = 0.05$ to describe the practical detectors, which is standard in experiments. It is obvious that the higher performance of the proposed protocol can be achieved with the larger amplification gain. That is to say the PSA can effectively overcome the limitation caused by the imperfection of realistic detectors. Besides, the curve which represents the performance of simultaneous MDI-CVQKD protocol using practical detectors becomes closer to that of the ideal case and the PLOB bound with the increased amplification gain G.

5 Security of simultaneous MDI-CVQKD protocol in finite-size regime

The asymptotic secret key rate mentioned above is in view of an assumption that Alice can transmit infinitely many signals to Bob. However, this is impossible since the length of secret key is limited in practice. Therefore, it is necessary to consider the finite-size effect [27, 49, 66]. Different from the asymptotic regime, the raw keys are finite and part of them are taken advantage of for parameters estimation in finite-size regime. However, this introduces a trade-off between the secret key rate and the accuracy of parameter estimation step. Very recently, Ref. [67] shows that this problem can be solved in conventional MDI framework. Such a property has been applied in the dual-phase-modulated plug-and-play MDI-CVQKD [68] and passive MDI-CVQKD [69]. Here we extend it to our simultaneous MDI-CVQKD protocol without compromising the security.

Note that parameter estimation is an important step to achieve the information of the quantum channel be-

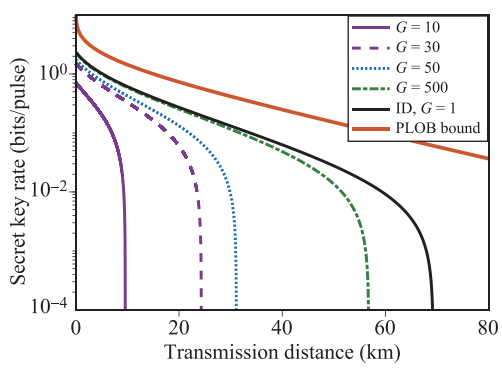


Fig. 8 The relationship between the secret key rate and the transmission distance in the most asymmetric case for different gains of amplification. The practical homodyne detectors with $\eta = 0.6$ and $\nu_{el} = 0.05$ is used, which is standard in experiment. The modulation variance $V_A = V_B = 40$, the reconciliation efficiency $\beta = 0.98$, the channel excess noise $\varepsilon_A = \varepsilon_B = 0.002$, the real parameter $\alpha = 100$.

tween Alice and Bob. Generally speaking, local information without classical communication is not sufficient to perform parameter estimation. In order to perform this procedure successfully, Alice and Bob need to sacrifice part of their local data, which causes the final secret key rate lower. In fact, the covariance matrix Ψ_{XYC} of $(x'_A, p'_A, x'_B, p'_B, x_C, p_C)$ can be directly estimated by Alice and Bob without employing part of the raw data. The covariance matrix of $(x'_A, p'_A, x'_B, p'_B, x_C, p_C)$ is given by

$$\Psi_{XYC} = \begin{pmatrix} VI & 0 & \kappa_{XC} \\ 0 & VI & \kappa_{YC} \\ \kappa_{XC}^T & \kappa_{YC}^T & C \end{pmatrix}, \tag{11}$$

where I is 2×2 identity matrix, and the matrix

$$C = \begin{pmatrix} \langle x_C^2 \rangle & \langle x_C p_C \rangle \\ \langle x_C p_C \rangle & \langle p_C^2 \rangle \end{pmatrix} \tag{12}$$

represents the empirical covariance matrix of (x_C, p_C), and

$$\kappa_{XC} = \begin{pmatrix} \langle x'_A x_C \rangle & \langle x'_A p_C \rangle \\ \langle p'_A x_C \rangle & \langle p'_A p_C \rangle \end{pmatrix},$$
$$\kappa_{YC} = \begin{pmatrix} \langle x'_B x_C \rangle & \langle x'_B p_C \rangle \\ \langle p'_B x_C \rangle & \langle p'_B p_C \rangle \end{pmatrix} \tag{13}$$

stand for the correlation items.

It is remarkable that the variances of parameters x'_A, p'_A, x'_B and p'_B are locally known by Alice and Bob. What is more, these parameters are uncorrelated with known variances V_A and V_B. Based on Charlie's measurement result $\theta = (x_C + \mathrm{i}p_C)/2$, Alice can perform estimation locally for the correlation terms $\langle x'_A x_C \rangle$, $\langle x'_A p_C \rangle$, $\langle p'_A x_C \rangle$ and $\langle p'_A p_C \rangle$ shown in covariance matrix κ_{XC}. Similarly, Bob can achieve the correlation terms $\langle x'_B x_C \rangle$, $\langle x'_B p_C \rangle$, $\langle p'_B x_C \rangle$ and $\langle p'_B p_C \rangle$ shown in covariance matrix κ_{YC}. That is to say Alice and Bob can estimate all the entries of the covariance matrix of $(x'_A, p'_A, x'_B, p'_B, x_C, p_C)$ locally without any extra public communication. Although such a property is achieved for simultaneous MDI-CVQKD protocol, the MDI-CVQKD can simulate one-way CV-QKD protocols with arbitrary precision [67]. Therefore, the whole raw keys can be used to generate the final secret key as well in the real-life CV-QKD system. Detailed calculation of the finite-size secret key rate is shown in Appendix B.

In the following, we plot the performance of the simultaneous MDI-CVQKD protocol with almost the whole raw keys are utilized to generate the final secret key compared with traditional finite-size scenario in the symmetric case and the most asymmetric case, as shown in Fig. 9 and Fig. 10, respectively. Here solid lines stand for the new conceptual finite-size scenario and dotted lines represent the traditional finite-size calculation. It is noteworthy that at least 10^7 samples are needed when Gaussian collective attacks are considered [70]. Simulation results show that

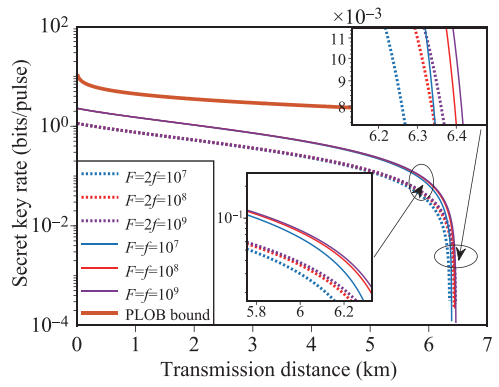


Fig. 9 The relationship between the secret key rate and the transmission distance in the symmetric case. Solid lines represent the performance of new conceptual finite-size regime ($F = f$) and the dotted lines represent the performance of the traditional finite-size scenario ($F = 2f$). From left to right, the block length F for both lines are 10^7, 10^8 and 10^9. The gain factor $G = 500$. Other parameters are fixed the same as Fig. 8.

the secret key rates of the new conceptual finite-size scenario are significantly higher than that of the traditional one whether in the symmetric case or in the most asymmetric case. What is more, the maximum transmission distance for each block is lengthened by directly employing the locally achieved covariance matrix. That is because all raw keys are taken advantage of to generate the final secret key instead of using part of them for parameter estimation.

6 Conclusion and discussion

We have suggested a simultaneous MDI-CVQKD protocol where each sender can superimpose random numbers for QKD on classical information by taking advantage of the

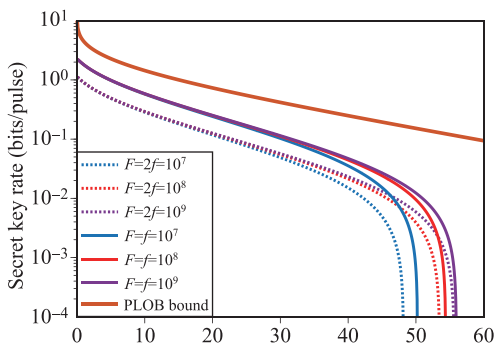


Fig. 10 The relationship between the secret key rate and the transmission distance in the most asymmetric case. Solid lines represent the performance of new conceptual finite-size regime ($F = f$) and the dotted lines represent the performance of the traditional finite-size scenario ($F = 2f$). From left to right, the block length F for both lines are 10^7, 10^8 and 10^9. Other parameters are fixed the same as Fig. 9.

same weak coherent pulse and an untrusted third party (Charlie) decodes it by using the same coherent detectors. This protocol can realize the secret key distribution based on the background of classical communication at a minimal cost in MDI framework. Simulation results show that the imperfection of the realistic detectors at Charlie's side has an important effect on the performance of simultaneous MDI-CVQKD protocol. To overcome this limitation and thus achieve high-performance of the proposed protocol, the PSA technology is adopted to make up for the imperfections. Furthermore, we perform security analysis of the simultaneous MDI-CVQKD protocol in finite-size regime. We show that almost entire raw keys can be taken advantage of for final secret key extraction, instead of sacrificing part of them for parameter estimation. Therefore, the performance of the simultaneous MDI-CVQKD protocol can be further improved in finite-size regime. The proposed protocol can be deemed as an appealing solution for the future MDI framework.

In experimental implementation, there are important challenges of such simultaneous protocols to be addressed. On the one hand, for the one-way simultaneous protocol, the main challenge is its low tolerance of phase noise. Nevertheless, the real local oscillator design [71–73] shows relatively high phase noise since two independent lasers are used respectively to generate the signal and the LO, which indicates incompatibility with the one-way simultaneous protocol. While the plug-and-play configuration [60] waives the necessity of two independent lasers and can make the phase noise relatively low, but it suffers from source noise. That is to say the higher source noise leads to the worse performance of plug-and-play simultaneous protocol. On the other hand, for the experimental implementation of simultaneous MDI protocol, the potential challenge is that the practical homodyne detectors owned by Charlie cannot be the always ideal apparatuses. The imperfection of the detectors has an important effect on the performance of simultaneous MDI protocol due to the fact that it significantly increases the total noise. Consequently, it is meaningful to make the realistic detector compensation using phase-sensitive optical amplifiers, which has been analyzed above. Since the repetition rate of today's classical communication systems can be operated 10 to 100 GHz, a technology for developing high-speed homodyne detectors (above 10 GHz) is needed in future experimental implementation to match these two kinds of communication well. At present, a 1-GHz shot-noise-limited homodyne detector has been developed [73, 74]. With the development of high-speed homodyne detector technology, the gap between repetition rates of classical and quantum communications may finally vanish in future.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant No. 61801522) and National Nature Science Foundation of Hunan Province, China (Grant No. 2019JJ40352).

Appendix A Calculation of asymptotic secret key rate

The asymptotic secret key rate of simultaneous MDI-CVQKD protocol, in the case of Bob performs reverse reconciliation, is calculated as

$$K_{asy} = \beta I_{AB} - \chi_{BE}, \tag{A1}$$

where I_{AB} represents the Shannon mutual information between Alice and Bob, β represents reconciliation efficiency, and χ_{BE} represents the Holevo bound between Eve and Bob. The total channel-added noise is given in shot-noise units by

$$\chi_{line} = \frac{1}{T} - 1 + \xi_{th} + \frac{4\alpha^2}{N_0} Q_{BER}, \tag{A2}$$

where the term $[(4\alpha^2)/N_0]Q_{BER}$ stands for the excess noise caused by the BER of the classical QPSK.

The overall noise referred to the channel input is expressed as

$$\chi_{tot} = \chi_{line} + \frac{2\chi_h}{T_A}. \tag{A3}$$

Considering that the secret key is generated utilizing both quadratures, thus the mutual information between Alice and Bob is expresses as

$$I_{AB} = \log_2 \left[\frac{a+1}{a+1-c^2/(b+1)} \right], \tag{A4}$$

where parameters $a = V_A = V_B = V$, $b = T(V + \chi_{tot})$ and $c = \sqrt{T(V^2-1)}$. The Holevo bound of the information between Alice and Bob can be expresses as

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right), \tag{A5}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. And

$$\lambda_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B^2}), \tag{A6}$$

where

$$A = a^2 + b^2 - 2c^2,$$
$$B = ab - c^2. \tag{A7}$$

While $\lambda_3 = a - c^2/(b+1)$. See Ref. [75] for the detailed derivations.

Appendix B Calculation of finite-size secret key rate

The finite-size secret key rate is given by

$$K_{fin}^{PSA} = \frac{f}{F}[\beta I_{AB} - S_{\epsilon_{PE}} - \Delta(f)], \tag{B1}$$

where β and I_{AB} have been defined in asymptotic case, ϵ_{PE} represents the failure probability of parameter estimation and Δ is associated with the security of the privacy amplification expressed as

$$\Delta(f) = (2dim\Re + 3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{f}} + \frac{2}{f}\log_2(1/\epsilon_{PA}), \tag{B2}$$

where $\bar{\epsilon}$ stands for a smoothing parameter, ϵ_{PA} represents the failure probability of privacy amplification, and $\Re$ represents the Hilbert space corresponding to the raw key. Here, the total exchanged signals and the number of signals used share key between Alice and Bob are assumed as F and f, respectively. It is remarkable that in the framework of traditional finite-size analysis, the remained $h = F - f$ signals are used for parameter estimation. Therefore, the parameter h is usually set to be $h = f = \frac{1}{2}F$. However, in the new conceptual framework of finite-size scenario analyzed above, it is no need to sacrifice part of Alice's and Bob's raw data to perform parameter estimation step since this step can be performed locally without any extra public information. In other words, the whole raw keys can be taken advantage of to generate the final secret key. Based on this, it can be set to be $f \approx F$.

Note that in traditional finite-size scenario, it is necessary to calculate the $S_{\epsilon_{PE}}$ in parameter estimation step. A simple way to compute the $S_{\epsilon_{PE}}$ is that we can perform evaluation for the covariance matrix $\Lambda_{\epsilon_{PE}}$, which minimizes the secret key rate with a probability of $1-\epsilon_{PE}$. By the sampling of $h = F - f$ couples of correlated variables $(x_i, y_i)_{i=1\cdots h}$, we can estimate $\Lambda_{\epsilon_{PE}}$. Here we need to use a normal linear model to link the Alice's and Bob's data, which is given by

$$y = tx + z, \tag{B3}$$

where $t = \sqrt{T}$ and z follows a centered normal distribution with variance ϖ^2. Here we assume $\delta = \xi_{th} + \frac{4\alpha^2}{N_0}Q_{BER}$, then we have $\varpi^2 = 1 + T\delta$. The covariance matrix $\Lambda_{\epsilon_{PE}}$ has the following form

$$\Lambda_{\epsilon_{PE}} = \begin{pmatrix} VI & t_{min}Z\sigma_z \\ t_{min}Z\sigma_z & (t_{min}^2 V + \varpi_{max}^2)I \end{pmatrix}, \tag{B4}$$

where t_{min} and ϖ_{max}^2 are, respectively, the minimal value of t and the maximal value of ϖ^2 compatible with the sampled data, except with probability $\epsilon_{PE}/2$. For the normal linear model, maximum-likelihood estimators $\hat{t}$ and $\hat{\varpi}^2$ are expressed as

$$\hat{t} = \frac{\sum_{i=1}^{h} x_i y_i}{\sum_{i=1}^{h} x_i^2} \quad \text{and} \quad \hat{\varpi}^2 = \frac{1}{h}\sum_{i=1}^{h}(y_i - \hat{t}x_i)^2. \tag{B5}$$

In view of Eq. (B5), we can obtain the minimal value of t (t_{min}) and maximal value of ϖ (ϖ_{max}), which are given by

$$t_{min} \approx \sqrt{T} - z_{\epsilon_{PE}/2}\sqrt{\frac{1+T\delta}{hV}},$$
$$\varpi_{max}^2 \approx 1 + T\delta + z_{\epsilon_{PE}/2}\frac{\sqrt{2}(1+T\delta)}{\sqrt{h}}, \tag{B6}$$

where $z_{\epsilon_{PE}/2}$ is such that $1 - erf(z_{\epsilon_{PE}/2}/\sqrt{2})/2 = \epsilon_{PE}/2$, and $erf(x) = \frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\mathrm{d}t$ stands for error function. It is noteworthy that the optimal value of the error probabilities shown above can be achieved as $\bar{\epsilon} = \epsilon_{PE} = \epsilon_{PA} = 10^{-10}$ [27]. Based on this, we can employ the derived bounds t_{min} and ϖ_{max}^2 to calculate the finite-size secret key rate.

References

1. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, arXiv: 1906.01645 (2019)
2. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, *npj Quantum Inf.* 2, 16025 (2016)
3. H. K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* 8(8), 595 (2014)
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* 74(1), 145 (2002)
5. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* 81(3), 1301 (2009)
6. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, *Rev. Mod. Phys.* 84(2), 621 (2012)
7. L. M. Liang, S. H. Sun, M. S. Jiang, and C. Y. Li, Security analysis on some experimental quantum key distribution systems with imperfect optical and electrical devices, *Front. Phys.* 9(5), 613 (2014)
8. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* 67(6), 661 (1991)
9. H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* 283(5410), 2050 (1999)
10. J. Y. Wang, B. Yang, S. K. Liao, L. Zhang, Q. Shen, X. F. Hu, J. C. Wu, S. J. Yang, H. Jiang, Y. L. Tang, B. Zhong, H. Liang, W. Y. Liu, Y. H. Hu, Y. M. Huang, B. Qi, J. G. Ren, G. S. Pan, J. Yin, J. J. Jia, Y. A. Chen, K. Chen, C. Z. Peng, and J. W. Pan, Direct and full-scale experimental verifications towards ground–satellite quantum key distribution, *Nat. Photonics* 7(5), 387 (2013)

11. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, *Nature* 557(7705), 400 (2018)
12. A. Farouk, J. Batle, M. Elhoseny, M. Naseri, M. Lone, A. Fedorov, M. Alkhambashi, S. H. Ahmed, and M. Abdel-Aty, Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states, *Front. Phys.* 13(2), 130306 (2018)
13. F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* 88(5), 057902 (2002)
14. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, *Nature* 421(6920), 238 (2003)
15. T. C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A* 61(1), 010303 (1999)
16. F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation – the theory of practical implementations, *Adv. Quantum Technol.* 1(1), 1800011 (2018)
17. B. Qi, L. L. Huang, L. Qian, and H. K. Lo, Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers, *Phys. Rev. A* 76(5), 052323 (2007)
18. X. D. Wu, Q. Liao, D. Huang, X. H. Wu, and Y. Guo, Balancing four-state continuous-variable quantum key distribution with linear optics cloning machine, *Chin. Phys. B* 26(11), 110304 (2017)
19. W. Liu, P. Huang, J. Peng, J. Fan, and G. Zeng, Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution, *Phys. Rev. A* 97(2), 022316 (2018)
20. T. Wang, P. Huang, Y. Zhou, W. Liu, and G. Zeng, Practical performance of real-time shot-noise measurement in continuous-variable quantum key distribution, *Quantum Inform. Process.* 17(1), 11 (2018)
21. R. García-Patrón and N. J. Cerf, Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution, *Phys. Rev. Lett.* 97, 190503 (2006)
22. P. Huang, J. Fang, and G. Zeng, State-discrimination attack on discretely modulated continuous-variable quantum key distribution, *Phys. Rev. A* 89(4), 042330 (2014)
23. X. D. Wu, Y. J. Wang, H. Zhong, Q. Liao, and Y. Guo, Plug-and-play dual-phase-modulated continuous-variable quantum key distribution with photon subtraction, *Front. Phys.* 14(4), 41501 (2019)
24. C. Xie, J. Zhang, Q. Pan, X. Jia, and K. Peng, Continuous variable quantum communication with bright entangled optical beams, *Front. Phys. China* 1(4), 383 (2006)
25. S. Pirandola, S. L. Braunstein, and S. Lloyd, Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography, *Phys. Rev. Lett.* 101(20), 200504 (2008)
26. R. Renner and J. I. Cirac, de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography, *Phys. Rev. Lett.* 102(11), 110504 (2009)
27. A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, *Phys. Rev. A* 81(6), 062343 (2010)
28. F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks, *Phys. Rev. Lett.* 109(10), 100502 (2012)
29. A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Security of continuous-variable quantum key distribution against general attacks, *Phys. Rev. Lett.* 110(3), 030502 (2013)
30. A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, *Phys. Rev. Lett.* 114(7), 070501 (2015)
31. D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, *Sci. Rep.* 6(1), 19201 (2016)
32. D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Field demonstration of a continuous-variable quantum key distribution network, *Opt. Lett.* 41(15), 3511 (2016)
33. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nat. Photonics* 7(5), 378 (2013)
34. C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel, *Sci. Rep.* 5(1), 14607 (2015)
35. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, *Phys. Rev. Lett.* 85(6), 1330 (2000)
36. Z. Yuan, J. Dynes, and A. Shields, Avoiding the blinding attack in QKD, *Nat. Photonics* 4(12), 800 (2010)
37. J. Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Quantum hacking on quantum key distribution using homodyne detection, *Phys. Rev. A* 89(3), 032304 (2014)
38. P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, *Phys. Rev. A* 87(6), 062313 (2013)
39. X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems, *Phys. Rev. A* 88(2), 022339 (2013)
40. X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol, *Phys. Rev. A* 87(5), 052309 (2013)

41. H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Homodyne-detector-blinding attack in continuous-variable quantum key distribution, *Phys. Rev. A* 98(1), 012312 (2018)
42. H. Qin, R. Kumar, and R. Alléaume, Saturation attack on continuous-variable quantum key distribution system, *Proc. SPIE* 8899, 88990N (2013)
43. S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, *Phys. Rev. Lett.* 108(13), 130502 (2012)
44. H. K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* 108(13), 130503 (2012)
45. F. Xu, M. Curty, B. Qi, and H. K. Lo, Practical aspects of measurement-device-independent quantum key distribution, *New J. Phys.* 15(11), 113007 (2013)
46. X. B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, *Phys. Rev. A* 87(1), 012320 (2013)
47. M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H. K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* 5(1), 3732 (2014)
48. C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration, *Phys. Rev. A* 91(2), 022320 (2015)
49. P. Papanastasiou, C. Ottaviani, and S. Pirandola, Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables, *Phys. Rev. A* 96(4), 042332 (2017)
50. Y. Liu, T. Y. Chen, L. J. Wang, H. Liang, G. L. Shentu, J. Wang, K. Cui, H. L. Yin, N. L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C. Z. Peng, Q. Zhang, and J. W. Pan, Experimental measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* 111(13), 130502 (2013)
51. T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, *Phys. Rev. A* 88(5), 052303 (2013)
52. Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H. K. Lo, Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* 112(19), 190503 (2014)
53. H. W. Li, Z. Q. Yin, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Quantum key distribution based on quantum dimension and independent devices, *Phys. Rev. A* 89(3), 032302 (2014)
54. F. Xu, B. Qi, Z. Liao, and H. K. Lo, Long distance measurement-device-independent quantum key distribution with entangled photon sources, *Appl. Phys. Lett.* 103(6), 061101 (2013)
55. X. C. Ma, S. H. Sun, M. S. Jiang, M. Gui, and L. M. Liang, Gaussian-modulated coherent-state measurement-device-independent quantum key distribution, *Phys. Rev. A* 89(4), 042335 (2014)
56. S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, *Nat. Photonics* 9(6), 397 (2015)
57. Z. Li, Y. C. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* 89(5), 052301 (2014)
58. B. Qi, Simultaneous classical communication and quantum key distribution using continuous variables, *Phys. Rev. A* 94(4), 042340 (2016)
59. B. Qi and C. C. W. Lim, Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator, *Phys. Rev. Appl.* 9(5), 054008 (2018)
60. X. Wu, Y. Wang, Q. Liao, H. Zhong, and Y. Guo, Simultaneous classical communication and quantum key distribution based on plug-and-play configuration with an optical amplifier, *Entropy* 21(4), 333 (2019)
61. T. Wang, P. Huang, S. Wang, and G. Zeng, Carrier-phase estimation for simultaneous quantum key distribution and classical communication using a real local oscillator, *Phys. Rev. A* 99(2), 022318 (2019)
62. W. A. Hofer, Solving the Einstein-Podolsky-Rosen puzzle: The origin of non-locality in Aspect-type experiments, *Front. Phys.* 7(5), 504 (2012)
63. M. Navascués and A. Acín, Security bounds for continuous variables quantum key distribution, *Phys. Rev. Lett.* 94(2), 020505 (2005)
64. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* 8(1), 15043 (2017)
65. S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, *J. Phys. At. Mol. Opt. Phys.* 42(11), 114014 (2009)
66. X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* 96(4), 042334 (2017)
67. C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Parameter estimation with almost no public communication for continuous-variable quantum key distribution, *Phys. Rev. Lett.* 120(22), 220505 (2018)
68. Q. Liao, Y. Wang, D. Huang, and Y. Guo, Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution, *Opt. Express* 26(16), 19907 (2018)
69. X. Wu, Y. Wang, S. Li, W. Zhang, D. Huang, and Y. Guo, Security analysis of passive measurement-device-independent continuous-variable quantum key distribution with almost no public communication, *Quantum Inform. Process.* 18(12), 372 (2019)

70. C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, *Phys. Rev. A* 97(5), 052327 (2018)

71. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection, *Phys. Rev. X* 5(4), 041009 (2015)

72. D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-referenced continuous-variable quantum key distribution protocol, *Phys. Rev. X* 5(4), 041010 (2015)

73. D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, High-speed continuous-variable quantum key distribution without sending a local oscillator, *Opt. Lett.* 40(16), 3695 (2015)

74. X. Zhang, Y. Zhang, Z. Li, S. Yu, and H. Guo, *IEEE Photonics J.* 10, 1 (2018)

75. G.-P. Sanchez, Universite Libre de Bruxelles, 2007