Frontiers of Physics
https://doi.org/10.1007/s11467-019-0881-8
Front. Phys.
14(4), 41501 (2019)

LETTER

Plug-and-play dual-phase-modulated continuous-variable quantum key distribution with photon subtraction

Xiao-Dong Wu, Yi-Jun Wang†, Hai Zhong, Qin Liao, Ying Guo‡

School of Automation, Central South University, Changsha 410083, China
Corresponding authors. E-mail: †xxywyj@sina.com, ‡guoyingcsu@sina.com
Received December 4, 2018; accepted January 10, 2019

Plug-and-play dual-phase-modulated continuous-variable quantum key distribution (CVQKD) protocol can effectively solve the security loopholes associated with transmitting local oscillator (LO). However, this protocol has larger excess noise compared with one-way Gaussian-modulated coherent-states scheme, which limits the maximal transmission distance to a certain degree. In this paper, we show a reliable solution for this problem by employing non-Gaussian operation, especially, photon subtraction operation, which provides a way to improve the performance of plug-and-play dual-phase-modulated CVQKD protocol. The photon subtraction operation shows experimental feasibility in the plug-and-play configuration since it can be implemented under current technology. Security results indicate that the photon subtraction operation can evidently enhance the maximal transmission distance of the plug-and-play dual-phase-modulated CVQKD protocol, which effectively makes up the drawback of the original one. Furthermore, we achieve the tighter bound of the transmission distance by considering the finite-size effect, which is more practical compared with that achieved in the asymptotic limit.

Keywords plug-and-play, dual-phase-modulated, continuous variable, quantum key distribution, photon subtraction

1 Introduction

Quantum key distribution (QKD) allows two remote parties, Alice and Bob, to share a sequence of random secure key, even in the presence of eavesdroppers (Eve) [1–4]. The security of a key is guaranteed by the laws of quantum physics [5, 6]. Generally speaking, QKD has two main approaches, namely, discrete-variable (DV) QKD [7, 8] and continuous-variable (CV) QKD [9–13]. In the first approach, the information of key bit is carried by the properties of a single photon [14, 15]. For example, Ref. [16] utilized the transverse momentum of single photons to encode high-dimensional secure keys and demonstrated it with the existing telecommunication infrastructure. While in CVQKD, the key bits are encoded on the quadrature variables of the optical field, and the detection is realized through high-efficiency homodyne or heterodyne detection techniques [17–20].

At present, CVQKD has been implemented by using standard telecommunication technology [21], which provides more simple and cost-effective implementation compared with its DV counterpart. In addition, CVQKD has been proved to be secure against arbitrary collective attacks not only in the asymptotic limit [22–25] but also the finite-size scenario [26–28].

Recently, several experiments of CVQKD have been carried out in the laboratory [10, 11, 29–31] and most of them were demonstrated in view of the one-way Gaussian-modulated coherent-states (GMCS) protocol. In the one-way GMCS CVQKD experiments, quantum signals encoded in two quadratures of coherent states were transmitted together with a strong local oscillator (LO) through a single-fiber channel. Unfortunately, the nonlocal arrangement of LO would cause wavelength attacks [32, 33], saturation attacks [34] and LO fluctuation attacks [35], which are closely related to the security loopholes of LO. In order to solve this problem, self-referenced CVQKD protocols without sending a LO is proposed [36–38]. Such protocols can effectively deal with the security loopholes of LO by employing an independent laser source at the receiver's side. However, a major problem, common to those protocols is that it is difficult to guarantee the frequency instabilities of two independent laser sources in real-life experiments. Besides, environmental perturbations can lead to the fiber channel length fluctuations, the polarization drifts and phase diffusion [39–41], which also have negative effects on the security and performance of those protocols.

Different from the aforementioned protocols, in the preliminary experiment of plug-and-play configuration [42], it uses a single laser source instead of two separate lasers to generate a local LO for legitimate parties. However, this plug-and-play scheme is more sensitive to excess noise compared with one-way GMCS protocol and suffers

the Trojan-horse attack [43, 44]. More recently, CVQKD based on a plug-and-play dual-phase-modulated coherent-states (DPMCS) protocol is proposed and experimentally demonstrated [45]. In this protocol, Bob prepares quantum states and Alice generates the LO locally for quantum state measurement, which is in contrast to the one-way GMCS protocol. Therefore, this protocol can remove the security loopholes of LO and automatically compensate the polarization drifts. What is more, a tight security bound can be derived against collective attacks since the plug-and-play DPMCS protocol considers the untrusted source noise. Unfortunately, this proposed protocol has larger excess noise compared with one-way GMCS QKD scheme, which limits the maximal transmission distance to a certain degree.

Currently, non-Gaussian operations, including photon subtraction and photon addition operations, have been theoretically and experimentally demonstrated to be able to significantly enhance the transmission distance of CVQKD protocols in view of the fact that these operations can be employed to increase and distill the entanglement in Gaussian entangled states [46–49]. What the photon subtraction operation attracts us is that it can be easily implemented in practice with existing technologies, thus providing more cost-effective solution than photon addition operation. Therefore, in this paper, we propose a method to improve the performance of plug-and-play DPMCS protocol by mainly considering the photon subtraction operation. Through performing a suitable photon subtraction operation with the entangled source at Bob's side, the protocol can extend the maximum transmission distance under a relatively high key rate compared with the original protocols in consideration of the untrusted source noise. In addition, we also consider the influence of finite-size effect on the plug-and-play DPMCS protocol with photon-subtraction operation, which is more accordant with practical circumstances than the asymptotic limit. That is to say, our proposal can provide a feasible method for the demonstration of the plug-and-play DPMCS protocol in the real experimental implementation.

This paper is structured as follows. In Section 2, we first introduce the original plug-and-play DPMCS protocol, then present the model of plug-and-play DPMCS QKD protocol with photon subtraction and photon addition operations, respectively. In Section 3, we show numeric simulation and performance analysis. Finally, conclusions are drawn in Section 4.

2 Non-Gaussian operations in the plug-and-play DPMCS protocol

In this section, we first review the original plug-and-play DPMCS protocol, particularly the entanglement-based (EB) scheme [50]. After that, we show the model of plug-and-play DPMCS protocol with non-Gaussian operations (based on EB scheme), namely, photon subtraction and photon addition.

2.1 Description of plug-and-play DPMCS protocol

In practice, the implementation of the plug-and-play DPMCS protocol is based on the prepare-and-measure (PM) scheme. However, the PM scheme cannot provide a powerful description to establish security proofs. Therefore, it is necessary to introduce the EB scheme (see Fig. 1) to conveniently analyze the security of plug-and-play DPMCS protocol, which is fully equivalent to the PM version. Here we do not introduce the PM scheme of plug-and-play DPMCS protocol since it has been analyzed in detail in Ref. [45].

In the EB version, the general collective attack is taken into consideration, which is viewed as the optimality of Gaussian attack [51]. A entanglement state denoted as $|\Psi_{ABF}\rangle$ is prepared by Fred. The state (denoted as B) is

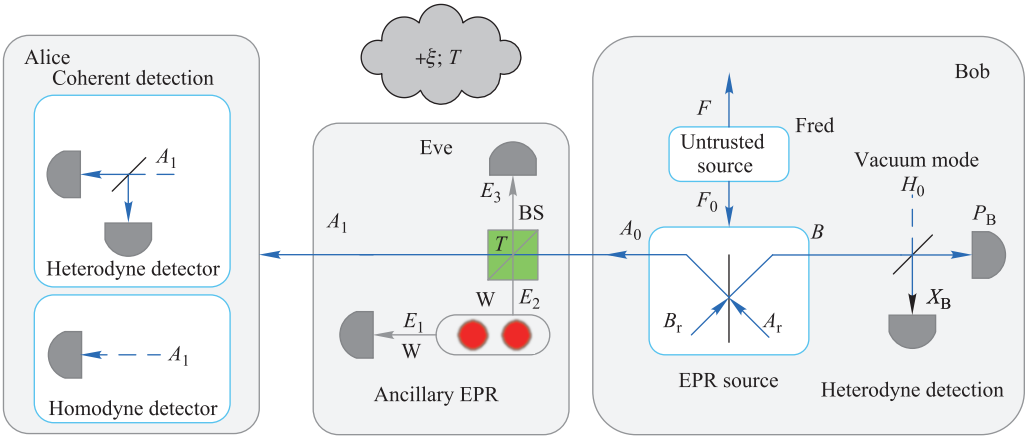

Fig. 1 The equivalent entanglement-based scheme of the plug-and-play DPMCS protocol. Here the source is equivalently controlled by Eve. Thus Fred cannot be regarded as a neutral party. In fact, Fred should be supposed as untrusted party controlled by Eve and then a tight security bound can be achieved. T represents the transmittance of the untrusted quantum channel and ξ represents the channel excess noise.

kept by Bob and another state (denoted as A_0) is sent to Alice through the quantum channel. Note that the quadratures of modes A_0 and B are, respectively, denoted as $\langle X'^2\rangle = \langle P'^2\rangle = V + \zeta$ and $\langle X^2\rangle = \langle P^2\rangle = V$, where $V = V_B + 1$ and $\zeta = g - 1 + (g-1)V_I$. Here V_B represents the modulation variance of mode B, V_I is the noise variance of a vacuum state, and g ($g \geq 1$) is the gain of a phase-insensitive amplifier (PIA), which is used to characterize the untrusted source noise in the PM scheme of plug-and-play DPMCS protocol [45]. Besides, the quantum channel features a transmittance T and an excess noise ξ. Bob applies a heterodyne detection on mode B to prepare the coherent state and Alice performs homodyne detection to measure the incoming mode A_1. Once enough quantity of correlated data has been collected, Alice and Bob take advantage of an authenticated public channel for parameter estimation. Finally, they obtain the final secret key by information reconciliation and privacy amplification. Here, the total channel-added noise (denoted as χ_{line}) referred to the channel input can be calculated as $\chi_{line} = 1/T - 1 + \xi$.

It is remarkable that Fred here is not a neutral party and is assumed to be controlled by Eve. In other words, the entanglement state $|\Psi_{ABF}\rangle$ in the EB scheme is used to model the noisy coherent source in the PM scheme. Therefore, the entanglement state $|\Psi_{ABF}\rangle$ is virtually a two-mode state and the calculation of the entanglement state is similar to the traditional two-mode squeezed vacuum state in CVQKD protocol. Under this assumption, we can obtain a tight security bound. While, if Fred is assumed to be a neutral party, the entanglement state $|\Psi_{ABF}\rangle$ becomes a three-mode state since Fred is not controlled by Eve and can be considered equal to legitimate parties, Alice and Bob. Detailed analysis has been shown in Ref. [52].

2.2 Plug-and-play DPMCS protocol with photon subtraction

As shown in Fig. 2, we suggest the plug-and-play DPMCS protocol with photon subtraction operation applied at Bob's station. In this new version of the protocol, Bob employs a BS with transmission μ to split the mode A_0 and the vacuum state C_0 into modes A_1 and C. Consequently, we can obtain the yielded tripartite state ρ_{FBA_1C}, which can be expressed as

$$\rho_{FBA_1C} = U_{BS}[|\Phi\rangle_{FBA_0}\langle\Phi|_{FBA_0} \bigotimes |0\rangle\langle 0|]U_{BS}^{\dagger}. \tag{1}$$

Through using the positive operator-valued measurement (POVM) $\{\Upsilon_0^m, \Upsilon_1^m\}$, the photon-number-resolving detector (PNRD) can be applied to measure mode C [53, 54]. The photon number of subtraction operation m depends on $\Upsilon_1^m = |m\rangle\langle m|$. Note that Bob can successfully perform the photon subtraction operation only when the POVM element Υ_1^m clicks. The photon-subtracted state $\rho_{FBA_1}^{PS}$ can be given by

$$\rho_{FBA_1}^{PS} = \frac{\mathrm{tr}_C(\Upsilon_1^m \rho_{FBA_1C})}{P^{\Upsilon_1^m}(m)}, \tag{2}$$

where $\mathrm{tr}_X(Y)$ stands for the partial trace of the multimode quantum state. $P^{\Upsilon_1^m}(m)$ stands for the success probability of subtracting m photons, which can be calculated as

$$\begin{aligned} P^{\Upsilon_1^m}(m) &= \mathrm{tr}_{FBA_1C}(\Upsilon_1^m \rho_{FBA_1C}) \\ &= (1-\vartheta^2)\sum_{n=m}^{\infty} C_n^m \vartheta^{2n}(1-\mu)^m \mu^{n-m} \\ &= (1-\vartheta^2)\left(\frac{1-\mu}{\mu}\right)^m \sum_{n=m}^{\infty} C_n^m (\vartheta^2\mu)^n \\ &= (1-\vartheta^2)\vartheta^{2m}\frac{(1-\mu)^m}{(1-\vartheta^2\mu)^{m+1}}, \end{aligned} \tag{3}$$

where C_n^m is a combinatorial number and $n \geq m$ and $\vartheta = \sqrt{\frac{V-1}{V+1}}$. Here, we assume $\rho_{FBA_1C} = |\alpha\rangle\langle\alpha|$, where

$$\begin{aligned} |\alpha\rangle &= U_{BS}|\Phi\rangle_{FBA_0} \bigotimes |0\rangle \\ &= \sqrt{1-\vartheta^2}\sum_{n=0}^{\infty}\vartheta^n (U_{BS}|n,0\rangle) \bigotimes |n\rangle_B \\ &= \sqrt{1-\vartheta^2}\sum_{n=0}^{\infty}\sum_{t=0}^{n}\vartheta^n \sqrt{C_n^t(1-\mu)^t\mu^{n-t}}|n,t,n-t\rangle. \end{aligned} \tag{4}$$

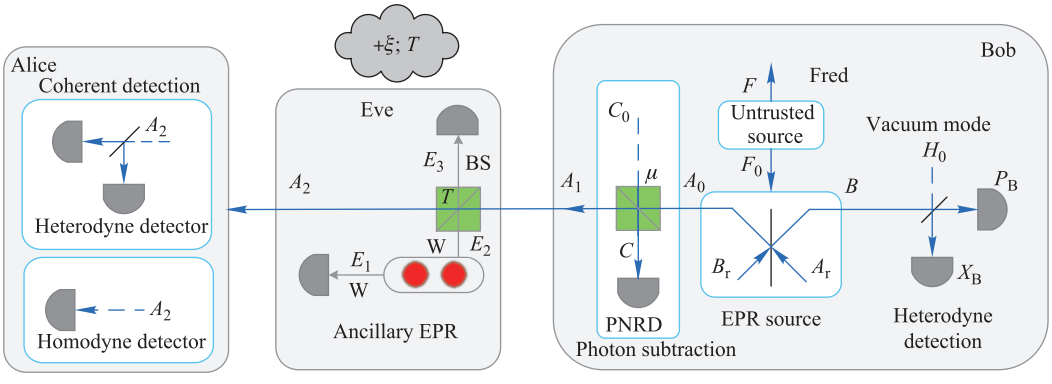

Fig. 2 EB scheme of the plug-and-play DPMCS QKD protocol with photon subtraction operation. EPR: Two-mode squeezed state. PNRD: Photon number resolving detector. BS: Beam splitter.

Based on Eq. (2) and Eq. (3), the covariance matrix of $\rho^{PS}_{FBA_1}$ can be expressed as

$$\Gamma^{PS}_{FBA_1} = \begin{pmatrix} UI_2 & S\sigma_z \\ S\sigma_z & RI_2 \end{pmatrix}, \tag{5}$$

where I_2 and σ_z are 2×2 identity matrix and diag$(1,-1)$, respectively, and

$$\begin{aligned} U &= \frac{2(1+m)}{1-\mu\vartheta^2} - 1, \\ R &= \frac{2(1+m\vartheta^2\mu)}{1-\mu\vartheta^2} - 1, \\ S &= \frac{\sqrt{\mu}\vartheta(1+m)}{1-\mu\vartheta^2}. \end{aligned} \tag{6}$$

According to above analysis, the POVM Υ_1^m becomes Υ_1^1 and clicks with a probability $P^{\Upsilon_1^1}(1)$ if we want to subtract 1 photons in practice. Similarly, the POVM Υ_1^m becomes Υ_1^2 and clicks with a probability $P^{\Upsilon_1^2}(2)$ if we want to subtract 2 photons. By using this way, we can subtract more photons in real implementation. It is remarkable that the afore-derived bipartite state $\rho^{PS}_{FBA_1}$ is not Gaussian anymore. However, its entangle degree can be increased through introducing the photon-subtraction operation [46].

2.3 Plug-and-play DPMCS protocol with photon addition

We depict the EB scheme of the plug-and-play DPMCS protocol with photon addition operation in part of Fig. 3. Here we only show the part of Bob's side since the part of Alice's side is the same as Fig. 2. Different from the implementation of the photon subtraction operation shown above, in this subsection, we implement the photon addition operation at both sides of the entanglement state $|\Psi_{ABF}\rangle$. It has been proved that this arrangement can improve both the quality of distilled entanglement and the success probability for a weak two-mode squeezed vacuum state [49]. In practice, to effectively implement the photon addition operation, conditional spontaneous parametric down-conversion (SPDC) in a nonlinear crystal is needed. Besides, a careful mode match between the signal mode and input quantum mode is required to achieve the successful photon addition.

As shown in Fig. 3, we introduce the photon addition scheme, which can be accomplished by using beam splitters and on-off photon detectors. Here Bob uses two beam splitters with transmittance η, namely, BS_1 and BS_2, to respectively split modes A_0, X_0 and B, Y_0 into modes A_1, X and B_1, Y. Bob then performs heterodyne detection on the mode B_1 and sends mode A_1 to Alice through the quantum channel. The photons $|1\rangle$ in modes X_0 and Y_0 are projected into vacuum state $|0\rangle\langle 0|$. The unitary coupling between modes A_0X_0 and BY_0 is expressed by

$$\begin{aligned} &|\Theta\rangle_{FA_0BX_0Y_0} \\ &= U_{FA_0X_0}(\eta)\bigotimes U_{BY_0}(\eta)(|\phi\rangle_{FA_0B}\bigotimes|1\rangle_{X_0}\bigotimes|1\rangle_{Y_0}). \end{aligned} \tag{7}$$

In this scheme, we employ on-off photon detectors as the measuring device, which are usually used in quantum optics experiments. Note that the on-off photon detectors D_1 and D_2 have only two measurement results: on (one or more photons) and off (no photon). We can use positive operators $\{\hat{\prod}^{on}, \hat{\prod}^{off}\}$ to express these two results in Fock-state space, namely,

$$\hat{\prod}^{off} = |0\rangle\langle 0|, \quad \hat{\prod}^{on} = I - |0\rangle\langle 0|. \tag{8}$$

It is worth mentioning that a successful photon addition operation can be obtained when both detectors register "off" results. Note that $\hat{\prod}^{off} = |0\rangle\langle 0|$ stands for a projection operation into a vacuum state, thus the unnormalized entangled state is given by

$$\begin{aligned} &|\phi_{unnorm}\rangle_{FA_0B} \\ &= {}_{X_0}\langle 0|\bigotimes_{E}\langle 0|\Theta\rangle_{FA_0BX_0Y_0} \\ &= \sum_{n=0}^{\infty}\sqrt{1-\delta^2}(\delta\eta)^n(n+1)(1-\eta)|n+1\rangle_{FA_0}|n+1\rangle_B, \end{aligned} \tag{9}$$

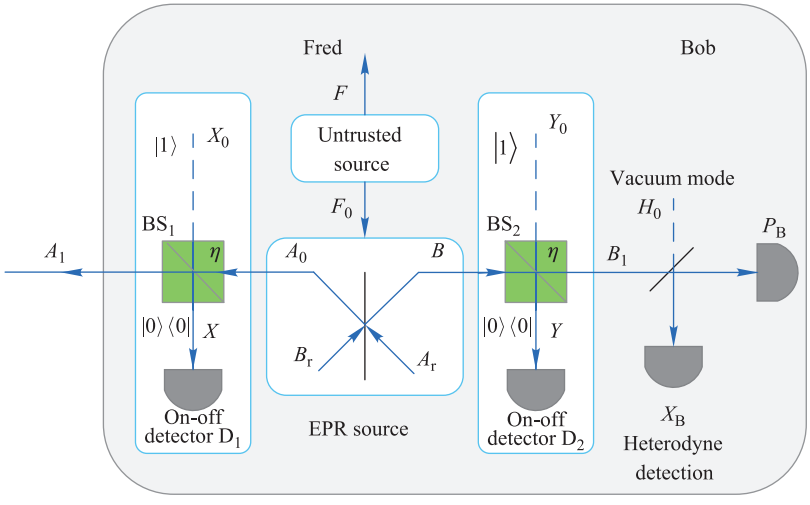

Fig. 3 EB scheme of the plug-and-play DPMCS QKD protocol with photon addition operation. The photon addition operation is individually implemented in each outgoing mode. BS_1 and BS_2 stand for two beam splitters with transmittance η. D_1 and D_2 represent two conventional on-off detectors.

where $\delta = tanh(r)$ $(0 < \delta < 1)$ is the squeezing parameter in the two-mode squeezed state.

Since the success probability of photon addition operation is determined by the norm of state $|\phi_{unnorm}\rangle_{FA_0B}$, which can be given by

$$P_{add} = {}_{FA_0B}\langle\phi_{unnorm}|\phi_{unnorm}\rangle_{FA_0B} = \frac{(1-\eta)^2(1-\delta^2)(1+\eta^2\delta^2)}{(1-\eta^2\delta^2)^3}. \quad (10)$$

We can derive the normalized entangled state, which follows as

$$|\phi\rangle_{FA_0B} = \sum_{n=0}^{\infty} \frac{(1-\eta^2\delta^2)^{3/2}}{\sqrt{1+\eta^2\delta^2}}(n+1)(\eta\delta)^n|n+1\rangle_{FA_0}|n+1\rangle_B. \quad (11)$$

The entangled state shown in Eq. (11) happens to be in the form of Schmidt decomposition [55]. In addition, we can employ logarithmic negativity to estimate the entanglement [56], which is given by

$$E_{add} = 2\log_2\left[\sum_{n=0}^{\infty}\frac{(n+1)(\eta\delta)^2(1-\eta^2\delta^2)^{3/2}}{\sqrt{1+\eta^2\delta^2}}\right] = \log_2\left[\frac{(1+\eta\delta)^2}{(1-\eta\delta)(1+\eta^2\delta^2)}\right]. \quad (12)$$

It is important to point out that the photon addition operation is more sensitive to detection efficiency compared with photon subtraction operation. This problem could be solved by taking advantage of a superconducting single-photon detector (SSPD) [49]. However, the cost of SSPD is high and its efficiency is low. Besides, the implementation of photon addition operation is more complex than that of photon subtraction operation based on above analysis. From a practical point of view, the photon subtraction operation is more attractive than the photon addition operation because of its relative simple and cost-effective implementation. Therefore, in the following, we focus our attention on the performance analysis and calculation of the photon subtraction since those of the photon addition can be performed in similar way.

3 Performance analysis and discussion

In this section, we show the the theoretical security simulation results of plug-and-play DPMCS protocol with photon subtraction compared with the original plug-and-play DPMCS protocol. We first consider the relationship between the success probability $P^{\Upsilon_1^m}(m)$ of subtracting m $(m = 1, 2, 3, 4)$ photons and the transmittance μ since the success probability is very important in calculating the secret key rate. As shown in Fig. 4, it is clear that whether gain $g = 1$ or $g = 2$, the success probability of subtracting one photon is higher than subtracting other numbers of photon. In addition, the optimal success probability

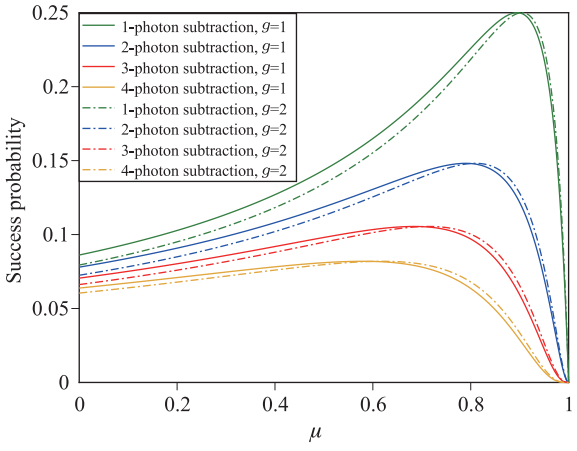

Fig. 4 The success probability of subtracting m photons as a function of transmittance μ of Bob's BS. The variance of EPR state is V_B=20. Solid lines refer to no source noise case $(g = 1)$ and dash lines refer to source noise case $(g = 2)$.

decreases with increasing photon number of subtraction. Thus, it cannot guarantee that only 1 or 2 photons are subtracted, the 3 or 4 photons may also be subtracted with lower probability. We can also observe from Fig. 4 that the success probability is slightly affected by the source noise which is weighted by parameter g.

Considering the fact that the change of the transmittance μ of Bob's beam splitter will lead to the change of the covariance matrix $\rho^{PS}_{FBA_1}$ and the success probability $P^{\Upsilon_1^m}(m)$ when Bob performs the m-photon subtraction. Therefore, we may find an optimal μ to maximize the secret key rate for each channel loss. Here we show the maximal secret key rate as a function of channel loss for optimal μ in Fig. 5(a) and show the optimal choice of μ for each channel loss in Fig. 5(b). As illustrated in Fig. 5(a) and Fig. 5(b), the solid lines and dash lines stand for two different scenes where $g = 1$ and $g = 1.005$, respectively. The blue lines denote the case of the original plug-and-play DPMCS protocol, whose performance is worse than the plug-and-play DPMCS protocol with photon subtraction in the high channel-loss range. That is to say the photon-subtraction operation contributes to expand the maximal transmission distance in the usual case. However, in the low channel loss range, even we choose the optimal μ, the secret key rate of the plug-and-play DPMCS protocol with photon subtraction is still worse than that of the original plug-and-play DPMCS protocol. The reason can be found from Fig. 4 that the success probability of subtracting m photons is relatively low in low channel-loss range. We also observe that the plug-and-play DPMCS protocol with one-photon subtraction operation can tolerate more channel losses while the secret key rates of the protocol are relatively high. In addition, the source noise weighted by parameters g (dash lines) can reduce the tolerance in channel losses and decrease the secret key rates.

It is remarkable that Fig. 5 shown above is simulated

using the optimal transmittance μ of Bob's beam splitter and considering the effect of Fred's behaviors. In the following, to provide more general analysis in the proposed protocol, Fig. 6 shows the secret key rate of plug-and-play DPMCS protocol with optimal one-photon subtraction operation as a function of μ at each channel loss under different g. The values of parameter g in Fig. 6(a), Fig. 6(b), Fig. 6(c) and Fig. 6(d) are, respectively, set to $g = 1$, $g = 1.005$, $g = 1.01$ and $g = 1.015$. We can observe that the unsecure region (blank area) enlarges with increasing the parameter g. In unsecure region, it shows the unsuitable values of transmittance μ can lead

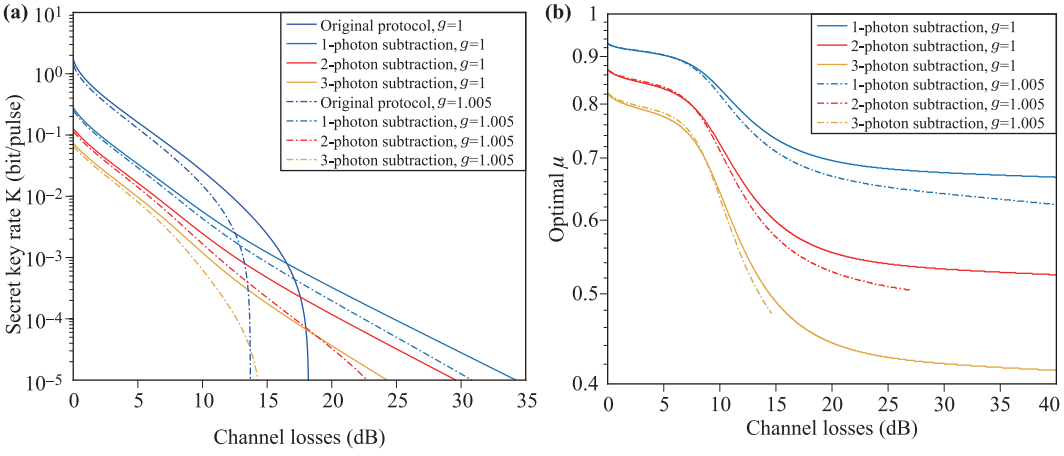

Fig. 5 **(a)** The maximal secret key rate as a function of channel loss for every optimal transmittance μ in the asymptotic case by considering the effect of the untrusted source noise. **(b)** The optimal μ for the maximal secret key rate in (a) by considering the effect of the untrusted source noise. The simulation parameters are fixed as follows: the reconciliation efficiency $\beta = 0.95$, channel excess noise $\xi = 0.01$, and the variance of EPR state is $V_B = 20$. Solid lines refer to no source noise case ($g = 1$) and dash lines refer to source noise case ($g = 1.005$).

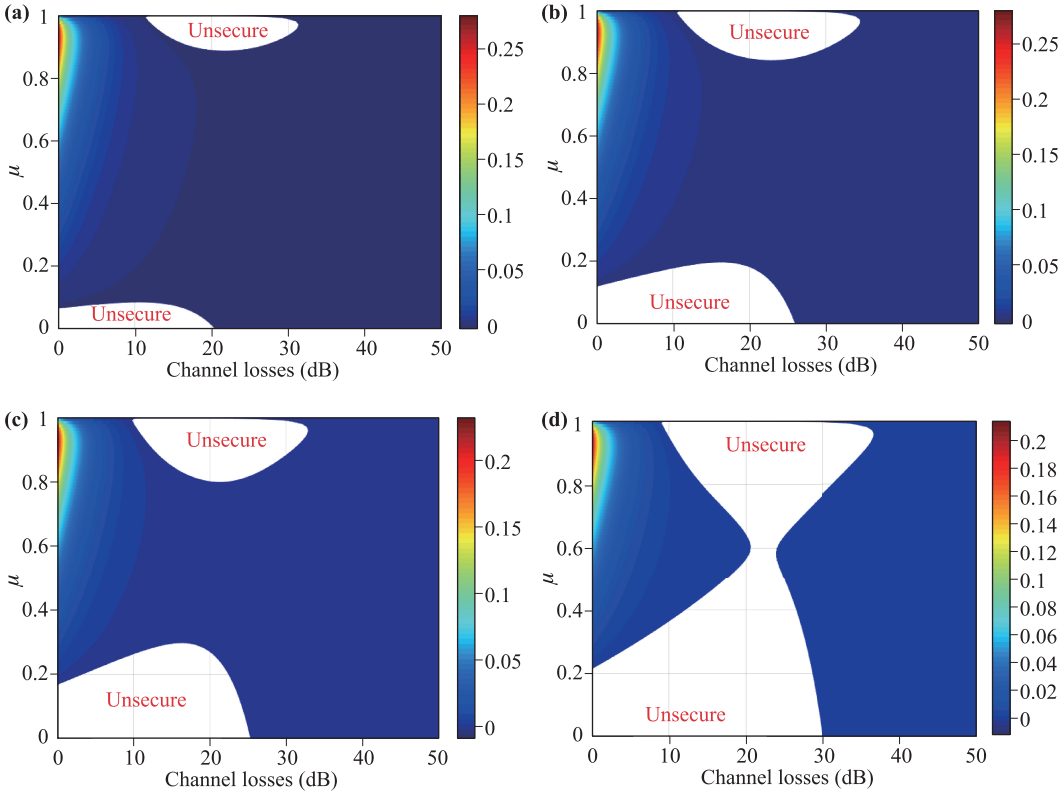

Fig. 6 The secret key rate of plug-and-play DPMCS protocol with optimal one-photon subtraction operation as a function of μ at each channel loss under different g. **(a)** The parameter $g = 1$. **(b)** The parameter $g = 1.005$. **(c)** The parameter $g = 1.01$. **(d)** The parameter $g = 1.015$.

to the unphysical negative secret key rate, as illustrated in Fig. 6(a), Fig. 6(b), Fig. 6(c). However, when $g = 1.015$, the maximum channel-loss tolerance of the plug-and-play DPMCS protocol with one-photon subtraction is decrease even using the optimal transmittance μ. Therefore, it is very important to control the untrusted source noise to ensure the security of the proposed protocol. Detailed calculation of the asymptotic secret key rate is shown in Appendix A.

In addition, from a practical point of view, it is necessary for us to consider the finite-size effect since the number of exchanged signals is impossibly unlimited in practice. Generally speaking, in the asymptotic case, it assumes that the quantum channel is perfectly known before the transmission is performed. However, in the finite-size scenario, one does not know in advance the characteristics of the quantum channel. The reason is that a portion of exchanged signals needs to be employed to estimate parameter. Since the finite-size scenario takes into account the loss of parameter estimation, the analysis is more realistic than the asymptotic regime. The main plots in Fig. 7 illustrate the finite-size secret key rate of plug-and-play DPMCS protocol with photon subtraction operation as a function of channel loss. Here Fig. 7(a), Fig. 7(b), Fig. 7(c) and Fig. 7(d) show the proposed schemes with one-photon subtraction, two-photon subtraction, three-photon subtraction and four-photon subtraction, respectively. We notice that whether in the proposed schemes or in the original scheme, the asymptotic scenario tolerates more channel losses than the finite-size scenario. In other words, the maximal transmission distance in the the asymptotic scenario is longer than that in the finite-size scenario. Besides, the curves of the finite-size scenario are more and more close to the curve of asymptotic case with increasing the number of exchanged signals N. The reason is that we can use the more signals to perform the parameter estimation procedure and thus make it closer to perfection when increasing the number of exchanged signals. It is worth mentioning that the one-photon subtraction operation still achieves the optimal performance in the finite-size scenario. Detailed calculation of secret key rate in the finite-size regime is shown in Appendix B.

4 Conclusions

We have suggested a method to improve the performance of the plug-and-play DPMCS protocol by applying non-

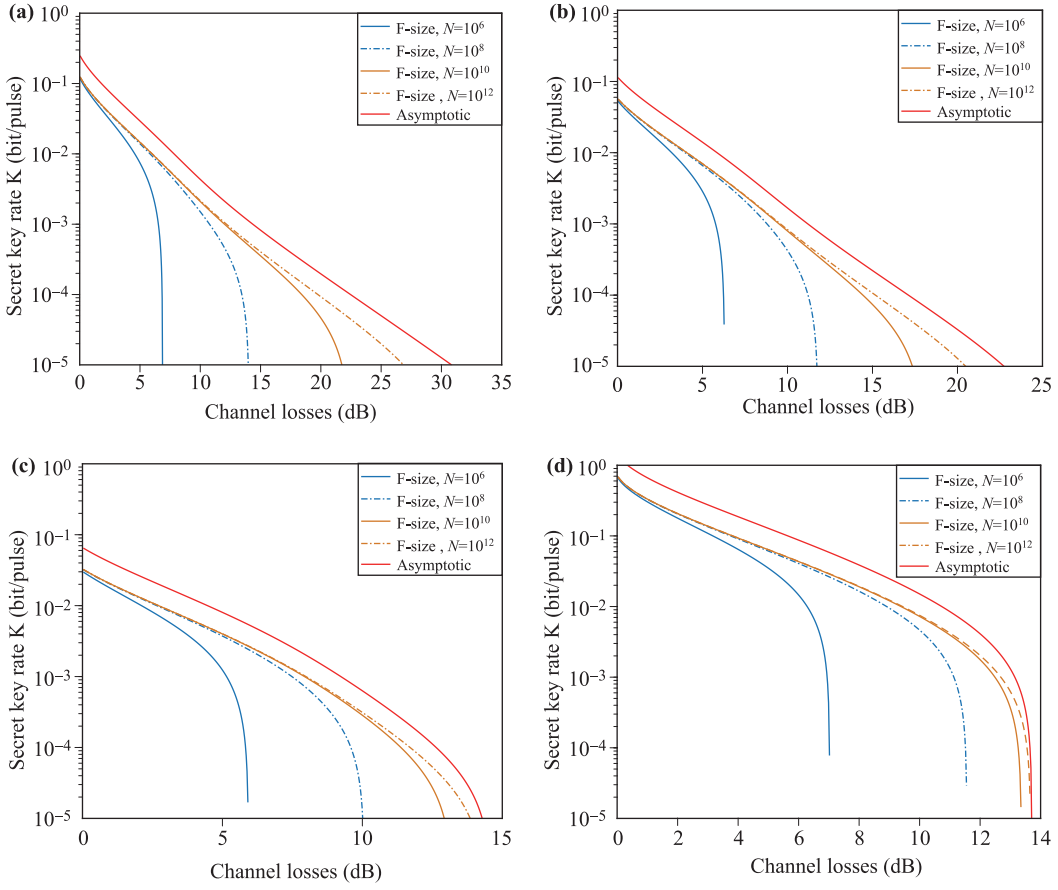

Fig. 7 The finite-size secret key rate of the plug-and-play DPMCS protocol with photon subtraction operation as a function of channel loss under parameter $g = 1.005$ and channel excess noise $\xi = 0.01$. **(a)** One-photon subtraction. **(b)** Two-photon subtraction. **(c)** Three-photon subtraction. **(d)** The original scenario.

Gaussian operations in Bob's entangled source, mainly considering the photon subtraction operation. The proposed method can be easily implemented with existing technologies and thus shows better experimental feasibility in the plug-and-play configuration. We analyze the impact of the transmittance μ of the beam splitter on the photon-subtraction operation and the untrusted source noise weighted by parameter g on the performance of our proposal. The numerical simulations show that the photon subtraction operation can remarkably enhance the maximal transmission distance in the plug-and-play DPMCS protocol, which effectively makes up the drawback of the original plug-and-play DPMCS protocol. However, the unsuitable transmittance μ can lead to the unphysical negative secret key rate and the increase of g can reduce the tolerance in channel losses and decrease the secret key rates. Therefore, it is very important to control these two parameters to improve the performance in practical implementation. Furthermore, we can achieve the tighter bound of the transmission distance by considering the finite-size effect, which is more practical compared with that of achieved in the asymptotic limit.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 61379153 and 61572529).

Appendix A Calculation of asymptotic secret key rate

Here we compute the asymptotic secret key rate of our protocol with reverse reconciliation. Supposing the Fred's state can be controlled by Eve, therefore, a tight security bound can be derived. Without loss of generality, Bob and Alice in this protocol are assumed to perform herterodyne detection and homodyne detection, respectively. Consequently, the lower bound of asymptotic secret key rate can be calculated as

$$K_{asym}^{PS} = P^{\Upsilon_1^m}(m)(\beta I^{PS}(A{:}B) - \chi^{PS}(A{:}E)), \tag{A1}$$

where β is the reconciliation efficiency, $I^{PS}(A{:}B)$ represents the Shannon mutual information shared by Alice and Bob and χ_{AE}^{PS} represents the maximum information available to eavesdropper on the key of Alice.

After passing through the untrusted quantum channel and Alice's detection, the covariance matrix of $\rho_{FBA_2}^{PS}$ can be written as

$$\Gamma_{FBA_2}^{PS} = \begin{pmatrix} aI_2 & c\sigma_z \\ c\sigma_z & bI_2 \end{pmatrix} = \begin{pmatrix} UI_2 & \sqrt{T}S\sigma_z \\ \sqrt{T}S\sigma_z & T(R+\chi_{line})I_2 \end{pmatrix}. \tag{A2}$$

The Shannon mutual information shared by Alice and Bob $I^{PS}(A{:}B)$ can be given by

$$I^{PS}(A{:}B) = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}}, \tag{A3}$$

where $V_B = (a+1)/2$, $V_A = b$, and

$$V_{B|A} = V_B - \frac{TS^2}{2V_A}. \tag{A4}$$

Note that χ_{AE}^{PS} can use the Holevo quantity to bound with form

$$\chi_{AE}^{PS} = S(\rho_E) - \int \mathrm{d}m_A p(m_A) S(\rho_E^{m_A}), \tag{A5}$$

where m_A is the homodyne measurement of Alice with form $m_A = Q_A$, $p(m_A)$ represents the probability density of Alice's homodyne measurement, $\rho_E^{m_A}$ stands for the state of Eve conditional on the homodyne measurement result of Alice, and S represents the von Neumann entropy of the state ρ. Considering the fact that the system FBA_2 can be purified by Eve and the system FBE can be purified by Alice's measurement, therefore, we can obtain $S(\rho_E) = S(\rho_{FBA_2}^{PS})$ and $S(\rho_E^{m_A}) = S(\rho_{FB})$, respectively. Because $S(\rho_E^{m_A})$ is independent of Alice's measurement result m_A, based on this, we can get

$$\begin{aligned}\chi_{AE}^{PS} &= S(\rho_{FBA_2}^{PS}) - S(\rho_{FB}^{m_A}) \\ &= G[(\lambda_1-1)/2] + G[(\lambda_2-1)/2] - G[(\lambda_3-1)/2],\end{aligned} \tag{A6}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, and the symplectic eigenvalues $\lambda_{1,2}$ can be expressed as

$$\lambda_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B^2}), \tag{A7}$$

with

$$\begin{aligned} A &= a^2 + b^2 - 2c^2, \\ B &= ab - c^2. \end{aligned} \tag{A8}$$

To derive $S(\rho_{FB}^{m_A})$, it is necessary for us to calculate the conditional matrix $\Gamma_{FB}^{m_A}$ describing the state $\rho_{FB}^{m_A}$, which can be calculated by

$$\Gamma_{FB}^{m_A} = \Gamma_{FB} - \sigma_{FBA_3}^T (X\Gamma_{A_3}X)^{MP} \sigma_{FBA_3}, \tag{A9}$$

where $X = \mathrm{diag}(1,0,1,0,\ldots,1,0)$ and MP stands for the inverse operation on the range. Therefore, the symplectic eigenvalue λ_3 can be calculated as

$$\lambda_3 = \sqrt{a^2 - \frac{ac^2}{b}}. \tag{A10}$$

In view of above description, we now can derive the lower bound of secret key rate as K_{asym}^{PS} in Eq. (A1) for the modified protocol.

Appendix B Calculation of secret key rate in the finite-size scenario

In the following, to simplify the analysis, the calculation is limited to the reverse reconciliation with homodyne detection. Here N represents the total exchanged signals and n represents the number of signals which is employed for derivation of QKD. The remained signals $s = N - n$ are used for parameter estimation. For the proposed protocol, the finite-size secret key rate is expressed as [27]

$$K_f^{PS} = \frac{nP^{\Upsilon_1^m}(m)}{N}[\beta I^{PS}(A{:}B) - \chi_{\epsilon_{PE}}^{PS}(A{:}E) - \Delta(n)], \tag{B1}$$

where β and $I^{PS}(A{:}B)$ are as the same as the definitions in asymptotic case mentioned in Appendix A. ϵ_{PE} is the failure probability of parameter estimation and $\chi_{\epsilon_{PE}}^{PS}(A{:}E)$ represents the maximum of the Holevo information between Eve's and Alice's classical variable compatible with the statistics except with probability ϵ_{PE}. $\Delta(n)$ is related to the security of the privacy amplification, which can be calculated as

$$\Delta(n) = (2\dim H_A+3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{PB}), \tag{B2}$$

where $\bar{\epsilon}$ and ϵ_{PB} are, respectively, the smoothing parameter and the failure probability of privacy amplification, and H_A stands for the Hilbert space corresponding to the Alice's raw key. We can take $\dim H_A = 2$ since binary bits are usually employed to encode the raw key in our protocol.

In parameter estimation procedure, it is remarkable that the covariance matrix $\Gamma_{\epsilon_{PE}}^{PS}$ plays an important role in calculating $\chi_{\epsilon_{PE}}^{PS}(A{:}E)$. What's more, this matrix can minimize the secret key rate with a probability of at least $1 - \epsilon_{PE}$. In order to calculate the covariance matrix $\Gamma_{\epsilon_{PE}}^{PS}$, we can sample of s couples of correlated variables $(x_i, y_i)_{i=1\cdots s}$. Besides, a normal model is considered for these correlated variables. Within this model, we can use the following relation to link Alice and Bob's data

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

where $t = \sqrt{T}$ and z follows a centered normal distribution with variance $\kappa^2 = 1 + T\xi$. Then the covariance matrix $\Gamma_{\epsilon_{PE}}^{PS}$ can be expressed as

$$\Gamma_{\epsilon_{PE}}^{PS} = \begin{pmatrix} UI_2 & t_{min}S\sigma_z \\ t_{min}S\sigma_z & (t_{min}^2U + \kappa_{max}^2)I_2 \end{pmatrix}, \tag{B4}$$

where t_{min} and κ_{max}^2 stand for minimum of t and maximum of κ^2 compatible with sampled couples. Note that the Maximum-likelihood estimators $\hat{t}$ and $\hat{\kappa}^2$ for the normal linear model, respectively, have the following forms

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

In addition, the following distributions

$$\hat{t} \sim N(t, \frac{\kappa^2}{\sum_{i=1}^s x_i^2}) \quad \text{and} \quad \frac{s\hat{\kappa}^2}{\kappa^2} \sim \chi^2(s-1) \tag{B6}$$

indicate that $\hat{t}$ and $\hat{\kappa}^2$ are independent estimators. In Eq. (B6), t and κ^2 are the true values of the parameters. Based on this, we can calculate t_{min} (the minimum of t) and $\kappa_{\max}^2$ (the maximum of κ^2), namely,

$$\begin{aligned} t_{min} &\approx \hat{t} - z_{\epsilon_{PE}/2}\sqrt{\frac{\hat{\kappa}^2}{sU}}, \\ \kappa_{max}^2 &\approx \hat{\kappa}^2 + z_{\epsilon_{PE}/2}\frac{\sqrt{2}\hat{\kappa}^2}{\sqrt{s}}, \end{aligned} \tag{B7}$$

where $z_{\epsilon_{PE}/2}$ is such that $1 - erf(z_{\epsilon_{PE}/\sqrt{2}})/2 = \epsilon/2$, and $erf(x) = \frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\mathrm{d}t$ is error function. Theoretically, the expected values of $\hat{t}$ and $\hat{\kappa}^2$ can, respectively, be expressed as

$$\begin{aligned} E[\hat{t}] &= \sqrt{T}, \\ E[\hat{\kappa}^2] &= 1 + T\xi. \end{aligned} \tag{B8}$$

Based on above derived equations, t_{min} and κ_{max}^2 can be calculated as follows:

$$\begin{aligned} t_{min} &\approx \sqrt{T} - z_{\epsilon_{PE}/2}\sqrt{\frac{1+T\xi}{sU}}, \\ \kappa_{max}^2 &\approx 1 + T\xi + z_{\epsilon_{PE}/2}\frac{\sqrt{2}(1+T\xi)}{\sqrt{s}}. \end{aligned} \tag{B9}$$

For the error probabilities mentioned above, we can take their optimal value

$$\bar{\epsilon} = \epsilon_{PE} = \epsilon_{PB} = 10^{-10}. \tag{B10}$$

Then the secret key rate in the finite-size scenario can be computed by employing the derived bounds t_{min} and κ_{max}^2.

References

1. H. K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* 8(8), 595 (2014)
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* 74(1), 145 (2002)
3. V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* 81(3), 1301 (2009)
4. 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)
5. W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* 299(5886), 802 (1982)

6. H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* 283(5410), 2050 (1999)
7. M. Gessner, L. Pezzè, and A. Smerzi, Efficient entanglement criteria for discrete, continuous, and hybrid variables, *Phys. Rev. A* 94(2), 020101 (2016)
8. S. Takeda, M. Fuwa, P. van Loock, and A. Furusawa, Entanglement swapping between discrete and continuous variables, *Phys. Rev. Lett.* 114(10), 100501 (2015)
9. 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)
10. D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Continuous-variable quantum key distribution with 1 Mbps secure key rate, *Opt. Express* 23(13), 17511 (2015)
11. 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)
12. 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)
13. 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)
14. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Entanglement-based quantum communication over 144 km, *Nat. Phys.* 3(7), 481 (2007)
15. C. Erven, C. Couteau, R. Laflamme, and G. Weihs, Entangled quantum key distribution over two free-space optical links, *Opt. Express* 16(21), 16840 (2008)
16. Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits, *npj Quantum Inform.* 3(1), 25 (2017)
17. J. Fang, P. Huang, and G. Zeng, Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation, *Phys. Rev. A* 89(2), 022315 (2014)
18. F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* 88(5), 057902 (2002)
19. 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)
20. Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction, *Phys. Rev. A* 95(3), 032304 (2017)
21. P. Jouguet, S. Kunzjacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nat. Photonics* 7(5), 378 (2013)
22. A. Leverrier and P. Grangier, Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation, *Phys. Rev. Lett.* 102(18), 180504 (2009)
23. A. Leverrier and P. Grangier, Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation, *Phys. Rev. A* 83(4), 042312 (2011)
24. F. Grosshans, Collective attacks and unconditional security in continuous variable quantum key distribution, *Phys. Rev. Lett.* 94(2), 020504 (2005)
25. M. Navascués and A. Acín, Security bounds for continuous variables quantum key distribution, *Phys. Rev. Lett.* 94(2), 020505 (2005)
26. 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)
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. A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, *Phys. Rev. Lett.* 114(7), 070501 (2015)
29. 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)
30. X. Q. Dinh, Z. Zhang, and P. L. Voss, A 24 km fiber-based discretely signaled continuous variable quantum key distribution system, *Opt. Express* 17(26), 24244 (2009)
31. J. Lodewyck, M. Bloch, R. Garc'ıa-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuiss-chert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, *Phys. Rev. A* 76(4), 042305 (2007)
32. J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, *Phys. Rev. A* 87(6), 062329 (2013)
33. 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)
34. H. Qin, R. Kumar, and R. Alléaume, Saturation attack on continuous-variable quantum key distribution system, *Proc. SPIE* 8899, *Emerging Technologies in Security and Defence, and Quantum Security II, and Unmanned Sensor Systems X*, 88990N (2013)

35. 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)
36. 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)
37. 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)
38. 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)
39. J. Trapani, B. Teklu, S. Olivares, and M. G. Paris, Quantum phase communication channels in the presence of static and dynamical phase diffusion, *Phys. Rev. A* 92(1), 012317 (2015)
40. B. Teklu, J. Trapani, S. Olivares, and M. G. Paris, Noisy quantum phase communication channels, *Phys. Scr.* 90(7), 074027 (2015)
41. Y. Y. Jin, S. X. Qin, H. Zu, L. Zhou, W. Zhong, and Y. B. Sheng, Heralded amplification of single-photon entanglement with polarization feature, *Front. Phys.* 13(5), 130321 (2018)
42. M. Legre, H. Zbinden, and N. Gisin, Implementation of continuous variable quantum cryptography in optical fibres using a go-&-return configuration, *Quantum Inf. Comput.* 6, 326 (2006)
43. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Phys. Rev. A* 73(2), 022320 (2006)
44. N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, *New J. Phys.* 16(12), 123030 (2014)
45. D. Huang, P. Huang, T. Wang, H. Li, Y. Zhou, and G. Zeng, Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol, *Phys. Rev. A* 94(3), 032305 (2016)
46. P. Huang, G. He, J. Fang, and G. Zeng, Performance improvement of continuous-variable quantum key distribution via photon subtraction, *Phys. Rev. A* 87(1), 012317 (2013)
47. C. J. Liu, W. Ye, W. D. Zhou, H. L. Zhang, J. H. Huang, and L. Y. Hu, Entanglement of coherent superposition of photon-subtraction squeezed vacuum, *Front. Phys.* 12(5), 120307 (2017)
48. Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution, *Phys. Rev. A* 93(1), 012310 (2016)
49. S. Zhang, Y. Dong, X. Zou, B. Shi, and G. Guo, Continuous-variable-entanglement distillation with photon addition, *Phys. Rev. A* 88(3), 032324 (2013)
50. X. G. Meng, J. S. Wang, B. L. Liang, and C. X. Han, Evolution of a two-mode squeezed vacuum for amplitude decay via continuous-variable entangled state approach, *Front. Phys.* 13(5), 130322 (2018)
51. R. García-Patrón and N. J. Cerf, Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution, *Phys. Rev. Lett.* 97(19), 190503 (2006)
52. Y. Shen, X. Peng, J. Yang, and H. Guo, Continuous-variable quantum key distribution with Gaussian source noise, *Phys. Rev. A* 83(5), 052304 (2011)
53. K. Wang, X. T. Yu, and Z. C. Zhang, Two-qubit entangled state teleportation via optimal POVM and partially entangled GHZ state, *Front. Phys.* 13(5), 130320 (2018)
54. M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Single-photon sources and detectors, *Rev. Sci. Instrum.* 82(7), 071101 (2011)
55. A. Kitagawa, M. Takeoka, M. Sasaki, and A. Chefles, Entanglement evaluation of non-Gaussian states generated by photon subtraction from squeezed states, *Phys. Rev. A* 73(4), 042310 (2006)
56. G. Vidal and R. F. Werner, Computable measure of entanglement, *Phys. Rev. A* 65(3), 032314 (2002)