

Continuous-variable measurement-device-independent quantum key distribution via quantum catalysis

Wei Ye,¹ Hai Zhong,¹ Xiaodong Wu,¹ Liyun Hu,^{2,*} and Ying Guo^{1,†}

¹*School of Computer Science and Engineering, Central South University, Changsha 410083, China*

²*Center for Quantum Science and Technology, Jiangxi Normal University, Nanchang 330022, China*

(Dated: July 18, 2019)

The continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) is a promising candidate for the immunity to side-channel attacks, but unfortunately seems to face the limitation of transmission distance in contrast to discrete-variable (DV) counterpart. In this paper, we suggest a method of improving the performance of CV-MDI-QKD involving the achievable secret key rate and transmission distance by using zero-photon catalysis (ZPC), which is indeed a noiseless attenuation process. The numerical stimulation results show that the transmission distance of ZPC-based CV-MDI-QKD under the extreme asymmetric case is better than that of the original protocol. Attractively, in contrast to the previous single-photon subtraction (SPS)-based CV-MDI-QKD, the proposed scheme enables a higher secret key rate and a longer transmission distance. In particular, the ZPC-based CV-MDI-QKD can tolerate more imperfections of detectors than both the original protocol and the SPS-based CV-MDI-QKD.

I. INTRODUCTION

Quantum key distribution (QKD) [1–4] is one of the most mature domains of quantum information processing, aiming to establish a shared key between two distance honest parties (Alice and Bob) over an insecure channel controlled by an eavesdropper (Eve), and its security can be ensured by quantum mechanics. A review of the latest developments in quantum cryptography can be found in [5]. In particular, the first theoretical Bennett-Brassard 1984 (BB84) protocol [6] was proposed, so that the discrete-variable (DV) QKD [6–8] has received increasing attention, and are even available on the commerce. It can perform outstandingly with respect to the transmission distance, but may suffer from the restriction of lower secret key rates due to the dependence of the single-photon generation and detection.

In order to overcome this shortcoming, the continuous-variable (CV) QKD [9–13] has emerged as a new solution to promise higher secret key rates with the help of the homodyne or heterodyne detection rather than photon counters, which make it more attractive from a practical viewpoint. Especially, the coherent-state Gaussian modulated CVQKD [9] has been rigorously proved to be secure against arbitrary collective attacks [14], which are optimal in the asymptotical limit [15]. Moreover, it has an advantage of compatibility with traditional telecommunication technologies, and thus shows the potential to be used for the next-generation quantum communication networks [16]. Unfortunately, when considering the imperfection of the detector from a realistic scenario, it opens the door to potential security loopholes that could be successfully exploited by Eve to execute attack strategies, such as the local oscillator calibration attack [17],

the wavelength attack [18], and the detector saturation attack [19]. To resist these attacks, there are usually two solutions, i.e., the device-independent QKD [20, 21] and the measurement-device-independent (MDI) QKD [22–27]. Different from the former that based on the violation of a Bell inequality [20], the latter is a more practical way to prevent all side-channel attacks on detection where the security of the protocol does not rely on the reliability of the measurement devices. Even so, when comparing with that of DV-MDI-QKD [28, 29], the maximal transmission distance of CV-MDI-QKD is still unsatisfactory. Thus, how to effectively improve the maximal transmission distance in CV-MDI-QKD is an interesting and challenging task.

Till now, many efforts have been devoted to improving its performance in CV-MDI-QKD systems. In general, the use of discrete modulations [30] or quantum operations [31–33] is a viable means. For instance, a discrete-modulated CV-MDI-QKD protocol has been proposed recently, which outperforms the Gaussian-modulated CV-MDI-QKD protocol with respect to the achievable maximal transmission distance since such a discrete modulation has efficient reconciliation error correction codes in the regime of low signal-to-noise ratio [30]. However, it has a problem that the modulation variance should be sufficient low in order to derive the Eve’s Holevo information, which may cause the transmitting power of the quantum signal to be too low and hence has much effect on the performance of QKD. In addition, a novel CV-MDI-QKD protocol using optical amplifiers has shown that it can achieve a higher secret key rate and a longer transmission distance, compared with previous coherent- and squeezed-states protocols [31]. Recently, the photon-subtraction operation [34, 35], which can be emulated by non-Gaussian postsselection [36], has been proved to lengthen the maximal transmission distance of CV-MDI-QKD [32, 33]. More interesting, the single-photon subtraction (SPS) presents the best performance. In spite of the photon subtraction

* Corresponding author: hlyun2008@126.com

† Corresponding author: yingguo@csu.edu.cn

showing its unique advantages, however, there are still restricted to the low success probability of implementing such an operation for a given certain variance of the Einstein-Podolsky-Rosen (EPR) state, thereby resulting in the loss of information between Alice and Bob during the distillation of secret keys. Fortunately, the quantum catalysis operation [37], which can be implemented with existing technologies, may become an alternative method of improving the performance of CVQKD systems in terms of secret key rate and transmission distance, especially in the case of zero-photon catalysis (ZPC) [38, 39]. Currently, the characteristics of quantum catalysis have been widely utilized in quantum coherence [40], nonclassicality [41], entanglement property [42, 43], and so on. As far as we know, there is few applications of quantum catalysis in CV-MDI-QKD. Inspired by the aforementioned analysis, in this paper, we suggest a method to improve the performance of coherent-state CV-MDI-QKD by using the ZPC, which has the characteristics of noiseless attenuation and can keep the Gaussian behavior of Wigner function. The proposed ZPC-based CV-MDI-QKD can lengthen the maximal transmission distance with the achievable high secret key rate. It performs better than the SPS case with respect to both secret key rate and transmission distance.

This paper is structured as follows. In Sec. II, we describes the characteristics of the CV-MDI-QKD protocol involving the ZPC operation. In Sec.III, we show the performance of the ZPC-based CV-MDI-QKD system. The secret key rate of the ZPC-based CV-MDI-QKD is first derived according to the optimality of Gaussian attack. After that, the simulations and performance analysis results are provided. Finally, conclusions are drawn in Sec.IV.

II. THE ZPC-BASED CV-MDI-QKD PROTOCOL

In order to improve the performance of the CVQKD system, we elaborate the ZPC-based CV-MDI-QKD protocol with Gaussian-modulated coherent states in Fig. 1. Among them, Fig. 1(a) shows the prepare-and-measure (PM) scheme of the ZPC-based CV-MDI-QKD protocol. It is easy to implement the PM scheme in practice, but not conducive to security analysis. Consequently, we consider its equivalent entanglement-based (EB) scheme of the ZPC-based CV-MDI-QKD, as depicted in Fig. 1(b), where Alice and Bob respectively prepare an entanglement resource, i.e., EPR_1 and EPR_2 with variances V_A and V_B . They retain modes A_1 and B_1 , and send other modes A_2 and B_2 to an untrusted third party Charlie through the quantum channel with length L_{AC} and L_{BC} , respectively. To reduce equipment requirements, we assume that the ZPC operation is controlled by an untrusted party David, who is close to Alice's station. On top of that, Charlie, first interferes with two received modes \tilde{A}_2 and B_2 via a 50:50 beam splitter and obtains two output modes C_1 and C_2 , and then per-

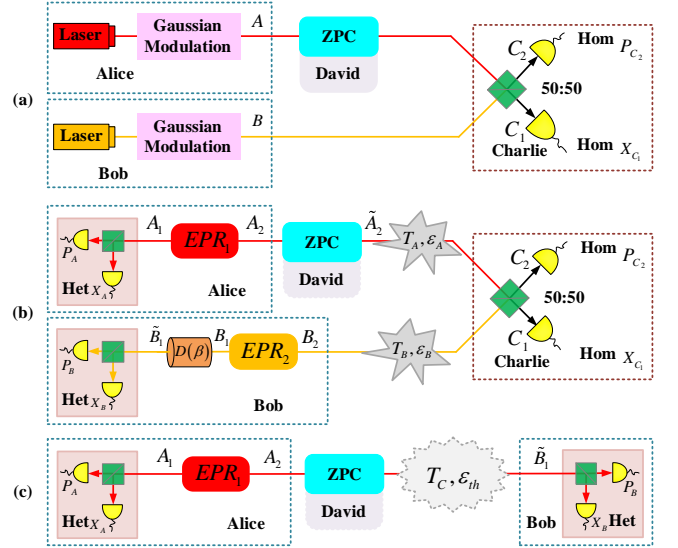


FIG. 1. (Color online) Schematic diagram of the CV-MDI-QKD protocol with the ZPC operation (cyan box). (a) Prepare-and-measure (PM) scheme of the ZPC-based CV-MDI-QKD. (b) Entanglement-based (EB) scheme of the ZPC-based CV-MDI-QKD. (c) Equivalent one-way protocol of the EB scheme of the ZPC-based CV-MDI-QKD under the assumption that Eve is aware of David, Charlie, and Bob's EPR_2 state and displacement except for heterodyne detection. EPR_1 and EPR_2 : Alice's and Bob's two-mode squeezed state, respectively. Het: heterodyne detection. Hom: homodyne detection. $\{X_A, P_A\}$ and $\{X_B, P_B\}$: Alice's and Bob's measurement results of heterodyne detection, respectively. X_{C_1}, P_{C_2} : measurement results of homodyne detection of measuring the X and P quadrature, respectively. $\hat{\Pi}^{off}$: projection operator $|0\rangle\langle 0|$. $T_A(\varepsilon_A), T_B(\varepsilon_B)$: channel parameters for Alice-Charlie and Bob-Charlie. $T_c(\varepsilon_{th})$: equivalent channel transmittance (excess noise). $D(\beta)$: displacement operation of Bob.

forms homodyne detection to obtain a measurement results $\{X_{C_1}, P_{C_2}\}$, which are publicly announced through a classical channel. After receiving $\{X_{C_1}, P_{C_2}\}$, Bob uses a displacement operation $D(\beta)$ with $\beta = g(X_{C_1} + iP_{C_2})$ to modify mode B_1 to \tilde{B}_1 , where g is a gain factor. By using heterodyne detection, Alice and Bob respectively measure modes A_1 and \tilde{B}_1 to obtain their own data $\{X_A, P_A\}$ and $\{X_B, P_B\}$ of which the data can be used for implementing parameter estimations. Finally, a string of secret key can be extracted via data post-processing.

Due to the assumption that both the EPR_2 state and the displacement operation $D(\beta)$ are untrusted, the EB scheme of the ZPC-based CV-MDI-QKD can be equivalent to that of the one-way protocol using heterodyne detection [12, 24, 32, 33], which is illustrated in Fig. 1(c). It is worth noting that, different from the equivalent one-way protocol, the model of CV-MDI-QKD has two lossy quantum channels. Thus, from the point of view of the attack strategies, Eve can take two attacks, e.g. one-mode attack and two-mode attack. However, in a practi-

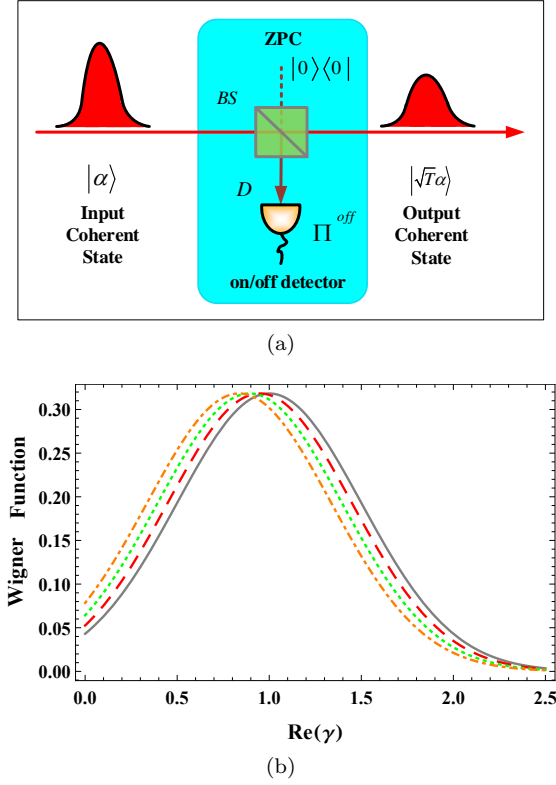


FIG. 2. (Color online) (a) Schematic structure of the ZPC (cyan box) in the PM scheme of CV-MDI-QKD. BS: beam splitter with a transmittance T . $|\alpha\rangle$: coherent state. $\hat{\Pi}^{off}$: projection operator $|0\rangle\langle 0|$. (b) Wigner function of $|\sqrt{T}\alpha\rangle$ and $|\alpha\rangle$ at a given amplitude $|\alpha| = 1$ as a function of $\text{Re}(\gamma)$ in the phase space $\gamma \in (q, p)$ with several different values of T . The highest peaks from right to left correspond to $T \in \{1, 0.9, 0.8, 0.7\}$, respectively. For convenience, here we take $p = 0$, and the black line represents the input coherent state $|\alpha\rangle$.

cal system, adopting a two-mode attack is difficult to be achieved thanks to the immaturity of quantum memory technologies. Furthermore, if two lossy quantum channels are independent, then two-mode attack can be reduced to the one-mode attack. As a result, one can take the security analysis under two Markovian memoryless Gaussian channels where no entanglement can be distributed, so that in CV-MDI-QKD, two quantum channels degenerate into the one-mode channel [44]. In this situation, the optimal attack strategy for Eve is regarded as one-mode collective Gaussian attack.

Now, let us turn attention to the relationship of channel parameters between the ZPC-based CV-MDI-QKD and its equivalent one-way protocol. In Fig. 1(b), since the channels of both Alice-Charlie and Bob-Charlie are both linear, these channels that controlled by Eve can be emulated by using two independent entangling cloner attacks where $T_A = 10^{-\kappa L_{AC}/10}$ ($T_B = 10^{-\kappa L_{BC}/10}$) and ε_A (ε_B) represent the transmittance and excess noise of the channel between Alice (Bob) and Charlie, $\kappa = 0.2$

dB/km. In Fig. 1(c), T_c and ε_{th} respectively represent the transmittance and excess noise of the equivalent one-way protocol, i.e., $T_c = g^2 T_A / 2$, and $\varepsilon_{th} = (\sqrt{2V_B - 2}/g - \sqrt{T_B V_B + T_B})^2 / T_A + T_B (\chi_B - 1) T_A + \chi_A + 1$, where $\chi_j = (1 - T_j) / T_j + \varepsilon_j$ with $j \in \{A, B\}$. In order to minimize the equivalent excess noise ε_{th} , we take into account $g^2 = 2(V_B - 1) / [T_B (V_B + 1)]$, and then have excess noise given by

$$\varepsilon_{th} = \frac{T_B}{T_A} (\varepsilon_B - 2) + \varepsilon_A + \frac{2}{T_A}. \quad (1)$$

From a practical point of view, we need to consider Charlie's inefficient detections, which can be characterized by a quantum efficiency η and an electronic noise v_{el} . Thus, the detection-added noise can be given by $\chi_{hom} = (v_{el} + 1 - \eta) / \eta$, and the total noise referred to the channel input is expressed as $\chi_{tot} = \chi_{line} + 2\chi_{hom} / T_A$ where $\chi_{line} = (1 - T_c) / T_c + \varepsilon_{th}$ refers to the channel-added noise. Note that all the above noises are in the shot-noise units (SNU).

Before evaluating the performance of the ZPC-based CV-MDI-QKD system, we suggest the physical characteristics of quantum catalysis. As shown in Fig. 2, the specific structure of ZPC operation (cyan box) is that a vacuum state $|0\rangle_D$ in auxiliary mode D is sent to a beam splitter (BS) with a transmittance $T = 1 - R$, and subsequently an on/off detector only registers zero-photon (no click). Such a catalytic process can, in fact, be taken as an equivalent operator \hat{O}_0

$$\hat{O}_0 \equiv \text{Tr} [B(T) \hat{\Pi}_{off}] = \sqrt{T} a_2^\dagger a_2, \quad (2)$$

where $B(T)$ is the normal ordering form of a BS operator given by $\exp[(\sqrt{T} - 1)(a_2^\dagger a_2 + d^\dagger d) + (d^\dagger a_2 - d a_2^\dagger)\sqrt{R}]$, and $\hat{\Pi}_{off} = |0\rangle_D \langle 0|$ is one of the projection operators in the on/off detector.

After performing by David the ZPC operation for the incoming EPR_1 state in mode A_2 , where EPR_1 on Alice's side can be prepared by applying a two-mode squeezed operator $S_{A_1 A_2}(r) = \exp[r(a_1 a_2 - a_1^\dagger a_2^\dagger)]$ with a squeezing parameter r into the two-mode vacuum state, i.e.,

$$|\text{EPR}_1\rangle_{A_1 A_2} = S_{A_1 A_2}(r) |00\rangle_{A_1 A_2} = \sqrt{1 - \lambda^2} \exp\left(\lambda a_1^\dagger a_2^\dagger\right) |00\rangle_{A_1 A_2}, \quad (3)$$

where $\lambda = \sqrt{(V_A - 1) / (V_A + 1)}$ with $V_A = \cosh 2r$. The resulting state $|\Phi\rangle_{A_1 \tilde{A}_2}$ can be described as

$$|\Phi\rangle_{A_1 \tilde{A}_2} = \frac{\hat{O}_0}{\sqrt{P_d}} |\text{EPR}_1\rangle_{A_1 A_2} = \sqrt{\frac{1 - \lambda^2}{P_d}} \exp\left(\lambda \sqrt{T} a_1^\dagger a_2^\dagger\right) |00\rangle_{A_1 \tilde{A}_2}, \quad (4)$$

with the normalization factor P_d

$$P_d = \frac{2}{1 + T + R V_A}, \quad (5)$$

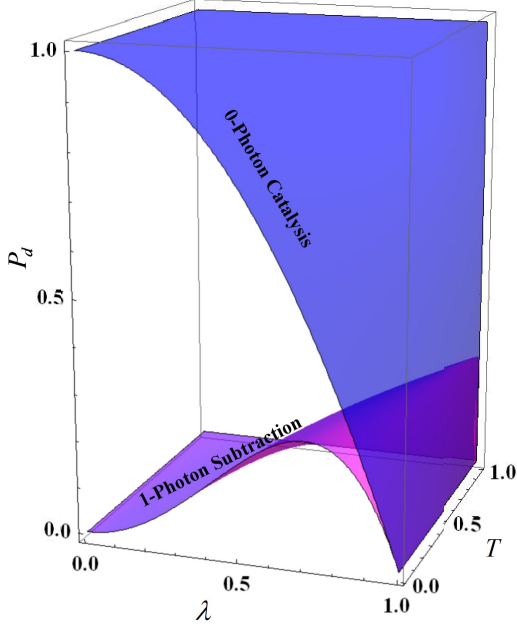


FIG. 3. (Color online) The success probability P_d of the ZPC operation as a function of T and λ . As a comparison, the magenta surface represents the SPS case.

representing the success probability of implementing the ZPC. Based on Eq. (4), the covariance matrix of the state $|\Phi\rangle_{A_1\tilde{A}_2}$ can be calculated as

$$\Gamma_{A_1\tilde{A}_2} = \begin{pmatrix} x\Pi & z\sigma_z \\ z\sigma_z & y\Pi \end{pmatrix}, \quad (6)$$

where Π represents two-dimensional identity matrix, $\sigma_z = \text{diag}(1, -1)$, and x, y, z are given by

$$\begin{aligned} x &= y = \frac{2V_A - RV_A + R}{1 + T + RV_A}, \\ z &= \frac{2\sqrt{T(V_A^2 - 1)}}{1 + T + RV_A}. \end{aligned} \quad (7)$$

As shown in Eq. (2), the ZPC happens to be a noiseless attenuation described as $\hat{O}_0|\alpha\rangle \rightarrow |\sqrt{T}\alpha\rangle$, where $|\alpha\rangle$ is the coherent state in the PM scheme of CV-MDI-QKD. To this end, we plot the Wigner function between the input and output states at a fixed amplitude $|\alpha| = 1$ as a function of $\text{Re}(\gamma)$ in the phase space $\gamma \in (q, p)$ with several different values of $T \in \{1, 0.9, 0.8, 0.7\}$, as shown in Fig. 2b. We can find that the ZPC not only can effectively maintain the Gaussian behavior of Wigner function, but also does not introduce noises in terms of the Gaussian distribution between $|\alpha\rangle$ and $|\sqrt{T}\alpha\rangle$. In addition, unlike the photon-subtraction operation, the ZPC can facilitate the transformation of the target ensemble between modes A_1 and \tilde{A}_2 since the auxiliary vacuum state itself keeps unaffected in mode D . To clearly see this viewpoint, Fig. 3 illustrates the success probabilities

of both ZPC (blue surface) and SPS (magenta surface) with different transmittances T at each λ . We find that the success probability of implementing the ZPC is always better than the SPS case and the gap at a given transmittance T extends with the decrease of λ . This means that the ZPC has the advantage of the success probability over the photon-subtraction case, thereby effectively preventing data loss between Alice and Bob in the process of extracting the secret key. Moreover, after the ZPC, interestingly, the resulting state $|\Phi\rangle_{A_1\tilde{A}_2}$ in Eq. (4) is still an EPR state with an updated squeezing parameter $\lambda\sqrt{T}$.

III. PERFORMANCE ANALYSIS OF THE ZPC-BASED CV-MDI-QKD

So far we have suggested the structure characteristics of the ZPC-based CV-MDI-QKD system. In what follows, we calculate the asymptotic secret key rate under the equivalent one-way CVQKD protocol using heterodyne detection, where Bob performs a reverse reconciliation. We analyze the security through numerical simulations and demonstrate the performance improvement of the ZPC-based CV-MDI-QKD system in terms of secret key rate and transmission distance.

A. Derivation of the secret key rate

It is interesting to note that, after performing the ZPC, the traveling state $|\Phi\rangle_{A_1\tilde{A}_2}$ is still a Gaussian state, which makes it suitable to directly derive the secret key rate from the conventional Gaussian CVQKD. According to the optimality of Gaussian attack [45–47], one can calculate the asymptotic secret key rate K by using the covariance matrix in Eq. (6). Subsequently, the asymptotic secret key rate of the equivalent one-way ZPC-based CVQKD system for reverse reconciliation against one-mode collective Gaussian attack is given by

$$K = P_d \{ \beta I(A:B) - \chi(B:E) \}, \quad (8)$$

where P_d has been defined in Eq. (5), β is the reverse-reconciliation efficiency, $I(A:B)$ denotes the Shannon mutual information between Alice and Bob, and $\chi(B:E)$ represents the Holevo bound between Bob and Eve.

As shown in Fig. 1(c), when the state $|\Phi\rangle_{A_1\tilde{A}_2}$ passes through an untrusted quantum channel characterized by T_c and ε_{th} , the covariance matrix of the state $|\Phi\rangle_{A_1\tilde{B}_1}$ can be described as follows

$$\begin{aligned} \Gamma_{A_1\tilde{B}_1} &= \begin{pmatrix} X\Pi & Z\sigma_z \\ Z\sigma_z & Y\Pi \end{pmatrix} \\ &= \begin{pmatrix} x\Pi & \sqrt{T_c}z\sigma_z \\ \sqrt{T_c}z\sigma_z & T_c(x + \chi_{tot})\Pi \end{pmatrix}. \end{aligned} \quad (9)$$

Thus, the Shannon mutual information $I(A:B)$ can be

calculated as

$$\begin{aligned} I(A:B) &= \log_2 \frac{V_{A_M}}{V_{A_M|B_M}} \\ &= \log_2 \frac{(X+1)(Y+1)}{(X+1)(Y+1)-Z^2}. \end{aligned} \quad (10)$$

In order to obtain the Holevo bound $\chi(B:E)$, we assume that Eve perceives the existence of the untrusted party David and purifies the whole system $\rho_{A_1 \tilde{B}_1 ED}$, so that

$$\begin{aligned} \chi(B:E) &= S(E) - S(E|B) \\ &= S(A_1 \tilde{B}_1) - S(A_1 | \tilde{B}_1^{m_B}), \\ &= \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right), \end{aligned} \quad (11)$$

with the von Neumann entropy

$$G(\varsigma) = (\varsigma + 1) \log_2 (\varsigma + 1) - \varsigma \log_2 \varsigma, \quad (12)$$

where $S(A_1 \tilde{B}_1)$ is a function of the symplectic eigenvalues $\lambda_{1,2}$ of $\Gamma_{A_1 \tilde{B}_1}$ given by $\lambda_{1,2}^2 = (\Delta \pm \sqrt{\Delta^2 - 4\xi^2})/2$, with $\Delta = X^2 + Y^2 - 2Z^2$ and $\xi = XY - Z^2$, and Eve's condition entropy $S(A_1 | \tilde{B}_1^{m_B})$ based on Bob's measurement result m_B , is a function of the symplectic eigenvalues λ_3 of $\Gamma_{A_1}^{B_1^{m_B}} = \Gamma_{A_1} - \sigma_{A_1 B_1'} (\Gamma_{B_1'} + \Pi)^{-1} \sigma_{A_1 B_1'}^T$, which is given by $\lambda_3 = X - Z^2/(Y+1)$.

B. Simulation results and analysis

In the traditional CV-MDI-QKD protocols, the performance of the symmetric case ($L_{AC} = L_{BC}$) is worse than that of the asymmetric case ($L_{AC} \neq L_{BC}$) with respect to the maximal transmission distance. In particular, for the extreme asymmetric case $L_{BC} = 0$, the total transmission distance $L_{AB} = L_{AC} + L_{BC}$ can reach the longest ultimate transmission distance. Based on this circumstance, we consider the performance of CV-MDI-QKD protocol in the extreme asymmetric case involving ZPC and SPS. To compare with the previous work [32], we set $V_A = V_B = 40$, $\varepsilon_A = \varepsilon_B = 0.002$ [13] and $\beta = 0.95$. Moreover, taking Charlie's homodyne detection imperfections into account, in the following we consider the ideal detection ($\eta = 1, v_{el} = 0$) and the imperfect detection ($\eta = 0.975, v_{el} = 0.002$), respectively.

For the optimal transmittance T corresponding to Fig. 4(b), Fig. 4(a) shows the secret key rate as a function of L_{AB} involving the ideal and imperfect detections where the black dotted line stands for the traditional protocol. We find that the ZPC-based CV-MDI-QKD protocol (blue dashed line), even in the imperfect detection case, can be superior to the traditional protocol. Namely, the ZPC can be used not only for increasing the secret key rate, but also for lengthening the transmission

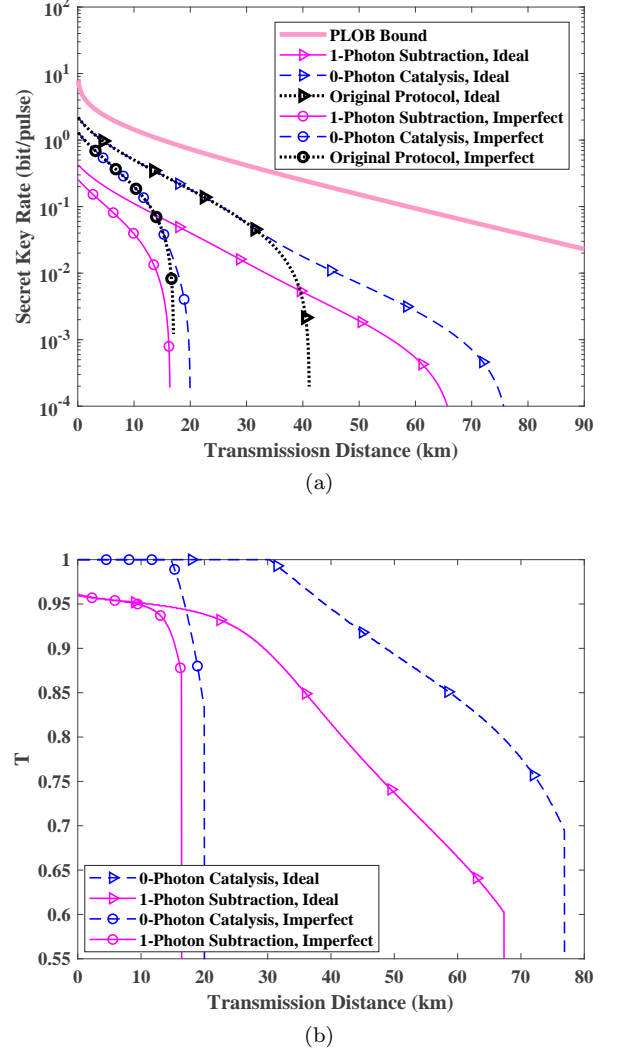


FIG. 4. (Color online) (a) The maximal secret key rate of the ZPC-based CV-MDI-QKD (blue dashed line) versus the transmission distance under the ideal and imperfect detections. (b) The optimal transmittance T versus the transmission distance corresponding to (a). To make comparisons, the black dotted line stands for the original protocol. The thin magenta solid line stands for the SPS-based CV-MDI-QKD. The thick pink solid line stands for the PLOB bound.

distance. Compared with the performance of the original protocol, the maximal transmission distance L_{AB} of the ZPC-based CV-MDI-QKD for a given secret key rate 10^{-4} bit/pulse can be extended approximately 35.6 km for the ideal detection (2.95 km for the imperfect detection). Even if the transmittance T of BS is optimized, the performance of the proposed protocol is equivalent to that of the original protocol at the short-transmission distance. The reason is that there is no quantum catalytic effect when $T = 1$ of the BS.

Moreover, the tolerable excess noise is another common criteria for evaluating the performance of CVQKD

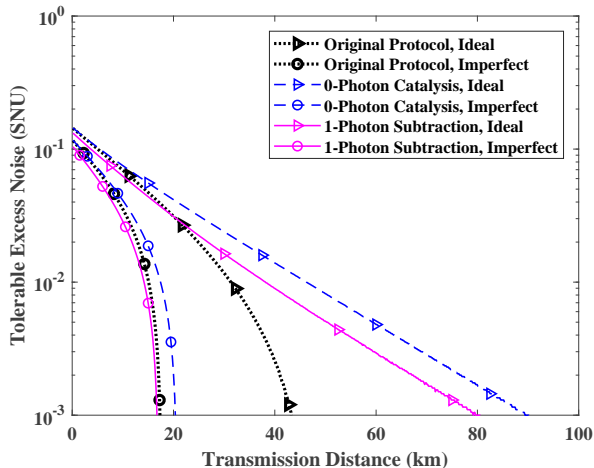


FIG. 5. (Color online) The maximal tolerable excess noise of the ZPC-based CV-MDI-QKD (blue dashed line) versus the transmission distance under the ideal and imperfect detections. As comparisons, the black dotted line stands for the original protocol. The thin magenta solid line stands for the SPS-based CV-MDI-QKD.

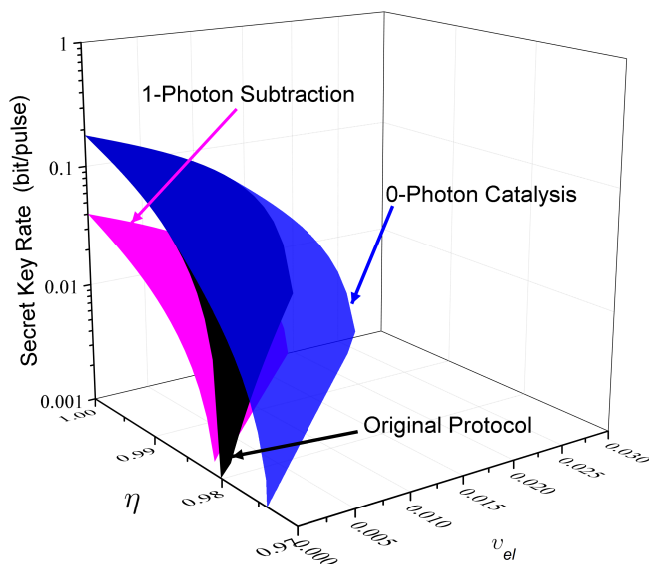


FIG. 6. (Color online) The secret key rate of the ZPC-based CV-MDI-QKD protocol (blue surface), the SPS-based CV-MDI-QKD protocol (magenta surface) and the original protocol (black surface) as a function of detection efficiency η and electronic noise v_{el} at a given transmission distance $L_{AB} = 20$ km.

protocols. In Fig. 5, we illustrate the maximal tolerable excess noise of the ZPC-based CV-MDI-QKD system as a function of L_{AB} with two cases of the ideal detection and the imperfect detection, when optimized over the transmittance T . The numerical simulation results show that, with the same parameters, the proposed protocol presents better than other cases in terms of the maximal tolerable excess noise. The reason is that the

ZPC is indeed regarded as a noiseless attenuation, which has been proved to increase the maximal tolerable excess noise [48]. For instance, if $\varepsilon \sim 0.001$, the proposed protocol enables to lengthen the transmission distance up to 90 km for the ideal detection (20 km for the imperfect detection) between two remote users, which indicates that the ZPC makes the CV-MDI-QKD protocol more tolerant to excess noise.

In order to highlight the advantages of quantum catalysis, we show the performance of the SPS-based CV-MDI-QKD system (thin magenta solid line) with respect to the secret key rate and tolerable excess noise, shown in Fig. 4(a) and Fig. 5. We find that the performance of our protocol with the same parameters surpasses the SPS-based CV-MDI-QKD case. The reason is that the success probability of the ZPC is higher than that of SPS, thereby enabling to avoid the loss of information during the extraction of the secret key rate by Alice and Bob. In addition, the physical mechanism of the ZPC is regarded as a noiseless attenuation, which makes signal states strongly indistinguishable to Eve and thus reduces the amount of information stolen. Despite its appealing merits, the proposed protocol is closer to the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [49] that represents the ultimate limit of repeaterless communication than the SPS-based CV-MDI-QKD.

From the above-mentioned analysis, it shows that not only are channel imperfections the threat to the security of CV-MDI-QKD protocols, but also both detection efficiency η and electronic noise v_{el} can affect the information on the secret key rate. Therefore, from this practical viewpoint, Fig. 6 shows the performance comparisons of the ZPC-based CV-MDI-QKD, the SPS-based CV-MDI-QKD and the original protocol as a function of η and v_{el} . It is found that under the framework of a metropolitan area the performance of CV-MDI-QKD protocol using the ZPC is superior to the other two cases when both detection efficiency η and electronic noise v_{el} take a definite value. That is to say, our protocol allows lower detection efficiency and higher electronic noise in the case of achieving the same performance.

IV. CONCLUSION

In summary, under the extreme asymmetric case, we have suggested an approach to performance improvement of the CV-MDI-QKD involving the ZPC that can be seen as a noiseless attenuation. We derive the secret key rate of the the ZPC-based CV-MDI-QKD system in the asymptotic regime. The simulation results show that the performance of our protocol can outperform that of the original protocol in terms of the maximal tolerable excess noise and the achievable transmission distance, which means that exploiting such a ZPC operation can provide guidance in designing long distance CVQKD systems. Furthermore, to highlight the advantages of the ZPC in CV-MDI-QKD, as a comparison, the previous

SPS-based CV-MDI-QKD is presented. We find that the proposed protocol is superior to the previous SPS case with respect to the secret key rate, the transmission distance and the tolerable excess noise. In particular, from a practical implementation, adding the ZPC operation makes the CV-MDI-QKD protocol more tolerant of homodyne detection imperfections under the framework of a metropolitan area in contrast to the SPS case. Although both of them cannot overcome the PLOB bound at any transmission distance, this prompts us to find other approaches (e.g., two-way CVQKD [50]) to break through the bound.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61572529, 61821407, 11664017), the Outstanding Young Talent Program of Jiangxi Province (20171BCB23034) and the Postgraduate Independent Exploration and Innovation Project of Central South University (Grant No: 2019zzts070).

-
- [1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lutkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* 81, 1301 (2009).
 - [2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* 74, 145 (2002).
 - [3] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, *Rev. Mod. Phys.* 84, 621 (2012).
 - [4] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, *Rev. Mod. Phys.* 77, 513 (2005).
 - [5] 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 [quant-ph] (2019).
 - [6] C. H. Bennett and G. Brassard, In proceedings of the IEEE international conference on computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York, 1984), pp. 175–179.
 - [7] M. Gessner, L. Pezze and A. Smerzi, Efficient entanglement criteria for discrete, continuous, and hybrid variables, *Phys. Rev. A* 94, 020101 (2016).
 - [8] V. Scarani and Renato Renner, Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing, *Phys. Rev. Lett.* 100, 200501 (2008).
 - [9] T. C. Ralph, Security of continuous-variable quantum cryptography, *Phys. Rev. A* 62, 062306 (2000).
 - [10] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* 88, 057902 (2002).
 - [11] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Broui, S. W. McLaughlin, and P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, *Phys. Rev. A* 76, 042305 (2007).
 - [12] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum cryptography without switching, *Phys. Rev. Lett.* 93, 170504 (2004).
 - [13] 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, 378–381 (2013).
 - [14] F. Grosshans, Collective attacks and unconditional security in continuous variable quantum key distribution, *Phys. Rev. Lett.* 94, 020504 (2005).
 - [15] R. Renner and J. I. Cirac, de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography, *Phys. Rev. Lett.* 102, 110504 (2009).
 - [16] H. J. Kimble, The quantum internet, *Nature (London)* 453, 1023 (2008).
 - [17] 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, 022339 (2013).
 - [18] 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, 062329 (2013).
 - [19] H. Qin, R. Kumar, and R. Alleaume, Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, *Phys. Rev. A* 94, 012325 (2016).
 - [20] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, *Phys. Rev. Lett.* 98, 230501 (2007).
 - [21] K. Marshall and C. Weedbrook, Device-independent quantum cryptography for continuous variables, *Phys. Rev. A* 90, 042311 (2014).
 - [22] 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. Photon.* 9, 397 (2015).
 - [23] X. Y. Zhang, Y. C. Zhang, Y. J. Zhao, X. Y. Wang, S. Yu, and H. Guo, Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* 96, 042334 (2017).
 - [24] Z. Y. Li, Y. C. Zhang, F. H. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* 89, 052301 (2014).
 - [25] 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, 042335 (2014).
- [26] Chandan Kumar, Jaskaran Singh, Soumyakanti Bose, and Arvind, Coherence assisted non-Gaussian measurement device independent quantum key distribution, arXiv:1906.11799 [quant-ph] (2019).
 - [27] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, *Phys. Rev. Lett.* 108, 130502 (2012).
 - [28] H. K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* 108, 130503 (2012).
 - [29] 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, 061101 (2013).
 - [30] H. X. Ma, P. Huang, D. Y. Bai, T. Wang, S. Y. Wang, W. S. Bao, and G. H. Zeng, Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation, *Phys. Rev. A* 99, 022322 (2019).
 - [31] P. Wang, X. Y. Wang, and Y. M. Li, Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers, *Phys. Rev. A* 99, 042309 (2019).
 - [32] Y. J. Zhao, Y. C. Zhang, B. J. Xu, S. Yu, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction, *Phys. Rev. A* 97, 042328 (2018).
 - [33] H. X. Ma, P. Huang, D. Y. Bai, S. Y. Wang, W. S. Bao, and G. H. Zeng, Continuous-variable measurement-device-independent quantum key distribution with photon subtraction, *Phys. Rev. A* 97, 042329 (2018).
 - [34] T. J. Bartley, P. J. D. Crowley, A. Datta, J. Nunn, L. Zhang, and I. Walmsley, Strategies for enhancing quantum entanglement by local photon subtraction, *Phys. Rev. A* 87, 022313 (2013).
 - [35] J. N. Wu, S. Y. Liu, L. Y. Hu, J. H. Huang, Z. L. Duan, and Y. H. Ji, Improving entanglement of even entangled coherent states by a coherent superposition of photon subtraction and addition, *J. Opt. Soc. Am. B* 32, 2299 (2015).
 - [36] Z. Y. Li, Y. C. Zhang, X. Y. Wang, B. J. Xu, X. Peng, and H. Guo, Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution, *Phys. Rev. A* 93, 012310 (2016).
 - [37] A. I. Lvovsky and J. Mlynek, Quantum-optical catalysis: generating nonclassical states of light by means of linear optics, *Phys. Rev. Lett.* 88, 250401 (2002).
 - [38] Y. Guo, W. Ye, H. Zhong, and Q. Liao, Continuous-variable quantum key distribution with non-Gaussian quantum catalysis, *Phys. Rev. A* 99, 032327 (2019).
 - [39] W. Ye, H. Zhong, Q. Liao, D. Huang, L. Y. Hu, and Y. Guo, Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis, *Opt. Express* 27, 17186-17198 (2019).
 - [40] S. L. Zhang and X. D. Zhang, Photon catalysis acting as noiseless linear amplification and its application in coherence enhancement, *Phys. Rev. A* 97, 043830 (2018).
 - [41] L. Y. Hu, J. N. Wu, Z. Y. Liao, and M. S. Zubairy, Multiphoton catalysis with coherent state input: Nonclassicality and decoherence, *J. Phys. B: At. Mol. Phys.* 49, 175504 (2016).
 - [42] L. Y. Hu, Z. Y. Liao, and M. S. Zubairy, Continuous-variable entanglement via multiphoton catalysis, *Phys. Rev. A* 95, 012310 (2017).
 - [43] W. D. Zhou, W. Ye, C. J. Liu, L. Y. Hu, and S. Q. Liu, Entanglement improvement of entangled coherent state via multiphoton catalysis, *Laser Phys. Lett.* 15, 065203 (2018).
 - [44] S. Pirandola, Entanglement reactivation in separable environments, *New J. Phys.* 15, 113046 (2013).
 - [45] M. Navascues, F. Grosshans, and A. Acin, Optimality of gaussian attacks in continuous-variable quantum cryptography, *Phys. Rev. Lett.* 97, 190502 (2006).
 - [46] R. Garcia-Patron and N. J. Cerf, Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution, *Phys. Rev. Lett.* 97, 190503 (2006).
 - [47] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of gaussian quantum states, *Phys. Rev. Lett.* 96, 080502 (2006).
 - [48] J. Fiurasek and N. J. Cerf, Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution, *Phys. Rev. A* 86, 060302(R) (2012).
 - [49] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* 8, 15043 (2017).
 - [50] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Continuous-variable quantum cryptography using two-way quantum communication, *Nat. Phys.* 4, 726-730 (2008).