Continuous-variable quantum key distribution with non-Gaussian quantum catalysis

Ying Guo,[1] Wei Ye,[1] Hai Zhong,[1] and Qin Liao[2,*]
[1]*School of Automation, Central South University, Changsha 410083, China*
[2]*School of Information Science and Engineering, Hunan University, Changsha 410082, China*

(Received 17 November 2018; published 18 March 2019)

The non-Gaussian operation can be used not only to enhance and distill the entanglement between Gaussian entangled states, but also to improve the performance of quantum communications. In this paper, we propose a non-Gaussian continuous-variable quantum key distribution (CVQKD) by using quantum catalysis (QC), which is an intriguing non-Gaussian operation in essence that can be implemented with current technologies. We perform quantum catalysis on both ends of the Einstein-Podolsky-Rosen pair prepared by a sender, Alice, and find that for the single-photon QC-CVQKD, the bilateral symmetrical quantum catalysis performs better than the single-side quantum catalysis. Attributing to characteristics of an integral within an ordered product of operators, we find that the quantum-catalysis operation can improve the entanglement property of Gaussian entangled states by enhancing the success probability of non-Gaussian operation, leading to the improvement of the QC-CVQKD system. As a comparison, the QC-CVQKD system involving zero-photon and single-photon quantum catalysis outperforms the previous non-Gaussian CVQKD scheme via photon subtraction in terms of a secret key rate, maximal transmission distance, and tolerable excess noise.

DOI: 10.1103/PhysRevA.99.032327

I. INTRODUCTION

Quantum key distribution (QKD) [1–5], as one of the mature practical applications in quantum information processing, allows two distant legitimate parties (normally say a sender Alice and a receiver Bob) to establish a set of secure keys even in the presence of the untrusted environment controlled by an eavesdropper (Eve), and its unconditional security can be guaranteed by the laws of quantum physics, e.g., the uncertainty principle [6] and the noncloning theorem [7]. In general, QKD mainly includes two families, namely, discrete-variable quantum key distribution (DVQKD) and continuous-variable quantum key distribution (CVQKD) [2,8–15]. In the CVQKD system, the sender Alice encodes information on the quadratures of the optical field with Gaussian modulation, and the receiver Bob decodes the secret information with high-speed and high-efficiency homodyne or heterodyne detection so that this system promises a more higher secret key rate than its DVQKD and, thus, has been a subject of increasing interest in recent years [16,17]. In addition, since the security proofs of the Gaussian-modulated CVQKD protocols against collective attacks [16,18] and coherent attacks [19,20] have been proven theoretically [21–23], the Gaussian-modulated CVQKD protocols take on the potential application prospects of long-distance communication. Among them, the Grosshans-Grangier 2002 protocol [17] performs outstandingly over short distances but seems unfortunately to be facing the problem of long-secure distances compared with its DVQKD counterpart.

Untill now, many remarkable theoretical and experimental efforts have been devoted to extending the maximal transmission distance with high rates in CVQKD systems [23–28]. By the use of multidimensional reconciliation protocols in the regime of low signal-to-noise ratio (SNR) [23], it was demonstrated experimentally that CVQKD over an 80-km transmission distance can be realized. The reason is that the multidimensional reconciliation is, in a sense, to design a suitable reconciliation code with high efficiency even at low SNR, which can increase the secure distance [28]. Alternatively, the discrete modulation protocols, such as the four-state protocol [13,27,29,30] and the eight-state protocol [31] were shown to improve the secure distance as there does exist suitable error-correlation codes with high efficiency for discrete possible values at low SNR. Especially for the eight-state protocol, not only can the secret key rate be improved, but also a transmission distance of more than 100 km can be achieved [31,32]. From a practical point of view, the maximal transmission distance and the unconditional security of the secret key are usually disturbed by the environmental noise and dissipation. To solve these problems, the methods of source monitoring [33] and a linear optics cloning machine [34] have been proposed subsequently.

Thanks to the development of experimental techniques, on the other hand, some quantum operations have been used to improve the performance of the CVQKD in terms of the secret key rate and tolerable excess noise. For example, a heralded noiseless amplifier [26,27,35] was proposed to improve the maximal transmission distance roughly by the equivalent of 20 $\log_{10} g$-dB losses resulting from the compensation of the losses [27]. Recently, due to the fact that the non-Gaussian operation can be used for improving the entanglement [36–38] and quantum teleportation in the CV system [39,40], the photon-subtraction operation, which is one of the non-Gaussian operations, has been proposed to improve the secret key rate, the maximal tolerable excess noise, and

*Corresponding author: llqqlq@hnu.edu.cn

the transmission distance of the CVQKD protocol [11,14,15,29]. In particular, the single-photon-subtraction (SPS) operation in the enhanced CVQKD protocol outperforms other numbers of photon subtraction. Unfortunately, the success probability for implementing this single-photon subtraction operation at the variance of two-mode squeezed vacuum (TMSV) state $V = 20$ is limited to below 0.25, which may lead to loss more information between Alice and Bob in the process of extracting the secret key. In order to overcome the limitation, in this paper, we propose an improved performance scheme for CVQKD by using another non-Gaussian operation, the quantum catalysis (QC) [41], which can be implemented with current experimental technologies. Attractively, the quantum-catalysis operation is a feasible way to enhance the nonclassicality [42], and the entanglement property of Gaussian entangled states [43] thereby has become one of the research hot spots in quantum physics. Different from the previous studied photon-subtraction operations, although no photon is subtracted and added in the quantum-catalysis process, quantum catalysis can be applied to facilitate the conversion of the target ensemble, which could prevent the loss of information effectively. Besides, due to the problem of noncommutativity in quantum operators, the integral of a classical function cannot be applied directly to the quantum operator integral. In order to deal with the above problem, the technique of an integral within an ordered product (IWOP) of operators including the normal ordering, antinormal ordering, and Weyl ordering was introduced in Refs. [44–47]. With the help of this technique, we can easily obtain the analytical expression for the equivalent operator of quantum catalysis. Numerical simulation shows that the entanglement and the success probability for implementing quantum catalysis can be improved efficiently. Specifically, the success probability for implementing zero-photon quantum catalysis can be dramatically enhanced when compared with the previous CVQKD with single-photon subtraction. In addition, we illustrate the performance of QC-CVQKD with different photon-catalyzed numbers and find that zero-photon and single-photon catalysis presents the best performance when optimized over the transmittance T of the untrusted party's beam splitter (BS).

This paper is organized as follows. In Sec. II, we suggest a quantum-catalysis operator and detail the process of QC-CVQKD. In Sec. III, the success probability and the entanglement property for implementing quantum catalysis are analyzed, and the security analysis for the QC-CVQKD system is subsequently discussed. Finally, conclusions are drawn in Sec. IV.

II. QUANTUM-CATALYSIS-BASED CVQKD

To make the derivation self-contained, we suggest a quantum-catalysis operator by means of the IWOP technique and then detail the QC-CVQKD.

A. Quantum-catalysis operation

As shown in Fig. 1(a), an n-photon Fock state $|n\rangle$ in auxiliary mode C is injected at one of the input ports of the BS with transmittance T_2, and simultaneously detected

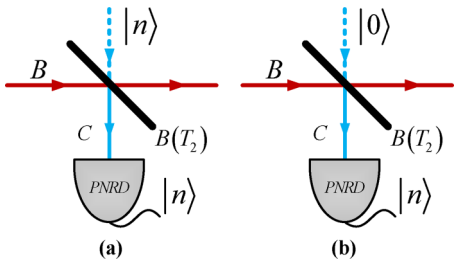

FIG. 1. Schematic of the non-Gaussian operations. (a) The QC. An n-photon Fock state $|n\rangle$ in auxiliary mode C is split on the asymmetrical BS with transmittance T_2. Subsequently, n photons at the auxiliary mode are registered by an ideal photon number resolving detector (PNRD), which is the so-called n-photon quantum catalysis represented by an equivalent operator $\hat{O}_n$. (b) The n-photon-subtraction operation. Vacuum state $|0\rangle$ in auxiliary mode C is injected into the asymmetrical BS with transmittance T_2. Likewise, n photons at the auxiliary mode are detected by the ideal PNRD.

by the PNRD at the corresponding output port of the BS, which is the so-called n-photon catalysis because the auxiliary n-photon Fock state remains unaffected by this interaction. It is worth noting that the number of detected photons by the PNRD is consistent with the number of input photons, which can facilitate the conversion of the target ensemble in mode B. In principle, it is reasonable and correct not to change the effect of modifying the photon number population in the catalytic process. Besides, this process is often regarded as an equivalent operator $\hat{O}_n$ given by

$$\hat{O}_n \equiv {}_C\langle n|B(T_2)|n\rangle_C, \tag{1}$$

where $B(T_2)$ is the BS operator with transmittance T_2. To obtain the specific expression of the equivalent operator $\hat{O}_n$, we employ the normally ordering form of $B(T_2)$ by the IWOP technique and the coherent-state representation of Fock state $|n\rangle$, which are expressed as $B(T) = :\exp[(\sqrt{T_2}-1)(b^\dagger b + c^\dagger c) + (c^\dagger b - c b^\dagger)\sqrt{1-T_2}]:$ and $|n\rangle = 1/\sqrt{n!}\frac{\partial^n}{\partial \beta^n}\|\beta\rangle|_{\beta=0}$, respectively, where the notations $:\cdot\cdot:$ and $\|\beta\rangle = \exp(\beta c^\dagger)|0\rangle$ represent the normal ordering of an operator and an un-normalized coherent state, respectively. As a result, Eq. (1) can be described as

$$\hat{O}_n = :L_n\left(\frac{1-T_2}{T_2}b^\dagger b\right):(\sqrt{T_2})^{b^\dagger b+n}, \tag{2}$$

where $L_n(\cdot)$ denotes the Laguerre polynomials (see Refs. [42,43] for the detailed calculation). By using the generating function of the Laguerre polynomials, i.e.,

$$L_n(x) = \frac{\partial^n}{n!\,\partial\gamma^n}\left\{\frac{e^{(-x\gamma)/(1-\gamma)}}{1-\gamma}\right\}_{\gamma=0}, \tag{3}$$

and the operator relation $e^{\lambda b^\dagger b} = :\exp\{(e^\lambda - 1)b^\dagger b\}:$, Eq. (2) can be further rewritten as

$$\hat{O}_n = G_{T_2}(b^\dagger b)(\sqrt{T_2})^{b^\dagger b+n}, \tag{4}$$

where

$$G_{T_2}(b^\dagger b) = \frac{\partial^n}{n!\,\partial\gamma^n}\left\{\frac{1}{1-\gamma}\left(\frac{1-\gamma/T_2}{1-\gamma}\right)^{b^\dagger b}\right\}_{\gamma=0}. \tag{5}$$

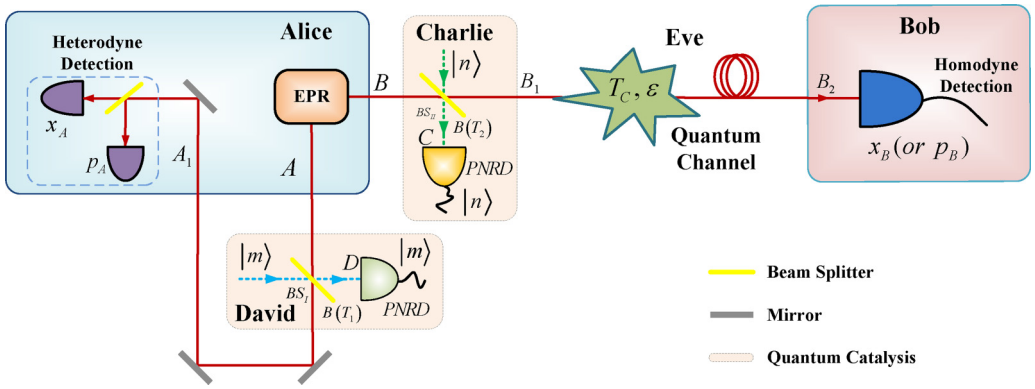

FIG. 2. Schematic of QC-CVQKD. Einstein-Podolsky-Rosen (EPR): two-mode squeezed vacuum state. $|m\rangle$ and $|n\rangle$: m-photon and n-photon Fock states. $\mathrm{PD_I}$ and $\mathrm{PD_{II}}$: photon detector by conditional measurement of $|m\rangle$ and $|n\rangle$. $B(T_1)$ and $B(T_2)$: $\mathrm{BS_I}$ operator with transmittance T_1 and the $\mathrm{BS_{II}}$ operator with transmittance T_2. T_c and ε: quantum channel parameters.

From Eq. (4), we find that the quantum-catalysis operation belongs to a kind of non-Gaussian operation. Moreover, as shown in Fig. 1(a), for an arbitrary input state $|\varphi\rangle_{\mathrm{in}}$ in mode B, the output state $|\psi\rangle_{\mathrm{out}}$ can be expressed as $|\psi\rangle_{\mathrm{out}} = \hat{O}_n/\sqrt{p}|\varphi\rangle_{\mathrm{in}}$ with the success probability p for implementing the n-photon catalysis $\hat{O}_n$, which is beneficial for calculating the analytical expressions of the Alice output state and the covariance matrix between Alice and Bob in the following. In addition, different from the n-photon-subtraction operation shown in Fig. 1(b), the auxiliary n-photon Fock state will not be destroyed at all in the n-photon catalysis operation. Such an operation facilitates the transformation between input and output states thereby effectively preventing useful information from being lost. However, no matter how many photons are catalyzed or subtracted, there is no quantum-catalysis or photon-subtraction effect when $T_2 = 1$.

B. The CVQKD protocol with quantum catalysis

In what follows, we elaborate the schematic of the QC-CVQKD protocol as shown in Fig. 2. The sender Alice generates a TMSV state (which is also called an EPR pair) involving two modes A and B with a modulation variance V, which is usually expressed as the two-mode squeezed operator $S_2(r) = \exp\{r(a^\dagger b^\dagger - ab)\}$ on the two-mode vacuum state $|0,0\rangle_{AB}$, i.e.,

$$|\mathrm{TMSV}\rangle_{AB} = S_2(r)|0,0\rangle_{AB} = \sqrt{1-\lambda^2}\sum_{l=0}^{\infty}\lambda^l|l,l\rangle_{AB}, \tag{6}$$

where $\lambda = \tanh r = \sqrt{(V-1)/(V+1)}$ for $V = 2\alpha^2 + 1$ and $|l,l\rangle_{AB} = |l\rangle_A \otimes |l\rangle_B$ denotes the two-mode Fock state of both modes A and B. After that, she performs m-photon and n-photon catalysis operations in modes A and B, respectively, giving birth to state $|\psi\rangle_{A_1B_1}$. Note that, before Alice performs heterodyne detection, inserting another quantum-catalysis operation $\hat{O}_m$ is designed to figure out what effect quantum catalysis has on the information between Alice and Bob when comparing with the single-side quantum-catalysis $\hat{O}_n$ case. Besides, to lower requirements for the apparatus perfection of the quantum catalysis and assume that the eavesdropper Eve is more powerful, the quantum catalysis of both $\hat{O}_m$ and $\hat{O}_n$, respectively, should be held by the untrusted parties David and Charlie controlled by Eve. According to the aforementioned method of the quantum-catalysis operation, likewise in Eq. (4), we obtain the m-photon quantum-catalysis operation, i.e.,

$$\hat{O}_m = G_{T_1}(a^\dagger a)(\sqrt{T_1})^{a^\dagger a + m}, \tag{7}$$

with the notation $G_{T_1}(a^\dagger a)$ given by

$$G_{T_1}(a^\dagger a) = \frac{\partial^m}{m!\,\partial\tau^m}\left\{\frac{1}{1-\tau}\left(\frac{1-\tau/T_1}{1-\tau}\right)^{a^\dagger a}\right\}_{\tau=0}. \tag{8}$$

Then, the yielded state $|\psi\rangle_{A_1B_1}$ turns out to be

$$\begin{aligned}|\psi\rangle_{A_1B_1} &= \frac{\hat{O}_m\hat{O}_n}{\sqrt{P_d}}|\mathrm{TMSV}\rangle \\ &= \sum_{l=0}^{\infty}\frac{W_0}{\sqrt{P_d}}\frac{\partial^m}{\partial\tau^m}\frac{\partial^n}{\partial\gamma^n}\frac{W^l}{(1-\tau)(1-\gamma)}|l,l\rangle_{AB},\end{aligned} \tag{9}$$

where P_d denotes the success probability of implementing quantum catalysis, which is an important indicator that affects the mutual information in the process of distilling a common secret key between Alice and Bob and can be calculated as

$$P_d = W_0^2\Re^{m,n}\left\{\frac{\Pi}{1-W_1W}\right\}, \tag{10}$$

with $\Re^{m,n}$, Π, W_0, W, and W_1 defined in Eq. (A2). Detailed calculations of the success probability P_d can be shown in Appendix A. From Eq. (9), state $|\psi\rangle_{A_1B_1}$ becomes a non-Gaussian entangled state.

At Alice's station, the quadratures of both x_A and p_A are measured via heterodyne detection on the incoming one-half of state $|\psi\rangle_{A_1B_1}$, and the other half of $|\psi\rangle_{A_1B_1}$ is sent to Bob through an insecure quantum channel that can be controlled by Eve with the transmission efficiency T_c and the excess noise ε. After receiving the state, Bob randomly chooses to measure either x_B or p_B via homodyne detection and informs Alice about the measured observable. Finally, Alice and Bob can share a string of secret keys by data postprocessing.

Before deriving the performance of the QC-CVQKD protocol, we demonstrate the entanglement of both the Gaussian entangled state $|\mathrm{TMSV}\rangle_{AB}$ and the transformed state $|\psi\rangle_{A_1B_1}$. As a computable measurement of entanglement and an upper

bound on the distillable entanglement, the logarithmic negativity is usually used to quantify the degree of entanglement, which is given by

$$E_N = \log_2 \|\rho^{\mathrm{PT}}\|, \tag{11}$$

in which ρ^{PT} is the partial transpose of density operator ρ about the arbitrary subsystem, and the symbol $\|\cdot\|$ is the trace norm. By using the Schmidt decomposition, if an arbitrary state $|\Psi\rangle$ can be decomposed as $|\Psi\rangle = \sum_{n=0}^{\infty} w_n |n\rangle_A |n'\rangle_B$ with the positive real number w_n and the orthonormal states $|n\rangle_A$ and $|n'\rangle_B$, its logarithmic negativity can be calculated as

$$E_N = 2\,\log_2 \left| \sum_{n=0}^{\infty} w_n \right|. \tag{12}$$

According to Eqs. (6), (9), and (C2), the logarithmic negativity of both the TMSV state [14,15] and the resulted state $|\psi\rangle_{A_1B_1}$ as well as the photon-subtraction state $|\Psi\rangle_{AB_1}$, respectively [see Appendix C] can be calculated as

$$\begin{aligned} E_N(|\mathrm{TMSV}\rangle_{AB}) &= -\log_2(1+\alpha^2) - 2\log_2(\sqrt{1+\alpha^2}-\alpha), \\ E_N(|\psi\rangle_{A_1B_1}) &= 2\,\log_2 \left| \sum_{l=0}^{\infty} \frac{W_0}{\sqrt{P_d}} \frac{\partial^m}{\partial \tau^m} \frac{\partial^n}{\partial \gamma^n} \frac{W^l}{(1-\tau)(1-\gamma)} \right|, \\ E_N(|\Psi\rangle_{AB_1}) &= 2\,\log_2 \left| \sum_{l=0}^{\infty} \widetilde{A}\widetilde{B}^{l+1} \sqrt{\frac{l+1}{P_1}} \right|, \end{aligned} \tag{13}$$

where $\widetilde{A}$, $\widetilde{B}$, and P_1 have been defined in Eqs. (C3) and (C4), respectively.

III. PERFORMANCE ANALYSIS

In this section, we demonstrate the success probability regarding the quantum catalysis operation and derive the performance of the QC-CVQKD system in terms of the secret key rate and tolerable excess noise. A performance comparison between the QC-CVQKD and the photon-subtracted CVQKD is made to highlight the merits of the QC-based system. Note that, for a simple and convenient discussion, we consider two special cases, i.e., the bilateral symmetrical quantum catalysis [(BSQC) in which $T_1 = T_2 = T$ and $m = n$] and the single-side quantum catalysis [(SSQC) in which $T_1 = 1$, $T_2 = T$, and n].

A. Success probability for quantum catalysis

The explicit form of the success probability for implementing quantum catalysis operations has been given in Eq. (9). In particular, for the zero-photon BSQC ($T_1 = T_2 = T$ and $m = n = 0$) and SSQC ($T_1 = 1$, $T_2 = T$, and $n = 0$), the success probabilities for implementing such zero-photon quantum-catalysis operations can be given by $1/[1-(T^2-1)\alpha^2]$ and $1/[1-(T-1)\alpha^2]$, respectively. Given a high transmittance $T = 0.95$, the success probabilities P_d can be plotted as a function of α with several different photon-catalysis numbers, such as $m, n \in \{0\text{–}2\}$. Figure 3 shows that the overall trend of success probability P_d decreases as α increases. It indicates that, for the increased modulation variance $V = 2\alpha^2 + 1$, the success probability P_d for implementing quantum-catalysis decreases. Meanwhile, the success probabilities decrease with

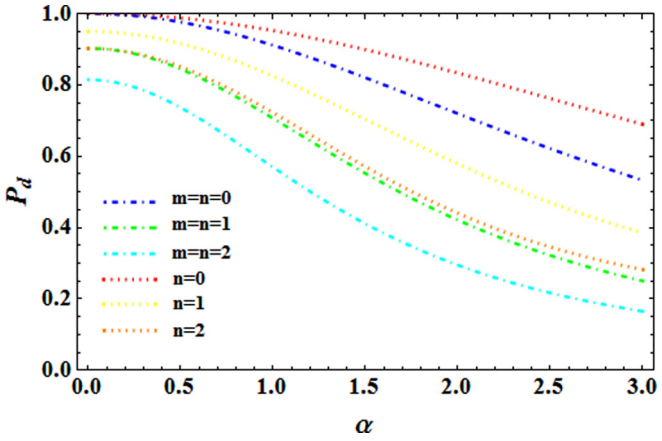

FIG. 3. The success probability P_d of quantum catalysis as a function of α for BSQC ($T_1 = T_2 = T$ and $m = n \in \{0\text{–}2\}$) (dashed-dotted line) and SSQC ($T_1 = 1$, $T_2 = T$, and $n \in \{0\text{–}2\}$) (dotted line) for $T = 0.95$.

the increased number of photon catalyses for both SSQC and SBQC. The above-mentioned phenomenon explains that the implementation of multiphoton catalysis ($m = n > 1$ and $n > 1$) may be relatively difficult to achieve. Whereas, the success probability P_d of SSQC provides better performance than that of BSQC when one considers same photon-catalyzed numbers. For the zero-photon SSQC ($n = 0$) and BSQC ($m = n = 0$), the success probabilities P_d for the given large α ($\alpha = 3$) are approximately 0.68 and 0.53, respectively. It is worth noting that, for the two-photon BSQC ($m = n = 2$), the success probability P_d for the given large α ($\alpha = 3$) is below 0.2, which may leak much information in the CVQKD system.

Now, we consider the effect of entanglement variation on the QC-CVQKD system, which can be evaluated by the logarithmic negativity in Eq. (14). For arbitrary photon-catalyzed numbers m and n, we can obtain the logarithmic negativity of state $|\psi\rangle_{A_1B_1}$. Given a high transmittance $T = 0.95$, we plot the logarithmic negativity among $E_N(|\psi\rangle_{A_1B_1})$, $E_N(|\Psi\rangle_{AB_1})$, and $E_N(|\mathrm{TMSV}\rangle_{AB})$ as a function of α involving different photon-catalyzed numbers as shown in Fig. 4. For the zero-photon and single-photon quantum catalyses, the entanglement property can be improved for $\alpha = 3$, which may have an important impact on the correlation strength of mutual information between Alice and Bob. However, for $\alpha = 3$, the gap of the enhanced entanglement in BSQC decreases with the increase in $m, n \in \{0\text{–}2\}$. A similar trend occurs for SSQC, and there is no improvement of the entanglement for $n = 2$. Although the entanglement for $m = n = 2$ can be improved at a large region of α, there does exist the limitation of its success probability. These results show that the zero-photon and single-photon quantum catalyses (i.e., $m = n \in \{0, 1\}$ and $n \in \{0, 1\}$) perform well in terms of the success probability and the entanglement property when comparing with the two-photon cases (i.e, $m = n = 2$ and $n = 2$). On the other hand, for the optimized T, we give the optimal logarithmic negativity E_N as a function of α for $m = n \in \{0, 1\}$ and $n \in \{0, 1\}$ as shown in Fig. 5. We find that the optimal entanglements of different zero-photon and single-photon quantum-catalysis cases overlap together, and then the gap of the improved entanglement increases with the increasing α.

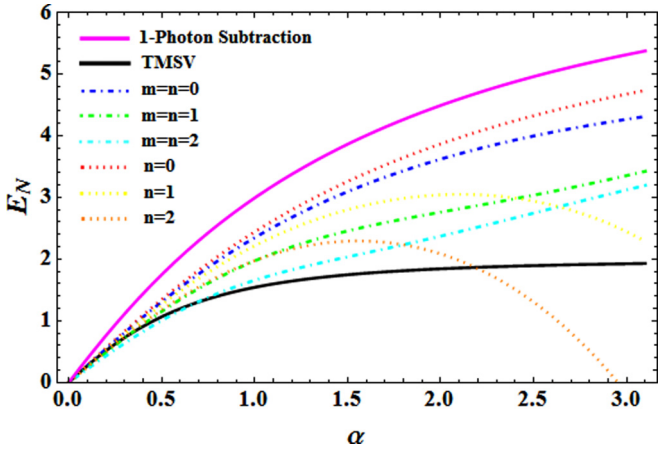

FIG. 4. The logarithmic negativity of $E_N(|\psi\rangle_{A_1B_1})$ as a function of α for BSQC ($T_1 = T_2 = T$ and $m = n \in \{0\text{–}2\}$) (dashed-dotted line) and SSQC ($T_1 = 1,\ T_2 = T$, and $n \in \{0, 1, 2\}$) (dotted line) for $T = 0.95$.

To highlight the contribution of the quantum-catalysis operation, compared with single-photon subtraction, we illustrate the success probability and the entanglement property in Fig. 6. For $T \to 1$, although the improvement of the entanglement for the single-photon subtraction (magenta surface) performs better than that for the quantum-catalysis operation, the success probability for the former is worse than that for the latter. As a result, the quantum-catalysis operation is superior to the single-photon subtraction in terms of the success probability. These results indicate that the quantum catalysis as a novel non-Gaussian operation can be used to improve the entanglement property of Gaussian entangled states and has an advantage of the success probability over the photon-subtraction operation. Consequently, in what follows, we focus on quantum catalysis to enhance the performance of the CVQKD system.

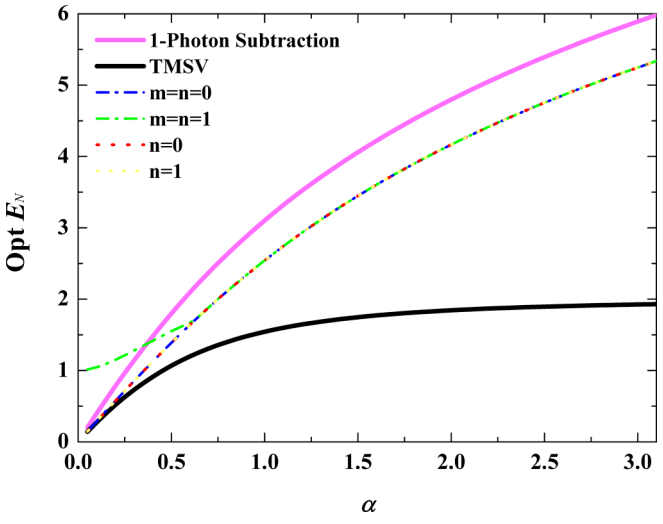

FIG. 5. The optimal logarithmic negativity of $E_N(|\psi\rangle_{A_1B_1})$ as a function of α for BSQC ($T_1 = T_2 = T$ and $m = n \in \{0, 1\}$) (dashed-dotted line) and SSQC ($T_1 = 1,\ T_2 = T$, and $n \in \{0, 1\}$) (dotted line) for the optimal choice of T.

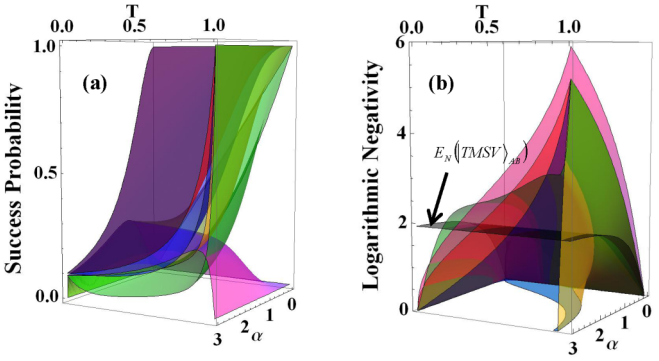

FIG. 6. (a) The success probability of implementing between QC and single-photon subtraction in the (T, α) space with different photon-catalyzed numbers. (b) The logarithmic negativity for the resulted state $|\psi\rangle_{A_1B_1}$ using QC and the single-photon-subtraction-state $|\Psi\rangle_{AB_1}$ as well as the TMSV state $|\mathrm{TMSV}\rangle_{AB}$ in the (T, α) space with different photon-catalyzed numbers. In (a) and (b), the magenta surface stands for the single-photon-subtraction case. Other surfaces denote $m = n = 0$ (blue surface), $m = n = 1$ (green surface), $n = 0$ (red surface), and $n = 1$ (yellow surface).

B. Security analysis

To evaluate the performance of the QC-CVQKD system, according to the detailed calculations of the asymptotic secret key rate [see Appendix B], we demonstrate the numerical simulations of the secret key rate and tolerable excess noise.

Figure 7 shows that, for a given transmittance $T = 0.95$, the asymptotic secret key rate $\widetilde{K}_R$ as a function of transmission distance can be plotted with different photon-catalyzed numbers $m = n \in \{0\text{–}2\}$ and $n \in \{0\text{–}2\}$. The black solid line denotes the secret key rate of the original protocol, which is exceeded by the QC-CVQKD system with zero-photon and single-photon quantum catalyses within the long-distance

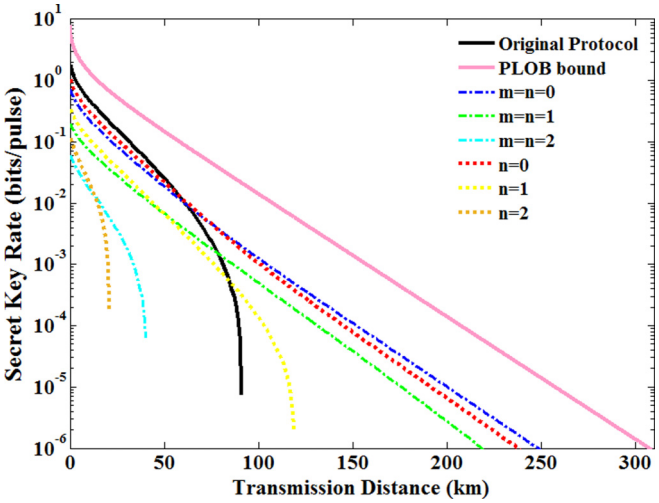

FIG. 7. The asymptotic secret key rates of the QC-CVQKD system (dashed-dotted lines and dotted lines) as a function of the transmission distance for BSQC cases ($T_1 = T_2 = T$ and $m = n \in \{0\text{–}2\}$) (dashed-dotted line) and SSQC cases ($T_1 = 1,\ T_2 = T$, and $n \in \{0\text{–}2\}$) (dotted line) with $T = 0.95$. The variance of the EPR state is $V = 20$, the excess noise is $\varepsilon = 0.01$, and the reconciliation efficiency is $\beta = 0.95$.

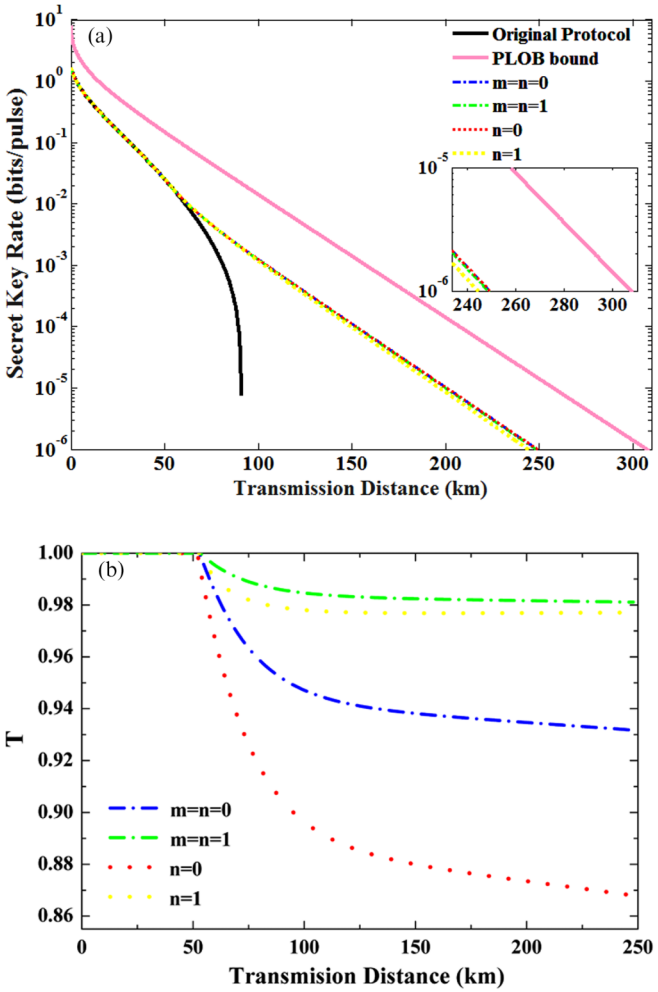

FIG. 8. (a) The secret key rates of the QC-CVQKD system (dashed-dotted lines and dotted lines) as a function of the transmission distance for the BSQC cases ($T_1 = T_2 = T$ and $m = n \in \{0, 1\}$) (dashed-dotted line) and the SSQC cases ($T_1 = 1$, $T_2 = T$, and $n \in \{0, 1\}$) (dotted line) for the optimal choice of T. (b) The secret key rates of the QC-CVQKD system with the optimal T. The variance of the EPR state is $V = 20$, the excess noise is $\varepsilon = 0.01$, and the reconciliation efficiency is $\beta = 0.95$.

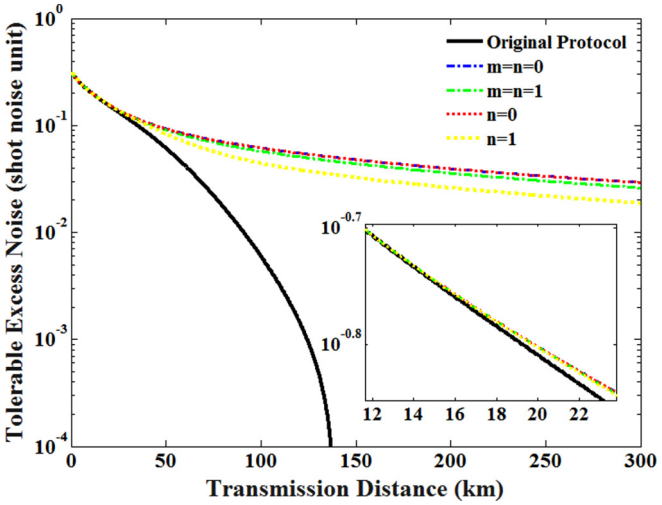

FIG. 9. The maximal tolerable excess noise of the QC-CVQKD system (dashed-dotted lines and dotted lines) as a function of the transmission distance for BSQC cases ($T_1 = T_2 = T$ and $m = n \in \{0, 1\}$) (dashed-dotted line) and SSQC cases ($T_1 = 1$, $T_2 = T$, and $n \in \{0, 1\}$) (dotted line) for the optimal choice of T. The variance of the EPR state is $V = 20$, and the reconciliation efficiency is $\beta = 0.95$.

range. To be specific, the proposed system of using the zero-photon BSQC (blue dashed-dotted line) has the longer transmission distance when compared with the zero-photon SSQC case (red dotted line). Whereas for the single-photon QC-CVQKD system, the BSQC (green dashed-dotted line) in terms of the maximum transmission distance is better than the SSQC case (yellow dotted line). The reason may be that, for the single-photon BSQC, adding the extra model of quantum catalysis $\hat{O}_m$ before Alice takes heterodyne detection can be regarded as the generation of trusted noise thereby resulting in the diminution of the Holevo bound $S^G(B{:}E)$. However, for the two-photon QC-CVQKD system, the BSQC (cyan dashed-dotted line) and SSQC (orange dotted line) are worse than the original one, resulted from the fact that the more photons are catalyzed, the higher the non-Gaussianity thereby making the more noise for the covariance matrix [42,43]. In addition, within the shortening distance, the secret key of the QC-CVQKD system is worse than that of the original system because of the limitation of the success probability of quantum catalysis. As a result, for a given large transmittance $T = 0.95$, the QC-CVQKD system of using the zero-photon and single-photon quantum catalyses can lengthen the maximal transmission distance apart from the two-photon QC-CVQKD system.

Since it is so, for the optimal choice of T, we obtain the maximal secret key rate of the proposed system with the zero-photon and single-photon quantum catalyses. In Fig. 8, we show the maximal secret key rate as a function of transmission distance for $m = n \in \{0, 1\}$ and $n \in \{0, 1\}$ when compared with the original protocol (black solid line). In Fig. 8(b), it is a case of the optimal T that achieves the maximal secret key rate. We find that, for the long-distance range, the zero-photon and single-photon QC-CVQKD systems at the optimal transmittance range ($0.86 \leqslant T \leqslant 1$) perform better than the original system in terms of both secret key rate and transmission distance. It indicates that the quantum catalysis can be used for improving the performance of CVQKD. For the single-photon QC-CVQKD system (green dashed-dotted line and yellow dotted line) at the long transmission distance, the range of the optimal T is approximately $0.978 \leqslant T \leqslant 1$ in which there does exist a high success probability for single-photon quantum catalysis [see Fig. 6(a)]. However, for the short-distance range, even if for the optimal choice of T, the secret key rate of the QC-CVQKD system is similar to that of the original system because for $T_1 = T_2 = 1$ of the untrusted party's $\mathrm{BS_I}$ and $\mathrm{BS_{II}}$, there is no quantum catalysis effect resulting from the CVQKD system.

Additionally, the other factor that has an effect on the QC-CVQKD system is the tolerable excess noise. In Fig. 9, we illustrate the tolerable excess noise as a function of transmission distance for the optimal choice of T. Analogous to Fig. 8,

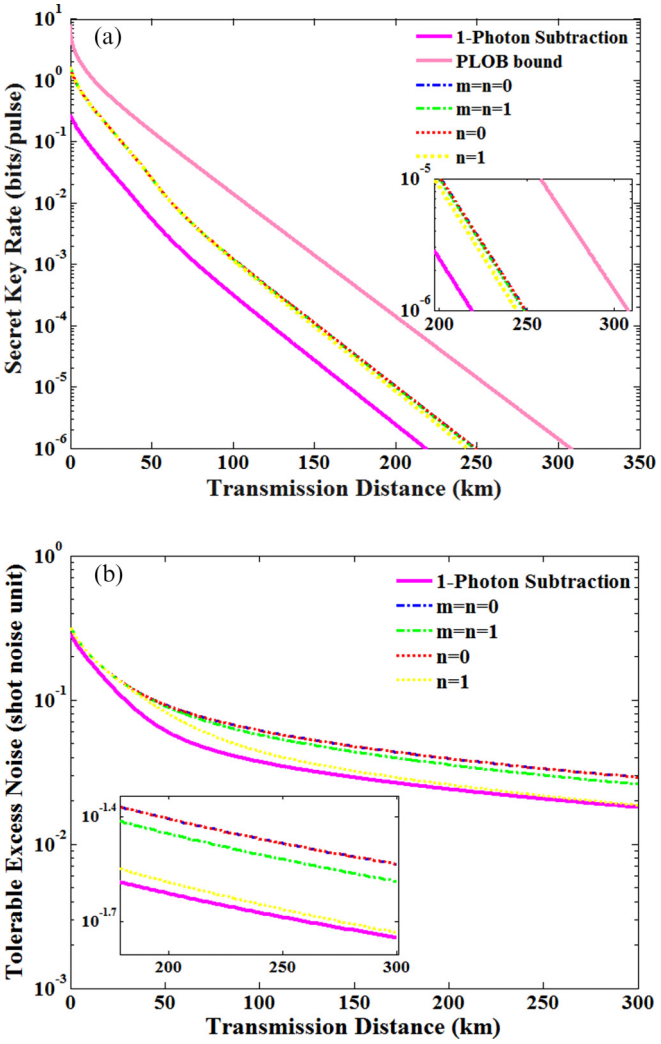

FIG. 10. (a) The maximal secret key rate for $\epsilon = 0.01$ and (b) the maximal tolerable excess noise of the QC-CVQKD system (dashed-dotted lines and dotted lines) and the CVQKD with the single-photon subtraction (magenta solid line) as a function of the transmission distance for the BSQC cases ($T_1 = T_2 = T$ and $m = n = 0, 1$) (dashed-dotted line) and SSQC cases ($T_1 = 1$, $T_2 = T$, and $n = 0, 1$) (dotted line) for the optimal choice of T. The variance of the EPR state is $V = 20$, and the reconciliation efficiency is $\beta = 0.95$.

at the long-distance range, the QC-CVQKD system with the zero-photon and single-photon quantum catalyses exceed the original system with respect to the maximal tolerable excess noise for remote users. More specifically, the zero-photon QC-CVQKD system (blue dashed-dotted line and red dotted line) presents the best performance since the maximal tolerable excess noise approaches about 0.0292 at the transmission distance of 300 km. Besides, at the transmission distance of 300 km, for the single-photon BSQC (i.e., $m = n = 1$) (green dashed-dotted line) and SSQC (i.e., $n = 1$) (yellow dotted line), the maximal tolerable excess noises can approach about 0.0261 and 0.0185, respectively. There, results indicate that, when the quantum channel has less noise ($\varepsilon \sim 0.0185$), the zero-photon and single-photon quantum catalyses can be applied to lengthen the maximal transmission distance up to

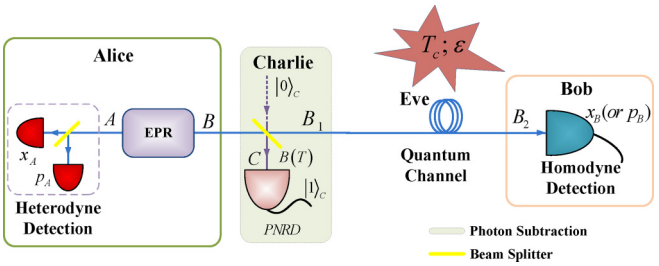

FIG. 11. The schematic of the Gaussian modulation CVQKD scheme with single-photon subtraction.

hundreds of kilometers. In addition, we find that, from Figs. 8(a) and 9, at the long-distance range, for the single-photon QC-CVQKD schemes, the BSQC case (green dashed-dotted line) performs better than the SSQC case (yellow dotted line). It indicates that the single-photon QC-CVQKD system by adding the extra model of quantum catalysis $\hat{O}_m$ in mode A may be useful for improving the performance of the CVQKD protocol when compared with the SSQC $\hat{O}_n$ in mode B.

Interestingly, in Ref. [11], it was pointed out that, for the photon-subtraction-involved CVQKD system, the single-photon-subtraction operation can usually improve the performance of the related system. Therefore, in order to make comparisons of the QC-CVQKD and the SPS-CVQKD, here we give the schematic of the SPS-CVQKD system in Fig. 11. We consider the asymptotic secret key rate K_{asy} of reverse reconciliation under collective attack with the assistant of the IWOP technique [the more detailed calculations can be seen in Appendix C]. To display the effect of quantum catalysis on the performance of CVQKD, we plot the secret key rate and the tolerable excess noise of the CVQKD system involving quantum catalysis and single-photon subtraction as a function of transmission distance for photon-catalyzed numbers $m = n \in \{0, 1\}$ and $n \in \{0, 1\}$ as shown in Figs. 10(a) and 10(b), respectively. It is found that the performance of the SPS-CVQKD system (magenta solid line) in terms of the maximal secret key rate and the maximal tolerable excess noise is outperformed by the QC-CVQKD system at the long transmission distance range. The reason may be that the success probability for single-photon subtraction is lower than that for quantum catalysis at the optimal transmittance T range [see Fig. 8(b)]. It implies that the former loses more information than the latter in the process of distilling a common secret key. Without loss of generality, we assume that the minimal secret key rate is confined to above 10^{-6} bits per pulse. For the single-photon QC-CVQKD system (green dashed-dotted line and yellow dotted line), for the optimal choice of the transmittance T of the untrusted party's beam splitters, the maximal transmission distances is more than 240 km. Whereas for the SPS-CVQKD system, the maximal transmission distance is approximately 218 km because its success probability is limited to below 0.25 [magenta surface in Fig. 6(a)]. These comparison results show that the performance of the QC-CVQKD system using zero-photon and single-photon quantum catalyses performs better than the SPS-CVQKD system when optimized over the transmittance T.

Attractively, from Figs. 7, 8(a), and 10(a), we also consider the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound that

stands for the fundamental rate-loss scaling (secret key capacity) [48]. By comparison, it is found that, for a given transmittance $T = 0.95$, the performance of the QC-CVQKD system using the zero-photon BSQC (i.e., $m = n = 0$) is closer to the PLOB bound than that of the original protocol when the transmission distance reaches longer than 57.6851 km. Whereas for the optimal choice of the transmittance T, we can easily see that our proposed QC-CVQKD system involving the zero-photon and single-photon quantum catalyses is closer to the PLOB bound when comparing with the SPS-CVQKD. However, both of them are unable to exceed the PLOB bound at any transmission distance. Therefore, in order to beat the PLOB bound that is the ultimate limit of repeaterless point-to-point communication, we can design the one-way continuous-variable measurement-device-independent system acting as an active repeater.

IV. CONCLUSION

We have suggested the effect of quantum catalysis on the performance of the CVQKD system by using the IWOP technique. From the equivalent operator of quantum catalysis, the quantum catalysis that is a non-Gaussian operation, in essence, can be used for improving the CVQKD system. Different from the traditional TMSV, the entanglement of the resulting state using quantum catalysis can be improved significantly after optimizing the transmittance T of the untrusted party's beam splitters, and the success probability for quantum catalysis in high transmittance T performs better than the single-photon-subtraction case especially for the zero-photon quantum catalysis. Taking into account the Gaussian optimality, we derive the lower bound of the asymptotic secret key rate of the QC-CVQKD for reverse reconciliation against the collective attack. Numerical simulations show that, when comparing with the SPS-CVQKD system, the QC-CVQKD system has the advantage of lengthening the maximal transmission distance with the raised secret key rates. For all the QC-CVQKD systems, the zero-photon quantum catalysis has the best performance. Whereas for the QC-CVQKD system using single-photon quantum catalysis, the BSQC performs better than the SSQC due to the fact that adding the extra model of quantum catalysis $\hat{O}_m$ is useful for improving the performance of the CVQKD system. We make a comparison of the CVQKD systems involving quantum catalysis and single-photon subtraction. It is found that the QC-CVQKD system using the zero-photon and single-photon quantum catalyses is superior to the single-photon-subtraction case in terms of the maximal transmission distance.

ACKNOWLEDGMENTS

We would like to thank Professor S. Pirandola for his helpful suggestion. This work was supported by the National Natural Science Foundation of China (Grants No. 61572529 and No. 61871407).

APPENDIX A: DERIVATION OF THE SUCCESS PROBABILITY P_d

In order to derive the analytical expression of the success probability P_d shown in Eq. (10), we rewrite the state in Eq. (9) as the density operator $\rho = |\psi\rangle\langle\psi|$, i.e.,

$$\begin{aligned}\rho_{A_1B_1} &= \frac{1}{P_d}\hat{O}_m\hat{O}_n|\mathrm{TMSV}\rangle\langle\mathrm{TMSV}|\hat{O}_n^\dagger\hat{O}_m^\dagger \\ &= \frac{W_0^2}{P_d}\Re^{m,n}\Pi\ \exp[a^\dagger b^\dagger W]00\rangle\langle 00|\exp[abW_1], \end{aligned} \tag{A1}$$

where we have used the equivalent operators of the photon-catalysis operations in Eq. (4), $e^{\zeta a^\dagger a}a^\dagger e^{-\zeta a^\dagger a} = a^\dagger e^{\zeta}$ and set

$$\begin{aligned} W &= \frac{\lambda(T_2-\gamma)(T_1-\tau)}{\sqrt{T_1T_2}(1-\gamma)(1-\tau)}, \\ W_0 &= \frac{\sqrt{T_1^mT_2^n(1-\lambda^2)}}{n!m!}, \\ W_1 &= \frac{\lambda(T_2-\gamma_1)(T_1-\tau_1)}{\sqrt{T_1T_2}(1-\gamma_1)(1-\tau_1)}, \\ \Pi &= \frac{1}{1-\tau}\frac{1}{1-\gamma}\frac{1}{1-\tau_1}\frac{1}{1-\gamma_1}, \\ \Re^{m,n} &= \frac{\partial^m}{\partial\tau^m}\frac{\partial^n}{\partial\gamma^n}\frac{\partial^m}{\partial\tau_1^m}\frac{\partial^n}{\partial\gamma_1^n}\{\cdots\}\Big|_{\tau=\gamma=\tau_1=\gamma_1=0}. \end{aligned} \tag{A2}$$

Then, according to the completeness relation of coherent-state representation $\int d^2z|z\rangle\langle z|/\pi = 1$, the integrational formula,

$$\begin{aligned}&\int\frac{d^2z}{\pi}\exp(\zeta|z|^2+\xi z+\eta z^*+fz^2+gz^{*2}) \\ &\quad= \frac{1}{\sqrt{\zeta^2-4fg}}\exp\left[\frac{-\zeta\xi\eta+\xi^2g+\eta^2f}{\zeta^2-4fg}\right], \end{aligned} \tag{A3}$$

and the completeness of the resulted state $\mathrm{Tr}(\rho_{A_1B_1}) = 1$, we can obtain the success probability P_d given by

$$\begin{aligned} P_d &= W_0^2\Re^{m,n}\Pi\langle 00|\exp[abW_1]\exp[a^\dagger b^\dagger W]00\rangle \\ &= W_0^2\Re^{m,n}\Pi\int\frac{d^2z}{\pi^2}\int\frac{d^2\beta}{\pi^2}\exp[-|z|^2-|\beta|^2+z\beta W_1 \\ &\quad+z^*\beta^*W] \\ &= W_0^2\Re^{m,n}\left\{\frac{\Pi}{1-W_1W}\right\}. \end{aligned} \tag{A4}$$

APPENDIX B: CALCULATION OF THE ASYMPTOTIC SECRET KEY RATE

Here, we present the calculation of the asymptotic secret key rates of the QC-CVQKD system where Alice performs heterodyne detection and Bob performs homodyne detection. As mentioned above, state $|\psi\rangle_{A_1B_1}$ belongs to a new kind of non-Gaussian state, thus we cannot directly use the results of the conventional Gaussian CVQKD to calculate its secret key rate. Fortunately, thanks to the extremity of the Gaussian quantum states that the rendering secret key rate of the non-Gaussian state $|\psi\rangle_{A_1B_1}$ is no less than that of a Gaussian state $|\psi\rangle^G_{A_1B_1}$ with the same covariance matrix $\Gamma_{A_1B_1} = \Gamma^G_{A_1B_1}$, we obtain $K(|\psi\rangle_{A_1B_1}) \geqslant K(|\psi\rangle^G_{A_1B_1})$ [16,18]. For reverse reconciliation, therefore, the lower bound of the asymptotic secret key rate under optimal collective attack can be given by

$$\widetilde{K}_R = P_d\{\beta I^G(A{:}B) - S^G(B{:}E)\}, \tag{B1}$$

where β denotes the reconciliation efficiency, $I^G(A{:}B)$ denotes Alice and Bob's mutual information, and $S^G(B{:}E)$ denotes the Holevo bound, which is defined as the maximum information on Bob's final key available to Eve.

In order to derive the analytical expression of the asymptotic secret key rate $K(|\psi\rangle^G_{A_1B_1})$, we consider the covariance matrix $\Gamma_{A_1B_1}$ of the resulted state $|\psi\rangle_{A_1B_1}$ given by

$$\Gamma_{A_1B_1} = \begin{pmatrix} X_A \mathrm{II} & Z_{AB}\sigma_z \\ Z_{AB}\sigma_z & Y_B \mathrm{II} \end{pmatrix}, \tag{B2}$$

where $\mathrm{II} = \mathrm{diag}(1,1)$, $\sigma_z = \mathrm{diag}(1,-1)$, and X_A, Y_B, and Z_{AB} can be derived by using the IWOP technique as follows: It is first required to derive the average values, such as $\langle a^\dagger a\rangle$, $\langle b^\dagger b\rangle$, and $\langle ab\rangle$. According to Eqs. (A1) and (A3), thus, it is straightforward to get

$$\begin{aligned}
\langle a^\dagger a\rangle &= \mathrm{Tr}[\rho_{A_1B_1}(aa^\dagger - 1)] \\
&= \frac{W_0^2}{P_d}\Re^{m,n}\Pi\int\frac{d^2\alpha}{\pi^2}\int\frac{d^2\beta}{\pi^2}\alpha\alpha^*\exp[-|\alpha|^2-|\beta|^2 \\
&\quad +\alpha\beta W_1 + \alpha^*\beta^* W] - 1 \\
&= \frac{W_0^2}{P_d}\Re^{m,n}\left\{\frac{\Pi}{(1-W_1W)^2}\right\} - 1, \qquad \text{(B3)} \\
\langle b^\dagger b\rangle &= \mathrm{Tr}[\rho_{A_1B_1}(bb^\dagger - 1)] \\
&= \frac{W_0^2}{P_d}\Re^{m,n}\Pi\int\frac{d^2\alpha}{\pi^2}\int\frac{d^2\beta}{\pi^2}\beta\beta^*\exp[-|\alpha|^2-|\beta|^2 \\
&\quad +\alpha\beta W_1 + \alpha^*\beta^* W] - 1 \\
&= \frac{W_0^2}{P_d}\Re^{m,n}\left\{\frac{\Pi}{(1-W_1W)^2}\right\} - 1, \\
&= \langle a^\dagger a\rangle, \qquad \text{(B4)} \\
\langle ab\rangle &= \mathrm{Tr}[\rho_{A_1B_1}ab] \\
&= \frac{W_0^2}{P_d}\Re^{m,n}\Pi\int\frac{d^2\alpha}{\pi^2}\int\frac{d^2\beta}{\pi^2}\alpha\beta\exp[-|\alpha|^2-|\beta|^2 \\
&\quad +\alpha\beta W_1 + \alpha^*\beta^* W] \\
&= \frac{W_0^2}{P_d}\Re^{m,n}\left\{\frac{\Pi W}{(1-W_1W)^2}\right\}. \qquad \text{(B5)}
\end{aligned}$$

Note that $\langle ab\rangle = \langle a^\dagger b^\dagger\rangle^\dagger$. By combining Eqs. (B3)– (B5), therefore, we can directly obtain the elements of covariance matrix $\Gamma^N_{A_1B_1}$ as the following form:

$$\begin{aligned}
X_A &= \mathrm{Tr}[\rho_{A_1B_1}(1+2a^\dagger a)] \\
&= \frac{2W_0^2}{P_d}\Re^{m,n}\left\{\frac{\Pi}{(1-W_1W)^2}\right\} - 1, \\
Y_B &= \mathrm{Tr}[\rho_{A_1B_1}(1+2b^\dagger b)] \\
&= X_A, \\
Z_{AB} &= \mathrm{Tr}[\rho_{A_1B_1}(ab + a^\dagger b^\dagger)] \\
&= \frac{2W_0^2}{P_d}\Re^{m,n}\left\{\frac{\Pi W}{(1-W_1W)^2}\right\}. \qquad \text{(B6)}
\end{aligned}$$

After passing the untrusted quantum channel, which is characterized by the transmission efficiency T_c and the excess noise ε, the covariance matrix $\Gamma^G_{A_1B_2}$ reads

$$\Gamma^G_{A_1B_2} = \begin{pmatrix} X_A II & \sqrt{T_c}Z_{AB}\sigma_z \\ \sqrt{T_c}Z_{AB}\sigma_z & T_c(X_A+\xi)II \end{pmatrix}, \tag{B7}$$

where $\xi = (1-T_c)/T_c + \varepsilon$ denotes the channel-added noise referred to as the input of the Gaussian channel. The mutual information between Alice and Bob now can be expressed as

$$\begin{aligned}
I^G(A{:}B) &= \frac{1}{2}\log_2\frac{V_{A_1}}{V_{A_1|B_2}} \\
&= \log_2\left\{\sqrt{\frac{(X_A+1)(X_A+\xi)}{(X_A+1)(X_A+\xi)-Z_{AB}^2}}\right\}. \qquad \text{(B8)}
\end{aligned}$$

Furthermore, Eve's accessible quantum information on Bob's measurement can be calculated by assuming Eve can purify the whole system $S^G(B{:}E) = S(E) - S(E|B) = S(AB) - S(A|B)$. For the Gaussian modulation, the first term $S(AB)$ is a function of the symplectic eigenvalues $\lambda_{1,2}$ of $\Gamma^G_{A_1B_2}$, which is given by

$$S(AB) = G[(\lambda_1-1)/2] + G[(\lambda_2-1)/2], \tag{B9}$$

where the Von Neumann entropy $G[x]$ is

$$G[x] = (x+1)\log_2(x+1) - x\log_2 x, \tag{B10}$$

and

$$\lambda^2_{1,2} = \tfrac{1}{2}[\Lambda \pm \sqrt{\Lambda^2 - 4D^2}], \tag{B11}$$

with the notation,

$$\begin{aligned}
\Lambda &= X_A^2 + T_c^2(X_A+\xi)^2 - 2T_cZ_{AB}^2, \\
D &= X_AT_c(X_A+\xi) - T_cZ_{AB}^2. \qquad \text{(B12)}
\end{aligned}$$

Moreover, the second term $S(A|B) = G[(\lambda_3-1)/2]$ is a function of the symplectic eigenvalue λ_3 of the covariance matrix Γ^b_A of Alice's mode after Bob performs homodyne detection where the square of the symplectic eigenvalue λ_3 is

$$\lambda_3^2 = X_A\left[X_A - \frac{Z_{AB}^2}{X_A+\xi}\right]. \tag{B13}$$

As a result, the asymptotic secret key rate can be written as

$$\widetilde{K}_R = P_d\{\beta I^G(A{:}B) - S(AB) + S(A|B)\}. \tag{B14}$$

APPENDIX C: THE SECRET KEY RATE OF THE SINGLE-PHOTON-SUBTRACTION EB-CVQKD PROTOCOL UNDER COLLECTIVE ATTACK

In order to make a comparison of the proposed long-distance CVQKD scheme via quantum catalysis, here, we review the CVQKD protocol of applying single-photon subtraction controlled by an untrusted party Charlie and then assume that these two schemes have the same quantum channel

controlled by Eve. As can be seen from Fig. 11, Alice generates a two-mode squeezed vacuum state $|\mathrm{TMSV}\rangle_{AB}$ (EPR) and performs heterodyne detection of one-half of $|\mathrm{TMSV}\rangle_{AB}$. The other half of $|\mathrm{TMSV}\rangle_{AB}$ after operating single-photon subtraction is sent to Bob through the same quantum channel marked by transmission efficiency T_c and excess noise ε. Afterwards, Bob performs homodyne detection of the received state and then informs Alice about which observable he measured so that two correlated variables, which are shared by both Alice and Bob, can be used to exact a common secret key.

Indeed, starting from the concept of quantum operators, the single-photon-subtraction operation can be seen as an equivalent operator Θ which is given by

$$\Theta = {}_C\langle 1|B(T)|0\rangle_C = \frac{1-T}{T} b \exp[b^\dagger b \ln\sqrt{T}]. \tag{C1}$$

Thus, the photon-subtraction state $|\Psi\rangle_{AB_1}$ after operating single-photon subtraction is expressed as

$$|\Psi\rangle_{AB_1} = \frac{1}{\sqrt{P_1}}\Theta|\mathrm{TMSV}\rangle_{AB} = \frac{\widetilde{A}\widetilde{B}}{\sqrt{P_1}} \exp[\widetilde{B}a^\dagger b^\dagger]a^\dagger|00\rangle_{AB}, \tag{C2}$$

where

$$\widetilde{A} = \sqrt{\frac{(1-\lambda^2)(1-T)}{T}},$$
$$\widetilde{B} = \lambda\sqrt{T}, \tag{C3}$$

and

$$P_1 = \frac{\widetilde{A}^2\widetilde{B}^2}{(1-\widetilde{B}^2)^2} \tag{C4}$$

is the success probability of implementing the single-photon-subtraction operation. After the photon-subtraction state $|\Psi\rangle_{AB_1}$ goes through the quantum channel, similar to Eq. (B7), we also can obtain the covariance matrix Γ^1 as the following form:

$$\Gamma^1 = \begin{pmatrix} X\mathrm{II} & \sqrt{T_c}Z\sigma_z \\ \sqrt{T_c}Z\sigma_z & T_c(Y+\xi)\mathrm{II} \end{pmatrix}, \tag{C5}$$

where $\xi = (1-T_c)/T_c + \varepsilon$ and

$$X = \frac{4\widetilde{A}^2\widetilde{B}^2}{P_1(1-\widetilde{B}^2)^3} - 1,$$
$$Y = \frac{2\widetilde{A}^2\widetilde{B}^2(1+\widetilde{B}^2)}{P_1(1-\widetilde{B}^2)^3} - 1,$$
$$Z = \frac{4\widetilde{A}^2\widetilde{B}^3}{P_1(1-\widetilde{B}^2)^3}. \tag{C6}$$

Now, let us consider the calculation of the asymptotic secret key rate of the single-photon-subtraction EB-CVQKD protocol in the context of the Gaussian optimality theorem. Thus, the lower bound of the asymptotic secret key rate K_{asy} of reverse reconciliation under collective attack is

$$K_{\mathrm{asy}} = P_1\{\beta I^{\mathrm{Hom}}(A{:}B) - S^{\mathrm{Hom}}(B{:}E)\}, \tag{C7}$$

where P_1 has been derived in Eq. (C4), β is the efficiency for reverse reconciliation, and the superscript Hom represents Bob taking homodyne detection. Additionally, the mutual information between Alice and Bob is given by

$$I^{\mathrm{Hom}}(A{:}B) = \log_2\left\{\sqrt{\frac{(X+1)(Y+\xi)}{(X+1)(Y+\xi)-Z^2}}\right\}. \tag{C8}$$

Under the assumption that Eve is able to purify the whole system $S^G(B{:}E) = S(E) - S(E|B) = S(AB) - S(A|B)$, we can directly obtain the symplectic eigenvalues $\widetilde{\lambda}_{1,2}$ of covariance matrix Γ^1 as the following form:

$$\widetilde{\lambda}^2_{1,2} = \tfrac{1}{2}[\widetilde{C} \pm \sqrt{\widetilde{C}^2 - 4\widetilde{D}^2}], \tag{C9}$$

with

$$\widetilde{C} = X^2 + T_c^2(Y+\xi)^2 - 2T_cZ^2,$$
$$\widetilde{D} = XT_c(Y+\xi) - T_cZ^2, \tag{C10}$$

and

$$\widetilde{\lambda}^2_3 = X\left[X - \frac{Z^2}{Y+\xi}\right]. \tag{C11}$$

Furthermore, $S(AB) = G[(\widetilde{\lambda}_1 - 1)/2] + G[(\widetilde{\lambda}_2 - 1)/2]$ and $S(A|B) = G[(\widetilde{\lambda}_3 - 1)/2]$ where the Von Neumann entropy $G[x]$ is defined in Eq. (B10).

[1] P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, UK, 2010).

[2] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[3] M. A. Nielseen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2000).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[6] J. Y. Bang and M. S. Berger, Quantum mechanics and the generalized uncertainty principle, Phys. Rev. D **74**, 125012 (2006).

[7] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature (London) **299**, 802 (1982).

[8] 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).

[9] C. Weedbrook, Continuous-variable quantum key distribution with entanglement in the middle, Phys. Rev. A **87**, 022308 (2013).

[10] 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).

[11] 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).

[12] P. Huang, J. Fang, and G. H. Zeng, State-discrimination attack on discretely modulated continuous-variable quantum key distribution, Phys. Rev. A **89**, 042330 (2014).

[13] H. Zhang, J. Fang, and G. Q. He, Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers, Phys. Rev. A **86**, 022338 (2012).

[14] P. Huang, G. Q. He, J. Fang, and G. H. Zeng, Performance improvement of continuous-variable quantum key distribution via photon subtraction, Phys. Rev. A **87**, 012317 (2013).

[15] Y. Guo, Q. Liao, Y. J. Wang, D. Huang, P. Huang, and G. H. Zeng, Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction, Phys. Rev. A **95**, 032304 (2017).

[16] R. G. Patron and N. J. Cerf, Unconditional Optimality of Gaussian Attacks Against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[17] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[18] M. Navascues, F. Grosshans, and A. Acin, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[19] 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).

[20] 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**, 100502 (2012).

[21] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[22] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, 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**, 042305 (2007).

[23] P. Jouguet, S. K. Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photon. **7**, 378 (2013).

[24] A. Leverrier, R. Aleaume, J. Boutros, G. Zemor, and P. Grangier, Multidimensional reconciliation for a continuous-variable quantum key distribution, Phys. Rev. A **77**, 042325 (2008).

[25] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Long-distance continuous-variable quantum key distribution with a Gaussian modulation, Phys. Rev. A **84**, 062317 (2011).

[26] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier, Phys. Rev. A **86**, 012327 (2012).

[27] B. J. Xu, C. M. Tang, H. Chen, W. Z. Zhang, and F. C. Zhu, Improving the maximum transmission distance of four-state continuous-variable quantum key distribution by using a noiseless linear amplifier, Phys. Rev. A **87**, 062311 (2013).

[28] D. Huang, P. Huang, D. K. Lin, and G. H. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[29] Q. Liao, Y. Guo, D. Huang, P. Huang, and G. H. Zeng, Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection, New J. Phys. **20**, 023015 (2018).

[30] A. Leverrier and P. Grangier, Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation, Phys. Rev. Lett. **102**, 180504 (2009).

[31] Y. Guo, R. J. Li, Q. Liao, J. Zhou, and D. Huang, Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier, Phys. Lett. A **382**, 372 (2018)

[32] A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, Continuous-variable quantum key distribution protocols with eight-state discrete modulation, Int. J. Quantum Inf. **10**, 1250004 (2012).

[33] J. Yang, B. J. Xu, and H. Guo, Source monitoring for continuous-variable quantum key distribution, Phys. Rev. A **86**, 042314 (2012).

[34] Y. Guo, G. L. Lv, and G. H. Zeng, Balancing continuous-variable quantum key distribution with source-tunable linear optics cloning machine, Quantum Inf. Process. **14**, 4323 (2015).

[35] F. L. Yang, R. H. Shi, Y. Guo, J. J. Shi, and G. H. Zeng, Continuous-variable quantum key distribution under the local oscillator intensity attack with noiseless linear amplifier, Quantum Inf. Process. **14**, 1 (2015).

[36] 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).

[37] S. Y. Lee, S. W. Ji, H. J. Kim, and H. Nha, Enhancing quantum entanglement for continuous variables by a coherent superposition of photon subtraction and addition, Phys. Rev. A **84**, 012302 (2011).

[38] 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).

[39] S. Olivares, M. G. A. Paris, and R. Bonifacio, Teleportation improvement by inconclusive photon subtraction, Phys. Rev. A **67**, 032314 (2003).

[40] T. Opatrny, G. Kurizki, and D. G. Welsch, Improvement on teleportation of continuous variables by photon subtraction via conditional measurement, Phys. Rev. A **61**, 032302 (2000).

[41] 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).

[42] 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).

[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] H. Y. Fan, Normally ordering some multimode exponential operators by virtue of the IWOP technique, J. Phys. A **23**, L913 (1990).

[45] H. Y. Fan, H. R. Zaidi, and J. R. Klauder, New approach for calculating the normally ordered form of squeeze operators, Phys. Rev. D **35**, 1831 (1987).

[46] H. Y. Fan, Operator ordering in quantum optics theory and the development of Dirac's symbolic method, J. Opt. B **5**, R147 (2003).

[47] H. Y. Fan, H. L. Lu, and Y. Fan, Newton–Leibniz integration for ket–bra operators in quantum mechanics and derivation of entangled state representations, Ann. Phys. (NY) **321**, 480 (2006).

[48] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).