Performance improvement of continuous-variable quantum key distribution via photon subtraction

Peng Huang, Guangqiang He,* Jian Fang, and Guihua Zeng†
State Key Laboratory of Advanced Optical Communication Systems and Networks, Key Lab on Navigation and Location-based Service, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240, China

(Received 14 October 2012; published 17 January 2013)

It has been found that non-Gaussian operations can be applied to increase and distill entanglement between Gaussian entangled states. We propose here a method to improve the performance of entanglement-based (EB) continuous-variable quantum-key-distribution protocol by using the non-Gaussian operation, in particular, the subtraction operation, which can be implemented under current technology easily. Security analysis shows that the subtraction operation can well increase the secure distance and tolerable excess noise of the EB scheme and also the corresponding prepare-and-measure scheme.

DOI: 10.1103/PhysRevA.87.012317 PACS number(s): 03.67.Dd, 42.50.−p

I. INTRODUCTION

Quantum key distribution (QKD) provides a novel way to allow two distant parties, the sender Alice and the receiver Bob, to establish a secret key through unsecure quantum and classical channels. Different from the discrete-variable quantum key distribution (DVQKD) [1–3], in continuous-variable quantum key distribution (CVQKD) [3–8], Alice usually encodes information in the quadratures of optical field with Gaussian modulation, and Bob can decode the secret information with high-efficiency and high-speed homodyne or heterodyne detection. So CVQKD schemes avoid the use of a single-photon detector, and have the prospect of high rate secure key distribution. Moreover, these protocols have been proved secure against arbitrary collective attacks [9–11], which are clarified to be coincident with coherent attacks asymptotically by the quantum De Finetti theorem [12].

Despite the above merits, the secure distance of CVQKD is too short when comparing to DVQKD. The main reason is that, for Gaussian modulation, Alice and Bob should construct a key from shared continuous random values in the reconciliation procedure with quite low efficiency, especially when the transmission distance is long. Another reason is that the applied modulated variance in practice does not run in an optimal value for long-distance communication because of the limit precision and efficiency of homodyne detectors. To solve the main problem, one solution is to design a good reconciliation code with high efficiency even at low signal-to-noise ratio (SNR) [13]. Another solution is to apply discrete modulation, such as the four-state protocol proposed by Leverrier *et al.* [14]. Since there exists an error correction code with high efficiency for discrete values even for low SNR, the four-state protocol can then extremely improve the secure distance. In a sense, the four-state protocol also corresponds to the continuous modulation CVQKD protocol with low modulated variance.

However, the unconditional security proof in [14] relies on a hidden assumption that the quantum channel is linear. Actually, Alice and Bob cannot estimate the covariance matrix from their experimental data without the linear channel assumption. Recently, Leverrier *et al.* modified their protocol by introducing decoy states [15] such that the mixed state sent to Bob is Gaussian. Then Alice can randomly choose a Gaussian modulation mode which is used for parameter estimation, or choose a non-Gaussian modulation mode which is used for key distillation, without discrimination by Eve. Lately, an improved four-state protocol is proposed [16], where Alice takes heterodyne detection, and Alice and Bob can evaluate the covariance matrix directly without the linear channel assumption. The remaining problem is that the correlation between Alice and Bob's quadratures cannot reach that of an Einstein-Podolsky-Rosen (EPR) pair, which restricts the secure key rate.

Interestingly, it has been demonstrated theoretically and experimentally that the non-Gaussian operations, for instance, the photon subtraction and photon addition operations, can be used to increase and distill the entanglement in Gaussian entangled states [17–22], and thus to improve the performance of quantum teleportation [22] and quantum linear amplifiers [23]. In this paper, we propose a method to improve the performance of entanglement-based (EB) CVQKD protocol by using non-Gaussian operation, i.e., the subtraction operation. We show that the subtraction operation, which can be easily implemented under current technology, can increase the entanglement degree of the two-mode state, and thus improve the correlation between Alice and Bob's quadratures. The security analysis demonstrates that this method allows distribution of secret keys over much longer secure distances with much better performance to resist excess noise contact to the original Gaussian modulation schemes.

This paper is organized as follows. In Sec. II, we first introduce the EB CVQKD protocol, then introduce the model of the proposed method by using non-Gaussian operation. In Sec. III, we briefly review the logarithmic negativity as computable entanglement measures, and then analyze the evolution of the logarithmic negativity under the subtraction operation. We calculate the secret key rate in detail under general collective attack and show the performance of the renewed protocol in Sec. IV. Finally, conclusions are drawn in Sec. V.

II. GAUSSIAN MODULATION EB CVQKD WITH NON-GAUSSIAN OPERATION

Before introducing the method to improve the performance of CVQKD under study, we first briefly review the Gaussian

*gqhe@sjtu.edu.cn
†ghzeng@sjtu.edu.cn

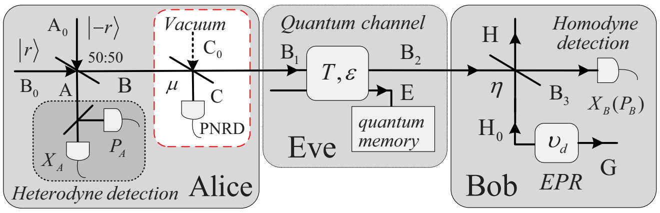

FIG. 1. (Color online) The Gaussian modulation EB CVQKD protocol with non-Gaussian operations. PNRD stands for photon number resolving detector.

modulation EB CVQKD protocol as shown in Fig. 1 (the module within the red dashed line excluded).

Alice prepares a two-mode squeezed vacuum (EPR) state ρ_{AB} with variance $V = V_A + 1$, where the modulation variance $V_A = 2\alpha^2$, and takes heterodyne measurement of one half of state ρ_{AB}. Then, the other half of state ρ_{AB} is sent to Bob through the quantum channel characterized by transmission efficiency T and excess noise ε. After receiving the state, Bob takes homodyne detection and informs Alice which observable he obtained. Finally, Alice and Bob will share two correlated Gaussian variables which can be further used to exact a private binary key.

Bob's inefficient detection is modeled by a beam splitter (BS) with transmission η, while its electronic noise ν_{el} is modeled by an EPR state of variance ν_d, with one half entering the other input port of the BS. Since the quantum channel and Bob's detection are not the ideal apparatus, the channel-added noise referred to channel input and detection-added noise referred to Bob's input are expressed in shot noise units as $\chi_{\text{line}} = 1/T - 1 + \varepsilon$ and $\chi_h = [(1-\eta) + \nu_{\text{el}}]/\eta$, respectively. ν_d is related to the detection-added noise χ_h as $\nu_d = \eta\chi_h/(1-\eta)$.

As shown in Fig. 1, the EPR state $|\Psi\rangle_{AB}$ is generated by using two single-mode squeezed vacuum states $|r\rangle$ and $|-r\rangle$ with

$$|r\rangle_k = \hat{S}_k(r)|0\rangle, \tag{1}$$

where $\hat{S}_k(r)$ is the squeezing operator on mode k with the form

$$\hat{S}_k(r) = \exp\left[-\frac{r}{2}\left(\hat{a}_k^{\dagger 2} - \hat{a}_k^2\right)\right], \tag{2}$$

and r is the squeezing parameter. The two modes are combined with a balanced BS to generate the two-mode squeezed vacuum (EPR) state $|\Psi_{AB}\rangle$ in the form

$$|\Psi\rangle_{AB} = \hat{U}_{AB}\left(\frac{\pi}{4}\right)|r\rangle_A|-r\rangle_B = \sum_{n=0}^{\infty}\alpha_n|n\rangle_A|n\rangle_B, \tag{3}$$

where

$$\hat{U}_{AB}(\theta) = \exp[\theta(\hat{a}_A^\dagger\hat{a}_B - \hat{a}_A\hat{a}_B^\dagger)] \tag{4}$$

is the beam splitter operator, and parameter θ is related to the transmission efficiency ζ with the function $\zeta = 1/(1+\tan^2\theta)$. So $\theta = \pi/4$ corresponds to the balanced beam splitter. As known, the EPR state can be also generated by using a two-mode squeezing operator. Actually, the combination of two single-squeezed vacuum states through a balanced BS acts as a two-mode squeezing operator on two vacuum states,

$$|\Psi\rangle_{AB} = \hat{S}_{AB}(-r)|0\rangle_A|0\rangle_B = \sum_{n=0}^{\infty}\alpha_n|n\rangle_A|n\rangle_B, \tag{5}$$

with $\hat{S}_{AB}(r) = \exp[-r(\hat{a}_A^\dagger\hat{a}_B^\dagger - \hat{a}_A\hat{a}_B)]$. The Schmidt coefficients are given by

$$\alpha_n = \sqrt{\frac{\alpha^{2n}}{(1+\alpha^2)^{n+1}}}, \tag{6}$$

where $\alpha = \sinh r$.

Now we consider the protocol when non-Gaussian operation, i.e., photon subtraction, is introduced. As shown by the module within the red dashed line in Fig. 1, the combination of a BS and a photon number resolving detector works as a practical photon substraction operator. The beam in mode B is tapped off by a BS with transmission μ, which results in the state

$$\begin{aligned} |\Psi\rangle_{AB_1C} &= [I_A \otimes \hat{U}_{BC_0}(\theta)]|\Psi\rangle_{AB}|0\rangle_{C_0} \\ &= \sum_n \alpha_n \sum_{k=0}^{n} \xi_{nk}|n\rangle_A|n-k\rangle_{B_1}|k\rangle_C, \end{aligned} \tag{7}$$

where

$$\xi_{nk} = (-1)^k\sqrt{\binom{n}{k}}\mu^{(n-k)/2}(1-\mu)^{k/2}, \tag{8}$$

with $\binom{n}{k}$ the binomial coefficient.

When k photons are detected in the beam on mode C by an ideal photon number resolving detector, the conditional state is given by

$$|\Psi^{(k)}\rangle_{AB_1} = \sum_{n=k}^{\infty}\alpha_n\xi_{nk}|n\rangle_A|n-k\rangle_{B_1} = {}_C\langle k|\Psi\rangle_{AB_1C}. \tag{9}$$

It can be seen $|\Psi^{(k)}\rangle_{AB_1}$ is still a pure state. For $k = 1$,

$$\begin{aligned} |\Psi^{(1)}\rangle_{AB_1} &= \sum_{n=1}^{\infty} c_n^{(1)}|n\rangle_A|n-1\rangle_{B_1} \\ &= \frac{1}{\sqrt{P^{(1)}}}\sum_{n=1}^{\infty}\alpha_n\xi_{n1}|n\rangle_A|n-1\rangle_{B_1}, \end{aligned} \tag{10}$$

where $P^{(1)} = \alpha^2(1-\mu)/(1+\alpha^2-\alpha^2\mu)^2$ is the normalization factor which denotes the probability of detecting one photon in mode C. The bipartite state $|\Psi^{(1)}\rangle_{AB_1}$ in Eq. (10) is not Gaussian anymore. In the following, we will explore the performance of the renewed CVQKD scheme with photon subtraction, and we will first consider the change of entanglement of the EPR state.

III. ENTANGLEMENT EVOLUTION UNDER ONE-PHOTON SUBTRACTION OPERATION

Intuitionally, the entanglement degree of bipartite source states of the EB CVQKD scheme quantifies the correlation between the two subsystems, which is positively related to the performance of the scheme. Essentially, the performance and even the security of the CVQKD system is restricted by all of the imperfections of practical modules in the CVQKD system, which deteriorate the correlation of the distributed states. It can been seen from Fig. 1 that the introduction of subtraction operation changes the EPR source in the original EB CVQKD scheme. So in order to explore whether the introduction of photon subtraction can improve the performance of the CVQKD scheme, we should first analyze the entanglement of the renewed EPR source.

Now we consider the entanglement evolution of the bipartite state $|\Psi\rangle_{AB}$ under non-Gaussian operation. Here we apply logarithmic negativity [24] as entanglement measures, which as known is an upper bound on the distillable entanglement. These measures, which are based on the Peres criterion [25], are defined in terms of the eigenvalues of the partially transposed density operator. Numerically, the logarithmic negativity is easy to compute with linear algebra packages. Consider a bipartite pure entangled state

$$|\phi\rangle_{AB} = \sum_{ij} \chi_{ij} |i\rangle_A |j\rangle_B, \tag{11}$$

where $|i\rangle_A$ and $|j\rangle_B$ are bases in two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. We can easily find

$$\| [|\phi\rangle_{AB}\langle\phi|]^{\mathrm{PT}} \| = \left(\sum_{i,j} \chi_{ij} \right)^2, \tag{12}$$

where ρ^{PT} is the partial transpose of ρ with respect to either subsystem, and $\|\cdot\|$ denotes the trace norm. The logarithmic negativity can then be obtained as [24]

$$E(|\phi\rangle_{AB}) = 2\,\log_2 \left| \sum_{i,j} \chi_{ij} \right|. \tag{13}$$

Thus, we can calculate the logarithmic negativities of the EPR state $|\Psi\rangle_{AB}$ and $|\Psi^{(1)}\rangle_{AB_1}$ as

$$E(|\Psi\rangle_{AB}) = -\log_2(1+\alpha^2) - 2\,\log_2(\sqrt{1+\alpha^2}-\alpha), \tag{14}$$

$$E(|\Psi^{(1)}\rangle_{AB_1}) = 2\,\log_2 \left(K \cdot \mathrm{PolyLog}\left[-\frac{1}{2}, \frac{\alpha\sqrt{\mu}}{\sqrt{1+\alpha^2}} \right] \right), \tag{15}$$

where the polylogarithm $\mathrm{PolyLog}[k,z]$ is the function $\mathrm{PolyLog}[k,z] \equiv \sum_{n=1}^{\infty} \frac{z^n}{n^k}$, and $K = \frac{1+\alpha^2(1-\mu)}{\alpha\sqrt{\mu(1+\alpha^2)}}$. Figure 2 depicts the comparison of the entanglement of Gaussian state $|\Psi\rangle_{AB}$ and the photon subtracted non-Gaussian state $|\Psi^{(1)}\rangle_{AB_1}$ in the measure of logarithmic negativity.

As can be seen in Fig. 2, the photon subtracted non-Gaussian state always has a larger amount of entanglement than the input Gaussian two-mode squeezed vacuum state, and the gap extends with μ. In this sense, the non-Gaussian operations have improved the correlation between the two modes of bipartite states. It should be mentioned that the photon number resolving detector can be used instead of the on-off type detector [18], which will lead to a photon subtracted non-Gaussian mixed state. In the following, we will show whether the increase of entanglement will improve the performance of CVQKD.

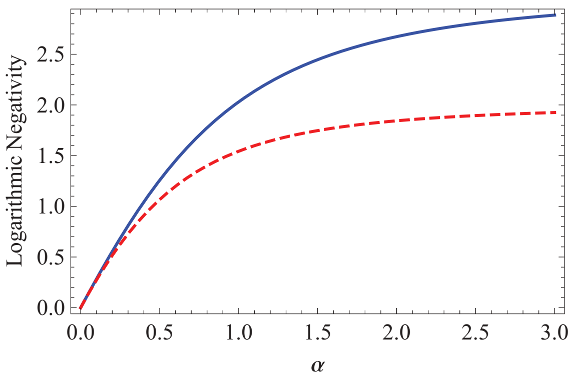

FIG. 2. (Color online) Comparison of the logarithmic negativity for state $|\Psi\rangle_{AB}$ [dashed (red) curve] and $|\Psi^{(1)}\rangle_{AB_1}$ for the non-Gaussian operations [solid (blue) curve] as the function of α with $\mu = 0.5$.

IV. SECRET KEY RATE OF CVQKD WITH PHOTON SUBTRACTION OPERATION

Now we consider the performance of the renewed CVQKD protocol with non-Gaussian operations. For simplicity, we consider the secret key rate and tolerable channel excess noise for collective attack when Bob performs homodyne detection and reverse reconciliation. Because the schemes with reverse reconciliation admit longer security distance, we can deduce the performance for heterodyne detection with the same method. As clarified above, the total noise referred to the channel input can then be expressed as $\chi_{\mathrm{thom}} = \chi_{\mathrm{line}} + \chi_{\mathrm{hom}}/T$. As known, for the Gaussian CVQKD scheme, the raw key rate can be calculated as

$$K_G = \beta I_{AB}^G - \chi_{BE}^G, \tag{16}$$

where β is the reconciliation efficiency, I_{AB}^G is the Shannon mutual information between Alice and Bob, and χ_{BE}^G is the Holevo bound [26], which defines the maximum information available to Eve on Bob's key, with the form

$$\begin{aligned} \chi_{BE}^G &= S(\rho_E) - \sum_{m_B} p(m_B) S(\rho_E^{m_B}) \\ &= S(\rho_{AB_2}) - S(\rho_{AHG}^{m_B}) \\ &= \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \end{aligned} \tag{17}$$

where $G(x) = (x+1)\log_2(x+1) - x\,\log_2 x$, $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix of state ρ_{AB_2}, and $\lambda_{3,4,5}$ are the symplectic eigenvalues of the covariance matrix characterizing the state $\rho_{AHG}^{m_B}$ after Bob's measurement. It should be noted that we use the fact that system Eve could purify the Alice-Bob system so we can get $S(\rho_E) = S(\rho_{AB_2})$ and $S(\rho_E^{m_B}) = S(\rho_{AHG}^{m_B})$. When using homodyne detection, the mutual information I_{AB}^{hom} can be derived from Bob's measured variance V_{B_3} and the conditional variance $V_{B_3|A}$ as

$$I_{AB}^{\mathrm{hom}} = \frac{1}{2} \log_2 \frac{V_{B_3}}{V_{B_3|A}}. \tag{18}$$

For simplicity, the secret key rate we considered here is the asymptotic rate, since the improvement for asymptotic rate will indicate the same exhibition for nonasymptotic rate.

Thus, to calculate Eve's information χ_{BE}^{G}, we should derive the covariance matrix Γ_{AB}^{G} of the bipartite state $\rho_{AB} = |\Psi\rangle_{AB}\langle\Psi|$, since the quantity of χ_{BE}^{G} is always upper bounded by the function of the covariance matrix of the bipartite state shared by Alice and Bob [9].

Also, the covariance matrix $\Gamma_{AB_1}^{N}$ of the state $\rho_{AB_1} = |\Psi^{(1)}\rangle_{AB_1}\langle\Psi^{(1)}|$ in the EB scheme of the protocol can be calculated in the following form:

$$\Gamma_{AB_1}^{N} = \begin{pmatrix} X\mathbf{1}_2 & Z\sigma_z \\ Z\sigma_z & Y\mathbf{1}_2 \end{pmatrix}, \tag{19}$$

where

$$X = {}_{AB_1}\langle\Psi^{(1)}|1 + 2\hat{a}^{\dagger}\hat{a}|\Psi^{(1)}\rangle_{AB_1} = 2V' + 1, \tag{20}$$

$$Y = {}_{AB_1}\langle\Psi^{(1)}|1 + 2\hat{b}^{\dagger}\hat{b}|\Psi^{(1)}\rangle_{AB_1} = 2V' - 1, \tag{21}$$

and

$$Z = {}_{AB_1}\langle\Psi^{(1)}|\hat{a}\hat{b} + \hat{a}^{\dagger}\hat{b}^{\dagger}|\Psi^{(1)}\rangle_{AB_1} = 2\sqrt{V'^2 - 1}. \tag{22}$$

In addition, $\mathbf{1}_2$ is the 2×2 identity matrix, $\sigma_z = \mathrm{diag}(1,-1)$, $\hat{a}$ and $\hat{b}$ are the photon subtraction operators on the two modes A and B_1, and $V' = \frac{1+\alpha^2(1+\mu)}{1+\alpha^2(1-\mu)}$. It can be seen that subtraction operation does not exist for $\mu = 1$, which corresponds to the original scheme $V' = V$. However, we cannot use the above method directly to obtain the secret key rate K_N for the non-Gaussian states. According to the Gaussian optimality theorem [9,10], the most powerful attack by Eve is the Gaussian attack. Suppose there exists a Gaussian state ρ'_{AB_1} with the covariance matrix $\Gamma_{AB_1}^{G} = \Gamma_{AB_1}^{N}$. In the following, we take analysis of the scheme by using the Gaussian state ρ'_{AB_1} instead of ρ'_{AB_1}. Thus we can apply the above method to obtain a lower bound of the secret key rate for non-Gaussian states as

$$\tilde{K}_N = P^{(1)}\big(\beta I_{AB}^{G} - \chi_{BE}^{G}\big), \tag{23}$$

where $P^{(1)}$ is the probability of successful implementation of photon subtraction.

After the quantum channel, the covariance matrix of ρ'_{AB_2} will be dependent on the quantum channel, which has the following form:

$$\Gamma_{AB_2}^{G} = \begin{pmatrix} X\mathbf{1}_2 & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & T(Y + \chi_{\mathrm{line}})\mathbf{1}_2 \end{pmatrix}. \tag{24}$$

Thus, Bob's measured variance $V_{B_3} = \eta T(X + \chi_{\mathrm{thom}})$ and the conditional variance $V_{B_3|A} = \eta T(1 + \chi_{\mathrm{thom}})$, the mutual information between Alice and Bob is given by

$$I_{AB}^{\mathrm{hom}} = \frac{1}{2}\log_2 \frac{X + \chi_{\mathrm{thom}}}{1 + \chi_{\mathrm{thom}}}. \tag{25}$$

Also, we can obtain the symplectic eigenvalues $\lambda_{1,2} \geqslant 1$ of the covariance matrix $\Gamma_{AB_2}^{G}$ as

$$\lambda_{1,2}^2 = \tfrac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{26}$$

where

$$A = (1 + 2V')^2 - 4T(V'^2 - 1) + T^2(2V' + \chi_{\mathrm{line}} - 1)^2,$$
$$B = T^2(2V'\chi_{\mathrm{line}} + \chi_{\mathrm{line}} + 3)^2, \tag{27}$$

and

$$\lambda_{3,4}^2 = \tfrac{1}{2}[C \pm \sqrt{C^2 - 4D}], \qquad \lambda_5 = 1, \tag{28}$$

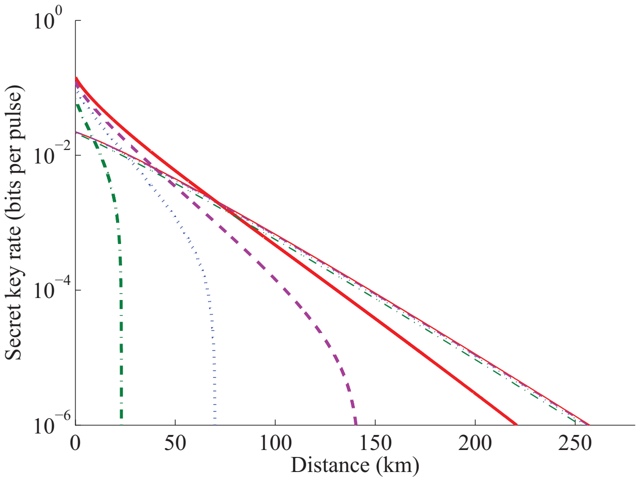

FIG. 3. (Color online) Asymptotic secret key rate $\tilde{K}_N$ of the EB scheme with photon subtraction (thin curves), and K_G of the original scheme (thick curves) as a function of distance for different values of the excess noise: the solid (red), dashed (purple), dotted (blue), and dot-dashed (green) curves correspond to $\varepsilon = 0.01$, 0.02, 0.03, and 0.05, respectively.

where

$$C = \frac{A\chi_{\mathrm{hom}} + X\sqrt{B} + T[Y + \chi_{\mathrm{line}} - 4\chi_{\mathrm{hom}}(V'^2 - 1)]}{T(Y + \chi_{\mathrm{thom}})},$$
$$D = \frac{\sqrt{B}(X + \sqrt{B}\chi_{\mathrm{hom}})}{T(Y + \chi_{\mathrm{thom}})}. \tag{29}$$

Supposing modulation variance $V_A = 0.7$, the reverse reconciliation efficiency is $\beta = 80\%$, quantum efficiency of Bob's detection is $\eta = 0.526$, electronic noise $\nu_{\mathrm{el}} = 0.043\,61$, and $\mu = 0.5$, the lower bound on the secret key rates of the EB CVQKD protocol with non-Gaussian operation are displayed in Fig. 3 (the four curves for the renewed scheme are very close for different values of channel excess noise). It can be seen that for all different channel excess noise, the renewed EB scheme admits longer secure distance communication than the original EB protocol. And interestingly, the curves denoting the secret key rates of the renewed scheme just have a tiny change in different values of channel excess noise, which shows the renewed scheme is very insensitive to the channel excess noise. So when the excess noise of the quantum channel becomes larger, the improvement of secure distance is more obvious. Thus, we can conclude the photon subtraction can well increase the secure distance and improve the tolerable excess noise. We will show below the improvement of tolerable excess noise in detail.

From simulation data, we can fit the distributions of a lower bound of tolerable channel excess noise of the renewed scheme and the exact bound of the tolerable channel excess noise of the original scheme as the function of transmission efficiency in Fig. 4. It is shown that the photon subtraction operator can quite improve the tolerable channel excess noise. Interestingly, the distribution of tolerable channel excess noise is not monotone anymore because of the change of the covariance matrix. Generally, the tolerable channel excess noise decreases in higher channel transmission efficiency, and it is less than 0.15

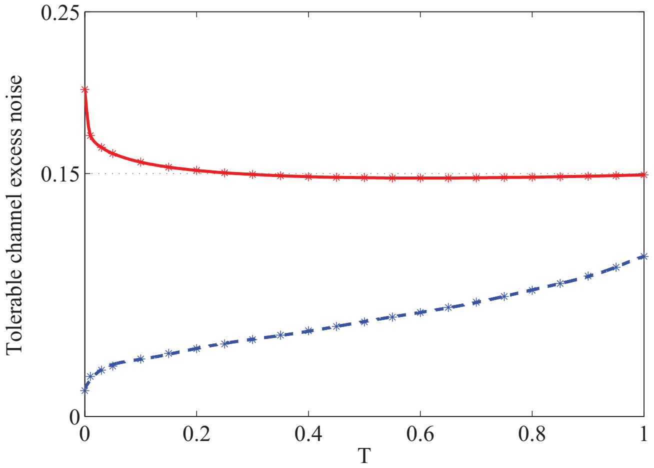

FIG. 4. (Color online) Lower bound of tolerable channel excess noise for the EB scheme with photon subtraction [upper (red) curve], and the original scheme [lower (blue) curve] as a function of transmission efficiency.

for $T \geqslant 0.3$. So the secret key rate may decrease to negative in the area 0–50 km as shown in Fig. 5, when channel excess noise increases to 0.15.

To confirm the relationship between the performance of the renewed protocol and the efficiency of photon subtraction operation, we display the secret key rate $\tilde{K}_N$ as the function of parameter μ, which affects the efficiency of photon subtraction operation, in Fig. 6. It can be seen there always exists an optimal μ to maximize the secret key rate $\tilde{K}_N$, whether the channel transmission efficiency or excess noise changes. Moreover, the communication will be insecure when μ is too small, and the minimal value of μ to keep secure CVQKD increases with channel excess noise. This coincides with the fact that almost all the beams sent to Bob are intercepted when μ is too small, which leads to low SNR. So the tolerable channel excess noise decreases with μ.

The modulation V_A is an important parameter for the CVQKD scheme, which is quite related to the secret key rate. In order to extract the optimal secret key rate $\tilde{K}_N$ at a given distance, we depict the secret key rate as a function of modulation variance V_A in Fig. 7. For the original scheme, the optional areas of V_A are gradually compressed with the increase of distance, while these areas for the proposed scheme are open. In this way, the proposed scheme can have a more flexible application. It can be seen from the figure that, the optimal value of V_A decreases with distance for the original scheme, but it increases for the scheme with a photon subtraction operator. Furthermore, since the increase of modulation variance will improve the SNR, the renewed scheme can increase modulation variance to improve the performance. So we can conclude that the introduction of photon subtraction can well improve the application flexibility of the CVQKD scheme. It should be emphasized that we

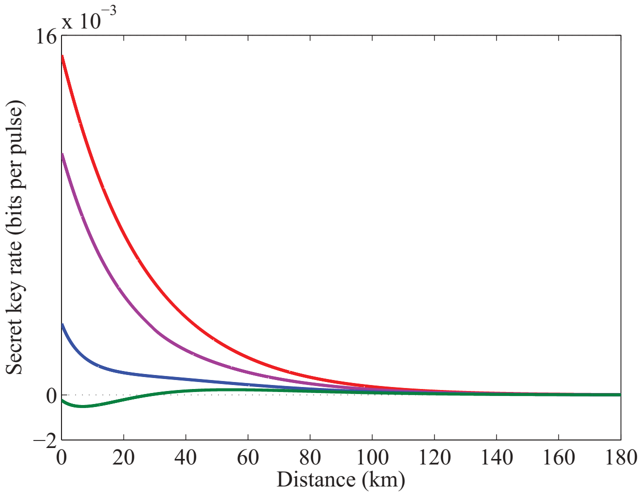

FIG. 5. (Color online) Asymptotic secret key rate $\tilde{K}_N$ of the EB scheme with photon subtraction as a function of distance for high channel excess noise. From top to bottom, $\varepsilon = 0.1$, 0.12, 0.14, 0.15.

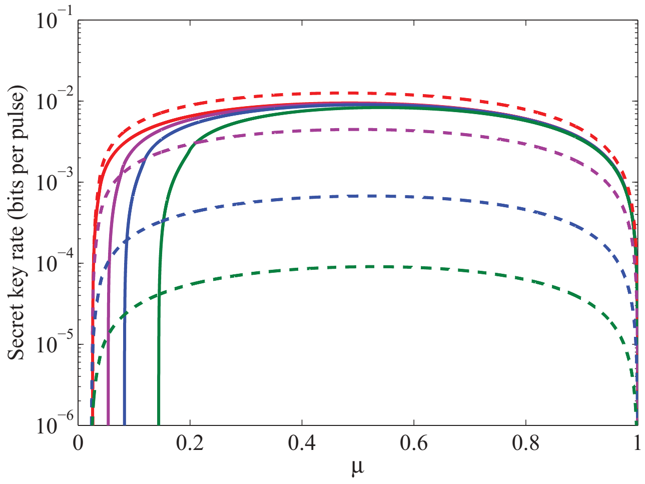

FIG. 6. (Color online) Asymptotic secret key rate $\tilde{K}_N$ as a function of μ for different values of the channel excess noise (solid curves) with given transmission efficiency $T = 0.268$, and for different distance (dashed curves) with given channel excess noise $\varepsilon = 0.01$. From top to bottom, $\varepsilon = 0.01$, 0.02, 0.03, and 0.05, and distance $d = 20$, 50, 100, and 150 km.

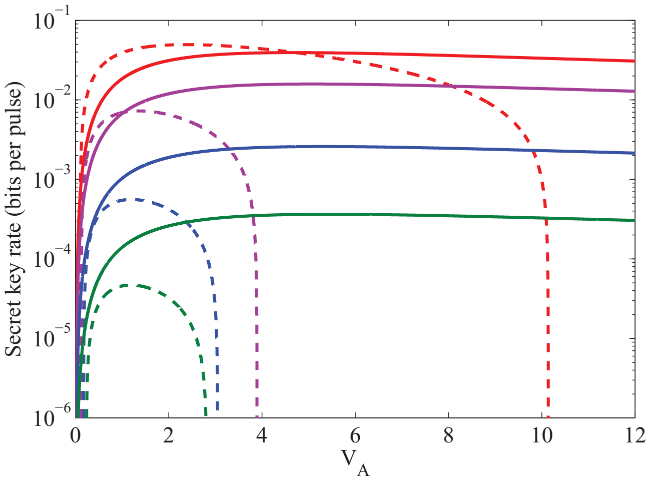

FIG. 7. (Color online) Asymptotic secret key rate $\tilde{K}_N$ of the EB scheme with photon subtraction (solid curves), and K_G of the original scheme (dashed curves) as a function of modulation variance V_A with $\mu = 0.5$, $\varepsilon = 0.01$. From bottom to top, $d = 20$, 50, 100, and 150 km.

calculate the secret key rate in consideration of the probability of successful implementation of photon subtraction. If the implementation of the non-Gaussian operators is designed to be deterministic, the improvement of performance will be considerably large.

As known, the original EB scheme is equivalent to the prepare-and-measure (P&M) scheme with coherent state source, since the symmetric measurement of X_A and P_A by Alice projects the beam (X_B, P_B) onto coherent states [27]. According to the virtual entanglement proposed in [27], the renewed EB scheme with photon subtraction can also be equivalent to a P&M scheme with a photon subtraction setting after Alice's modulation. If we generalize the transmission efficiency of the BS in the heterodyne detection of Alice's station in Fig. 1 as τ, the conditional variance $V_{X_{B_1}|X_A}$ $(V_{P_{B_1}|P_A})$, which quantifies the remaining uncertainty on X_{B_1} (P_{B_1}) after the measurement of mode A giving the estimate X_A (P_A) of X_{B_1} (P_{B_1}), is given by

$$V_{X_{B_1}|X_A} = \langle X_{B_1}^2 \rangle - \frac{\langle X_{B_1} X_A \rangle}{\langle X_A^2 \rangle} = \frac{2V'(1-\tau) + 4\tau - 1}{2V'\tau + 1} N_0, \tag{30}$$

$$V_{P_{B_1}|P_A} = \langle P_{B_1}^2 \rangle - \frac{\langle P_{B_1} P_A \rangle}{\langle P_A^2 \rangle} = \frac{2V'\tau - 4\tau + 3}{2V'(1-\tau) + 1} N_0, \tag{31}$$

where N_0 is the shot-noise variance. If $\tau = 0.5$, Alice performs heterodyne detection; one has $V_{X_{B_1}|X_A} = V_{P_{B_1}|P_A} = N_0$, i.e., the measurement of mode A also projects the beam (X_{B_1}, P_{B_1}) onto coherent states. This is also coincident with the fact that the coherent state is the eigenstate of photon subtraction operation. So the corresponding P&M scheme of the renewed protocol is also based on coherent states, but with more robust performance because of the improvement of the correlation between the legitimate parties derived from the non-Gaussian operation. Therefore, we may conclude that the performance of the P&M scheme of CVQKD based on coherent states can also be improved by using subtraction operations.

V. CONCLUSION

We have proposed a method to improve the performance of the EB CVQKD scheme with non-Gaussian operation, in particular, the photon subtraction operation. The proposed photon subtraction operation can be easily implemented under current technology. Since the states to be modulated are non-Gaussian, we calculate the lower bound on the secret key rate and tolerable channel excess noise against general collective attack with the assistance of the Gaussian optimality theorem. The results show that the proposed protocol allows much longer secure distances than the original protocol, and has much better performance in resisting the channel excess noise. Moreover, the proposed scheme has a more flexible application, since the areas for practicable modulation variance V_A can be open. Furthermore, we show the subtraction operation may also work in the equivalent P&M scheme. In summary, we have demonstrated that the photon subtraction not only can be used to improve the entanglement degree of the quantum states, but also the performance of CVQKD, including the longer secure distance, larger tolerable excess noise, and more flexible choice of modulation variance.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grants No. 61170228, No. 60970109, and No. 61102053).

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference Computers, System and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

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

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[4] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[5] F. Grosshan, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[6] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[7] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[8] 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, Phys. Rev. A **76**, 042305 (2007).

[9] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[10] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[11] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[12] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[13] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[14] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[15] A. Leverrier and P. Grangier, Phys. Rev. A **83**, 042312 (2011).

[16] J. Yang, B. Xu, X. Peng, and H. Guo, Phys. Rev. A **85**, 052302 (2012).

[17] D. E. Browne, J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. A **67**, 062320 (2003).

[18] A. Kitagawa, M. Takeoka, M. Sasaki, and A. Chefles, Phys. Rev. A **73**, 042310 (2006).

[19] S. L. Zhang and P. van Loock, Phys. Rev. A **82**, 062316 (2010).

[20] A. Ourjoumtsev, A. Dantan, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **98**, 030502 (2007).

[21] H. Takahashi, J. S. Neergaard-Nielsen, M. Takeuchi, M. Takeoka, K. Hayasaka, A. Furusawa, and M. Sasaki, Nature Photon. **4**, 178 (2010).

[22] S.-Y. Lee, S.-W. Ji, H.-J. Kim, and H. Nha, Phys. Rev. A **84**, 012302 (2011).

[23] H.-J. Kim, S.-Y. Lee, S.-W. Ji, and H. Nha, Phys. Rev. A **85**, 013839 (2012).

[24] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).

[25] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[26] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

[27] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).