

Continuous-variable quantum key distribution based on photon addition operation

Xiao-Ting Chen(陈小婷), Lu-Ping Zhang(张露萍), Shou-Kang Chang(常守康), Huan Zhang(张欢), and Li-Yun Hu(胡利云)

Citation: Chin. Phys. B, 2021, 30 (**6**): 060304. DOI: 10.1088/1674-1056/abd931
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states

Yu-Qian He(贺宇千), Yun Mao(毛云), Hai Zhong(钟海), Duang Huang(黄端), Ying Guo(郭迎)
Chin. Phys. B, 2020, 29 (**5**): 050309. DOI: 10.1088/1674-1056/ab8216

Quantifying non-classical correlations under thermal effects in a double cavity optomechanical system

Mohamed Amazioug, Larbi Jebli, Mostafa Nassik, Nabil Habiballah
Chin. Phys. B, 2020, 29 (**2**): 020304. DOI: 10.1088/1674-1056/ab65b6

Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states

Yan-Yan Feng(冯艳艳), Rong-Hua Shi(施荣华), Ying Guo(郭迎)
Chin. Phys. B, 2018, 27 (**2**): 020302. DOI: 10.1088/1674-1056/27/2/020302

Continuous variable quantum key distribution

Yong-Min Li(李永民), Xu-Yang Wang(王旭阳), Zeng-Liang Bai(白增亮), Wen-Yuan Liu(刘文元), Shen-Shen Yang(杨申申), Kun-Chi Peng(彭堃墀)
Chin. Phys. B, 2017, 26 (**4**): 040303. DOI: 10.1088/1674-1056/26/4/040303

Anonymous voting for multi-dimensional CV quantum system

Rong-Hua Shi(施荣华), Yi Xiao(肖伊), Jin-Jing Shi(石金晶), Ying Guo(郭迎), Moon-Ho Lee
Chin. Phys. B, 2016, 25 (**6**): 060301. DOI: 10.1088/1674-1056/25/6/060301

Continuous-variable quantum key distribution based on photon addition operation*

Xiao-Ting Chen(陈小婷)[1], Lu-Ping Zhang(张露萍)[1], Shou-Kang Chang(常守康)[1], Huan Zhang(张欢)[1], and Li-Yun Hu(胡利云)[1,2,†]

[1] *Center for Quantum Science and Technology, Jiangxi Normal University, Nanchang* 330022, *China*
[2] *Key Laboratory of Optoelectronic and Telecommunication, Jiangxi Normal University, Nanchang* 330022, *China*

(Received 8 December 2020; revised manuscript received 1 January 2021; accepted manuscript online 7 January 2021)

It is shown that the non-Gaussian operations can not only be used to prepare the nonclassical states, but also to improve the entanglement degree between Gaussian states. Thus these operations are naturally considered to enhance the performance of continuous variable quantum key distribution (CVQKD), in which the non-Gaussian operations are usually placed on the right-side of the entangled source. Here we propose another scheme for further improving the performance of CVQKD with the entangled-based scheme by operating photon-addition operation on the left-side of the entangled source. It is found that the photon-addition operation on the left-side presents both higher success probability and better secure key rate and transmission distance than the photon subtraction on the right-side, although they share the same maximal tolerable noise. In addition, compared to both photon subtraction and photon addition on the right-side, our scheme shows the best performance and the photon addition on the right-side is the worst.

Keywords: non-Gaussian operations, continuous variable, quantum key distribution, photon-addition operation

PACS: 03.67.–a, 05.30.–d, 42.50.Dv, 03.65.Wj **DOI:** 10.1088/1674-1056/abd931

1. Introduction

Quantum key distribution (QKD)[1–5] has been considered to be an unconditional security scheme, which is protected by the quantum mechanics principle, such as the Heisenberg uncertainty principle[6] and the noncloning theorem.[7] Generally, there are two kinds of types for realizing the QKD proposal, *i.e.*, discrete variable (DV) QKD and continuous variable (CV) QKD.[8–15] In the CVQKD protocol, the information of key bits is usually encoded by Alice (the sender) in two quadrature components of the optical field, while for the DVQKD protocol, the information of key bits is transmitted by the polarization of a single photon. This point is different from each other. On the other hand, for the former, Bob (the receiver) at the recipient port can decode the secret information by using high-speed and high-efficiency coherent detections, instead of a single-photon detection used in the latter. Thus the CVQKD protocol can achieve higher secret key rates especially in short transmission distance. In addition, the CVQKD protocols are more compatible with most classical telecommunication technologies. Based on these two reasons, much attention has been paid to the CVQKD systems. However, the performance of CVQKD for long distances is unsatisfactory.

In order to eliminate the short-distance problem, many efforts have been devoted to improving the secure transmission distance of CVQKD and lots of remarkable progress have been made both theoretically[16] and experimentally.[17,18] For instance, due to the efficient error correction codes, the CVQKD protocols with the discrete modulation,[19,20] first proposed by Leverrier and Grangier theoretically,[21] can be used to improve the secure distance to a great extent under the condition of the low signal-to-noise ratio (SNR). In addition, when the discrete-modulated scheme is applied to the measurement-device-independent (MDI) CVQKD,[22] it is shown that the maximal transmission distance can be improved compared to that of the MDI CVQKD with the Gaussian modulation.[23] Here we should notice that, in these discrete-modulated CVQKD protocols, the corresponding security proofs have not been rigorously demonstrated both theoretically and experimentally, and a way equivalent to the Gaussian modulation is still employed under the condition of a very small modulation variance. Actually, in the conventional Gaussian modulation CVQKD, the security of CVQKD against collective attack[24] and coherent attack[25] has been proved theoretically, say the Gaussian-modulated coherent states CVQKD (*i.e.*, the well-known "GG02" protocol).[26] Based on the Gaussian-modulation idea, a scheme of CVQKD with a multidimensional harmonic is proposed to improve the secure transmission distance.[27] In experiment, the field tests of CVQKD systems have lengthened the maximal transmission distance to 50 km over commercial fiber.[17] Very re-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 11664017 and 11964013) and the Training Program for Academic and Technical Leaders of Major Disciplines in Jiangxi Province, China (Grant No. 20204BCJL22053).

†Corresponding author. E-mail: hlyun@jxnu.edu.cn

© 2021 Chinese Physical Society and IOP Publishing Ltd

cently, a remote experiment CVQKD proposal has been proposed to extend the transmission distance to 202.81 km, which shortens the performance gap with the current point-to-point DVQKD systems.[18]

Except these methods above for extending the transmission distance of CVQKD, on the other hand, some local non-Gaussian operations are introduced to achieve this same purpose,[28–37] due to the fact non-Gaussian operations can be used to further distill the entanglement, such as photon addition (PA),[38–40] photon subtraction (PS),[38,39,41,42] quantum scissors,[43–45] and photon catalysis operations.[46–48] For example, the noiseless linear amplification (NLA) has been used to improve the maximal transmission distance roughly by the equivalent of $20\log_{10} g$ dB losses (g is the gain of the NLA) because of its compensation of the losses.[49,50] The PS-CVQKD protocol[29,36] has been proposed to improve its performances including secret key rate, maximal tolerable excess noise, and transmission distance. It is worth mentioning that the event of implementing non-Gaussian operations is probabilistic, especially for the success probability of the PS being less than 25%, which inevitably makes Alice and Bob lose more effective information. Recently, the performance of CVQKD is investigated when non-Gaussian operations are acted on both sides of the channels,[34] including PS, PA, and photon catalysis. It is shown that the PA operation performs the worst, although the PA presents higher success probability than the PS. However, the non-Gaussian operations are usually placed in mode B on the right-side of the entangled source. Here we propose another scheme for further improving the performance of CVQKD by operating PA operation in mode A on the left-side of the entangled source, under the entanglement-based (EB) version of CVQKD, denoted as the APA-CVQKD. It is shown that the PA operation on the left-side presents better secure key rate and transmission distance than the PS on the right-side, although both of them share the same maximal tolerable noise. Compared to both PS and PA on the right side, the proposed scheme shows the best performance. It is worth noting that the right (left) side of the entangled source means the mode from the entangled source to the quantum channel (from the entanglement source to the heterodyne detection at Alice's port (see Fig. 1)).

The rest of this paper is organized as follows. In Section 2, we first introduce the EB version of the APA-CVQKD and then achieve the relationship between input and output characteristic functions (CF) after general non-Gaussian operations, which is helpful to obtain the covariance matrix before the detections of both Alice and Bob. In Section 3, we give the performance analysis of the APA-CVQKD under the security against the collective attack. Finally, our main conclusions are drawn in Section 4.

2. The EB version of the APA-CVQKD

Figure 1(b) is our scheme, *i.e.*, the EB version of the APA-CVQKD. Here the sender, Alice, first prepares an EPR entangled source (also called two-mode squeezed state) on modes A and B, keeping mode A for going through the single-photon addition and the heterodyne detection on the left side of Fig. 1(b), while sending the other mode B through an insecure quantum channel to the receiver, Bob, for performing the homodyne detection. After Alice and Bob share two correlated Gaussian variables, the secret key rate can be extracted by the post-processing including reconciliation and privacy amplification.

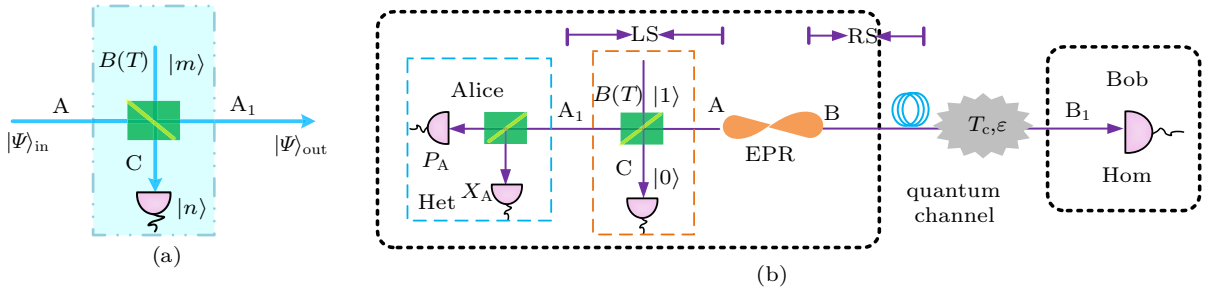


Fig. 1. (a) The schematic diagram of non-Gaussian operation. States $|m\rangle$ and $|n\rangle$ are, respectively, Fock state in auxiliary mode C $|\Psi\rangle_{\rm in}$: any input state; $|\Psi\rangle_{\rm out}$: output state after non-Gaussian operations; $B(T)$: beam splitter with a transmittance T. (b) The schematic diagram of the PA-embedded CVQKD; Einstein–Podolsky–Rosen (EPR): two-mode squeezed vacuum state, LS: left-side, RS: right-side, $T_{\rm c}$ and ε: quantum channel parameters.

In theory, the EPR entangled resource can be generated by acting a two-mode squeezing operator $S_2(r) = \exp\{r[a^\dagger b^\dagger - ab]\}$ on a two-mode vacuum state $|0,0\rangle_{\rm AB}$ on modes A and B, which is expressed as

$$\begin{aligned} |{\rm TMSV}\rangle_{\rm AB} &= S_2(r)\,|0,0\rangle_{\rm AB} \\ &= \sqrt{1-\lambda^2}\,{\rm e}^{\lambda a^\dagger b^\dagger}|0,0\rangle_{\rm AB}, \end{aligned} \tag{1}$$

where $\lambda = \tanh r = \sqrt{(V-1)/(V+1)}$ with a modulation variance V. The CF of EPR entangled resource can be calculated as

$$\begin{aligned} \chi_{\rm in}(\alpha,\beta) &= \exp\left[-\frac{1}{2}b_1|\alpha|^2 - \frac{1}{2}b_2|\beta|^2\right] \\ &\quad\times \exp\left[\frac{1}{2}(\alpha\beta + \alpha^*\beta^*)b_3\right], \end{aligned} \tag{2}$$

with $b_1 = b_2 = \cosh 2r$, $b_3 = \sinh 2r$.

In order to discuss the performance of APA-CVQKD, we

need to achieve the covariance matrix before Alice and Bob's detections. For this purpose, we first introduce the relation of CF between the input and output states after general non-Gaussian operations. As shown in Fig. 1(a), non-Gaussian operations, including PS, PA, and photon catalysis, can be realized with an asymmetrical beam splitter and condition measurement of photon number detector. The case for $m > n$ means the PA, while the cases for $m < n$ and $m = n$ are the PS and the quantum catalysis, respectively. In particular, for the case of single-photon as input and zero-photon detection, the single PA is achieved. In the following, we shall consider the single PA on Alice's left-side, which is different from previous works that the non-Gaussian operations are often placed on Alice's right-side.

For an arbitrary input state ρ, using the Weyl representation of density operators, *i.e.*,

$$\rho = \int_{-\infty}^{+\infty} \frac{\mathrm{d}^2\eta}{\pi} \chi(\eta) D(-\eta), \tag{3}$$

where $\chi(\eta)$ denotes the CF of ρ and $D(\eta) = \exp(\eta a^\dagger - \eta^* a)$ denotes the displacement operator, then the CF of the output state after undergoing the general non-Gaussian operation is shown as

$$\chi_{\mathrm{out}}(\alpha) = \int_{-\infty}^{+\infty} \frac{\mathrm{d}^2\eta}{\pi R} \chi_{\mathrm{in}}(\eta) \chi_m(\eta_1) \chi_n(\eta_2), \tag{4}$$

where $\eta_1 = \alpha/\sqrt{R} - \eta\sqrt{T/R}, \eta_2 = \eta/\sqrt{R} - \alpha\sqrt{T/R}$ $(R = 1-T)$. $\chi_{\mathrm{in}}(\eta)$ is the CF of input state and $\chi_j(x)$ $(j = m, n)$ denotes the CF of the Fock state $|j\rangle$ with

$$\chi_j(x) = \exp\left(-\frac{1}{2}|x|^2\right) \mathrm{L}_j(|x|^2), \tag{5}$$

where $\mathrm{L}_j(\cdot)$ are the Laguerre polynomials, and T is the transmissivity of the asymmetrical beam splitter.

Thus, according to Eqs. (2), (4), and (5), the CF after the single PA operation can be calculated as

$$\chi_{\mathrm{out}}(\alpha,\beta) = \frac{1}{F(0,0)} \chi_{\mathrm{in},\bar{\lambda}}(\alpha,\beta) F(\alpha,\beta), \tag{6}$$

where $\bar{\lambda} = \lambda\sqrt{T}$ and

$$F(0,0) = \frac{(1-\lambda^2)R}{(1-\bar{\lambda}^2)^2}, \tag{7}$$

is the success probability of performing the single PA, $\chi_{\mathrm{in},\bar{\lambda}}(\alpha,\beta)$ denotes the CF of the EPR obtained by replacing λ with $\bar{\lambda} = \lambda\sqrt{T}$ in Eq. (2), and $F(\alpha,\beta)$ denotes the non-Gaussian term resulted from the single PA, which is given by

$$F(\alpha,\beta) = \frac{(1-\lambda^2)R}{(1-\bar{\lambda}^2)^2} \mathrm{L}_1\left(|C|^2\right), \tag{8}$$

with $C = \alpha - \bar{\lambda}\beta^*/\sqrt{1-\bar{\lambda}^2}$.

In general, we assume that Eve is more powerful to control the quantum channel which is characteristic of transmittance T_{c} and excess noise ε. If Bob received the resulting state $\rho_{\mathrm{A_1B_1}}$ after going through the quantum channel, then the final CF of output state is given by

$$\begin{aligned}\chi_{\mathrm{fin}}(\alpha,\beta) = & \frac{\exp\left(-\dfrac{\varepsilon T_{\mathrm{c}}/R_{\mathrm{c}}+1}{2} R_{\mathrm{c}}|\beta|^2\right)}{F(0,0)} \chi_{\mathrm{in},\bar{\lambda}}(\alpha,\sqrt{T_{\mathrm{c}}}\beta) \\ & \times F(\alpha,\sqrt{T_{\mathrm{c}}}\beta),\end{aligned} \tag{9}$$

with $R_{\mathrm{c}} = 1 - T_{\mathrm{c}}$. When the CF is known, we can derive some average values of operators consisting of two orthogonal components, such as

$$\langle \hat{q}_1^2 \rangle = -\frac{\partial^2}{\partial p_1^2} \chi(0,p_1;0,0)\Big|_{p_1=0}, \tag{10}$$

$$\langle \hat{p}_1^2 \rangle = -\frac{\partial^2}{\partial q_1^2} \chi(q_1,0;0,0)\Big|_{q_1=0}, \tag{11}$$

$$\langle \hat{q}_1\hat{q}_2 \rangle = -\frac{\partial^2}{\partial p_1 \partial p_2} \chi(0,p_1;0,p_2)\Big|_{p_1,p_2=0}, \tag{12}$$

$$\langle \hat{p}_1\hat{p}_2 \rangle = -\frac{\partial^2}{\partial q_1 \partial q_2} \chi(q_1,0;q_2,0)\Big|_{q_1,q_2=0}, \tag{13}$$

where $\alpha = q_1 + \mathrm{i}p_1, \beta = q_2 + \mathrm{i}p_2$.

Thus, using Eqs. (9)–(13), the covariance matrix Γ of the final CF prior to the homodyne detection can be expressed as

$$\Gamma = \begin{pmatrix} wI & z\sigma_z \\ z\sigma_z & vI \end{pmatrix}, \tag{14}$$

where I is a 2×2 identity matrix, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is a Pauli matrix and

$$\begin{aligned} w &= 2\zeta_1^2 + \xi_1, \\ v &= 2\zeta_2^2 + \xi_2, \\ z &= 2\zeta_1\zeta_2 + \xi_3, \end{aligned} \tag{15}$$

with

$$\begin{aligned} \xi_1 &= \frac{(1+T)b_1 + R}{T + Rb_1 + 1}, \\ \xi_2 &= \frac{(1+T)b_2 + R\left(b_1b_2 - b_3^2\right)T_{\mathrm{c}}}{T + Rb_1 + 1} \\ &\quad + (\varepsilon T_{\mathrm{c}}/R_{\mathrm{c}} + 1), \\ \xi_3 &= \frac{\sqrt{T_{\mathrm{c}}}\sqrt{T}b_3}{Rb_1 + 1 + T}, \\ \zeta_1 &= \frac{\sqrt{(b_1+1)}}{\sqrt{Rb_1 + 1 + T}}, \\ \zeta_2 &= \frac{[\sqrt{T}b_3/\sqrt{(b_1+1)}]\sqrt{T_{\mathrm{c}}}}{\sqrt{Rb_1 + 1 + T}}. \end{aligned} \tag{16}$$

Equation (14) is just the covariance matrix corresponding to the non-Gaussian states before Alice and Bob's detections.

However, for non-Gaussian states, it should be noticed that equation (14) cannot be directly used to calculate the secret key rate. It is fortunate that one can employ a lower bound on secret key rate to describe the secure performance based on a Gaussian state with the same covariance matrix shown in Eq. (14), where $K^{\rm non} \geqslant K^{\rm G}$ ($K^{\rm non}$ and $K^{\rm G}$ are the secret key rates of the non-Gaussian and Gaussian states with the same covariance matrix, respectively).

3. Performance analysis of APA-CVQKD

In this section, we shall pay attention to the calculation of secret key rate for our scheme in the asymptotic limit, and provide the corresponding performance analysis.

3.1. Secure key rate

From the viewpoint of attack strategies executed by Eve, there exist three kinds of attacks: individual attack, collective attack, and coherent attack. For simplicity of calculations, here let us focus on the asymptotic secret key rate for reverse reconciliation under the collective attack which is the optimality of Gaussian attacks. According to the extremality theorem of Gaussian quantum states, the secret key rate $K^{\rm non}$ for our scheme in the asymptotic limit can be written as

$$K^{\rm non} = F(0,0)\{\beta I(A:B) - S(B:E)\}, \tag{17}$$

where $F(0,0)$ is the success probability for implementing the single-photon addition given in Eq. (7), β is the reconciliation efficiency, $I(A:B)$ is the Shannon mutual information between Alice and Bob. It is noticed that Alice and Bob perform heterodyne and homodyne detections, respectively, thus $I(A:B)$ can be derived using Eq. (14), *i.e.*,

$$I(A:B) = \frac{1}{2}\log_2 \frac{(w+1)v}{(w+1)v - z^2}, \tag{18}$$

and $S(B:E)$ is the Holevo bound which means the maximum information available to Eve on Bob's key, *i.e.*,

$$\begin{aligned} S(B:E) &= S(E) - S(E|B) \\ &= S(AB) - S(A|B). \end{aligned} \tag{19}$$

Here we have assumed that Eve can purify the whole system so that $S(E) = S(AB)$ and $S(E|B) = S(A|B)$, in which $S(AB)$ is a function of the symplectic eigenvalues $\lambda_{1,2}$ of Γ and $S(A|B)$ is a function of the symplectic eigenvalue λ_3 of $\Gamma^{\rm hom} = wI - z\sigma_Z(vI+I)^{-1}(z\sigma_Z)^{\rm T}$, $S(AB)$ and $S(A|B)$ can be calculated as

$$\begin{aligned} S(AB) &= \sum_{j=1}^{2} G\left[\frac{|\lambda_j| - 1}{2}\right], \\ S(A|B) &= G\left[\frac{\lambda_3 - 1}{2}\right], \end{aligned} \tag{20}$$

with $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2}\left[\sqrt{(w+v)^2 - 4z^2} \pm (w-v)\right], \\ \lambda_3 &= \sqrt{\frac{w(wv - z^2)}{v}}. \end{aligned} \tag{21}$$

3.2. Performance analysis

After deriving the secret key rate in the asymptotic limit, in this subsection, we shall first compare the success probabilities for the PS and PA cases, and then mainly focus on the security analyses for our scheme in terms of the secret key rate, the transmission distances and the tolerable excess noises.

According to Eq. (17), one can see that the success probability is closely related to the secret key rate. Thus, we first compare the success probabilities between the PS and the PA as a function of λ and T, as illustrated in Fig. 2. Distinctly, the success probability of implementing the PA is always higher than that of the PS, especially at the ranges of small squeezing λ and low transmittance T. This case makes it possible that the secret key rate with the PA-CVQKD can be higher than that with the PS-CVQKD.

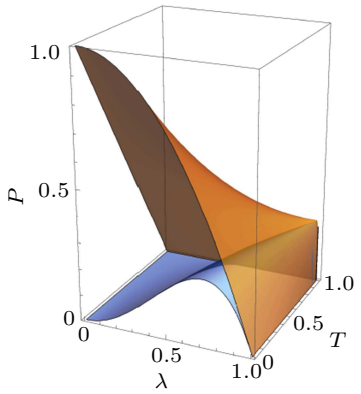


Fig. 2. The success probability as a function of squeezing parameter λ and transmittance T for single-photon subtraction and single-photon addition operations.

Actually, there are some non-Gaussian operations employed to improve the performance of EB-based CVQKD, such as the PA in mode A, the PA in mode B (denoted as BPA-CVQKD) and the PS in mode B (denoted as BPS-CVQKD). The latter two cases correspond to the case where the non-Gaussian operation is on the right side of the entangled source. Here we make a comparison about the performance of the secret key rate under these three schemes above. In Fig. 3, we show the secret key rate as a function of transmission distance and squeezing parameter λ at given some parameters $\varepsilon = 0.01$, $\beta = 0.95$, and $\lambda = 0.45, 0.50, 0.55, 0.60, 0.65, 0.70, 0.75, 0.80, 0.85, 0.90, 0.95, 0.999$, when optimized over the transmittance T. From Fig. 3, it is not difficult to see that the maximal transmission distance and the optimal secret key rate of both APA-CVQKD and BPS-CVQKD show a clear advantage over the BPA-CVQKD. In addition, our proposed APA-CVQKD scheme under the same accessible parameters

presents higher secret key rates than the BPS-CVQKD. To further see these points, at fixed parameters $\varepsilon = 0.01$, $\beta = 0.95$ and $\lambda = 0.95$, we further compare the three schemes in terms of secret key rates changing with the transmission distance for optimal choices of T in Fig. 4(a), and the optimal values of T corresponding to the maximum secret key rates are shown in Fig. 4(b). From Fig. 4(a) it is shown that the secret key rate for the original CVQKD (black solid line) shows the best performance within a short distance. The reason is that the secret key rate for several non-Gaussian schemes may be restricted by its implementation probability at short-distance ranges. However, it can be surpassed by both our scheme (APA-CVQKD) and BPS-CVQKD at long-distance ranges, especially for our scheme because of the higher probability of the PA compared to the PS case (see Fig. 2). The corresponding optimal T is about $0.666 \leq T \leq 0.670$ for the long distance transmission, see Fig. 4(b). In addition, the PA operation in mode B is the worst one among these schemes including the original CVQKD. The main reason may be that the PA operation on right side introduces more noise.[34]

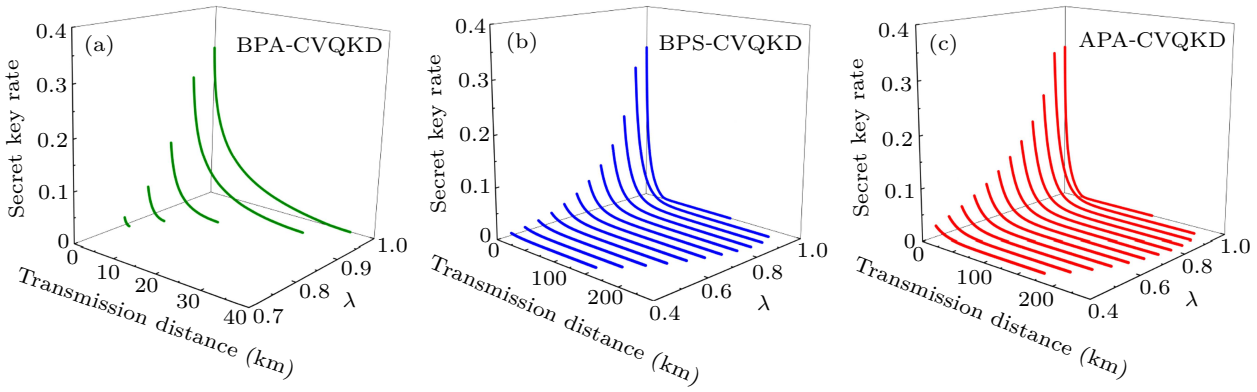


Fig. 3. The secret key rate of (a) the BPA-CVQKD, (b) the BPS-CVQKD, and (c) the APA-CVQKD as a function of transmission distance and λ for given tolerable excess noise $\varepsilon = 0.01$, $\beta = 0.95$. $\lambda = 0.45, 0.50, 0.55, 0.60, 0.65, 0.70, 0.75, 0.80, 0.85, 0.90, 0.95, 0.999$.

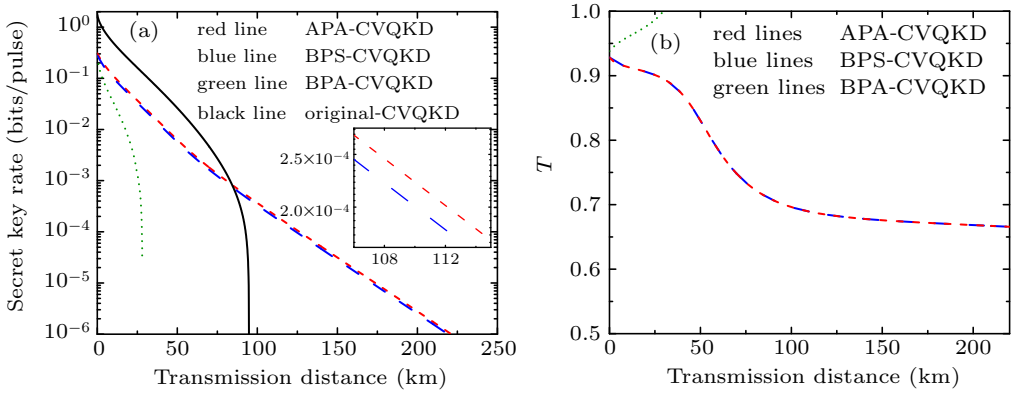


Fig. 4. (a) The optimal secret key rates over transmittance T of the APA-CVQKD (red line), the BPA-CVQKD (green line), the BPS-CVQKD (blue line), and the original protocol (black line) as a function of transmission distance when $\varepsilon = 0.01$, $\lambda = 0.95$, $\beta = 0.95$. (b) The optimal T changing with transmission distance for the maximal secret key rates in panel (a).

Next, we further consider the effects of different reconciliation efficiencies β and tolerable excess noises ε on the whole system performance. For several different values of β and ε, we plot the secret key rate as the function of the transmission distance in Fig. 5. For a comparison, both the BPS-CVQKD and the BPA-CVQKD cases are also shown here. From Fig. 5, it is shown that the transmission distance of all these schemes increases with either the increase of β or the decrease of ε, as expected. It is interesting that, for different excess noises (Fig. 5(b)) or reconciliation efficiencies (Fig. 5(a)), the performance of our scheme is the best, allowing a longer transmission distance and a better secret key rate. While the performance of the BPA-CVQKD is still the worst.

On the other hand, the tolerable excess noise is often used as an important factor of evaluating the performance of the CVQKD. Figure 6 shows the tolerable excess noise of all the schemes as the function of the transmission distance at given parameters $\beta = 0.95$ and $\lambda = 0.95$. It is worth mentioning that the two curves for both APA-CVQKD and BPS-CVQKD schemes are exactly coincident, which implies that the success probability of non-Gaussian operations has no effect on the maximal tolerable excess noise corresponding to the condition of $K^{\text{non}} = 0$, but on the special case when the distance is given. In addition, it is interesting that our scheme at long distance range can present better stability in contrast of the original CVQKD and BPA-CVQKD schemes, because the curve for APA-CVQKD has a tiny change with the increase of transmission distance. For instance, for our scheme, the max-

imal tolerable excess noise can approach about 0.0183 over the transmission distance of 293 km, which implies that when the tolerable excess noise of quantum channel has a low value $\varepsilon \in (0, 0.0183)$, the proposed scheme can satisfy the requirement of long-secure transmission distance with higher secret key rates.

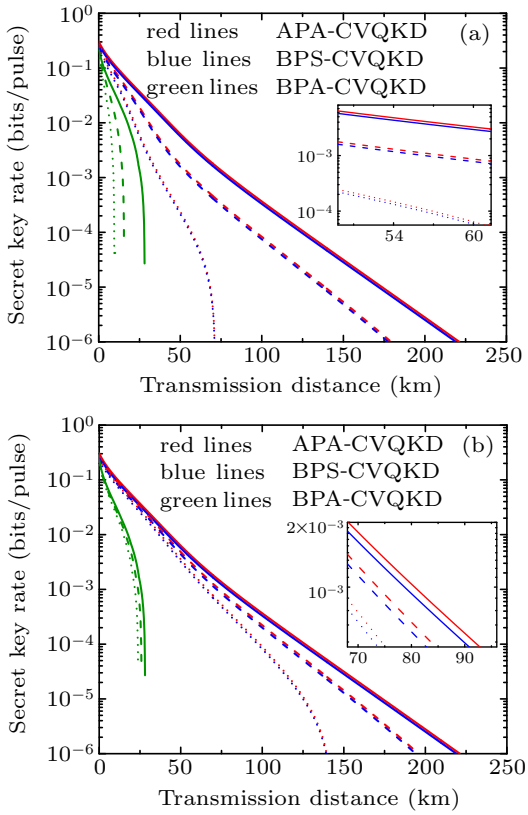


Fig. 5. The secret key rate of the APA-CVQKD, the BPA-CVQKD, the BPS-CVQKD, and original protocol as a function of transmission distance when the transmittance T is optimized for given different values of (a) $\beta = 0.95$ (solid lines), $\beta = 0.90$ (dash lines), $\beta = 0.85$ (short-dot lines), $\lambda = 0.95$ and $\varepsilon = 0.01$; (b) $\varepsilon = 0.01$ (solid lines), $\varepsilon = 0.02$ (dash lines), $\varepsilon = 0.03$ (short-dot lines), $\lambda = 0.95$ and $\beta = 0.95$.

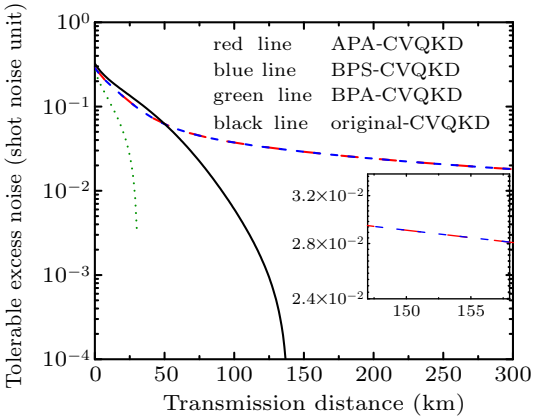


Fig. 6. The tolerable excess noise of the APA-CVQKD (red line), the BPS-CVQKD (blue line), the BPA-CVQKD (green line), and the original protocol (black line) as a function of transmission distance when T is optimized for given $\beta = 0.95$ and $\lambda = 0.95$.

4. Conclusions

In this paper, we have shown an improved performance of CVQKD with the photon-addition on the left-side of the entangled source under the EB scheme. Using the relation between the CF and the average values, we derived the covariance matrix between the legitimate communication parties prior to the corresponding detections. Then based on the Gaussian optimality theorem, we further discussed the lower bound of secret key rate for our scheme against the collective attack. It is found that the photon-addition operation on left side presents both higher success probability and better secure key rate and transmission distance than the photon subtraction on right side, although they share the same maximal tolerable noise. In addition, compared to both photon subtraction and photon addition on right side, our scheme shows the best performance and the photon addition on right side is the worst.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N L and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[2] Braunstein S L and van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[3] Wu G, Zhou C Y, Chen X L, Han X H and Zeng H P 2005 *Acta Phys. Sin.* **54** 3622 (in Chinese)
[4] Li H H, Gong L H and Zhou N R 2020 *Chin. Phys. B* **29** 110304
[5] Zhou N R, Zhu K N and Zou X F 2019 *Ann. Phys.* **531** 1800520
[6] Bang J Y and Berger M S 2006 *Phys. Rev. D* **74** 125012
[7] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[8] Bencheikh K, Symul T, Jankovic A and Levenson J A 2001 *J. Mod. Opt.* **48** 1903
[9] Ralph T C 2000 *Phys. Rev. A* **62** 062306
[10] Usenko V C and Grosshans F 2015 *Phys. Rev. A* **92** 062337
[11] Zhu J, He G Q and Zeng G H 2007 *Chin. Phys.* **16** 1364
[12] Li Y M, Wang X Y, Bai Z L, Liu W Y, Yang S S and Peng K C 2017 *Chin. Phys. B* **26** 040303
[13] Liu W Q, Peng J Y, Huang P, Wang S Y, Wang T and Zeng G H 2018 *Chin. Phys. B* **27** 070305
[14] Gong L H, Tian C, Li J F and Zou X F 2018 *Quantum Inf. Process.* **17** 331
[15] He Y Q, Mao Y, Zhong H, Huang D and Guo Y 2020 *Chin. Phys. B* **29** 050309
[16] Lim K Y, Suh C and Rhee J K 2019 *Quantum Inf. Process.* **18** 73
[17] Zhang Y C, Li Z Y, Chen Z Y, Weedbrook C, Zhao Y J, Wang X Y, Huang Y D, Xu C C, Zhang X X, Wang Z Y, Li M, Zhang X Y, Zheng Z Y, Chu B J, Gao X Y, Meng N, Cai W W, Wang Z, Wang G, Yu S and H Guo 2019 *Quantum Sci. Technol.* **4** 035006
[18] Zhang Y C, Chen Z Y, Pirandola S, Wang X Y, Zhou C, Chu B J, Zhao Y J, Xu B J, Yu S and Guo H 2020 *Phys. Rev. Lett.* **125** 010502
[19] Samsonov E, Goncharov R, Gaidash A, Kozubov A, Egorov V and Gleim A 2020 *Sci. Rep.* **10** 10034
[20] Shen Y and Zou H X 2010 *Acta Phys. Sin.* **59** 147308 (in Chinese)
[21] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[22] Ma H X, Huang P, Bai D Y, Wang T, Wang S Y, Bao W S and Zeng G H 2019 *Phys. Rev. A* **99** 022322
[23] Zhang S J, Xiao C, Zhou C, Wang X, Yao J S, Zhang H L and Bao W S 2020 *Chin. Phys. B* **29** 020301
[24] Patron R G and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[25] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502
[26] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[27] Jouguet P, Kunz-Jacques S and Leverrier A 2011 *Phys. Rev. A* **84** 062317
[28] Zhou J, Shi R H, Feng Y Y, Shi J J and Guo Y 2019 *J. Phys. A* **52** 245303
[29] Huang P, He G Q, Fang J and Zeng G H 2013 *Phys. Rev. A* **87** 012317
[30] Ye W, Guo Y, Xia Y, Zhong H, Zhang H, Ding J Z and Hu L Y 2020 *Acta Phys. Sin.* **69** 060301 (in Chinese)
[31] Wu J N, Liu S Y, Hu L Y, Huang J H, Duan Z L and Ji Y H 2015 *J. Opt. Soc. Am. B* **32** 2299
[32] Guo Y, Ye W, Zhong Hand Liao Q 2019 *Phys. Rev. A* **99** 032327

[33] Ye W, Zhong H, Liao Q, Huang D, Hu L Y and Guo Y 2019 *Opt. Express* **27** 17186
[34] Hu L Y, Al-amri M, Liao Z Y and Zubairy M S 2020 *Phys. Rev. A* **102** 012608
[35] Ye W, Zhang H, Wu X D, Hu L Y and Guo Y 2020 *Quantum Inf. Process.* **19** 346
[36] Li Z Y, Zhang Y C, Wang X Y, Xu B J, Peng X and Guo H 2016 *Phys. Rev. A* **93** 012310
[37] Ma H X, Huang P, Bai D Y, Wang S Y, Bao W S and Zeng G H 2018 *Phys. Rev. A* **97** 042329
[38] Zhang S L, Dong Y L, Zou X B, Shi B S and Guo G C 2013 *Phys. Rev. A* **88** 032324
[39] Benlloch C N, Patron R J, Shapiro J H and Cerf N J 2016 *Phys. Rev. A* **86** 012328
[40] Yang Y 2016 *J. Opt. Soc. Am. B* **33** 002545
[41] Bartley T J, Crowley P J D, Datta A, Nunn J, Zhang L J and Walmsley I 2013 *Phys. Rev. A* **87** 022313
[42] Zhang S L and van Loock P 2010 *Phys. Rev. A* **82** 062316
[43] X X Xu, L Y Hu and Z Y Liao 2018 *J. Opt. Soc. Am. B* **35** 000174
[44] Hu L Y, Al-amri M, Liao Z Y and Zubariy M S 2019 *Phys. Rev. A* **100** 052322
[45] Liu C J, Yu M, Ye W, Zhang H and Hu L Y 2020 *Results Phys.* **19** 103616
[46] Xu X X 2015 *Phys. Rev. A* **92** 012318
[47] Hu L Y, Liao Z Y and Zubairy M S 2017 *Phys. Rev. A* **95** 012310
[48] Zhou W D, Ye W, Liu C J, Hu L Y and Liu S Q 2018 *Laser Phys. Lett.* **15** 065203
[49] Xu B J, Tang C M and Chen H 2013 *Phys. Rev. A* **87** 062311
[50] Zhang Y C, Li Z Y, Weedbrook C, Marshall K, Pirandola S, Yu S and Guo H 2015 *Entropy* **17** 04547