Quantum relay schemes for continuous-variable quantum key distribution

Ying Guo,[1] Qin Liao,[1] Duan Huang,[1,2,*] and Guihua Zeng[2]
[1]*School of Information Science and Engineering, Central South University, Changsha 410083, China*
[2]*State Key Laboratory of Advanced Optical Communication Systems and Networks,*
and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China

(Received 18 February 2017; published 18 April 2017)

We propose several concatenated quantum relay continuous-variable quantum key distribution schemes based on the parametric amplifier (PA) and the beam splitter (BS). Instead of using only one BS in the traditional relay scheme, the proposed schemes provide two operations that involve both PA and BS, activating the beam splitting and recombining operations in turn. These schemes would benefit the system performance improvement by providing signal amplification and establishing quantum correlations. We show that the different effects of the relay schemes will cause different system performances because of the varied signal-to-noise ratio (SNR) of output fields. The system's secret key rate will be increased when equipping with the PA-BS relay scheme, because the output fields of the PA are entangled with the correlated quantum noises while input fields of the BS are superimposed, subsequently leading to the quantum noise reduction of the total output fields of relay station, while the reversed BS-PA relay scheme has little advantage over the traditional counterpart that contains only one BS in relay data postprocessing because it will not cause any SNR improvement. Moreover, the reinforced PA-PA relay scheme results in a slight improvement due to the increased SNR. These quantum relay schemes can be performed through the beam splitting, the recombining operations, and the relay data postprocessing, such that it would be suitable for secret information exchange in complex networks with intermediate stations.

DOI: 10.1103/PhysRevA.95.042326

I. INTRODUCTION

Quantum key distribution (QKD) techniques have a widely practical application and are being investigated actively [1,2]. Many QKD studies are based on an assumption that devices are perfect and cannot be eavesdropped by a third untrusted party. However, it may be insufficient to ensure its viability in a complex scenario, where two participants are usually not connected by one direct link but by one or more intermediate stations for relay communications. Some implicit flaws may exist in imperfect devices, so that it may provide alternative side channels being attacked by powerful eavesdroppers [3,4]. To remove all existing and yet-to-be-discovered detector side channels, an initial relay scheme known as measurement-device-independent (MDI) QKD was proposed [5,6]. It offers an immense security advantage over standard security proofs and has the power to double the secure distance while the third untrusted participant is located in the middle [5]. Much progress has been achieved in discrete-variable (DV) MDI-QKD [7–10] and continuous-variable (CV) MDI-QKD [11,12]. In a CV MDI-QKD protocol, the sender usually encodes information in quadratures of an optical field using Gaussian modulation, and the receiver decodes the secret information with homodyne or heterodyne detectors. It has become an important research topic since it has many practical advantages, especially for a metropolitan QKD network [13].

The motivation for developing a CV MDI-QKD protocol stems from its tempting promise of a high secret key rate. However, the transmission distances of the CV MDI-QKD protocol are short when compared with a DV counterpart [11]. The primal reason is that the raw keys distributed between legal participants are usually Gaussian random values, whereas the relay data postprocessing is sophisticated. Several proposed methods were developed to solve this problem, such as deploying a noiseless linear amplifier (NLA) [14] and designing a highly efficient reconciliation algorithm at a low signal-to-noise ratio (SNR) [15]. It has been demonstrated that the secure distance of CV-QKD can be increased when equipped with the separate parametric amplifier (PA) in the channels [16]. However, such a scheme cannot be directly concatenated and hence is unsuitable for secret information exchanging in complex networks with intermediate stations [5]. In a quantum relay configuration, both communication sides, Alice and Bob, can transmit the random coherent states to a relay station so that they can establish an exact secret relation [17,18] where relay data postprocessing occurs with concatenated relay schemes involving the beam splitting and recombining operations. Even though the untrusted relay station may be completely controlled by Eve and the links are subject to optimal coherent attacks, Alice and Bob can still extract a secret key after performing suitable reconciliation algorithms.

In this paper, we propose several concatenated quantum relay CV-QKD schemes based on the PA and the beam splitter (BS). These schemes would benefit the system performance improvement by providing signal amplification and establishing quantum correlations. Instead of using only one BS in the traditional relay scheme, the proposed schemes provide two operations that involve both PA and BS, activating the beam splitting and recombining operations in turn. In principle, the two operations can be rearranged in different orders. We show that the different effects of the PA-BS relay CV-QKD scheme and the reversed BS-PA relay CV-QKD scheme will cause different system performances because of the varied SNR of output fields. First, in the PA-BS relay scheme, the improvement of the secret key rate comes from the increased SNR of the output fields. This is because the quantum noise

[*] Corresponding author: duan.huang@foxmail.com

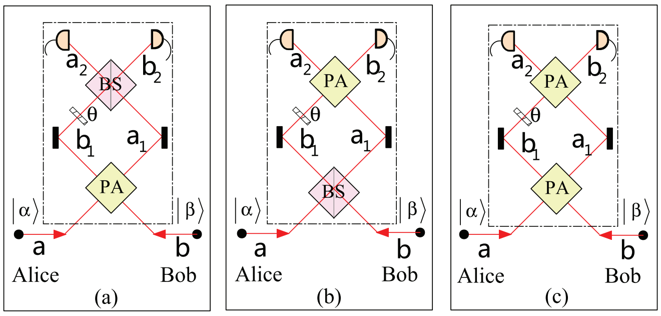

FIG. 1. Schematic diagram for the concatenated relay schemes in CV-QKD: (a) the PA-BS relay scheme, (b) the reverse BS-PA relay scheme, and (c) the reinforced PA-PA relay scheme.

of the output fields of the PA is entangled and the beam recombination operation at the BS incurs the quantum noise cancellation. However, in the reverse BS-PA relay scheme, although the signal is amplified, the noise is simultaneously amplified so that it will not cause any SNR improvement. Moreover, we also studied the reinforced scheme, which we called a PA-PA relay scheme. This scheme provides a slight improvement because the yielded entanglement in the first PA plays an important role in canceling the amplified noise, whereas the amplification in the second PA results in signal enhancement.

This paper is organized as follows. In Sec. II, we design the PA-BS relay scheme in CV-QKD with security analysis. In Sec. III, we show the PA concatenated relay schemes, including the reverse BS-PA relay scheme and the reinforced PA-PA relay scheme, discussing their performance in Sec. IV. Finally, we conclude the paper in Sec. V.

II. THE RELAY SCHEMES IN CV-QKD

Motivated by characteristics of the MDI-based quantum cryptograph with only one BS at the relay station [11], we consider the concatenated relay schemes involving the BS and PA operations in CV-QKD in which two participants, i.e., Alice and Bob, are not linked by a direct link but both are connected to an untrusted participant that establishes a secret relation in a cooperative fashion. The relay schemes are depicted in Fig. 1, where (a) is for the PA-BS relay scheme, (b) is for the reverse BS-PA relay scheme, and (c) is for the reinforced PA-PA relay scheme, respectively.

To create a secret relation on the target, Alice and Bob prepare modes a and b in coherent states $|\alpha\rangle$ and $|\beta\rangle$ whose amplitudes $\alpha = \frac{1}{\sqrt{2}}(x_\alpha + ip_\alpha)$ and $\beta = \frac{1}{\sqrt{2}}(x_\beta + ip_\beta)$ are respectively modulated by Gaussian distribution with zero mean and variance ν in each quadrature. After that, modes a and b are transmitted to a relay station, touching upon relay communications.

A. Design of the PA-BS relay scheme

In the PA-BS relay scheme, as shown in Fig. 1(a), the beam-splitting operation is a PA and the beam recombining operation is a BS. The effect of the PA can be expressed by

$$\hat{a}_1 = G\hat{a} + g\hat{b}^\dagger, \quad \hat{b}_1 = G\hat{b} + g\hat{a}^\dagger, \tag{1}$$

where G and g are positive and satisfy the constraint $G^2 - g^2 = 1$. The intensities of output modes a_1 and b_1 are $G^2\alpha^2 + g^2\beta^2 + g^2$ and $G^2\beta^2 + g^2\alpha^2 + g^2$, respectively. If the amplitude gain G is large enough, we have $G \approx g$, and hence the yielded intensities are almost equal to each other. The yielded output fields $\hat{a}_1$ and $\hat{b}_1$ are well correlated for the suitable G, causing the coherent states to recur.

A practical beam recombination operation comes into being from a successive operation performed on b_1 subject to a phase shift θ, before we composite a_1 and b_1 using a modulated BS with transmittance T. The effect of the BS is given by

$$\hat{a}_2 = \sqrt{T}\hat{a}_1 + e^{i\theta}\sqrt{R}\hat{b}_1, \quad \hat{b}_2 = e^{i\theta}\sqrt{T}\hat{b}_1 - \sqrt{R}\hat{a}_1, \tag{2}$$

where $T + R = 1$. Combining the relations in Eqs. (1) and (2), we achieve the total input-output relations as follows:

$$\hat{a}_2 = G\sqrt{T}\hat{a} + ge^{i\theta}\sqrt{R}\hat{a}^\dagger + Ge^{i\theta}\sqrt{R}\hat{b} + g\sqrt{T}\hat{b}^\dagger, \tag{3}$$

$$\hat{b}_2 = Ge^{i\theta}\sqrt{T}\hat{b} - g\sqrt{R}\hat{b}^\dagger - G\sqrt{R}\hat{a} + ge^{i\theta}\sqrt{T}\hat{a}^\dagger. \tag{4}$$

At output fields $\hat{a}_2$ and $\hat{b}_2$, we have $\hat{x}_{\tau_2} = \frac{1}{\sqrt{2}}(\hat{\tau}_2^\dagger + \hat{\tau}_2)$ and $\hat{p}_{\tau_2} = \frac{i}{\sqrt{2}}(\hat{\tau}_2^\dagger - \hat{\tau}_2)\ \hat{\tau}_2, \forall\tau \in \{a,b\}$, i.e.,

$$\hat{x}_{a_2} = G\sqrt{T}\hat{x}_a + g\sqrt{R}\hat{x}_a(\theta) + g\sqrt{T}\hat{x}_b + G\sqrt{R}\hat{x}_b(-\theta), \tag{5}$$

$$\hat{x}_{b_2} = G\sqrt{T}\hat{x}_b(-\theta) - g\sqrt{R}\hat{x}_b + g\sqrt{T}\hat{x}_a(\theta) - G\sqrt{R}\hat{x}_a, \tag{6}$$

$$\hat{p}_{a_2} = G\sqrt{T}\hat{p}_a - g\sqrt{R}\hat{p}_a(\theta) - g\sqrt{T}\hat{p}_b + G\sqrt{R}\hat{p}_b(-\theta), \tag{7}$$

$$\hat{p}_{b_2} = G\sqrt{T}\hat{p}_b(-\theta) + g\sqrt{R}\hat{p}_b - g\sqrt{T}\hat{p}_a(\theta) - G\sqrt{R}\hat{p}_a, \tag{8}$$

where $\hat{x}_\tau = \frac{1}{\sqrt{2}}(\hat{\tau}^\dagger + \hat{\tau})$, $\hat{x}_\tau(\theta) = \frac{1}{\sqrt{2}}(e^{i\theta}\hat{\tau}^\dagger + e^{-i\theta}\hat{\tau})$, $\hat{p}_\tau = \frac{i}{\sqrt{2}}(\hat{\tau}^\dagger - \hat{\tau})$, and $\hat{p}_\tau(\theta) = \frac{i}{\sqrt{2}}(e^{i\theta}\hat{\tau}^\dagger - e^{-i\theta}\hat{\tau})$, respectively. Without loss of generality, we consider quadrature momentums $\hat{x}_{a_2}$ and $\hat{x}_{b_2}$ of a_2 and b_2 in relay data processing. Taking $\theta = 0$, we obtain the signal variables

$$x_{a_2} = (G\sqrt{T} + g\sqrt{R})x_\alpha + (g\sqrt{T} + G\sqrt{R})x_\beta, \tag{9}$$

$$x_{b_2} = (G\sqrt{T} - g\sqrt{R})x_\beta + (g\sqrt{T} - G\sqrt{R})x_\alpha. \tag{10}$$

Consequently, the noise of $\hat{a}_2$ and $\hat{b}_2$ can be derived as

$$\langle\Delta^2\hat{x}_{a_2}\rangle = G^2 + g^2 + 4Gg\sqrt{RT}, \tag{11}$$

$$\langle\Delta^2\hat{x}_{b_2}\rangle = G^2 + g^2 - 4Gg\sqrt{RT}. \tag{12}$$

Because the noise of $\hat{a}_2$ is correlated with $\hat{b}_2$, we may subtract the current from the homodyne measurement of $\hat{b}_2$ and obtain output fields

$$\hat{x}_r = \hat{x}_{a_2} - \lambda_x\hat{x}_{b_2}, \tag{13}$$

where λ_x is an electronic gain that brings about an optimal noise reduction. The classical outcomes can be united in a quadrature-momentum amplitude variable

$$x_r = x_{a_2} - \lambda_x x_{b_2}, \tag{14}$$

and the noise can be described as

$$\langle \Delta^2 \hat{x}_r \rangle = \big\langle \big(\Delta \hat{x}_{a_2} - \lambda_x \Delta \hat{x}_{b_2} \big)^2 \big\rangle. \tag{15}$$

It is then straightforward to derive

$$\langle \Delta^2 \hat{x}_r \rangle_{\text{opt}} = \big\langle \Delta^2 \hat{x}_{a_2} \big\rangle - \big\langle \Delta^2 \hat{x}_{b_2} \big\rangle = 8Gg\sqrt{RT}, \tag{16}$$

with $\lambda_x = \langle \Delta \hat{x}_{a_2} \cdot \Delta \hat{x}_{b_2} \rangle / \langle \Delta^2 \hat{x}_{b_2} \rangle$ (see Appendix A for the derivation). For $T = 1/2$ corresponding to $\lambda_x = 1$, we obtain $\langle \Delta^2 \hat{x}_r \rangle_{\text{opt}} \simeq 4Gg$. After that, we have a classical outcome in a real variable x_r given by

$$x_r = x_{a_2} - x_{b_2} = \sqrt{2}(g x_\alpha + G x_\beta). \tag{17}$$

Similarly, we consider quadrature phases $\hat{p}_{a_2}$ and $\hat{p}_{b_2}$ of $\hat{a}_2$ and $\hat{b}_2$, resulting in another classical outcome,

$$p_r = p_{a_2} + p_{b_2} = \sqrt{2}(G p_\alpha - g p_\beta). \tag{18}$$

Combining x_r with p_r, we obtain a complex variable γ represented by

$$\gamma = \frac{1}{\sqrt{2}}(x_r + i p_r). \tag{19}$$

The outcome γ for $G \simeq g$, which establishes an approximative posterior correlation

$$\gamma \simeq G(\alpha + \beta^*) + \delta, \tag{20}$$

is then unveiled to Alice and Bob, where δ denotes the detection noise. For the given parameter G, knowledge of δ enables one participant to deduce the variable of another through data postprocessing. For example, to restore Alice's variable α, Bob can calculate

$$\alpha = \gamma / G - \beta^* + \delta / G. \tag{21}$$

According to the above-derived relay data postprocessing, the mutual information $I(A:B|\gamma)$ of Alice and Bob conditional on γ is increased due to the beam-splitting and recombining operations. Without knowledge of β (or α), Eve cannot steal any information on α (or β) even if she has full access to classical communications with the intercepted γ. In addition, exploiting the noises of a_2 and b_2 in Eq. (11), we have the SNRs $S_{x_{a_2}} = S_{x_{b_2}} = (x_\alpha + x_\beta)^2/2$ for the given $T = 1/2$. We assume that the relay information transfers of a_2 and b_2 can be characterized by $T_{a_2} = S_{x_{a_2}}/x_\alpha^2$ and $T_{b_2} = S_{x_{b_2}}/x_\beta^2$, respectively. The total relay information transfer for the proposed PA-BS relay scheme is $T_{\text{tot}} = T_{a_2} + T_{b_2}$, which reaches a minimum value of 4 for large gain $G \simeq g$. However, in the initial CV MDI-QKD protocol with only a BS at the relay station, the minimum total information transfer is calculated as 2, which is reduced by half. It implies that the PA-BS relay scheme can result in an improvement in terms of the relay information transfer.

B. Security analysis of coherent Gaussian attack

Before we consider the worst scenario with the PA-BS relay scheme against optimal coherent Gaussian attacks, we construct the general attack model first. As depicted in Fig. 2(a), the relay station is controlled by Eve, namely, the untrusted eavesdropper. Meanwhile, the two input modes a and b are intercepted with Eve's ancillary modes e_a and e_b, which are correlated in the globally combined system (e_a, e_b, and an extra system ε) and are equivalent to BSs with transmission efficiencies t_a and t_b, respectively. Thus, the reduced state $\sigma_{e_a e_b}$ can be repressed as a correlated thermal state with a zero mean and covariance matrix $V_{e_a e_b}$ given by

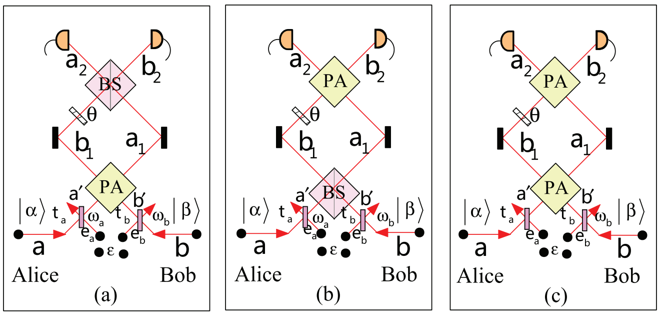

FIG. 2. Schematic diagram for the attacked CV-QKD system: (a) the attacked PA-BS relay scheme, (b) the attacked BS-PA relay scheme, and (c) the attacked PA-PA relay scheme.

$$V_{e_a e_b} = \begin{pmatrix} \omega_a \mathcal{I} & \mathcal{G} \\ \mathcal{G} & \omega_b \mathcal{I} \end{pmatrix}, \tag{22}$$

where $\mathcal{I} = \text{diag}(1,1)$, $\mathcal{G} = \text{diag}(g_1, g_2)$, with g_1 and g_2 satisfying the bona fide conditions [13], and the notations ω_a and ω_b denote variances of the thermal noises effecting links. Specifically, parameters g_1, g_2, and ω should satisfy the following constraints [11] given by

$$|g_1| < \omega, \quad |g_2| < \omega, \quad \sqrt{\omega^2 + g_1 g_2 - \omega |g_1 + g_2|} \geqslant 1, \tag{23}$$

where ω is the thermal state noise corresponding to ω_a and ω_b. In what follows, we analyze the worst scenario in which the vulnerable links are subject to the optimal coherent Gaussian attacks [19], $g_1 = -g_2 = \pm\sqrt{\omega^2 - 1}$. The different attacks satisfied by constraint Eq. (23) are detailed in Appendix D.

Assuming that Alice is a transmitter and Bob is the receiver, Bob can deduce Alice's variable α through using an optimal estimator of γ. This is an effective process, since for large gain $G \simeq g$ at the relay station it can offer the estimated variable $\tilde{\gamma}$ given by

$$\gamma \simeq \tilde{\gamma} = G\sqrt{t_a}\alpha^* + g\sqrt{t_b}\beta \simeq G(\sqrt{t_a}\alpha^* + \sqrt{t_b}\beta), \tag{24}$$

with transmission efficiencies t_a and t_b accessible to Alice and Bob.

Adopting an equivalent entanglement-based (EB) scheme, where each source of coherent state is an Einstein-Podolsky-Rosen (EPR) state, as shown in Fig. 3, Alice and Bob prepare two EPR states ρ_{Aa} and ρ_{Bb} with zero mean and the CM $V(\mu)$ given by

$$V(\mu) = \begin{pmatrix} \mu \mathcal{I} & \nu \mathcal{Z} \\ \nu \mathcal{Z} & \mu \mathcal{I} \end{pmatrix} \tag{25}$$

subject to $\mu^2 - \nu^2 = 1$, where $\mathcal{Z} = \text{diag}(1, -1)$. After heterodyning modes A and B, Alice and Bob create coherent states $|\alpha\rangle$ and $|\beta\rangle$ on modes a and b, whose amplitudes are modulated by two complex Gaussian variables α and β with variance $\varphi = \mu - 1$. For the given outcome γ, Alice, Bob, and Eve share the conditional state $\Phi_{ABe|\gamma}$ with the reduced

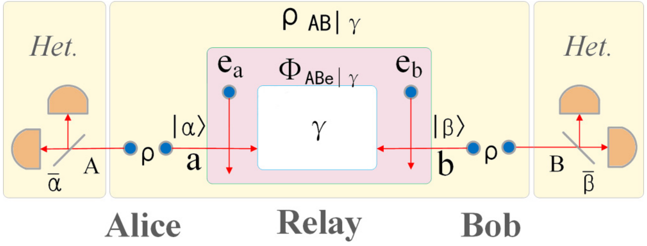

FIG. 3. Schematic diagram for the EB CV-QKD, where Alice's and Bob's measurements $\bar{\alpha}$ and $\bar{\beta}$ are equivalent to amplitudes of $|\alpha\rangle$ and $|\beta\rangle$. "*Het.*" denotes heterodyne detection.

$\rho_{e|\gamma}$ (for Eve) and $\rho_{AB|\gamma}$ (for Alice and Bob). The reduced states $\rho_{AB|\gamma}$ (or $\rho_{e|\gamma}$) have the same CM $V_{AB|\gamma}$ (or $V_{e|\gamma}$), even though their mean values vary with γ. Since Eve performs homodyne detections, the state $\Phi_{ABe|\gamma}$ is pure, leading to the Holevo quantities $S(\rho_{AB|\gamma}) = S(\rho_{e|\gamma})$.

After Alice encodes information by heterodyning mode A with outcome $\bar{\alpha}$, she projects $\Phi_{ABe|\gamma}$ into $\rho_{Be|\gamma\bar{\alpha}}$ so that $S(\rho_{B|\gamma}) = S(\rho_{e|\gamma\bar{\alpha}})$. It is worth noticing that the attack state noise ω can be tuned to match the noise of the real channel so that attacks can be deemed an extra channel loss and noise during the security analysis. As a result, Eve's intercepted information on Alice's variable $\bar{\alpha}$ is upper-bounded by [13]

$$I_{e|\gamma} = S(\rho_{e|\gamma}) - S(\rho_{e|\gamma\bar{\alpha}}) = S(\rho_{AB|\gamma}) - S(\rho_{B|\gamma}). \tag{26}$$

To recover $\bar{\alpha}$, Bob heterodynes mode B with outcome $\bar{\beta}$. Conditional on γ, the mutual information $I_{ab|\gamma}$ of Alice and Bob is derived as

$$I_{ab|\gamma} = I(\bar{\alpha},\bar{\beta}|\gamma) = I(\alpha,\beta|\gamma), \tag{27}$$

which is determined by $\rho_{AB|\gamma}$ with the CM $V_{AB|\gamma}$ given by (see Appendix B for the derivation)

$$V_{AB|\gamma} = \mu\mathcal{I}_{AB} - \nu^2 \times \begin{pmatrix} \frac{G^2 t_a}{\delta_1} & 0 & \frac{Gg\sqrt{t_a t_b}}{\delta_1} & 0 \\ 0 & \frac{g^2 t_a}{\delta_2} & 0 & -\frac{Gg\sqrt{t_a t_b}}{\delta_2} \\ \frac{Gg\sqrt{t_a t_b}}{\delta_1} & 0 & \frac{g^2 t_b}{\delta_1} & 0 \\ 0 & -\frac{Gg\sqrt{t_a t_b}}{\delta_2} & 0 & \frac{G^2 t_b}{\delta_2} \end{pmatrix}, \tag{28}$$

where δ_1 and δ_2 are the parameters determined by the attack strategies. Subsequently, we have the CM of Bob's reduced state $\rho_{B|\gamma}$ and the CM of Bob's state $\rho_{B|\gamma\hat{\alpha}}$ conditional on Alice's detection, i.e.,

$$V_{B|\gamma} = \begin{pmatrix} \mu - \frac{g^2\nu^2 t_b}{\delta_1} & 0 \\ 0 & \mu - \frac{G^2\nu^2 t_b}{\delta_2} \end{pmatrix}, \tag{29}$$

and

$$V_{B|\gamma\bar{\alpha}} = \begin{pmatrix} \mu - \frac{g^2\nu^2 t_b}{\delta_1 + G^2 t_a} & 0 \\ 0 & \mu - \frac{G^2\nu^2 t_b}{\delta_2 + g^2 t_a} \end{pmatrix}. \tag{30}$$

Therefore, the secret key rate can be calculated as

$$R(\gamma) = \eta I_{ab|\gamma} - I_{e|\gamma}, \tag{31}$$

with reconciliation efficiency $\eta \leqslant 1$ (see Appendix C for the derivation). The first term $I_{ab|\gamma}$ depends on $V_{B|\gamma}$ in Eq. (29) and $V_{B|\gamma\bar{\alpha}}$ in Eq. (30) because of the association of measurement outcomes $(\bar{\alpha},\bar{\beta})$ with Bob's reduced CM $V_{b|\gamma} = V_{B|\gamma} + \mathcal{I}$ and the conditional CM $V_{b|\gamma\bar{\alpha}} = V_{B|\gamma\bar{\alpha}} + \mathcal{I}$. Then we have

$$I_{ab|\gamma} = \frac{1}{2}\log_2 \frac{V_{b|\gamma}}{V_{b|\gamma\bar{\alpha}}}, \tag{32}$$

which can be rewritten as the SNR-based formula $I_{ab} = \frac{1}{2}\log_2 u/\chi$ with $\chi = \mu V_{b|\gamma\bar{\alpha}}/V_{b|\gamma}$. In addition, according to Eve's intercepted information $I_{e|\gamma}$ derived in Eq. (26), we have the second term calculated as [13]

$$I_{e|\gamma} = h(\lambda_1) + h(\lambda_2) - h(\lambda), \tag{33}$$

where $h(x) = (\frac{x+1}{2})\log_2(\frac{x+1}{2}) - (\frac{x-1}{2})\log_2(\frac{x-1}{2})$, $\{\lambda_1,\lambda_2\}$ are the symplectic spectrum of $V_{AB|\gamma}$, and $\lambda = \sqrt{\det V_{B|\gamma\bar{\alpha}}}$.

III. THE PA-CONCATENATED RELAY SCHEMES

Following the previous analysis, the MDI-based data postprocessing can be reduced to the beam-splitting and recombining operations, depending on the combined effect of the BS and PA schemes. A similar realization scenario as that of the PA-BS relay scheme is the reverse arrangement of the PA and BS schemes, namely, the so-called reverse BS-PA relay scheme. Unfortunately, because of the additional noise at output fields, there is little advantage of the reverse BS-PA relay scheme when comparing to either the only-one-BS relay scheme or the PA-BS relay scheme. To maintain the integrity of the wholeness, we also consider the reinforced PA-PA relay scheme, where input fields of the first PA and the second PA are correlated so that the additional noise can be suitably canceled out when superimposing at the second PA, giving rise to a slight SNR improvement of the CV-QKD protocol.

A. The reverse BS-PA relay scheme

We first consider design of the reverse BS-PA relay scheme, as shown in Fig. 1(b), where the beam-splitting operation is a BS and the beam recombining operation is a PA. The beam-splitting operation of a BS that separates the incoming states can be expressed as

$$\hat{a}_1 = \sqrt{T}\hat{a} + e^{i\theta_1}\sqrt{R}\hat{b},\ \hat{b}_1 = e^{i\theta_1}\sqrt{T}\hat{b} - \sqrt{R}\hat{a}, \tag{34}$$

subject to a phase shift θ_1 on mode b. After that a recombining operation a PA is subsequently applied on the resulting modes a_1 and b_1 as follows:

$$\hat{a}_2 = G\hat{a}_1 + ge^{-i\theta_2}\hat{b}_1^\dagger,\ \hat{b}_2 = Ge^{i\theta_2}\hat{b}_1 + g\hat{a}_1^\dagger, \tag{35}$$

subject to another phase shift θ_2 on mode b_1. As a result, for the given $\theta_1 = \theta_2 = \theta$, we achieve the following total input-output relations:

$$\begin{aligned} \hat{a}_2 &= G\sqrt{T}\hat{a} - ge^{-i\theta}\sqrt{R}\hat{a}^\dagger + Ge^{i\theta}\sqrt{R}\hat{b} + ge^{-2i\theta}\sqrt{T}\hat{b}^\dagger, \\ \hat{b}_2 &= Ge^{2i\theta}\sqrt{T}\hat{b} + ge^{-i\theta}\sqrt{R}\hat{b}^\dagger - Ge^{i\theta}\sqrt{R}\hat{a} + g\sqrt{T}\hat{a}^\dagger. \end{aligned} \tag{36}$$

Adopting the available modes a_2 and b_2, we can create quadrature momentums $\hat{x}_{a_2}$ and $\hat{x}_{b_2}$ given by

$$\hat{x}_{a_2} = G\sqrt{T}\hat{x}_a - g\sqrt{R}\hat{x}_a(-\theta) + G\sqrt{R}\hat{x}_b(-\theta) + g\sqrt{T}\hat{x}_b(-2\theta), \quad (37)$$

$$\hat{x}_{b_2} = G\sqrt{T}\hat{x}_b(-2\theta) + g\sqrt{R}\hat{x}_b(-\theta) - G\sqrt{R}\hat{x}_a(-\theta) + g\sqrt{T}\hat{x}_a. \quad (38)$$

When selecting $\theta = \pi/2$, we obtain the signal variables

$$x_{a_2} = G\sqrt{T}x_\alpha + g\sqrt{R}p_\alpha - g\sqrt{T}x_\beta - G\sqrt{R}p_\beta, \quad (39)$$

$$x_{b_2} = g\sqrt{T}x_\alpha + G\sqrt{R}p_\alpha - G\sqrt{T}x_\beta - g\sqrt{R}p_\beta. \quad (40)$$

The noise of a_2 and b_2 can be thus derived as

$$\langle\Delta^2\hat{x}_{a_2}\rangle = \langle\Delta^2\hat{x}_{b_2}\rangle = G^2 + g^2. \quad (41)$$

Using the homodyne measurements of $\hat{a}_2$ and $\hat{b}_2$, we achieve

$$\hat{x}_r = \hat{x}_{a_2} - \lambda_x\hat{x}_{b_2}, \quad (42)$$

with an adjustable parameter λ_x. The output signal variables can be represented by $x_r = x_{a_2} - \lambda_x x_{b_2}$, and hence the noise is calculated as $\langle\Delta^2\hat{x}_r\rangle = \langle(\Delta\hat{x}_{a_2} - \lambda_x\Delta\hat{x}_{b_2})^2\rangle$. Subsequently, we achieve $\langle\Delta^2\hat{x}_r\rangle_{\text{opt}} = \langle\Delta^2\hat{x}_{a_2}\rangle - \langle\Delta^2\hat{x}_{b_2}\rangle = 0$ for the selected parameter $\lambda_x = \langle\Delta\hat{x}_{a_2}\cdot\Delta\hat{x}_{b_2}\rangle/\langle\Delta^2\hat{x}_{b_2}\rangle$ in the optimal noise reduction processing. For $T = 1/2$, we obtain an approximative value $\lambda_x = 1$ with large $G \simeq g$, rendering a classical outcome $x_{r_{\pi/2}} = x_{a_2} - x_{b_2}$ in a real variable

$$x_{r_{\pi/2}} = \frac{1}{\sqrt{2}}(G-g)(x_\alpha - p_\alpha + x_\beta - p_\beta). \quad (43)$$

Similarly, we consider quadrature phases $\hat{p}_{a_2}$ and $\hat{p}_{b_2}$ of a_2 and b_2, and obtain another classical outcome $p_{r_{\pi/2}} = p_{a_2} + p_{b_2}$, expressed as

$$p_{r_{\pi/2}} = \frac{1}{\sqrt{2}}(G-g)(p_\alpha - x_\alpha + x_\beta - p_\beta). \quad (44)$$

According to the relations in Eq. (36), we take $\theta = 0$ and $\theta = \pi$, and obtain the variables

$$x_{r_0} = \sqrt{2}(G-g)x_\alpha, \quad p_{r_0} = \sqrt{2}(G-g)p_\beta,$$
$$x_{r_\pi} = \sqrt{2}(g-G)x_\beta, \quad p_{r_\pi} = \sqrt{2}(G-g)p_\alpha, \quad (45)$$

which can be combined to form the variables

$$x_{r_+} = x_{r_0} + x_{r_\pi} = \sqrt{2}(G-g)(x_\alpha - x_\beta),$$
$$p_{r_+} = p_{r_0} + p_{r_\pi} = \sqrt{2}(G-g)(p_\alpha + p_\beta). \quad (46)$$

As a result, we obtain

$$x_{r'} = 2x_{r_{\pi/2}} + p_{r_-} = \sqrt{2}(G-g)(x_\alpha + x_\beta),$$
$$p_{r'} = 2x_{r_{\pi/2}} + x_{r_-} = \sqrt{2}(G-g)(p_\alpha - p_\beta), \quad (47)$$

and create a classical complex variable

$$\gamma = \frac{1}{\sqrt{2}}(x_{r'} + ip_{r'}) = (G-g)(\alpha + \beta^*) \quad (48)$$

for relay data processing.

According to the above-derived signal and noises of a_2 and b_2, we have the SNRs expressed as $S_{x_{a_2}} = 2x_\alpha^2[1 - 2Gg/(G^2+g^2)]$ and $S_{x_{b_2}} = 2x_\beta^2[1 - 2Gg/(G^2+g^2)]$, resulting in the information transfers $T_{a_2} = T_{b_2} = 2 - 4Gg/(G^2+g^2)$. The total information transfer, $T_{\text{tot}} = T_{a_2} + T_{b_2}$, approaches zero for large $G \simeq g$. It implies that there is little advantage of the reverse BS-PA relay scheme as compared with only the one BS relay scheme, not to mention the previous PA-BS relay scheme. It is necessary to note that the resulting output noise is correspondingly increased by a factor of $G^2 + g^2$ as compared with the vacuum noise, whereas the intensities of output signals are decreased by a factor of $2(G-g)^2$. The amplification of the activated noise at output fields is due to the fact that two output fields of the BS are not correlated and hence the noises of output fields are amplified independently when being recombined at the PA.

B. The reinforced PA-PA relay scheme

Though the amplification of the additional noise may decrease the output SNR of the output fields, the decline in output SNR can be offset by the increased relations of input noise. To enhance the performance of the CV-QKD protocol, we consider the reinforced PA-PA relay scheme, as shown in Fig. 1(c), where the beam-splitting operation and the beam recombining operation are both performed with the PA. The beam-splitting effect of the first PA is given by

$$\hat{a}_1 = G\hat{a} + g\hat{b}^\dagger, \quad \hat{b}_1 = G\hat{b} + g\hat{a}^\dagger. \quad (49)$$

Adopting a recombining operation on a_1 and b_1 with the second PA establishes the input-output relations

$$\hat{a}_2 = G\hat{a}_1 + ge^{-i\theta}\hat{b}_1^\dagger, \quad \hat{b}_2 = Ge^{i\theta}\hat{b}_1 + g\hat{a}_1^\dagger, \quad (50)$$

subject to another phase shift θ on mode b_1. As a result, we achieve the total input-output relations

$$\hat{a}_2 = (G^2 + g^2e^{-i\theta})\hat{a} + (Gge^{-i\theta}\hat{b} + Gg)\hat{b}^\dagger,$$
$$\hat{b}_2 = (G^2e^{i\theta} + g^2)\hat{b} + (Gge^{i\theta} + Gg)\hat{a}^\dagger, \quad (51)$$

which generate $\hat{x}_{a_2}$ and $\hat{x}_{b_2}$ given by

$$\hat{x}_{a_2} = G^2\hat{x}_a + g^2\hat{x}_a(\theta) + Gg\hat{x}_b + Gg\hat{x}_b(-\theta),$$
$$\hat{x}_{b_2} = G^2\hat{x}_b(-\theta) + g^2\hat{x}_b + Gg\hat{x}_a + Gg\hat{x}_a(\theta). \quad (52)$$

For $\theta = 0$, we have the signal variables of a_2 and b_2, i.e.,

$$x_{a_2} = (G^2 + g^2)x_\alpha + 2Ggx_\beta,$$
$$x_{b_2} = (G^2 + g^2)x_\beta + 2Ggx_\alpha. \quad (53)$$

The noises of a_2 and b_2 can be calculated as

$$\langle\Delta^2\hat{x}_{a_2}\rangle = \langle\Delta^2\hat{x}_{b_2}\rangle = G^4 + g^4 + 6G^2g^2. \quad (54)$$

Because of the correlation noise of $\hat{a}_2$ and $\hat{b}_2$, for the given parameter λ_x, we consider the subtraction

$$\hat{x}_r = \hat{x}_{a_2} - \lambda_x\hat{x}_{b_2} \quad (55)$$

and obtain the output signal variable $x_r = x_{a_2} - \lambda_x x_{b_2}$, which generates the additional noise $\langle\Delta^2\hat{x}_r\rangle = \langle(\Delta\hat{x}_{a_2} - \lambda_x\Delta\hat{x}_{b_2})^2\rangle$.

Taking $\lambda_x = (\Delta\hat{x}_{a_2} \cdot \Delta\hat{x}_{b_2})/\langle\Delta^2\hat{x}_{b_2}\rangle$, we achieve the optimal noise reduction $\langle\Delta^2\hat{x}_r\rangle_{\text{opt}} = \langle\Delta^2\hat{x}_{a_2}\rangle - \langle\Delta^2\hat{x}_{b_2}\rangle = 0$. For the large $G \simeq g$ and hence $\lambda_x \simeq 1$, we have a classical outcome in a variable $x_r = x_{a_2} - x_{b_2}$ given by

$$x_r = (G+g)^2(x_\alpha - x_\beta). \tag{56}$$

Similarly, we consider $\hat{p}_{a_2}$ and $\hat{p}_{b_2}$ of a_2 and b_2 and obtain another classical outcome $p_r = p_{a_2} + p_{b_2}$ given by

$$p_r = (G+g)^2(p_\alpha + p_\beta). \tag{57}$$

After combining x_r with p_r, we can generate a complex variable $\gamma = \frac{1}{\sqrt{2}}(x_r + ip_r)$. Finally, the outcome γ, which establishes an *a posteriori* correlation

$$\gamma = \frac{1}{\sqrt{2}}(G+g)^2(\alpha + \beta^*) + \delta, \tag{58}$$

is then broadcasted to Alice and Bob for the data postprocessing, where δ denotes the detection noise.

As for the SNRs of a_2 and b_2 of the reinforced PA-PA relay scheme, we have the approximated values $S_{x_{a_2}} = S_{x_{b_2}} = (x_\alpha + x_\beta)^2/2$ for large $G \simeq g$. The information transfers of a_2 and b_2 can be characterized by $T_{a_2} = S_{x_{a_2}}/x_\alpha^2$ and $T_{b_2} = S_{x_{b_2}}/x_\beta^2$, respectively, and hence the total information transfer can be calculated as $T_{\text{tot}} = T_{a_2} + T_{b_2}$, approaching a minimum value 4, which is the same as that of the PA-BS relay scheme. Therefore, there is a similar behavior of the reinforced PA-PA relay scheme as that of the PA-BS relay scheme in terms of the total information transfer. This result is illustrated with numeric simulations in the following section.

IV. PERFORMANCE ANALYSIS AND DISCUSSION

In this section, we consider performance of the concatenated relay schemes by demonstrating the secret key rate of the CV-QKD protocol with numeric simulations. The detector imperfection is attributed to the channel loss and noise. In both symmetric and asymmetric scenarios, the coherent attack for the parameters $g_1 = -g_2 = 0.1$ is an effective attacking strategy for security proof (see Appendix D for the illustrations). In our simulations, we consider that Alice and Bob encode their information in coherent states, and at the relay station, the three concatenated relay schemes, i.e., the PA-BS relay scheme, the reverse BS-PA relay scheme, and the reinforced PA-PA relay scheme, may be employed for relay data postprocessing.

By contrast, when considering the effect of the PA on the relay schemes, we illustrate the secret key rates as a function of transmission distances, where the gain G of the PA is 5, the variances of α and β are both equal to 10, the reconciliation efficiency is $\eta = 0.97$, and the thermal state noise is 1.2. As depicted in Fig. 4, in a symmetric eavesdropping scenario, we take $L_{AR} = L_{BR}$, which denotes the equal lengths of quantum channels from Alice and Bob to the relay station, respectively. We find that the PA-BS relay scheme outperforms the only-one-BS relay scheme, whereas the only-one-BS relay scheme defeats the reverse BS-PA relay scheme in terms of the secret key rates. Meanwhile, the behavior of the PA-BS relay scheme is similar to that of the reinforced PA-PA relay scheme, which has been theoretically proved in the previous sections. It can be inferred that the suitably arranged PA-BS relay scheme can generate the increased SNRs at the output fields, causing the improvement of the CV-QKD protocol.

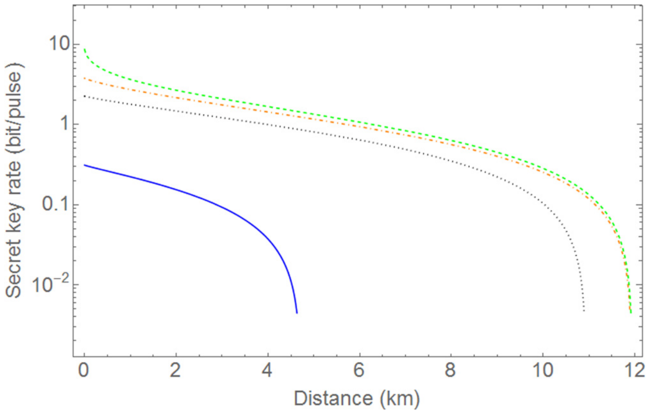

FIG. 4. The secret key rates (bits per relay use) of the CV-QKD protocol using the concatenated relay schemes versus Bob's transmission distances. The red dash-dotted line denotes the secret key rate of the PA-BS relay scheme, the blue solid line represents the secret key rate of the reverse BS-PA relay scheme, and the green dashed line is the secret key rate of the reinforced PA-PA relay scheme. For the tangible comparison, we plot the secret key rate of the CV MDI-based QKD with only one BS relay scheme with a black dotted line.

Apart from the symmetric scenario, the effect of the asymmetric eavesdropping strategy with the relay station close to one participant, say Alice, on the performance is also plotted in Fig. 5. Let $L_{AR} \in \{3\text{ km}, 1\text{ km}, 0.1\text{ km}\}$ for performance comparison. We find that there exists a slightly increased improvement of the secret key rate for the short relay

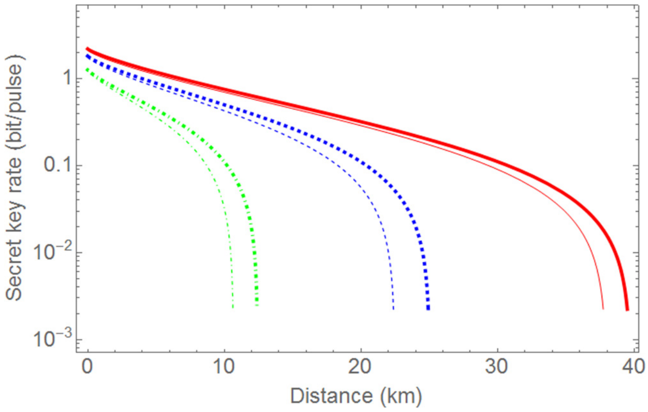

FIG. 5. The secret key rates (bits per relay use) of the CV-QKD protocol in an asymmetric scenario using the PA-BS relay scheme and the only-one-BS relay scheme versus Bob's transmission distances. The thin green dash-dotted line and the thick green dash-dotted line denote the secret key rates of the only-one-BS relay scheme and the PA-BS scheme with $L_{AR} = 3$ km. The thin blue dashed line and the thick blue dashed line represent the secret key rates of the only-one-BS relay scheme and the PA-BS scheme with $L_{AR} = 1$ km. The thin red solid line and the stick red solid line are the secret key rates of the only-one-BS relay scheme and the PA-BS scheme with $L_{AR} = 0.1$ km.

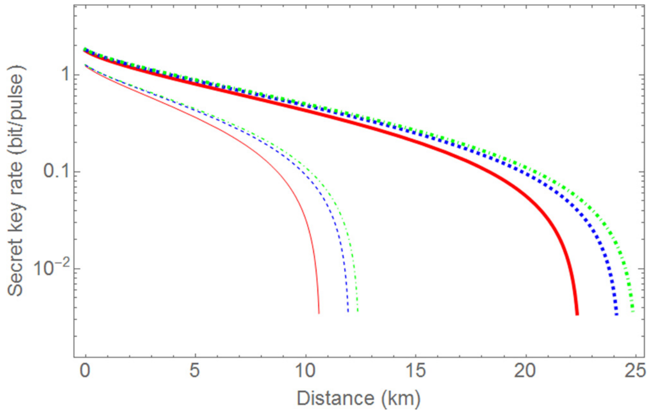

FIG. 6. The secret key rates (bits per relay use) of the CV-QKD protocol in the symmetric and the asymmetric scenarios with $L_{AR} = 1$ km using the only-one-BS relay scheme (red lines), the PA-BS relay scheme (blue lines), and the reinforced PA-PA relay scheme (green lines) versus Bob's transmission distances. The thin lines denote the secret key rates of the symmetric scenario and the thick lines denote those of the asymmetric scenario.

distance L_{AR}. Also, we show the effect of both symmetric and asymmetric scenarios on the secret key rates, as shown in Fig. 6. It implies that the secret key rate of the asymmetric system is higher than that of the symmetric one for the given distance $L_{AR} = 1$ km.

Finally, we demonstrate the effect of the modulated gain parameter G on the secret key rates of the CV-QKD protocol. We consider the PA-BS relay scheme for the distinct comparison in a symmetric scenario and include the secret key rates when the infinite gain is treated with the selected gain $G = 100$ and hence $g \simeq 99.995$. As shown in Fig. 7, we find that the large gain can usually increase the high secret key rate. However, for large enough gain, there is only a small advantage of the PA-BS relay scheme for the performance improvement of the CV-QKD protocol.

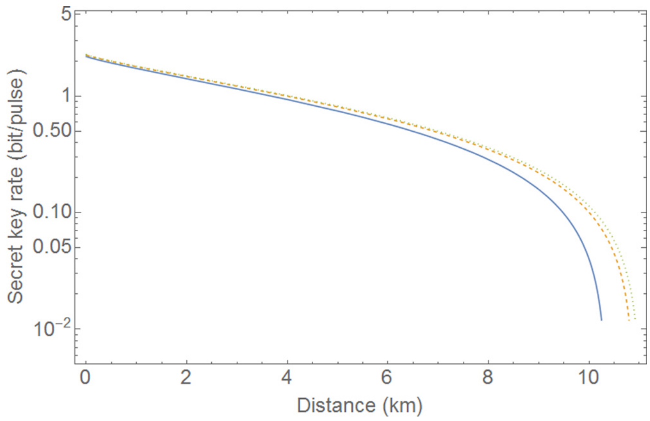

FIG. 7. The secret key rates (bits per relay use) of the CV-QKD protocol with the PA-BS relay scheme in the symmetric scenario versus Bob's transmission distances. The blue solid line is for the small gain $G = 1.1$, the red dashed line is for the medial gain $G = 5$, and the green dotted line is for the infinite gain $G = 100$, respectively.

V. CONCLUSION

We proposed several PA-concatenated relay CV-QKD schemes based on the PA and the BS, and we also analyzed the security of these schemes under the two-mode coherent attacks. These schemes would benefit the system performance improvement by providing signal amplification and establishing quantum correlations. Though the reverse BS-PA relay scheme has little advantage over the traditional counterpart that contains only one BS in relay data postprocessing, the simulations show that the PA-BS relay scheme with suitably selected gain G of the PA results in a higher secret key rate. This is because the output fields of the PA are entangled with the correlated quantum noises while the input fields of the BS are superimposed, subsequently leading to the quantum noise reduction of the total output fields of the relay station. In addition, the reinforced PA-PA relay scheme with a small gain G would outperform the PA-BS relay scheme and shows a slight improvement of the secret key rate. Furthermore, the proposed schemes implemented in an asymmetric scenario would provide a higher secret key rate, as opposed to the symmetric one. These proposed quantum relay schemes can be performed through the beam splitting, the recombining operations, and the relay data postprocessing, such that it would be suitable for secret information exchange in complex networks with intermediate stations.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grants No. 61379153 and No. 61572529).

APPENDIX A: DERIVATION OF THE OPTIMIZED OUTPUT NOISE

In what follows, we illustrate the derivation of Eq. (16) from Eq. (15). After expanding $\langle \Delta^2 \hat{x}_r \rangle$ in Eq. (15), we have

$$\begin{aligned}\langle \Delta^2 \hat{x}_r \rangle &= \lambda_x^2 \langle \Delta^2 \hat{x}_{b_2} \rangle + \langle \Delta^2 \hat{x}_{a_2} \rangle \\ &\quad - \lambda_x \left(\langle \Delta \hat{x}_{a_2} \Delta \hat{x}_{b_2} \rangle + \langle \Delta \hat{x}_{b_2} \Delta \hat{x}_{a_2} \rangle \right). \end{aligned} \tag{A1}$$

According to the derived input-output relations in Eq. (3), the signal input $\hat{a}$ is independent of the other signal input $\hat{b}$ in the coherent state. Then the correlation between them is calculated as

$$\langle \Delta \hat{x}_a \Delta \hat{x}_b \rangle = \langle \Delta \hat{x}_b \Delta \hat{x}_a \rangle = 0. \tag{A2}$$

Consequently, the entangled output $\hat{a}_2$ and $\hat{b}_2$ are highly correlated with the correlation that can be expressed as follows:

$$\langle \Delta \hat{x}_{a_2} \Delta \hat{x}_{b_2} \rangle = \langle \Delta \hat{x}_{b_2} \Delta \hat{x}_{a_2} \rangle. \tag{A3}$$

Substituting the correlation in Eq. (A3) into the noise $\langle \Delta^2 \hat{x}_r \rangle$ in Eq. (A1), we obtain

$$\langle \Delta^2 \hat{x}_r \rangle = \lambda_x^2 \langle \Delta^2 \hat{x}_{b_2} \rangle - 2\lambda_x \langle \Delta \hat{x}_{a_2} \Delta \hat{x}_{b_2} \rangle + \langle \Delta^2 \hat{x}_{a_2} \rangle. \tag{A4}$$

When selecting $\lambda_x = \langle \Delta \hat{x}_{a_2} \cdot \Delta \hat{x}_{b_2} \rangle / \langle \Delta^2 \hat{x}_{b_2} \rangle$, we can achieve the minimum value of

$$\langle \Delta^2 \hat{x}_r \rangle_{\text{opt}} = \langle \Delta^2 \hat{x}_{a_2} \rangle - \langle \Delta^2 \hat{x}_{b_2} \rangle. \tag{A5}$$

APPENDIX B: DERIVATION OF THE CM OF THE CV-QKD SYSTEM

We derive the covariance matrix (CM) of the CV MDI-QKD system with the EB PA-BS relay scheme. At the initial input phase, Alice's modes A and a, Bob's modes B and b, and Eve's modes e_a and e_b are expressed in a tensor-product state

$$\rho = \rho_{Aa} \otimes \rho_{Bb} \otimes \sigma_{e_a e_b}, \tag{B1}$$

where ρ_{Aa} and ρ_{Bb} are both the EPR states with the CM

$$V(\mu,\nu) = \begin{pmatrix} \mu\mathcal{I} & \nu\mathcal{Z} \\ \nu\mathcal{Z} & \mu\mathcal{I} \end{pmatrix}, \tag{B2}$$

and $\sigma_{e_a e_b}$ is Eve's zero-mean Gaussian state with the CM

$$V_{e_a e_b} = \begin{pmatrix} \omega_a\mathcal{I} & \mathcal{G} \\ \mathcal{G} & \omega_b\mathcal{I} \end{pmatrix}. \tag{B3}$$

It is a zero-mean Gaussian state with the CM described as

$$V_{aAbBe_a e_b} = V(\mu,\nu) \oplus V(\mu,\nu) \oplus V_{e_a e_b} \tag{B4}$$

which can be reordered as an equivalent system with the CM $V_{ABae_a e_b b}$. Eve's actions on modes τ and e_τ, $\forall\tau \in \{a,b\}$, can be described by the BS operation

$$\mathcal{E}_{\tau e_\tau} = \begin{pmatrix} \sqrt{t_\tau}\mathcal{I} & \sqrt{r_\tau}\mathcal{I} \\ -\sqrt{r_\tau}\mathcal{I} & \sqrt{\tau_\tau}\mathcal{I} \end{pmatrix}, \tag{B5}$$

subject to $t_\tau + r_\tau = 1$. The attacking operation can be represented as

$$\mathcal{E} = \mathcal{I}_{AB} \oplus \mathcal{E}_{ae_a} \oplus \mathcal{E}_{be_b}^{\mathrm{T}}. \tag{B6}$$

Then the state of output modes $ABa'e'_a e'_b b'$, as shown in Fig. 2(a), is a Gaussian state with zero mean and the CM

$$V_{ABa'e'_a e'_b b'} = \mathcal{E} V_{ABae_a e_b b} \mathcal{E}^{\mathrm{T}}, \tag{B7}$$

which results in the reduced CM of the modes $ABa'b'$ given by

$$V_{ABa'b'} = \begin{pmatrix} V_{AB} & \mathcal{C}_1 & \mathcal{C}_2 \\ \mathcal{C}_1^{\mathrm{T}} & \mathcal{A} & \mathcal{D} \\ \mathcal{C}_2^{\mathrm{T}} & \mathcal{D}^{\mathrm{T}} & \mathcal{B} \end{pmatrix}, \tag{B8}$$

where $V_{AB} = \mu\mathcal{I}_{AB}$, $\mathcal{A} = \kappa_a\mathcal{I}_a$, $\mathcal{B} = \kappa_b\mathcal{I}_b$, $\mathcal{D} = \sqrt{r_a r_b}\mathcal{G}$, and

$$C_1 = \begin{pmatrix} \nu\sqrt{t_a}\mathcal{Z} \\ 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 \\ \nu\sqrt{t_b}\mathcal{Z} \end{pmatrix}, \tag{B9}$$

with the notation $\kappa_\tau = t_\tau\mu + r_\tau\omega_\tau$ [11]. The effect of the PA-BS relay scheme on a' and b' can be described by applying an operation

$$\mathcal{P} = \mathcal{I}_{AB} \oplus \begin{pmatrix} \mathcal{P}_1 & \mathcal{P}_2 \\ \mathcal{P}_3 & \mathcal{P}_4 \end{pmatrix}, \tag{B10}$$

where $\mathcal{P}_1 = \mathcal{P}_2 = \frac{1}{\sqrt{2}}\mathrm{diag}(G+g, G-g)$, $\mathcal{P}_3 = -\frac{1}{\sqrt{2}}\mathrm{diag}(G-g, G+g)$, and $\mathcal{P}_4 = \frac{1}{\sqrt{2}}\mathrm{diag}(G-g, G+g)$. Then, the CM of the state of ABa_2b_2 is derived as

$$V_{ABa_2b_2} = \mathcal{P} V_{ABa'b'} \mathcal{P}^{\mathrm{T}}, \tag{B11}$$

which can be rewritten as

$$V_{ABa_2b_2} = \begin{pmatrix} V_{AB} & \mathcal{C}'_1 & \mathcal{C}'_2 \\ \mathcal{C}'^{\mathrm{T}}_1 & \mathcal{A}' & \mathcal{D}' \\ \mathcal{C}'^{\mathrm{T}}_2 & \mathcal{D}'^{\mathrm{T}} & \mathcal{B}' \end{pmatrix}, \tag{B12}$$

where $\mathcal{C}'_1 = \mathcal{C}_1\mathcal{P}_1 + \mathcal{C}_2\mathcal{P}_2$, $\mathcal{C}'_2 = \mathcal{C}_1\mathcal{P}_3 + \mathcal{C}_2\mathcal{P}_4$, $\mathcal{A}' = \mathcal{P}_1\mathcal{A}\mathcal{P}_1 + \mathcal{P}_2\mathcal{D}\mathcal{P}_1 + \mathcal{P}_1\mathcal{D}\mathcal{P}_2 + \mathcal{P}_2\mathcal{B}\mathcal{P}_2$, $\mathcal{B}' = \mathcal{P}_3\mathcal{A}\mathcal{P}_3 + \mathcal{P}_4\mathcal{D}\mathcal{P}_3 + \mathcal{P}_3\mathcal{D}\mathcal{P}_4 + \mathcal{P}_4\mathcal{B}\mathcal{P}_4$, and $\mathcal{D}' = \mathcal{P}_1\mathcal{A}\mathcal{P}_3 + \mathcal{P}_2\mathcal{D}\mathcal{P}_3 + \mathcal{P}_1\mathcal{D}\mathcal{P}_4 + \mathcal{P}_2\mathcal{B}\mathcal{P}_4$. Adopting the notation

$$\Delta = \mathrm{diag}(\delta_1,\delta_2) = \frac{1}{2}(\mathcal{Z}\mathcal{A}'\mathcal{Z} + \mathcal{B}' - \mathcal{Z}\mathcal{D}' - \mathcal{D}'^{\mathrm{T}}\mathcal{Z}), \tag{B13}$$

with $\delta_1 = 2G^2\kappa_a + 2g^2\kappa_b + 4Gg\sqrt{r_a r_b}g_1$ and $\delta_2 = 2G^2\kappa_a + 2g^2\kappa_b - 4Gg\sqrt{r_a r_b}g_2$, we obtain the conditional CM $V_{AB|\gamma}$ expressed as

$$\begin{aligned} V_{AB|\gamma} &= V_{AB} - \frac{1}{2\det\Delta}\sum_{i,j=1}^{2} \mathcal{C}_i(\mathcal{X}_i^{\mathrm{T}}\Delta\mathcal{X}_j)\mathcal{C}_j^{\mathrm{T}} \\ &= \mu\mathcal{I}_{AB} - \nu^2 \cdot \\ &\quad \begin{pmatrix} \frac{G^2 t_a}{\delta_1} & 0 & \frac{Gg\sqrt{t_a t_b}}{\delta_1} & 0 \\ 0 & \frac{g^2 t_a}{\delta_2} & 0 & -\frac{Gg\sqrt{t_a t_b}}{\delta_2} \\ \frac{Gg\sqrt{t_a t_b}}{\delta_1} & 0 & \frac{g^2 t_b}{\delta_1} & 0 \\ 0 & -\frac{Gg\sqrt{t_a t_b}}{\delta_2} & 0 & \frac{G^2 t_b}{\delta_2} \end{pmatrix}, \end{aligned} \tag{B14}$$

where

$$\mathcal{X}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathcal{X}_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{B15}$$

According to the aforementioned analysis, we can calculate the CM of the CV-QKD system with the reverse BS-PA relay scheme. Based on the derived CV in Eq. (B8), the effect of the relay data postprocessing on a' and b' can be described by using the operation

$$\mathcal{P}^{bp} = \mathcal{I}_{AB} \oplus \begin{pmatrix} \mathcal{P}_1^{bp} & \mathcal{P}_2^{bp} \\ \mathcal{P}_3^{bp} & \mathcal{P}_4^{bp} \end{pmatrix}, \tag{B16}$$

where

$$\mathcal{P}_1^{bp} = \begin{pmatrix} G & g \\ g & G \end{pmatrix}, \quad \mathcal{P}_2^{bp} = \begin{pmatrix} -g & -G \\ -G & -g \end{pmatrix},$$
$$\mathcal{P}_3^{bp} = \begin{pmatrix} -g & G \\ G & -g \end{pmatrix}, \quad \mathcal{P}_2^{bp} = \begin{pmatrix} -G & g \\ g & -G \end{pmatrix}. \tag{B17}$$

After adopting the reverse the BS-PA relay scheme in the CV-QKD protocol, we obtain

$$\Delta^{bp} = \begin{pmatrix} \delta_1^{'} & \delta_2^{'} \\ \delta_2^{'} & \delta_1^{'} \end{pmatrix}, \tag{B18}$$

with $\delta_1^{'} = 2(G^2 + g^2)(\kappa_a + \kappa_b) + 2(g_1 + g_2)\sqrt{r_a r_b}$ and $\delta_2^{'} = -2(G^2 + g^2)(g_1 + g_2)\sqrt{r_a r_b}$, respectively. Then we derive the conditional CM $V^{bp}_{AB|\gamma}$ expressed as

$$V^{bp}_{AB|\gamma} = \mu\mathcal{I}_{AB} - \frac{\nu^2}{\delta_1^{'}\delta_2^{'}}\cdot\begin{pmatrix} v_+ & Gg\delta_2^{'} & Gu_+ + Ggv_0 & gu_+ + G^2v_0 \\ t_aGg\delta_2^{'} & v_- & Gu_- - g^2v_0 & gu_- - Ggv_0 \\ gu_+ & -Gu_- & t_bGg\delta_1^{'} & t_bGg\delta_1^{'} \\ gu_+ & -gu_- & 2t_bG^2\delta_1^{'} & 2t_bG^2\delta_1^{'} \end{pmatrix},$$

where $v_\pm = t_a(G \pm g)(G+g)(\delta_1^{'} + \delta_2^{'})$, $u_\pm = \sqrt{t_at_b}(G \pm g)(\delta_1^{'} \pm \delta_2^{'})$, and $v_0 = \sqrt{t_at_b}\delta_2^{'}$.

Similarly, we derive the CM of the reinforced PA-PA relay scheme in the CV-QKD protocol by using the effect of the relay data processing on a' and b' with the operation

$$\mathcal{P}^{pp} = \mathcal{I}_{AB} \oplus \begin{pmatrix} \mathcal{P}_1^{pp} & \mathcal{P}_2^{pp} \\ \mathcal{P}_3^{pp} & \mathcal{P}_4^{pp} \end{pmatrix}, \tag{B19}$$

where $\mathcal{P}_1^{pp} = \mathcal{P}_4^{pp} = (G^2 + g^2)\mathcal{I}$, $\mathcal{P}_2^{pp} = 2Gg\mathcal{I}$, and $\mathcal{P}_3^{pp} = -2Gg\mathcal{I}$. After implementing the reinforced PA-PA relay scheme, we calculate $\Delta^{pp} = \mathrm{diag}(\delta_1^{''},\delta_2^{''})$, with $\delta_1^{''} = [(G^2+g^2)(G+g)^2 + 4G^2g^2]\kappa_a + [(G^2+g^2)(G-g)^2 + 4G^2g^2]\kappa_b - 2g_1\sqrt{r_ar_b}$, and $\delta_2^{''} = [(G^2+g^2)(G-g)^2 + 4G^2g^2]\kappa_a + [(G^2+g^2)(G+g)^2 - 4G^2g^2]\kappa_b - 2g_2\sqrt{r_ar_b}$. Finally, we derive the conditional CM $V^{pp}_{AB|\gamma}$ given by

$$V^{pp}_{AB|\gamma} = \mu\mathcal{I}_{AB} - \nu^2\cdot \times \begin{pmatrix} \frac{\xi t_a}{\delta_1^{''}} & 0 & \frac{\xi\sqrt{t_at_b}}{\delta_1^{''}} & 0 \\ 0 & \frac{(G-g)^4t_a}{\delta_2^{''}} & 0 & \frac{\sqrt{t_at_b}}{\delta_2^{''}} \\ \frac{-\sqrt{t_at_b}}{\delta_1^{''}} & 0 & \frac{\xi t_b}{\delta_1^{''}} & 0 \\ 0 & \frac{\sqrt{t_at_b}}{\delta_2^{''}} & 0 & \frac{(G+g)^4t_b}{\delta_2^{''}} \end{pmatrix},$$

with $\xi = (G^2+g^2)^2 + 4G^2g^2$.

APPENDIX C: PA-CONCATENATED RELAY DATA POSTPROCESSING

Assume that Alice and Bob prepare two modes a and b with $\hat{a} = (\hat{x}_\alpha + i\hat{p}_\alpha)/2$ and $\hat{b} = (\hat{x}_\beta + i\hat{p}_\beta)/2$, respectively, where $[\hat{x}_\alpha,\hat{p}_\alpha] = [\hat{x}_\beta,\hat{p}_\beta] = 2i$. Exploiting an EB-relay scheme, Alice and Bob prepare two EPR states ρ_{Aa} and ρ_{Bb} with the same zero mean and the CM given by

$$V(\mu) = \begin{pmatrix} \mu\mathcal{I} & \nu\mathcal{Z} \\ \nu\mathcal{Z} & \mu\mathcal{I} \end{pmatrix}. \tag{C1}$$

As shown in Fig. 3, after heterodyning modes A and B, Alice and Bob create coherent states $|\alpha\rangle$ and $|\beta\rangle$ on modes a and b, whose amplitudes are modulated by the complex Gaussian variables $\alpha = (x_\alpha + ip_\alpha)/2$ and $\beta = (x_\beta + ip_\beta)/2$ with the same variance $\varphi = \mu - 1$. The measurement outcomes $\bar{\alpha}$ and $\bar{\beta}$ are related to $|\alpha\rangle$ and $|\beta\rangle$ [11], i.e., $\bar{\alpha} = \iota\alpha$ and $\bar{\beta} = \iota\beta$ with $\iota = (\mu+1)/\nu$. We have $\bar{\alpha} \simeq \alpha$ and $\bar{\beta} \simeq \beta$ for the large modulation φ, and thus variables $\bar{\alpha}$ and $\bar{\beta}$ are equivalent to α and β from an informational-theoretical viewpoint.

In what follows, we calculate the secret key rate of the PA-concatenated relay scheme of the CV-QKD protocol. Without loss of generality, we assume that Alice encodes information through heterodyning mode A with outcome $\bar{\alpha}$, projecting $\Phi_{ABe|\gamma}$ into the pure state $\rho_{Be|\gamma\bar{\alpha}}$ so that $S(\rho_{B|\gamma}) = S(\rho_{e|\gamma\bar{\alpha}})$, where γ denotes the measurement of the PA-concatenated relay scheme at the relay station. Eve's information on Alice's variable $\bar{\alpha}$ is upper-bounded by the Holevo quantity [13]:

$$I_{E|\gamma} = S(\rho_{E|\gamma}) - S(\rho_{e|\gamma}) = S(\rho_{AB|\gamma}) - S(\rho_{B|\gamma}). \tag{C2}$$

In order to recover Alice's information $\bar{\alpha}$, Bob heterodynes mode B with outcome $\bar{\beta}$. As a result, conditioned on γ, the mutual information $I_{ab|\gamma}$ of Alice and Bob can be determined by $\rho_{AB|\gamma}$, which gives birth to $I_{ab|\gamma} = I(\bar{\alpha},\bar{\beta}|\gamma) = I(\alpha,\beta|\gamma)$. Consequently, the secret key rate can be calculated as [20]

$$R(\gamma) = \eta I_{ab|\gamma} - I_{e|\gamma}, \tag{C3}$$

with reconciliation efficiency satisfying the constraint $\eta \leqslant 1$.

Actually, the term $I_{ab|\gamma}$ is closely related to the CM $V_{AB|\gamma}$, which can be determined by Alice and Bob with the complex CM $V(\alpha,\beta,\gamma)$ yielded by PA-concatenated relay data postprocessing. According to [11], we can use the related variables α and β, and the matrix $V(\alpha,\beta,\gamma)$ is equivalent to a real CM given by

$$V(x_\alpha,p_\alpha,x_\beta,p_\beta,x_r,p_r) = \begin{pmatrix} V_{ab} & \mathcal{C} \\ \mathcal{C}^{\mathrm{T}} & \mathcal{R} \end{pmatrix}, \tag{C4}$$

where $V_{ab} = V_{ab}(x_\alpha,p_\alpha,x_\beta,p_\beta)$ denotes the CM of Alice and Bob's reduced state, $\mathcal{R} = \mathcal{R}(x_r,p_r)$ is the CM of output modes at the relay station, $\mathcal{C}$ is the correlation matrix, and the notation T denotes the transpose operation. For the given γ of the PA-concatenated relay scheme, the conditional CM of Alice and Bob can be estimated through calculating

$$V(x_\alpha,p_\alpha,x_\beta,p_\beta|\gamma) = V_{ab} - \mathcal{C}\mathcal{R}^{-1}\mathcal{C}^{\mathrm{T}}. \tag{C5}$$

In the EB PA-concatenated relay scheme, adopting the equivalent variables $\bar{\alpha} = (x_{\bar{\alpha}} + ip_{\bar{\alpha}})/2$ and $\bar{\beta} = (x_{\bar{\beta}} + ip_{\bar{\beta}})/2$ for the large modulation, we obtain an approximate CM $V(x_\alpha,p_\alpha,x_\beta,p_\beta|\gamma) = \iota^{-2}V(x_{\bar{\alpha}},p_{\bar{\alpha}},x_{\bar{\beta}},p_{\bar{\beta}}|\gamma)$. Then we obtain the CM

$$V_{AB|\gamma} = V(x_{\bar{\alpha}},p_{\bar{\alpha}},x_{\bar{\beta}},p_{\bar{\beta}}|\gamma) - \mathcal{I}, \tag{C6}$$

which can be rewritten as

$$V_{AB|\gamma} = \begin{pmatrix} a & c \\ c^{\mathrm{T}} & b \end{pmatrix}. \tag{C7}$$

For the given outcomes $\bar{\alpha}$, we achieve $V_{B|\gamma\bar{\alpha}} = b - c^{\mathrm{T}}(a + \mathcal{I})^{-1}c$, which can be thus estimated by

$$V_{B|\gamma\bar{\alpha}} = V(x_{\bar{\beta}},p_{\bar{\beta}}|\gamma\bar{\alpha}) - \mathcal{I} \tag{C8}$$

using the Gaussian elimination of Alice's outcome variables.

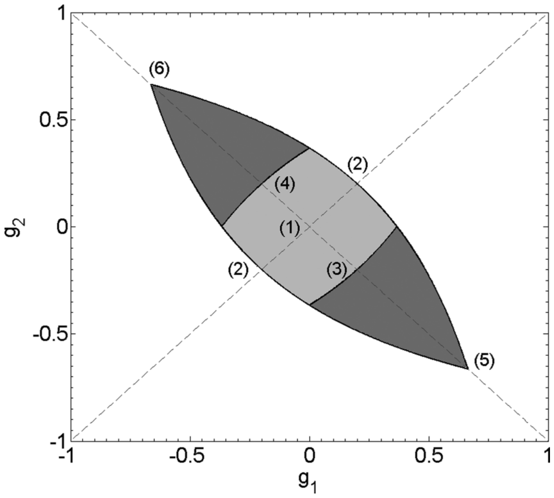

FIG. 8. Correlation plan of Gaussian attack with $\omega_a = \omega_b = 1.2$. The attack is determined by two coherent parameters g_1 and g_2. The gray region represents a separable attack and the black region denotes a coherent attack. The original point represents the collective attack.

APPENDIX D: PARAMETER-DEPENDENT ATTACKING STRATEGY

In the performance analysis of the CV-QKD protocol, the coherent attack will be used for the security analysis. Whether it is the symmetric eavesdropping scenario or not, plotting the coherent attack is an effective attacking strategy, where channel losses and noises play a key role with regard to the maximal transmission distance. Besides, for the accessible points in the correlation plane, as shown in Fig. 8, the pair of parameters (g_1,g_2) have a significant effect on the secret key rates and the maximal transmission distance as well. For example, the parameters (g_1,g_2) can be set to be zero, leading to the collective attack in the traditional CV-QKD protocol. In order to implement the coherent attack, Eve prepares two entangled states expressed in Eq. (B3). The parameters (g_1,g_2) should satisfy the bona fide constraints [11] in Eq. (23). To create two separable states, we can select the smallest partially transposed symplectic eigenvalue satisfying the separability constraints, i.e.,

$$\sqrt{\omega^2 - g_1g_2 - \omega|g_1 - g_2|} \geqslant 1. \tag{D1}$$

According to the constraints in Eqs. (23) and (D1), we have three kinds of attacking strategies. The first one is the *collective attack* [21], corresponding to the original point for $(g_1 = g_2 = 0)$ (or point 1 in Fig. 8). There is no entanglement between two EPR pairs prepared by Eve under this attack. The second one is the *separable attack*, which can be described in the gray region. For example, the points {2,3,4} that satisfy the condition $|g_1| = |g_2| = \omega - 1$ can be selected for the *separable attack*. The third one is the *coherent attack*, whose parameters g_1 and g_2 are characterized by the black area. Attacking channels E_1 and E_2 jointly may extract more information. Moreover, the points {5,6}, corresponding to $g_1 = -g_2 = \sqrt{\omega^2 - 1}$ and $g_1 = -g_2 = -\sqrt{\omega^2 - 1}$ that result in the most entanglement, are the suitable candidates for our coherent attacks in the performance analysis.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] L. B. Samuel and V. L. Peter, Rev. Mod. Phys. **77**, 513 (2005).
[3] H. K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).
[4] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[5] H. K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[6] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[7] M. Curty, F. H. Xu, W. Cui, C. C. Lim, K. Tamaki, and H. K. Lo, Nat. Commun. **5**, 643 (2014).
[8] F. H. Xu, M. Curty, B. Qi, L. Qian, and H. K. Lo, Nat. Photon. **9**, 772 (2015).
[9] H. W. Li, Z. Q. Yin, M. Pawlowski, G. C. Guo, and Z. F. Han, Phys. Rev. A **91**, 032305 (2015).
[10] H. W. Li, Z. Q. Yin, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Phys. Rev. A **89**, 032302 (2014).
[11] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).
[12] Z. Y. Li, Y. C. Zhang, F. H. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).
[13] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[14] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).
[15] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
[16] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B: At. Mol. Opt. Phys. **42**, 114014 (2009).
[17] D. Collins, N. Gisin, and H. D. Riedmatten, J. Mod. Opt. **52**, 735 (2005).
[18] H. deRiedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, Phys. Rev. Lett. **92**, 047904 (2004).
[19] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[20] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[21] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).