Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers

Ryo Namiki,[1] Akira Kitagawa,[2] and Takuya Hirano[1]

[1]*Department of Physics, Gakushuin University, 1-5-1 Mejiro, Toshima-ku, Tokyo 171-8588, Japan*
[2]*Faculty of Education, Kochi University, 2-5-1 Akebono-cho, Kochi 780-8520, Japan*

We have developed a method to calculate a secret key rate of a continuous-variable quantum-key-distribution scheme using four coherent states and postselection for a general model of Gaussian attacks. We assume that the transmission line and detection process are described by a pair of Gaussian channels. In our analysis, while the loss and noise on the transmission line are induced by an eavesdropper, Eve, who can replace the transmission line with a lossless and noiseless optical fiber, she is assumed inaccessible to the detection process. By separating the transmission noise and detection noise, we can always extract a larger key compared with the case that all loss and noises are induced by an eavesdropper's interference. An asymptotic key rate against collective Gaussian attacks can be determined numerically for the given channels' parameters. The improvement of the key rates turns out to be more significant for the reverse-reconciliation scheme.

I. INTRODUCTION

Quantum-key-distribution (QKD) protocols enable two remote parties, usually called Alice and Bob, to share a random bit sequence called the secret key [1–3]. Based on the laws of physics, the secret key can be proven information theoretically secure from an eavesdropper, Eve, who can access the transmission channels between Alice and Bob with possibly unlimited technology and computational power. There have been wide activities to demonstrate QKD beyond the proof-of-principle experiments, and several field tests have been reported [4–15].

In contrast to several no-go theorems in Gaussian continuous-variable (CV) quantum information protocols [16–19], CV-QKD protocols enjoy quantum optical homodyne measurements and the properties of coherent states to offer a possible solution in quantum safety [20]. In addition to the study of quantum optical methods, CV-QKD schemes potentially have an advantage in practical implementation. They could be operated with commercially available detectors and deployed in lit fiber networks possibly with the presence of classical channels [21–23]. An important theoretical challenge is to establish mathematical proof of its general safety [24]. It would be crucial to address how to generate secure local oscillator signals [25–29].

Physically, an essential point in QKD protocols is that quantum mechanical states are employed so that Eve's effort to read the transmission signal unavoidably induces errors on Bob's observation of the transmitted states. The amount of the secret key is usually calculated conservatively assuming that any observed signal loss and noises are induced by Eve. In practice, a portion of the loss and noises is induced at Bob's detector. Since the detector is inside Bob's station, it is feasible to assume that the detection process is inaccessible to Eve [1]. Therefore, if one can know how much of the

decoherence is given at the detector, a better key rate will be estimated by using the fact that Eve cannot extract correlation from the noise added inside Bob's station. Such scenario has been investigated in discrete-variable QKD schemes [30,31]. In CV-QKD schemes, a Gaussian description of state evolution is a basic approach to model the system performance. In the Gaussian modulated CV-QKD scheme, Eve's inaccessibility to the detector noise has been readily taken into account assuming the action of Gaussian channels [14,32–35]. However, these effects have not been extensively studied in the types of CV-QKD schemes which use discrete modulation and postselection [36–41].

For the postselection protocols of Refs. [36,38,39], an asymptotic key rate against collective Gaussian attacks was determined both in the direct-reconciliation (DR) and reverse-reconciliation (RR) scenarios [42,43]. For these discrete-modulation CV-QKD protocols, it has been unknown that a Gaussian attack could be the optimal attack, and the key rate against general attacks could be much lower than the key rate against Gaussian attacks [44]. Note that another type of discrete-modulation CV-QKD protocols which does not employ postselection has been investigated in Refs. [45–47].

In this paper, we investigate the security of the four-state CV-QKD protocol [38] when the loss and noises in the detection process are inaccessible to Eve. We derive a formula to determine Eve's density operator when the system describing the detector's loss and noises is simply traced out. Using this density operator, the key rate against collective Gaussian attacks can be calculated.

This paper is organized as follows. In Sec. II, we introduce basic notions on our protocol. In Sec. III, we describe the model of Eve's attack and how to determine her density operator. In Sec. IV, we show numerically calculated key rates for a couple of noise parameters. We conclude this paper in Sec. V.

II. PROTOCOL AND NOTATION

We consider the four coherent-state protocol [38]. We basically use the same notation as in Ref. [43]. Alice randomly sends one of four coherent states $|S\rangle \in \{|\pm\alpha\rangle, |\pm i\alpha\rangle\}$ with $\alpha > 0$ to Bob. Bob performs quadrature measurement in either x basis or p basis:

$$x = \frac{a + a^\dagger}{2}, \quad p = \frac{a - a^\dagger}{2i}, \quad (1)$$

where the commutation relation $[a, a^\dagger] = 1$ is assumed to hold. For notation convention, we may refer to the optical mode transmitted from Alice to Bob as the mode B. From the sequence that Alice sent $|\pm\alpha\rangle$ and Bob measured the x quadrature, a sifted key is generated by assigning bit value "0" for Bob's measurement outcome $m > 0$ and bit value "1" for $m < 0$. The same procedure is executed for the sequence that Alice sent $|\pm i\alpha\rangle$ and Bob measured the p quadrature. Bob may announce the absolute values of his measurement outcomes $|m|$, and a further classical key agreement procedure will be carried out by using the index $|m|$. Due to the phase-space symmetry with $\pi/2$ rotation, it is sufficient to consider the case that Alice sends $|S\rangle = |\pm\alpha\rangle$ and Bob obtains an outcome m associated with his measurement of the x quadrature. We assume linear loss and symmetric Gaussian excess noise through the transmission and detection of the signal. This implies that Bob's quadrature distribution when Alice's signal is S can be written as

$$P(m|S) = \sqrt{\frac{2}{\pi(1+\xi)}} e^{-2\frac{(m-\sqrt{\eta}S)^2}{1+\xi}}, \quad (2)$$

where η is the total transmission and ξ is the total excess noise. Note that this distribution reduces to the quadrature distribution of the coherent state $|\alpha\rangle$ when there is no loss and no excess noise, namely, we have $P(x|\alpha) = |\langle x|\alpha\rangle|^2$ when $(\eta, \xi) = (1, 0)$.

Conditioned on the absolute value of Bob's outcome $|m|$, the transmission is considered to be a binary symmetric channel with the bit error rate

$$\begin{aligned}\epsilon_{|m|} &:= \frac{P(-|m||\alpha)}{P(|m|\alpha) + P(-m|\alpha)} \\ &= \frac{P(|m||-\alpha)}{P(m|-\alpha) + P(-m|-\alpha)} \\ &= \left[1 + e^{8\frac{\sqrt{\eta}}{1+\xi}|m|\alpha}\right]^{-1}. \end{aligned} \quad (3)$$

From the bit error rate ϵ, the mutual information between Alice and Bob can be calculated as

$$I_{AB} = 1 - fh(\epsilon), \quad (4)$$

where $h(\epsilon) = -\epsilon \log_2 \epsilon - (1 - \epsilon) \log_2(1 - \epsilon)$ is the binary entropy function and $f \geqslant 1$ represents an efficiency of error correction. In what follows, we assume an ideal error correction and set $f = 1$.

III. INTERACTION MODEL AND EVE'S KNOWLEDGE

We consider the physical model of the signal transmission in Fig. 1. Let us assume the signal is transmitted from Alice
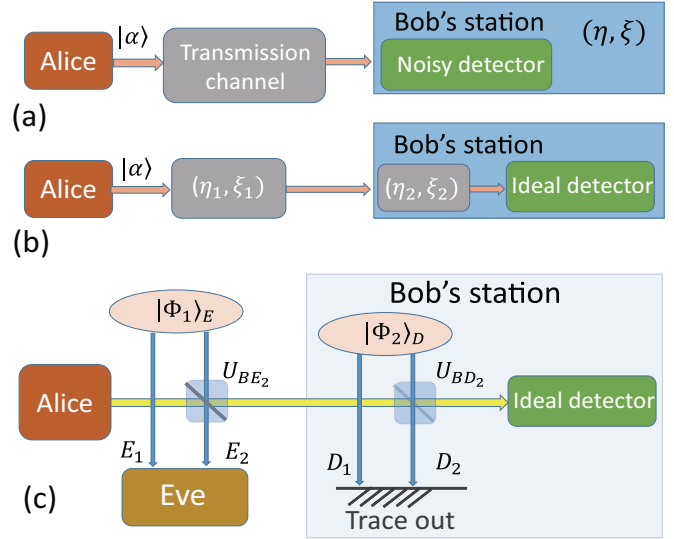

FIG. 1. (a) Alice sends a coherent state $|\alpha\rangle$ through a lossy and noisy channel. Bob observes quadrature with the total transmission η and the total excess noise ξ. (b) The transmission channel is modeled by a lossy and noisy Gaussian channel with the transmission η_1 and the excess noise ξ_1. Bob's detector is modeled by another lossy and noisy Gaussian channel with the transmission η_2 and the excess noise ξ_2 followed by an ideal homodyne detector. (c) The action of Gaussian channels (η_i, ξ_i) with $i = 1, 2$ can be described by beam-splitter unitaries U_{BE_2} and U_{BD_2} coupling to two-mode squeezed states $|\Phi_1\rangle_E$ and $|\Phi_2\rangle_D$.

to Bob through a lossy and noisy Gaussian channel with the transmission η_1 and excess noise ξ_1. The channel action is virtually described as follows: The signal is mixed with an ancillary mode E_2 of a two-mode squeezed state $|\Phi_1\rangle_{E_1E_2}$ at a beam splitter. Then, the extra modes E_1E_2 are traced out. We assume that Eve can access any signal information leaking out at the transmission line. This condition can be described by assuming that Eve holds the extra modes E_1E_2. The interaction model with a two-mode squeezed state and a beam splitter is often called the *entangling cloner* [48]. Due to the properties of the two-mode squeezed state, an entangling cloner induces linear loss and symmetric Gaussian noise on the signal mode in such a way that Eve holds correlation on the signal noise. There is another interaction model to simulate this effect with a two-mode squeezer and two beam splitters [49].

Let us also assume the signal is transmitted through another Gaussian channel with the transmission η_2 and excess noise ξ_2 at Bob's detection process in Bob's station. We assume that Eve is unable to access any signal information leaking out at the detection process inside Bob's station. The signal is mixed with an ancillary mode D_2 of a two-mode squeezed state $|\Phi_2\rangle_{D_1D_2}$ at a beam splitter. Then, the extra modes D_1D_2 are traced out, and Eve has no chance to hold the purifying modes D_1D_2. To this end, our model contains two entangling cloners associated with the pair of Gaussian channels. One is used to describe Eve's access. The other one, associated with the extra modes D_1D_2, is used to describe a realistic detection process.

Let us write Eve's initial two-mode squeezed state as

$$|\Phi_1\rangle_E = \sqrt{\frac{2}{\pi}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dx_1 dx_2 \, e^{-V_1 x_1^2 - x_2^2/V_1}$$
$$\times \left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1} \left|\frac{x_1-x_2}{\sqrt{2}}\right\rangle_{E_2}, \tag{5}$$

where $|x\rangle_{E_i}$ is the eigenket of a quadrature operator x of the mode E_i with eigenvalue x. The parameter V_1 is associated with the channel's parameters as [50]

$$\frac{1}{2}\left(V_1 + \frac{1}{V_1}\right) = \frac{1-\eta_1+\xi_1}{1-\eta_1}. \tag{6}$$

Since the coherent state $|S\rangle$ can be written as

$$|S\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \int_{-\infty}^{\infty} dx \, e^{-(x-S)^2} |x\rangle \tag{7}$$

and the beam splitter of transmission η leads to the transformation

$$|x\rangle |x_2\rangle_{E_2} \to |\sqrt{\eta}x - \sqrt{1-\eta}x_2\rangle |\sqrt{1-\eta}x + \sqrt{\eta}x_2\rangle_{E_2}, \tag{8}$$

the state after the beam-splitter interaction $U^{(\mathrm{BS})}$ takes the form of [43]

$$U_{\mathrm{BE2}}^{(\mathrm{BS})} |S\rangle_B |\Phi_1\rangle_E = \int_{-\infty}^{\infty} dm |m\rangle_B |\psi(S,m)\rangle_E, \tag{9}$$

where

$$|\psi(S,m)\rangle = \left(\frac{8}{\pi^3 \eta_1^2}\right)^{\frac{1}{4}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dx_1 dx_2 \, \psi(S,m) \left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1} \left|\sqrt{\frac{1-\eta_1}{\eta_1}}m + \frac{x_1-x_2}{\sqrt{2}\eta_1}\right\rangle_{E_2}, \tag{10}$$

with

$$\psi(S,m) = e^{-[\sqrt{\frac{1-\eta_1}{2\eta_1}}(x_1-x_2) + \frac{m}{\sqrt{\eta_1}} - S]^2 - V_1 x_1^2 - x_2^2/V_1}. \tag{11}$$

Let us write the initial state of the detector's environment for the second entangling cloner as

$$|\Phi_2\rangle_D = \sqrt{\frac{2}{\pi}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dy_1 dy_2 \, e^{-V_2 y_1^2 - y_2^2/V_2} \left|\frac{y_1+y_2}{\sqrt{2}}\right\rangle_{D_1} \left|\frac{y_1-y_2}{\sqrt{2}}\right\rangle_{D_2}, \tag{12}$$

where the parameter V_2 is associated with detector's parameters as

$$\frac{1}{2}\left(V_2 + \frac{1}{V_2}\right) = \frac{1-\eta_2+\xi_2}{1-\eta_2}. \tag{13}$$

Using the transformation given by Eq. (8), we can write the state before the ideal quadrature measurement device as

$$U_{\mathrm{BD2}}^{(\mathrm{BS})} U_{\mathrm{BE2}}^{(\mathrm{BS})} |S\rangle_B |\Phi_1\rangle_E |\Phi_2\rangle_D = \int_{-\infty}^{\infty} dm |m\rangle_B |\psi'(S,m)\rangle_{ED}, \tag{14}$$

where

$$|\psi'(S,m)\rangle = \sqrt{\frac{2}{\pi}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{dY_1 dY_2}{\sqrt{\eta_2}} \left|\psi\left(S, \frac{m}{\sqrt{\eta_2}} + \sqrt{\frac{1-\eta_2}{\eta_2}}Y_2\right)\right\rangle_E |Y_1\rangle_{D_1} \left|\sqrt{\frac{1-\eta_2}{\eta_2}}m + \frac{Y_2}{\sqrt{\eta_2}}\right\rangle_{D_2} e^{-\frac{V_2}{2}(Y_1+Y_2)^2 - \frac{(Y_1-Y_2)^2}{2V_2}}. \tag{15}$$

Since Eve cannot access the information leakage coming from detector's environment system D, we trace out the system D in what follows.

Supposing Bob's homodyne outcome is m, we obtain Eve's density operator,

$$\rho_{S,m} := \mathrm{tr}_{D_1 D_2} |\psi'(S,m)\rangle\langle\psi'(S,m)| = \sqrt{\frac{4}{\pi} \frac{1}{V_2 + \frac{1}{V_2}}} \int dY |\varphi_{S,m}\rangle\langle\varphi_{S,m}| e^{-\frac{4Y^2}{V_2+\frac{1}{V_2}}}, \tag{16}$$

where

$$|\varphi_{S,m}\rangle = \left(\frac{8}{\pi^3 \eta_1^2 \eta_2}\right)^{1/4} \iint dX_1 dX_2 e^{-[\sqrt{\frac{1-\eta_1}{\eta_1}}X_2 + \frac{1}{\sqrt{\eta_1 \eta_2}}(m+\sqrt{1-\eta_2}Y)-S]^2} e^{-\frac{V_1}{2}(X_1+X_2)^2 - \frac{(X_1-X_2)^2}{2V_1}} |X_1\rangle_{E_1}$$
$$\otimes \left|\frac{X_2}{\sqrt{\eta_1}} + \frac{\sqrt{1-\eta_1}}{\sqrt{\eta_1 \eta_2}}(m+\sqrt{1-\eta_2}Y)\right\rangle_{E_2} = \iint dx_1 dx_2 \varphi_Y(x_1,x_2) |x_1\rangle_{E_1} |x_2\rangle_{E_2}. \tag{17}$$

Here, in the final expression, we defined

$$\varphi_Y(x_1,x_2) := \left(\frac{8}{\pi^3 \eta_2}\right)^{\frac{1}{4}} e^{-\left[\sqrt{1-\eta_1}x_2 + \sqrt{\frac{\eta_1}{\eta_2}}(m+\sqrt{1-\eta_2}Y) - S\right]^2} e^{-\frac{V_1}{2}\left[x_1 + \sqrt{\eta_1}x_2 - \sqrt{\frac{1-\eta_1}{\eta_2}}(m+\sqrt{1-\eta_2}Y)\right]^2} e^{-\frac{1}{2V_1}\left[x_1 - \sqrt{\eta_1}x_2 + \sqrt{\frac{1-\eta_1}{\eta_2}}(m+\sqrt{1-\eta_2}Y)\right]^2}. \tag{18}$$

Further tracing out $\rho_{S,m}$ in Eq. (16), we obtain the probability that Bob gets m when Alice sends $|S\rangle$:

$$\mathrm{tr}\rho_{S,m} = \sqrt{\frac{2}{\pi}}\sqrt{\frac{1}{1+\xi_1\eta_2+\xi_2}}e^{-2\frac{(m-\sqrt{\eta_1\eta_2}S)^2}{1+\xi_1\eta_2+\xi_2}}. \quad (19)$$

Comparing this relation with Eq. (2), we find

$$\eta = \eta_1\eta_2,$$
$$\xi = \xi_1\eta_2 + \xi_2. \quad (20)$$

This is the central relation to associate the total channel parameters (η, ξ) with the parameters of the transmission line (η_1, ξ_1) and the parameters of the detection process in Figs. 1(a) and 1(b). From the expression of $\rho_{S,m}$ in Eq. (16), we define normalized states,

$$\omega_{i,j} = \frac{\rho_{(-1)^i|S|,(-1)^j|m|}}{\mathrm{tr}\rho_{(-1)^i|S|,(-1)^j|m|}}, \quad (21)$$

where $i, j \in \{0, 1\}$ can be associated with Alice's bit and Bob's bit, respectively. As we can see from Eq. (16), Eve's state $\rho_{S,m}$ is susceptible to both Alice's state preparation S and Bob's measurement outcome m. In fact, Eve's information can be bounded by the difference of her states due to the change of the signs of S and m, and the normalized state $\omega_{i,j}$ in Eq. (21) helps us to express the relevant information quantities [42,43].

Let us recall the bit error rate ϵ is given in Eq. (3). In the case of the DR scheme, Eve tries to know Alice's preparation of the bit. Eve's knowledge is determined from the difference of her states with Alice's choice $i = \{0, 1\}$,

$$\rho_A^0 = (1-\epsilon)\omega_{00} + \epsilon\omega_{01},$$
$$\rho_A^1 = (1-\epsilon)\omega_{11} + \epsilon\omega_{10}. \quad (22)$$

In the case of the RR scheme, Eve tries to know Bob's bit. Eve's knowledge is thus determined from the difference of her states with the sign of Bob's outcome $j = \{0, 1\}$,

$$\rho_B^0 = (1-\epsilon)\omega_{00} + \epsilon\omega_{10},$$
$$\rho_B^1 = (1-\epsilon)\omega_{11} + \epsilon\omega_{01}. \quad (23)$$

Therefore, the information potentially accessible to Eve is bounded from above by the Holevo quantity,

$$\chi = \begin{cases} S(\rho) - S(\rho_A^0)/2 - S(\rho_A^1)/2 & \text{for DR,} \\ S(\rho) - S(\rho_B^0)/2 - S(\rho_B^1)/2 & \text{for RR,} \end{cases} \quad (24)$$

where we define $\rho := (\rho_A^0 + \rho_A^1)/2 = (\rho_B^0 + \rho_B^1)/2$ and the von Neumann entropy is given by $S(\rho) = -\mathrm{Tr}(\rho\log_2\rho)$.

Although we have proceeded our calculation based on the notation convention of Refs. [42,43], it may be instructive to restate the connection to an entanglement based picture. In such a picture, Alice prepares a qubit-mode entangled state $|\phi\rangle_{AB} = (|0\rangle_A|\alpha\rangle_B + |1\rangle_A|-\alpha\rangle_B)/\sqrt{2}$, and sends the mode B to Bob. Note that the whole system consists of Alice, Bob, Eve, and the detector's environment, which are, respectively, denoted by the subscripts A, B, E, and D. Using the two-mode squeezed states $|\Phi_1\rangle$, $|\Phi_2\rangle$, and the unitary operators in Eq. (14), the whole system can be written as a pure state on the four modes,

$$|\Psi\rangle_{ABDE} = U_{BD2}^{(BS)}U_{BE2}^{(BS)}|\phi\rangle_{AB}|\Phi_1\rangle_E|\Phi_2\rangle_D. \quad (25)$$

Then, the tripartite state between Alice, Bob, and Eve is given by tracing out detector's environment,

$$\rho_{ABE} = \mathrm{tr}_D(|\Psi\rangle\langle\Psi|). \quad (26)$$

Associated with the absolute value of Bob's measurement outcome m, this state is filtered as

$$\rho_{ABE}^{|m|} = \frac{\hat{P}_m\rho_{ABE}\hat{P}_m}{\mathrm{tr}(\hat{P}_m\rho_{ABE}\hat{P}_m)}, \quad (27)$$

where we defined the projector as

$$\hat{P}_m = |m\rangle\langle m|_B + |-m\rangle\langle-m|_B. \quad (28)$$

Recall that Alice's bit value $i \in \{0, 1\}$ can be determined by projecting her qubit into $|i\rangle_A$ and Bob's bit value $j \in \{0, 1\}$ is determined by projecting his mode into $|(-1)^j|m|\rangle_B$. Therefore, Eve's states in Eq. (22) can be written as

$$\rho_A^i = \frac{\mathrm{tr}_B\langle i|\rho_{ABE}^{|m|}|i\rangle_A}{\mathrm{tr}\langle i|\rho_{ABE}^{|m|}|i\rangle_A}, \quad (29)$$

as well as Eve's states in Eq. (23),

$$\rho_B^j = \frac{\mathrm{tr}_A\langle(-1)^j|m||\rho_{ABE}^{|m|}|(-1)^j|m|\rangle_B}{\mathrm{tr}\langle(-1)^j|m||\rho_{ABE}^{|m|}|(-1)^j|m|\rangle_B}. \quad (30)$$

Since we have traced out the system D, it seems difficult to analytically find all eigenvalues of the relevant density operators in the Holevo quantity of Eq. (24), in sharp contrast to the previous approaches [42,43] where the rank of the density operators was a few and analytic expressions of all eigenvalues were found. In this paper, we expand the density operator in a photon-number basis (see the Appendix) and determine the Holevo quantity by numerically finding eigenvalues.

IV. KEY RATES

The secure key against collective Gaussian attacks can be calculated from the difference between the information of Alice and Bob in Eq. (4) and Eve's potential knowledge in Eq. (24) [43],

$$\int P(m|\alpha)\max[I_{AB} - \chi, 0]dm, \quad (31)$$

where $P(m|\alpha)$ is given by Eq. (2), and we carry out a postselection process that integrates measurement outcomes satisfying

$$\max[I_{AB} - \chi, 0] \geqslant 0. \quad (32)$$

In our previous work [43], an analytic expression of the Holevo quantity χ was obtained and a set of the key rates was shown as a function of transmission distance with the total excess noise $\xi = \{0.005, 0.01, 0.02\}$ where the photon number $|S|^2 = \alpha^2$ was selected to maximize the key rate and the detector was assumed to be an ideal homodyne detector [In the present notation, this corresponds to $(\eta, \xi) = (\eta_1, \xi_1)$ and $(\eta_2, \xi_2) = (1, 0)$]. Here we can calculate the key rate for the detector described by a Gaussian channel. We address the key rate with $\xi_2 > 0$ and $\eta_2 = 1$ based on the eavesdropping model described in the previous section.
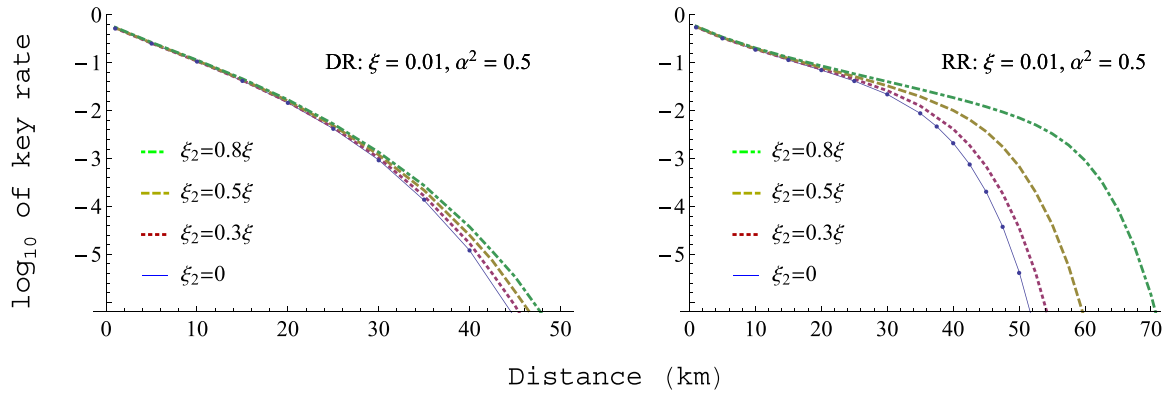
FIG. 2. Key rates for the direct-reconciliation (DR) scheme and the reverse-reconciliation (RR) scheme with the photon number $\alpha^2 = 0.5$ and the total excess noise $\xi = 0.01$. The amount of detector's excess noise ξ_2 is set to 0, 30%, 50%, and 80% of the total excess noise $\xi = 0.01$. The circles on the curve of $\xi_2 = 0$ are calculated from the analytic result in Ref. [43].

Figure 2 shows a set of numerically calculated key rates with the fixed photon number $\alpha^2 = 0.5$ and the total excess noise $\xi = 0.01$ for the detector noise $\xi_2 = \{0, 0.3\xi, 0.5\xi, 0.8\xi\}$ and detection efficiency $\eta_2 = 1$. Note that the relations of the channel parameters (η_1, ξ_1), the detector parameters (η_2, ξ_2), and the total observed transmission η and the total excess noise ξ are given in Eqs. (20). Note also that the value of the photon number $\alpha^2 = 0.5$ was close to the optimal photon number that maximizes the key rates in the case of $0.005 \leqslant \xi \leqslant 0.02$ when the distance d is located somewhere between 5 and 40 km both in the RR and DR schemes [43].

As expected, the decay of the key rate is to some extent delayed as the ratio of the detection noise to the excess noise ξ_2/ξ becomes larger. Notably, this effect is more significant in the case of the RR scheme. For instance, if we compare the solid curve of $\xi_2 = 0$ and the dot-dash-dotted curve of $\xi_2 = 0.8\xi$, we can observe that for a given key rate $G > 10^{-6}$, the difference of distance is less than 5 km for the DR scheme,

whereas the difference of distance can be more than 15 km for the RR scheme. In both cases, our result suggests that one can improve the key rate by separately specifying the channel parameters and the detector parameters. An intuitive reason that the RR scheme has more advantage in specifying the detection noise is that it becomes harder for Eve to infer Bob's outcome as the detection noise inside Bob's station becomes larger. The fact that the RR scheme maintains its flat decay for a longer distance suggests that CV-QKD schemes could be incorporated with a long-distance network beyond the metropolitan networks.

Since initially there is no specific constraint on the average photon number α^2 of four coherent states, we can choose this parameter so as to extract a higher key rate. The upper panels of Fig. 3 show the maximum key rates of the DR scheme for the excess noise $\xi = \{0.005, 0.01, 0.02\}$ when the photon number α^2 is optimized. The key rate is basically calculated in each 5-km-distance step and photon number step of 0.05 from $d = 5$ km. The lower panels of
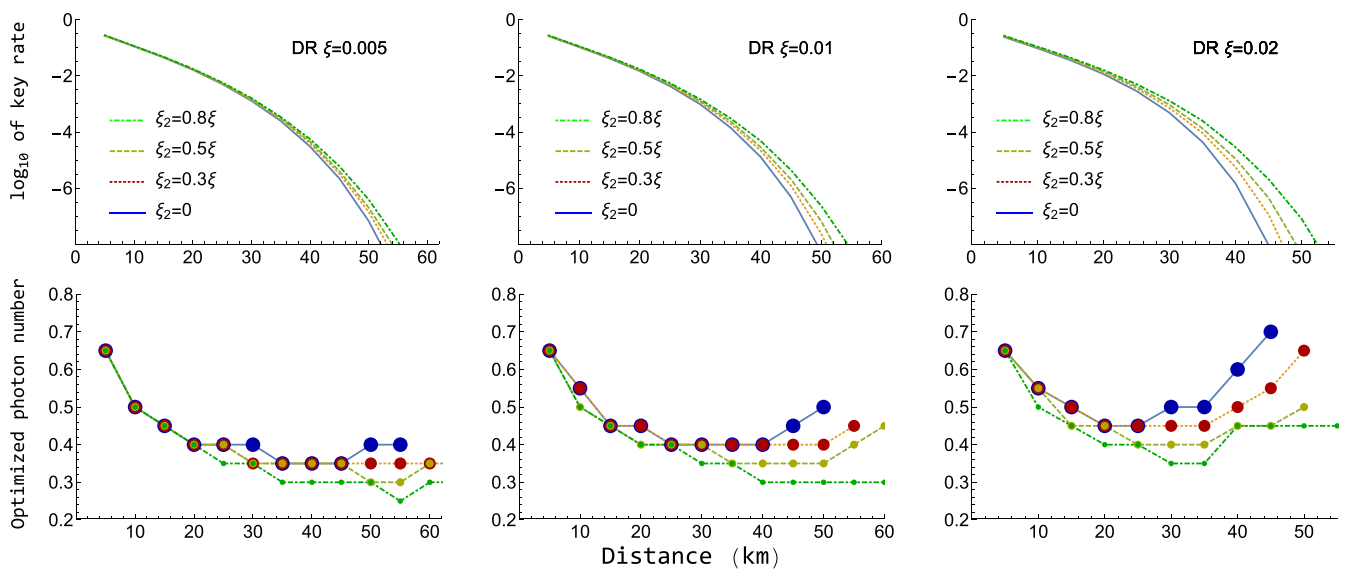

FIG. 3. Key rates for the direct-reconciliation (DR) scheme as functions of distance with the total excess noise $\xi = \{0.005, 0.01, 0.02\}$. The photon number α^2 is chosen to maximize the key rate with 0.05 steps. The amount of the detector's excess noise ξ_2 is set to 0, 30%, 50%, and 80% of the total excess noise ξ.
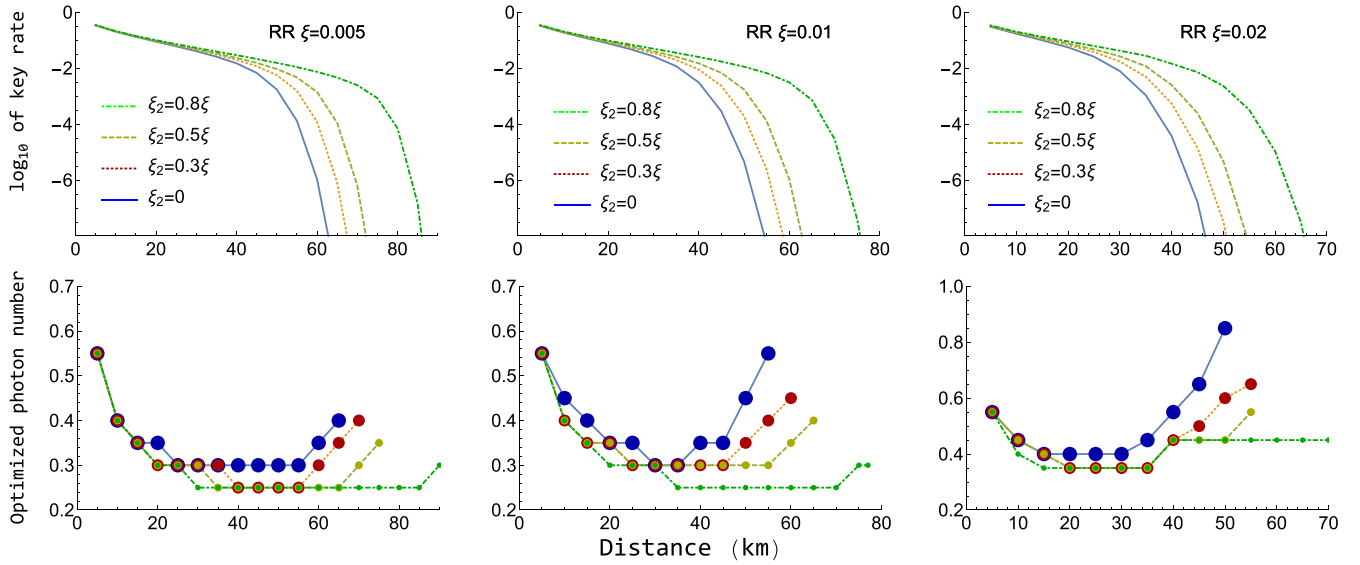
FIG. 4. Key rate for the reverse-reconciliation (RR) scheme as functions of distance with the total excess noise $\xi = \{0.005, 0.01, 0.02\}$. The photon number α^2 is chosen to maximize the key rate with 0.05 steps. The amount of the detector's excess noise ξ_2 is set to 0, 30%, 50%, and 80% of the total excess noise ξ.

Fig. 3 show the corresponding optimized values of the photon number α^2.

The upper panels of Fig. 4 show the maximum key rates of the RR scheme for the excess noise $\xi = \{0.005, 0.01, 0.02\}$. The key rate is basically calculated in each 5-km-distance steps and photon number steps of 0.05 from $d = 5$ km. The lower panels of Fig. 4 show the corresponding optimized values of the photon number. For a fixed total excess noise ξ, one can see that the shallow decay of the key rates sustains longer as the potion of the detection noise becomes larger. Thereby, depending on the distance, we can obtain a much better key rate by carefully calibrating the detection noise and the channel noise separately.

In optimizing the photon number α^2, it could be helpful to consider that there are three typical regions on the distance as follows: (i) For very short distances with smaller loss, Eve's information could be small. We thus can use a relatively higher value of the photon number for such as $d \sim 10$ km. (ii) For middle distances, the optimal photon number becomes smaller and its value is almost flat as a function of distance. The flatness suggests that the key rates are insensitive to the difference of the photon number with regard to the scale of such as the 0.5 photon number. This could be favorable for a practical implementation when a fine control of the photon number is difficult. (iii) Finally, for long distances, an increase of the optimal photon number is observed. In this regime, the key rate would drop more rapidly when one deviates the value of the photon number from the optimal value. Thereby, our numerical search of the optimal point could take a relatively long time, and the key rate itself is typically very low.

In summary, both in the DR and RR schemes, the typical behavior of the key rates with optimized photon number is not much different from the behavior of the key rate with the case of the fixed photon number $\alpha^2 = 0.5$ in Fig. 2 for all cases of the excess noise $\xi = \{0.005, 0.01, 0.02\}$. As far as our described model, the critical point in experiments is

to suppress the excess noise as low as possible both in the transmission process and the detection process. An essential observation is that for given total excess noise ξ, the optimal photon number becomes smaller as the portion of detection noise becomes larger. There is a trade-off relation that a smaller photon number implies lower information for Alice and Bob, and larger information leakage for Eve. Hence, one could not simply suggest that a better choice of the value of the initial photon number is high or low when the parameters change. In the present case of the numerically simulated regime, it turn out that a smaller photon number such as $\alpha^2 \in (0.3, 0.5)$ was widely feasible. In this respect, systematic numerical study would be more important to find out efficient settings in operating our QKD schemes.

V. CONCLUSION

We have developed a method to calculate the key rate of a CV-QKD scheme using four coherent states for a model of Gaussian attacks. We assume that the transmission channel and detection process are described by a pair of symmetric Gaussian channels. The key rate against collective Gaussian attacks can be essentially calculated for any set of the channel parameters. We use two entangling cloners to describe the two noise sources. One entangling cloner is assumed to be controlled by Eve as usual and represents the information leakage for her. The other entangling cloner represents the detection noise and is located inside Bob's station. Thereby, the signal outgoing to the detector's environment is simply traced out and gives no information leakage to Eve. We showed numerically determined key rates as functions of distance for a couple of possible combinations of excess noise parameters. By separating the channel noise and detection noise, we can always extract a larger key compared with the case that all loss and noises are induced by Eve's interference. The improvement of the key rates turns out to be more significant for the

RR schemes where the increase of inaccessible noises at the detector is thought to make Eve more difficult to infer Bob's outcomes. Note that our study is for an asymptotic key rate and limited to the case of eavesdropping models that induce symmetric Gaussian noise and linear loss. Since there is no proof that the Gaussian attack is the optimal attack for CV-QKD schemes with discrete modulation, achievable key rates in a general eavesdropping scenario could be significantly lower than the present key rates [44]. It may be worth noting that our method developed here would be applicable to the protocols proposed in Ref. [40], which include an efficient four-state protocol based on diagonally modulated coherent states, i.e., the coherent states in the form of $|\pm\alpha \pm i\alpha\rangle$.

APPENDIX: NUMBER-BASIS REPRESENTATION OF $\rho_{S,m}$ IN EQ. (16)

Given a matrix representation of the density operator $\rho_{S,m}$ in Eq. (16), we can determine its eigenvalues numerically. From the set of eigenvalues, we can determine the von Neumann entropy and thus the Holevo quantity χ in Eq. (24). In this Appendix, we present a basic calculation to expand the relevant density operator in the number basis so as to determine the matrix elements.

From the wave function of Eq. (17), we can carry out the integration of Y in $\rho_{S,m}$ of Eq. (16). For instance, we can write

$$\langle x_1, x_2|\rho_{S,m}|x_3, x_4\rangle e^{-\sum_{i=1}^{4} x_i^2}$$
$$= \sqrt{\frac{4}{\pi}\frac{1}{V_2 + \frac{1}{V_2}}} \int dY \varphi_Y(x_1, x_2)\varphi_Y(x_3, x_4) e^{-\frac{4Y^2}{V_2 + \frac{1}{V_2}} - \sum_{i=1}^{4} x_i^2}$$
$$= \sqrt{\frac{4}{\pi}\frac{1}{V_2 + \frac{1}{V_2}}} \sqrt{\frac{8}{\pi^2 \mathcal{P}\eta_2(1 - \eta_2)}} e^{-\boldsymbol{x}^t A \boldsymbol{x} + 2\boldsymbol{x}^t \boldsymbol{b} + c}, \quad \text{(A1)}$$

where

$$\mathcal{P} = \left(V_1 + \frac{1}{V_1}\right)\frac{1 - \eta_1}{\eta_2} + \frac{2\eta_1}{\eta_2} + \frac{4}{V_2 + \frac{1}{V_2}}\frac{1}{1 - \eta_2}, \quad \text{(A2)}$$

and we defined $(A, \boldsymbol{b}, c)$ so as to get the quadratic form of $\boldsymbol{x} = (x_1, x_2, x_3, x_4)^t$. The elements of $(A, \boldsymbol{b}, c)$ are determined as

$$A = \begin{pmatrix} \alpha_1 & \alpha_3 & \alpha_4 & \alpha_6 \\ \alpha_3 & \alpha_2 & \alpha_6 & \alpha_5 \\ \alpha_4 & \alpha_6 & \alpha_1 & \alpha_3 \\ \alpha_6 & \alpha_5 & \alpha_3 & \alpha_2 \end{pmatrix}, \quad \boldsymbol{b} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_1 \\ \beta_2 \end{pmatrix}, \quad \text{(A3)}$$

$$c = -\frac{4}{V_2 + \frac{1}{V_2}}\frac{m^2}{1 - \eta_2} + \frac{r^2}{\mathcal{P}} - 2S^2, \quad \text{(A4)}$$

with the help of the coefficients

$$\alpha_1 = 1 - \frac{p^2}{\mathcal{P}} + \frac{1}{2}\left(V_1 + \frac{1}{V_1}\right), \quad \text{(A5)}$$

$$\alpha_2 = 1 - \frac{q^2}{\mathcal{P}} + (1 - \eta_1) + \frac{\eta_1}{2}\left(V_1 + \frac{1}{V_1}\right), \quad \text{(A6)}$$

$$\alpha_3 = -\frac{pq}{\mathcal{P}} + \frac{\sqrt{\eta_1}}{2}\left(V_1 + \frac{1}{V_1}\right), \quad \text{(A7)}$$

$$\alpha_4 = -\frac{p^2}{\mathcal{P}}, \quad \alpha_5 = -\frac{q^2}{\mathcal{P}}, \quad \alpha_6 = -\frac{pq}{\mathcal{P}}, \quad \text{(A8)}$$

$$\beta_1 = \frac{pr}{\mathcal{P}}, \quad \beta_2 = \frac{qr}{\mathcal{P}} + \sqrt{1 - \eta_1}S, \quad \text{(A9)}$$

and the constants independent of the elements of $\boldsymbol{x}$,

$$p = -\frac{1}{2}\left(V_1 - \frac{1}{V_1}\right)\sqrt{\frac{1 - \eta_1}{\eta_2}}, \quad \text{(A10)}$$

$$q = \left[1 - \frac{1}{2}\left(V_1 + \frac{1}{V_1}\right)\right]\sqrt{\frac{\eta_1(1 - \eta_1)}{\eta_2}}, \quad \text{(A11)}$$

$$r = -2\sqrt{\frac{\eta_1}{\eta_2}}S - \frac{4}{V_2 + \frac{1}{V_2}}\frac{m}{1 - \eta_2}. \quad \text{(A12)}$$

Note that (V_1, V_2) are defined in Eqs. (6) and (13). They are equivalently written as

$$V_i = w_i + \sqrt{w_i^2 - 1},$$
$$w_i = \frac{1 - \eta_i + \xi_i}{1 - \eta_i}, \quad \text{(A13)}$$

for $i = 1, 2$.

In order to reach the number-state representation, let us write the wave functions of number states as

$$|n\rangle = \int_{-\infty}^{\infty} u_n(x)|x\rangle dx,$$

$$u_n(x) := \left(\frac{2}{\pi}\right)^{1/4}\frac{1}{\sqrt{2^n n!}}H_n(\sqrt{2}x)e^{-x^2},$$

$$H_n(x) := (-1)^n e^{x^2}\frac{d^n e^{-x^2}}{dx^n}. \quad \text{(A14)}$$

With these expressions and Eq. (A1), we can obtain the matrix element of $\rho_{S,m}$ as

$$\langle n_1, n_2|\rho_{S,m}|n_3, n_4\rangle = \frac{2}{\pi}\iiiint d^4x \prod_{i=1}^{4}\frac{H_{n_i}(\sqrt{2}x_i)e^{-x_i^2}}{\sqrt{2^{n_i}n_i!}}\langle x_1, x_2|\rho_{S,m}|x_3, x_4\rangle$$

$$= \frac{2}{\pi}\sqrt{\frac{4}{\pi}\frac{1}{V_2 + \frac{1}{V_2}}}\sqrt{\frac{8}{\pi^2 \mathcal{P}\eta_2(1 - \eta_2)}}\iiiint_{-\infty}^{\infty}\prod_{i=1}^{4}\frac{dx_i H_{n_i}(\sqrt{2}x_i)}{\sqrt{2^{n_i}n_i!}}e^{-\boldsymbol{x}^t A \boldsymbol{x} + 2\boldsymbol{x}^t \boldsymbol{b} + c}. \quad \text{(A15)}$$

Now, we can numerically determine the matrix elements. In our numerical approach, the matrix A is diagonalized. Then, we have a simpler quadratic form as

$$\boldsymbol{x}^t A \boldsymbol{x} - 2 \boldsymbol{x}^t \boldsymbol{b} - c = (A^{\frac{1}{2}} \boldsymbol{x} - A^{-\frac{1}{2}} \boldsymbol{b})^t (A^{\frac{1}{2}} \boldsymbol{x} - A^{-\frac{1}{2}} \boldsymbol{b}) - \boldsymbol{b}^t A^{-1} \boldsymbol{b} - c = \boldsymbol{y}^t \boldsymbol{y} - c', \tag{A16}$$

where

$$\boldsymbol{y} = (y_1, y_2, y_3, y_4)^t = A^{\frac{1}{2}} \boldsymbol{x} + A^{-\frac{1}{2}} \boldsymbol{b}, \tag{A17}$$

$$c' = c + \boldsymbol{b}^t A^{-1} \boldsymbol{b}. \tag{A18}$$

The volume element associated with this change of variables is given by $d^4 x = |\frac{\partial x_i}{\partial y_j}| d^4 y = \det(A^{-1/2}) d^4 y$. From the property of the determinant $\det(a) \det(b) = \det(ab)$, we can write $\det(A^{1/2}) = \sqrt{\det(A)}$. Using these relations, we have

$$\langle n_1, n_2 | \rho_{S,m} | n_3, n_4 \rangle = \frac{2}{\pi} \sqrt{\frac{4}{\pi} \frac{1}{V_2 + \frac{1}{V_2}}} \sqrt{\frac{8}{\pi^2 \mathcal{P} \eta_2 (1 - \eta_2)}} \frac{e^{-c'}}{\sqrt{\det(A)}} \iiint_{-\infty}^{\infty} \prod_{i=1}^{4} \frac{d y_i H_{n_i}(\sqrt{2} x_i)}{\sqrt{2^{n_i} n_i!}} e^{-y_i^2}, \tag{A19}$$

where $\{x_i\}$ will be represented in terms of $\{y_i\}$ through the inverse of Eq. (A17), namely,

$$\boldsymbol{x} = A^{-\frac{1}{2}} \boldsymbol{y} - A^{-1} \boldsymbol{b}. \tag{A20}$$

Since the product $\prod_i H_{n_i}(\sqrt{2} x_i)$ is a polynomial of (y_1, y_2, y_3, y_4), we can carry out the integration by recursively using the well-known formula for the Gaussian integral:

$$\int_{-\infty}^{\infty} y_i^{2n} e^{-y_i^2} d y_i = \sqrt{\pi} \frac{(2n-1)!!}{2^n}, \quad \int_{-\infty}^{\infty} y_i^{2n+1} e^{-y_i^2} d y_i = 0, \tag{A21}$$

for $n = 0, 1, 2, \dots$.

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

[2] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).

[3] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Inf. **2**, 16025 (2016).

[4] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Opt. Express **19**, 10387 (2011).

[5] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, New J. Phys. **13**, 123001 (2011).

[6] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, J. Lightwave Technol. **32**, 141 (2014).

[7] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, Opt. Express **22**, 21739 (2014).

[8] Y. L. Tang, H. L. Yin, S. J. Chen, Y. Liu, W. J. Zhang, X. Jiang, L. Zhang, J. Wang, L. X. You, J. Y. Guan, D. X. Yang, Z. Wang,

H. Liang, Z. Zhang, N. Zhou, X. Ma, T. Y. Chen, Q. Zhang, and J. W. Pan, IEEE J. Sel. Top. Quantum Electron. **21**, 116 (2015).

[9] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, Opt. Express **23**, 7583 (2015).

[10] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Frtekahlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, Sci. Rep. **7**, 1978 (2017).

[11] M. Sasaki, Quantum Sci. Technol. **2**, 020501 (2017).

[12] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, Phys. Rev. X **8**, 021009 (2018).

[13] A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami, and M. Sasaki, Quantum Sci. Technol. **2**, 034003 (2017).

[14] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).

[15] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Opt. Lett. **41**, 3511 (2016).

[16] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).

[17] J. Fiurášek, Phys. Rev. Lett. **89**, 137904 (2002).

[18] G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).

[19] S. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[20] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).

[21] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, New J. Phys. **12**, 103042 (2010).

[22] R. Kumar, H. Qin, and R. Alleaume, New J. Phys. **17**, 043027 (2015).

[23] M. Nakazawa, M. Yoshida, T. Hirooka, K. Kasai, T. Hirano, T. Ichikawa, and R. Namiki, IEEE J. Quantum Electron. **53**, 8000316 (2017).

[24] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).

[25] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).

[26] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).

[27] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, Opt. Lett. **40**, 3695 (2015).

[28] F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, arXiv:1712.10242.

[29] A. Marie and R. Alléaume, Phys. Rev. A **95**, 012316 (2017).

[30] J.-C. Boileau, J. Batuwantudawe, and R. Laflamme, Phys. Rev. A **72**, 032321 (2005).

[31] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).

[32] 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).

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

[34] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Opt. Express **20**, 14030 (2012).

[35] V. C. Usenko and R. Filip, Entropy **18**, 20 (2016).

[36] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[37] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).

[38] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).

[39] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

[40] R. Namiki and T. Hirano, Phys. Rev. A **74**, 032302 (2006).

[41] T. Ichikawa, T. Hirano, T. Matsubara, M. Ono, and R. Namiki, J. Phys. Soc. Jpn. **86**, 094001 (2017).

[42] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[43] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, Quantum Sci. Technol. **2**, 024010 (2017).

[44] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, Phys. Rev. A **79**, 012307 (2009).

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

[46] A. Leverrier and P. Grangier, Phys. Rev. Lett. **106**, 259902(E) (2011).

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

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

[49] R. Namiki, M. Koashi, and N. Imoto, Phys. Rev. A **73**, 032302 (2006).

[50] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303 (2007).