Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers

Heng Zhang, Jian Fang, and Guangqiang He*

State Key Laboratory of Advanced Optical Communication Systems and Networks, Key Laboratory on Navigation and Location-based Service, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240, China

(Received 3 May 2012; published 29 August 2012)

We propose a method to improve the secret key rates of four-state continuous-variable quantum key distribution by using an optical preamplifier. The modified protocol allows the distribution of higher secret key rates over long distances. Included in this paper is a detailed investigation of the effects of inserting an optical parametric amplifier into the output of the quantum channel in the four-state protocol, which will be instructive and meaningful about the usage of amplifiers in order to achieve the optimal performance of the protocol in a specific scenario.

DOI: 10.1103/PhysRevA.86.022338 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

A major practical application of quantum-information science is quantum key distribution, which allows two distant parties to communicate with absolute privacy, even in the presence of an eavesdropper [1,2]. Continuous-variable quantum key distribution (CVQKD) by using coherent states [3] is an alternative to the single-photon-based discrete-variable quantum key distribution protocol. In this protocol, information is encoded on quadratures of coherent states, which are easily generated and measured with remarkable precision by off-the-shelf telecommunication components.

A CVQKD protocol based on coherent states with Gaussian modulation was found to be a practical scheme [4,5]. It has been experimentally demonstrated [3,6] and has been shown secure against arbitrary collective attacks [7,8], which are optimal in the asymptotic limit [9]. But this kind of protocol is limited by its working range, which results from the low reconciliation efficiency β at long working distances. Even using the best present codes, such as low-density-parity-check codes [10] or turbo codes [11], or with the help of algebraic properties of $\mathbb{R}^8$ [12], one cannot expect to extend the range of the protocol well over 50 km.

Based on this background, discrete-modulation CVQKD was introduced to break this 50-km limitation. The four-state protocol [13] is a typical example, which has been proved secure against collective attacks and allows the distribution of secret keys over long distances at very low signal-to-noise ratio with a high reverse reconciliation efficiency.

In this paper, we continue to improve the performance of the four-state protocol. Inspired by the discussion in [14], we propose to insert an optical amplifier at the output of the quantum channel and inside Bob's apparatus in the four-state protocol, and we calculate in detail the resulting secret key rates, secure against collective attacks. For that purpose, we will assume that Bob's apparatus is inaccessible to the eavesdropper Eve.

The results are attractive, but are different from those of protocols based on Gaussian modulation with preamplifiers [14]. We analyze in general the effects introduced by using the preamplifiers on Alice's optimal modulation variance, the secret key rates, and the working distance. Then strategies are suggested to optimize the performance of the four-state protocol.

This paper is organized as follows: In Sec. II, a general theoretical analysis of the modified four-state protocol is given. In Sec. III, the results of numerical simulations are provided to show the effects introduced by optical amplifiers. The conclusions are drawn in Sec. IV.

II. THE MODIFIED FOUR-STATE PROTOCOL

In the following, we first review the basic notions related to the four-state protocol and present the assumptions of our calculations. We then derive the the expressions for the modified secret key rate when homodyne or heterodyne detectors are used, and for the case of collective eavesdropping attacks.

A. Notations and assumptions

The standard prepare-and-measure (PM) description of the four-state protocol is described as follows:

(a) Alice sends randomly one of the four coherent states $|\alpha_k\rangle = |\alpha e^{i(2k+1)\pi/4}\rangle$ with $k \in \{0,1,2,3\}$ to Bob through the quantum channel. The channel features a transmission efficiency T and an excess noise ϵ, resulting in a noise variance at Bob's input of $(1+T\epsilon)N_0$, where N_0 is the shot-noise variance. The total channel-added noise referred to the channel input is expressed as $\chi_{\text{line}} = 1/T + \epsilon - 1$.

(b) When Bob receives the modulated coherent states, he can take either homodyne or heterodyne detection using a practical detector characterized by its efficiency η and electronics noise v_{el}. We can define a detection-added noise referred to Bob's input and expressed in shot-noise units which we denote in general as χ_h and is given by the expressions $\chi_{\text{hom}} = [(1-\eta)+v_{\text{el}}]/\eta$ and $\chi_{\text{het}} = [1+(1-\eta)+2v_{\text{el}}]/\eta$ for homodyne and heterodyne detection, respectively. The total noise referred to the channel input can then be expressed as $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_h/T$.

The PM version of the protocol is equivalent to the entanglement-based (EB) scheme shown in Fig. 1. In this scheme, Alice has a pure two-mode entangled state:

$$|\Phi_4\rangle = \tfrac{1}{2}(|\psi_0\rangle|\alpha_0\rangle + |\psi_1\rangle|\alpha_1\rangle + |\psi_2\rangle|\alpha_2\rangle + |\psi_3\rangle|\alpha_3\rangle), \quad (1)$$

*gqhe@sjtu.edu.cn

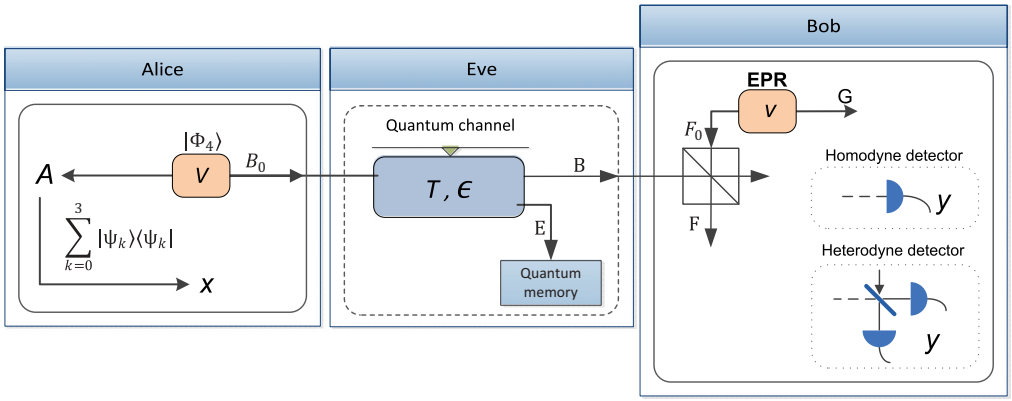

FIG. 1. (Color online) Entanglement-based scheme for the four-state protocol with homodyne or heterodyne detection. The quantum channel is controlled by Eve.

where the states

$$|\psi_k\rangle = \frac{1}{2}\sum_{m=0}^{3} e^{i(1+2k)m\pi/4}|\phi_m\rangle \tag{2}$$

are orthogonal non-Gaussian states. The state $|\phi_m\rangle$ is written as follows:

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}(-1)^n\frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}}|4n+k\rangle, \tag{3}$$

where

$$\begin{aligned}\lambda_{0,2} &= \tfrac{1}{2}e^{-\alpha^2}[\cosh(\alpha^2)\pm\cos(\alpha^2)],\\ \lambda_{1,3} &= \tfrac{1}{2}e^{-\alpha^2}[\sinh(\alpha^2)\pm\sin(\alpha^2)].\end{aligned} \tag{4}$$

The EB version of the four-state protocol can be described as follows:

(a) Alice prepares the entangled state $|\Phi_4\rangle$ of variance $V = 1 + V_A$, where $V_A = 2\alpha^2$ is the modulation variance of Alice in the PM scheme. Then she performs the projective measurements $|\psi_k\rangle\langle\psi_k|$ $(k = 0,1,2,3)$ on her half, thus preparing the coherent state $|\alpha_k\rangle$ when her measurement gives the result k. This modulated state is sent to Bob through the quantum channel.

(b) Bob's detector is modeled by a beam splitter with transmission η, and its electronic noise $v_{\rm el}$ is modeled by an Einstein-Podolsky-Rosen (EPR) state of variance v. For homodyne detection, $v = 1 + v_{\rm el}/(1-\eta)$, and for heterodyne detection, $v = 1 + 2v_{\rm el}/(1-\eta)$.

After the quantum transmission phase of the communication has ended, the signal of the modulated and measured value encodes the bit of the raw key. Bob and Alice share correlated strings of bits. By reverse reconciliation and privacy amplification, they can achieve a secret key.

B. Secret key rates for the four-state protocol

Under the assumptions that we have described above, we want to calculate the secret key rates for the four-state protocol with homodyne and heterodyne detection, for the case of collective eavesdropping attacks. When Alice and Bob use reverse reconciliation and the reconciliation efficiency is β, the secret key rate is

$$K_R = \beta I(x:y) - S_4(y:E), \tag{5}$$

where $I(x:y)$ is the Shannon mutual information between Alice and Bob, and $S_4(y:E)$ is the quantum mutual information between Bob and Eve in the four-state protocol.

The Shannon mutual information $I(x:y)$ between Alice and Bob is considered for homodyne and heterodyne detection. For the homodyne detection case, Shannon's equation is used:

$$I(x:y) = \frac{1}{2}\log_2\frac{V+\chi_{\rm tot}}{1+\chi_{\rm tot}} \tag{6}$$

and for the heterodyne detection case

$$I(x:y) = \log_2\frac{V+\chi_{\rm tot}}{1+\chi_{\rm tot}}. \tag{7}$$

According to the fact that the Holevo information between Eve and Bob's classical variable $S(y:E)$ is maximized when the state ρ_{AB} shared by Alice and Bob is Gaussian [15,16]. Hence, $S_4(y:E)$ can be bounded from above by a function of the covariance matrix γ_{AB} of ρ_{AB}:

$$\gamma_{AB} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T}Z_4\sigma_z \\ \sqrt{T}Z_4\sigma_z & T(V+\chi_{\rm line})\mathbb{I}_2 \end{bmatrix}, \tag{8}$$

where $Z_4 = 2\alpha^2(\lambda_0^{3/2}\lambda_1^{-1/2} + \lambda_1^{3/2}\lambda_2^{-1/2} + \lambda_2^{3/2}\lambda_3^{-1/2} + \lambda_3^{3/2}\lambda_0^{-1/2})$ reflects the correlation between mode A and mode B, $\mathbb{I}_2 = \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$, and $\sigma_z = \left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]$. This covariance matrix has the same form as in the Gaussian modulation scheme, where Z_4 would be replaced by the correlation of a two-mode squeezed vacuum $Z_G = \sqrt{V_A^2 + 2V_A}$. Note that when V_A is small enough, Z_4 is very close to Z_G, as shown in Fig. 2. For $V_A < 0.5$, Z_4 and Z_G are almost indistinguishable, meaning that in this region, the quantum mutual information between

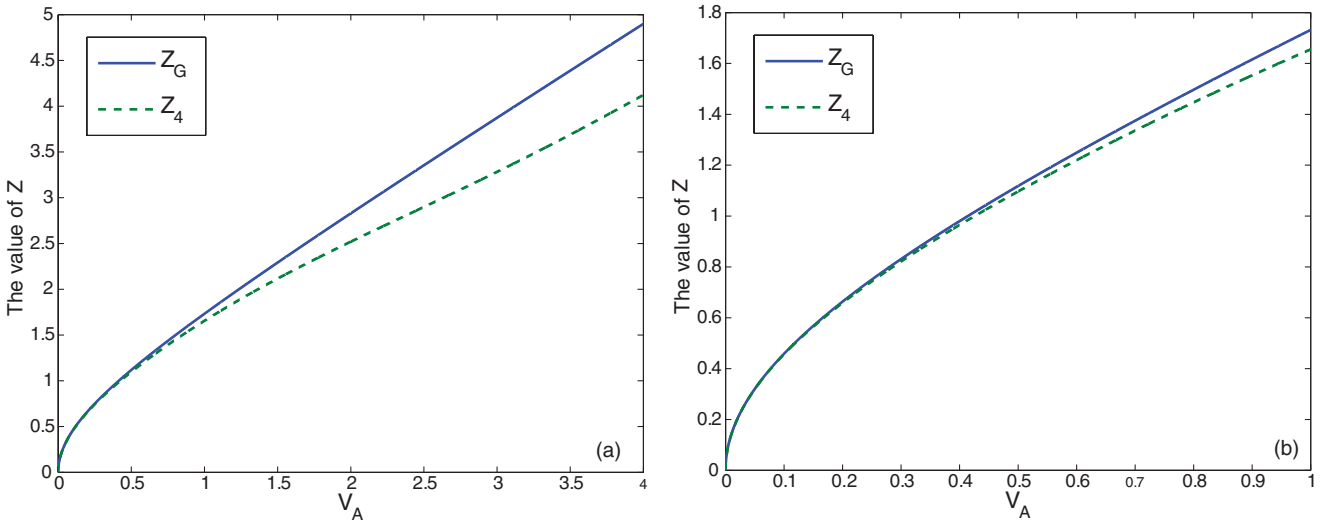

FIG. 2. (Color online) Comparison of the correlation Z_4 (dashed lines) for the four-state protocol protocol and Z_G (full lines) for the Gaussian modulation protocol as a function of V_A. (a) For large values of V_A. (b) For small values of V_A.

Bob and Eve is very similar in these two protocols. Hence one has $S_4(y:E) \approx S_G(y:E)$.

Based on this consequence, we will give the expression for $S_4(y:E)$:

$$S_4(y:E) = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right), \tag{9}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. The symplectic eigenvalues $\lambda_{1,2}$ are given by

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})}, \tag{10}$$

where

$$\begin{aligned} A &= V^2 + T^2(V + \chi_{\text{line}})^2 - 2TZ_4^2, \\ B &= \left(TV^2 + TV\chi_{\text{line}} - TZ_4^2\right)^2. \end{aligned} \tag{11}$$

The symplectic eigenvalues $\lambda_{3,4}$ are given by

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})}, \tag{12}$$

where for the homodyne case,

$$\begin{aligned} C_{\text{hom}} &= \frac{A\chi_{\text{hom}} + V\sqrt{B} + T(V + \chi_{\text{line}})}{T(V + \chi_{\text{tot}})}, \\ D_{\text{hom}} &= \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}, \end{aligned} \tag{13}$$

and for the heterodyne case,

$$C_{\text{het}} = \frac{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}[V\sqrt{B} + T(V + \chi_{\text{line}})] + 2TZ_4^2}{[T(V + \chi_{\text{tot}})]^2}, \quad D_{\text{het}} = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2, \tag{14}$$

and A and B are given in Eq. (11).

Now let us consider the reconciliation efficiency β in Eq. (5). The reconciliation scheme presented in [13] performs indeed much better at low signal-to-noise ratio (SNR) $R_{S/N}$(lower than 1) than reconciliation schemes used for a Gaussian modulation. By using the scheme, one can have a reconciliation efficiency greater than 80% for all SNRs below 1. So we can take $\beta = 0.8$ in our analysis only if the working region of V_A is small enough [$V_A = R_{S/N}(1 + x_{\text{tot}})$].

So far, we have obtained the value for the secret key rate K_R of the four-state protocol. Next we will consider the case which takes into account the use of amplifiers to enhance the performance of the four-state protocol.

C. Adding an amplifier to the protocol

In the practical case Bob's detection apparatus has inherent imperfections that degrade the secret key rates; inspired by the discussion in [14], we will use optical parametric amplifiers in the four-state protocol to compensate for the detectors' imperfections. In the following, models for two types of optical amplifiers are provided first. This allows us to determine the modified secret key rates of the system when an optical amplifier is placed at the input of Bob's apparatus.

1. Models for optical amplifiers

Here we consider two typical amplifiers: an ideal phase-sensitive amplifier and a practical phase-insensitive amplifier, which have been studied extensively [17].

Phase-sensitive amplifier. The phase-sensitive amplifier (PSA) is a degenerate optical parametric amplifier that ideally permits noiseless amplification of a chosen quadrature. Its behavior can be described by a transformation matrix Y^{PSA}:

$$Y^{PSA} = \begin{bmatrix} \sqrt{g} & 0 \\ 0 & \frac{1}{\sqrt{g}} \end{bmatrix}, \tag{15}$$

where $g \geqslant 1$ is the gain of the amplification.

Phase-insensitive amplifier. The phase-insensitive amplifier (PIA) is a nondegenerate optical parametric amplifier, which amplifies both quadratures symmetrically, but the amplification process is associated with a fundamental excess noise that arises from the coupling of the signal input to the internal modes of the amplifier [17,18]. This type of amplifier can be modeled as a noiseless amplifier that applies the appropriate gain factor to each input mode and uses an EPR state of variance N, one-half of which is entering the amplifier's second input port, to model the amplifier's inherent noise.

Its behavior can also be described by matrices. Y^{PIA} describes the transform of a PIA, and is written as

$$Y^{PIA} = \begin{bmatrix} \sqrt{g}\,\mathbb{I}_2 & \sqrt{g-1}\,\sigma_z \\ \sqrt{g-1}\,\sigma_z & \sqrt{g}\,\mathbb{I}_2 \end{bmatrix}. \tag{16}$$

γ^N describes the EPR state of variance Nused to model the amplifier's inherent noise, and is expressed as

$$\gamma^N = \begin{bmatrix} N\mathbb{I}_2 & \sqrt{N^2-1}\,\sigma_z \\ \sqrt{N^2-1}\,\sigma_z & N\mathbb{I}_2 \end{bmatrix}. \tag{17}$$

2. Modified secret key rate

Now we derive the modified secret key rates when an optical amplifier is employed in the system. As we discussed in Sec. II B, the four-state protocol can be very close to the Gaussian-modulation-based CVQKD protocol when V_A is very small, so the results derived in the CVQKD protocol with Gaussian modulation can also be applied in the four-state protocol. Here we can easily get the modified secret key rates using similar methods to that developed in [14].

Two promising cases, homodyne detection combined with a phase-sensitive amplifier placed at the output of the quantum channel, and heterodyne detection combined with a phase-insensitive amplifier placed at the output of the quantum channel, are considered in this paper. All effects introduced by an optical amplifier on the secret key rates are totally described by the modified parameters χ_{hom} and χ_{het}. We now give the modified parameters for these two cases.

Homodyne detection and phase-sensitive amplifier case. In this case, the usage of a phase-sensitive amplifier is equivalent to modifying χ_{hom} into χ_{hom}^{PSA}, which is written as

$$\chi_{\text{hom}}^{PSA} = \frac{(1-\eta)+v_{\text{el}}}{g\eta}. \tag{18}$$

Heterodyne detection and phase-insensitive amplifier case. As above, χ_{het} is modified to χ_{het}^{PIA}, which is written as

$$\chi_{\text{het}}^{PIA} = \frac{1+(1-\eta)+2v_{\text{el}}+N(g-1)\eta}{g\eta}. \tag{19}$$

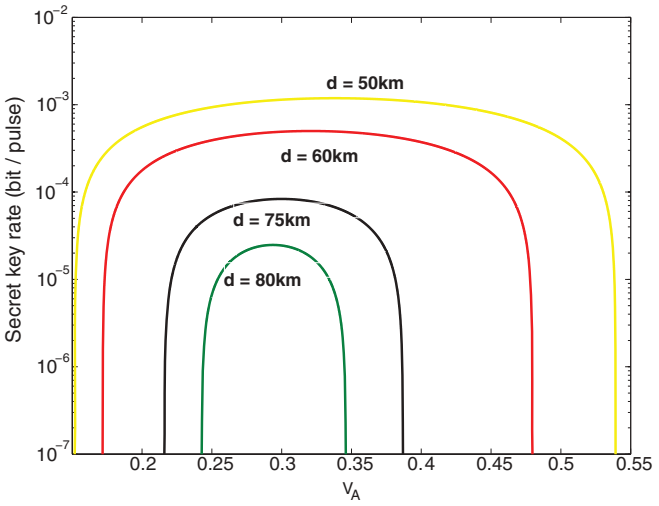

FIG. 3. (Color online) Heterodyne detection with a practical detector, $\epsilon = 0.01$, $g = 1$.

If we substitute χ_{hom}^{PSA} for χ_{hom} in Eq. (13), the modified secret key rate $\widetilde{K}_R$ with homodyne detection is obtained. Similarly, we can get the the modified secret key rate $\widetilde{K}_R$ with heterodyne detection as long as χ_{het} is replaced by χ_{het}^{PIA} in Eq. (14).

III. RESULTS AND DISCUSSION

In this section, we apply the results derived in Sec. II C2 to a practical system. In particular, we calculate the secret key rate as a function of the distance for fiber-optical implementation of the four-state protocol, for collective eavesdropping attacks in the configuration of heterodyne detection with a phase-insensitive amplifier placed at the output of the quantum channel. Similar results are obtained in the configuration of homodyne detection with a phase-sensitive amplifier.

The parameters included in the equations that will affect the value of $\widetilde{K}_R$ include the variance of Alice's modulation

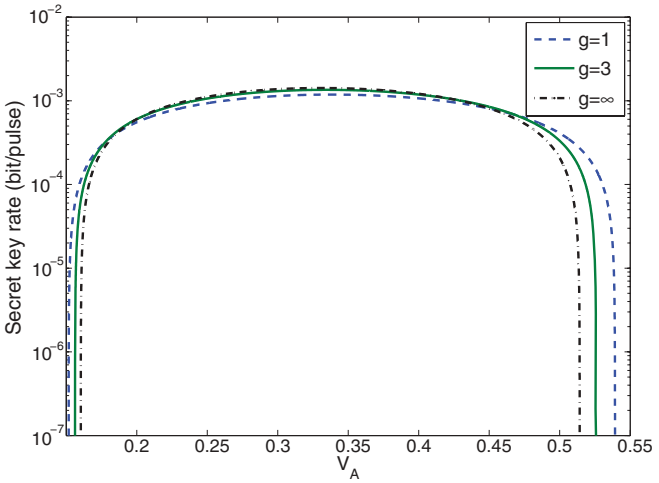

FIG. 4. (Color online) Heterodyne detection with a practical detector, $\epsilon = 0.01$, $d = 50$ km.

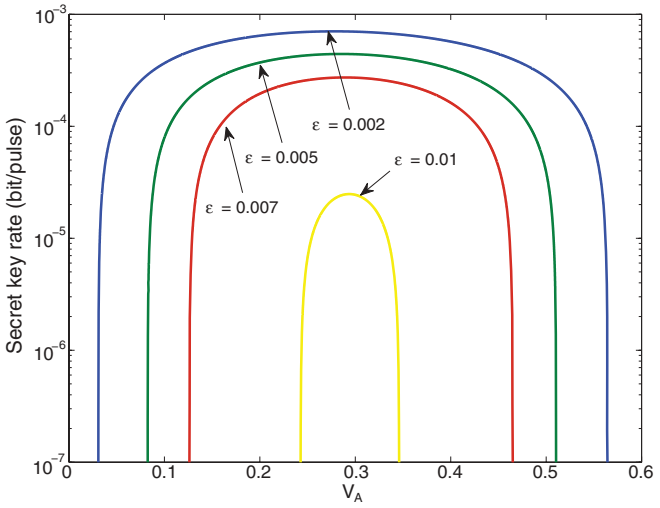

FIG. 5. (Color online) Heterodyne detection with a practical detector, $d = 80$ km, $g = 1$.

V_A; the transmission efficiency T and excess noise ϵ of the quantum channel; the efficiency η and electronic noise $v_{\rm el}$ of Bob's detector; the gain g and inherent noise N of the amplifier. The parameters η and $v_{\rm el}$ are fixed in all simulations to the values $\eta = 0.6$ and $v_{\rm el} = 0.05$ (in shot-noise units), which are standard in experiments. The gain of the amplifier g takes values 1, 3, and 20. (Note that when $g = 1$, $\chi_{\rm het}^{PIA} = \chi_{\rm het}$; thus the case $g = 1$ is equivalent to having no amplifier. It is better to make a comparison between results after the addition of the amplifier and the original setting.) We set the noise N of the phase-insensitive amplifier to the realistic value 1.5 (in shot-noise units, referred to the input). Furthermore, the channel transmission efficiency is $T = 10^{-ad/10}$, where $a = 0.2$ dB/km is the loss coefficient of the optical fibers, and d is the length of the channel.

In the remaining part of this section, numerical simulations are employed to reveal how the parameters V_A, ϵ, and g affect the secret key rate $\widetilde{K}_R$.

A. The optimal V_A

The variation of Alice's modulation V_A is an important parameter in the PM version of the protocol. In the general case, we need to scan V_A within a legitimate region to find an optimal V_A to maximize the secret key rate $\widetilde{K}_R$ for a specific scenario. However, we notice that the optimal V_A in the four-state protocol does not depend on the features of the quantum channel, i.e., T and ϵ, and the gain g of the amplifier. This is shown in Figs. 3, 4, and 5. There exists a global optimal V_A that makes $\widetilde{K}_R$ achieve the maximum value in different scenarios.

In Fig. 3, the parameters g and ϵ are fixed to legitimate values. When the distance d increases, the numerical areas of V_A that make $\widetilde{K}_R$ achieve maximum are gradually compressed. Fortunately, these optimal numerical areas of V_A have a public interval in which we can choose a public optimal V_A. In this case, we can let V_A equal 0.3.

In our modified protocol, optical amplifiers are used in the system to enhance the performance of the protocol. Use of different gains of the amplifiers has few effects on the optimal numerical areas of V_A. This is shown in Fig. 4, where we observe that in the limit of large amplification gain, the optimal numerical areas of V_A are compressed very little.

Excess noise ϵ of the quantum channel is possible in the environment of a practical experiment. So considering how the fluctuation of excess noise ϵ affects the optimal V_A would be very meaningful. From the results shown in Fig. 5, the optimal regions of V_A are compressed a lot when excess noise ϵ increases. However, the the optimal regions of V_A have a public symmetric point located at $V_A = 0.3$. So a public optimal V_A can be obtained as 0.3 regardless of the fluctuation of excess noise.

From the above analysis, we can obtain a global optimal value of V_A to maximize the secret key rate $\widetilde{K}_R$. This will help to simplify the experimental demonstrations. In the remaining part, we will treat V_A as a constant in our analysis.

B. Using amplifiers with caution

Now we consider the performance of the four-state protocol after using an optical amplifier inserted at the output of the

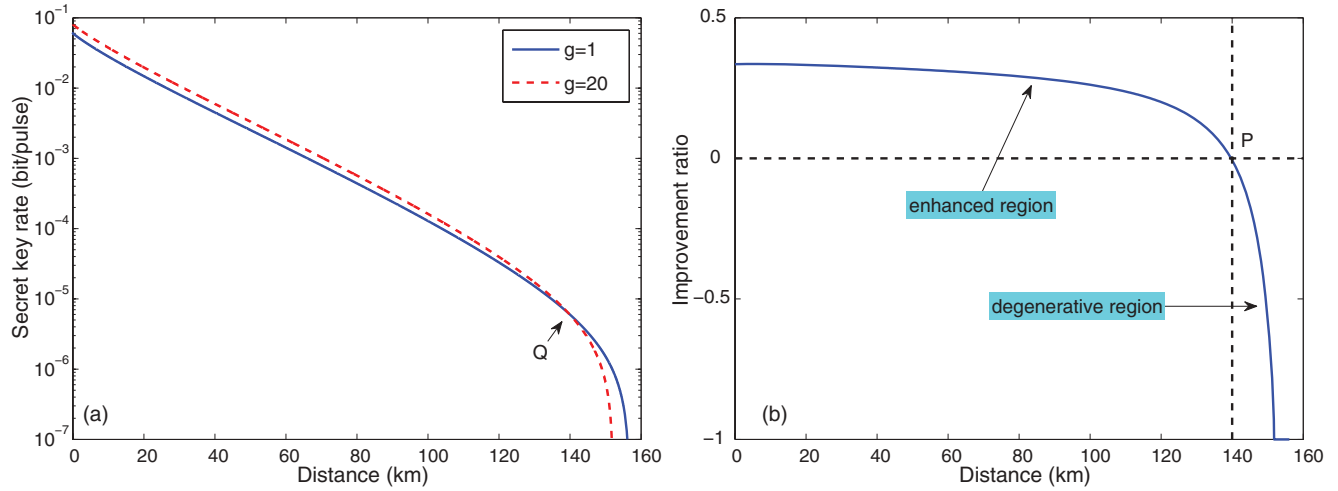

FIG. 6. (Color online) Heterodyne detection with an inserted PIA, $\epsilon = 0.005$, $V_A = 0.3$. (a) Secret key rate for $g = 1$ (full line), and $g = 20$ (dashed line). (b) Improvement ratio after inserting a PIA.

channel. Here we investigate the configuration of heterodyne detection with a phase-insensitive amplifier.

If the secret key rate $\widetilde{K}_R$ is too small, it will be meaningless for practical use. So here we consider only the scenarios in which $\widetilde{K}_R \gtrsim 10^{-7}$ bit/pulse. First, we calculate the secret key rate $\widetilde{K}_R$ as a function of distance d in the following scenario: $V_A = 0.3$, $\epsilon = 0.005$, and $g = 1,20$. The results are shown in Fig. 6. The curves in Fig. 6(a) are very close to each other; an equivalent curve is used to illustrate results in Fig. 6(b), where the improvement ratio is defined as

$$\text{Improvement ratio} = \frac{\widetilde{K}_R(d)|_{g=20} - \widetilde{K}_R(d)|_{g=1}}{\widetilde{K}_R(d)|_{g=1}}. \quad (20)$$

There are two points marked in the subgraphs. In Fig. 6(a), point **Q** is the intersection point of two curves, whose coordinates are written as (Q_x, Q_y). In Fig. 6(b), the point on the curve whose vertical coordinate equals 0 is denoted as point **P**, which is located at $(P_x,0)$. Here point **Q** and point **P** have the same meaning, and $Q_x = P_x$. We observe that the inserted optical amplifier may not work for the whole distance. There is an enhanced region and a degenerative region. If the length of the fiber d is smaller than P_x about 140 km, the usage of the amplifier does enhance the performance of the protocol in terms of secret key rates to some extent. However, if d goes beyond P_x, things take a sudden turn and become worse rapidly. So the position of the point **P** is very important. We want to enlarge the enhanced region and compress the degenerative region by controlling certain parameters.

Next we will investigate the movement of the point **Q** (**P**). The excess noise of the quantum channel ϵ and gain of the amplifier will affect the location of point **P**.

First, when ϵ is fixed to 0.005, the gain of the amplifier varies from a small value to infinity, but the variation of the abscissa of **P** is not obvious, which is shown Fig. 7. When $g = \infty$, P_x reaches its lowest value in this specific scenario. We define this value as the *critical distance*. When the gain of the amplifier is fixed, the fluctuation of the excess noise

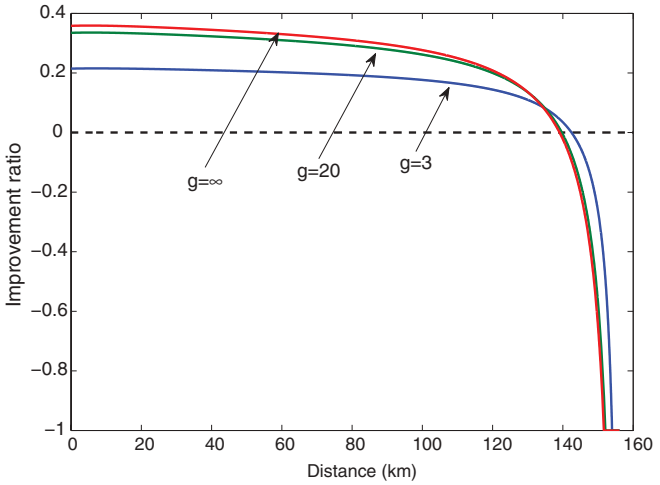

FIG. 7. (Color online) Heterodyne detection with an inserted PIA, $\epsilon = 0.005$, $V_A = 0.3$.

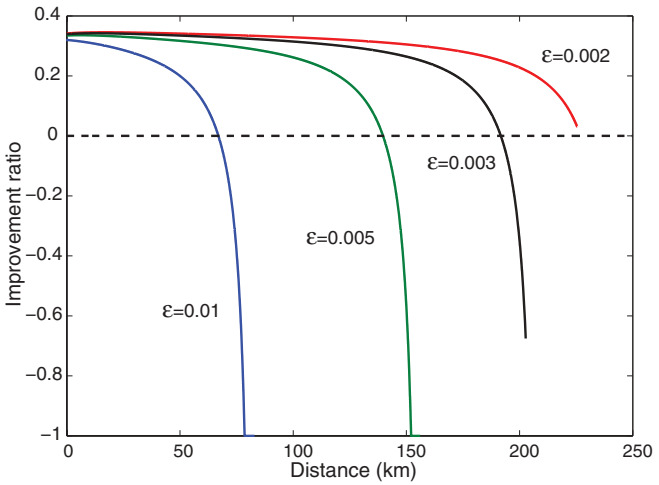

FIG. 8. (Color online) Heterodyne detection with an inserted PIA, $g = 20$, $V_A = 0.3$.

leads to a large change in the location of **P** (see Fig. 8). So it is important to find the relationship between excess noise and critical distance when g approaches infinity. From the simulation data, we fitted the curve, and obtained an analytical function:

$$y = Ae^{-x/t} + y_0, \quad (21)$$

where $A = 298.22$, $t = 0.005\,61$, and $y_0 = 16.76$. The raw data and fitted curve are shown in Fig. 9. We name this curve the *critical line*.

The region below the critical line is the enhanced region in which using an optical amplifier does improve the performance of the protocol in terms of secret key rates. And the larger gain of the amplification is, the larger is the improvement ratio. The region above the curve is the degenerative region. The

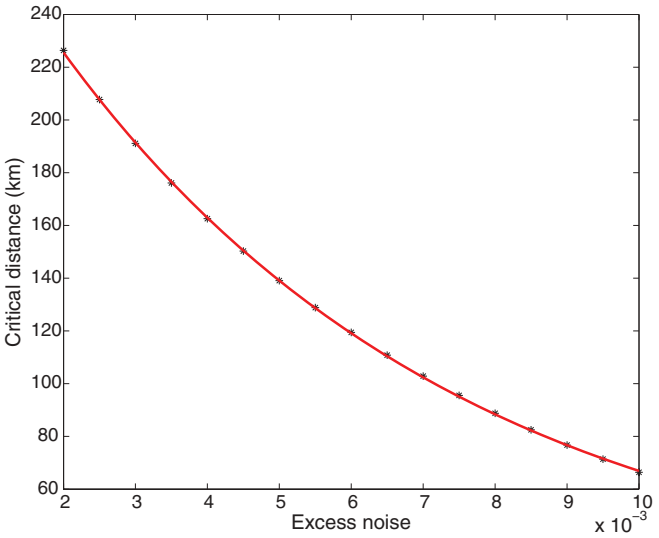

FIG. 9. (Color online) The critical distance as a function of excess noise ϵ, $g = \infty$, $V_A = 0.3$.

usage of an optical amplifier may lead to a worse performance compared with not using an amplifier.

IV. CONCLUSION

In this paper, we analyze the four-state protocol modified by optical preamplifiers inserted at the output of the quantum channel. We find that the modified protocol achieves higher secret key rates over long distances compared with the original protocol in specific scenarios. A critical line is given to separate enhanced and degenerative regions, which will be instructive and meaningful for experiments. In the enhanced region, the usage of amplifiers enhances the performance of the protocol to some extent. However, if working in the degenerative region, use of amplifiers leads to a negative effect, which should be avoided.

ACKNOWLEDGMENTS

We thank Peng Huang for helpful discussions. We also acknowledge support from the National Natural Science Foundation of China (Grants No. 61102053, No. 61170228, No. 60970109, and No. 60801051), the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry and SMC Excellent Young Faculty Award, SJTU 2011, and SJTU PRP (Grants No. T030PRP18001 and No. T030PRP19035).

[1] N. Gisin, G. Ribordy, W. Tittle, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[4] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[5] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[6] J. Lodewyck *et al*., Phys. Rev. A **76**, 042305 (2007).
[7] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
[8] M. Navascues and A. Acin, Phys. Rev.Lett. **94**, 020505 (2005).
[9] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[10] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, IEEE Trans. Inf. Theory **47**, 619 (2001).
[11] C. Berrou, A. Glavieux, and P. Thitimajshima, in *Proceedings of the IEEE International Conference on Communications*, Vol. 2 (IEEE, New York, 1993), pp. 1064–1070.
[12] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
[13] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
[14] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).
[15] M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).
[16] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[17] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).
[18] Z. Y. Ou, S. F. Pereira, and H. J. Kimble, Phys. Rev. Lett. **70**, 3239 (1993).