Performance Improvement of Two-way Quantum Key Distribution by Using a Heralded Noiseless Amplifier

Chenyang Li, Ruihang Miao, Xinbao Gong, Ying Guo & Guangqiang He

International Journal of Theoretical Physics

ISSN 0020-7748
Volume 55
Number 4

Int J Theor Phys (2016) 55:2199-2211
DOI 10.1007/s10773-015-2859-9

Volume 55 • Number 4 • April 2016

International Journal of Theoretical Physics

10773 · ISSN 0020-7748
55(4) 1937–2302 (2016)

Springer

Springer

Int J Theor Phys (2016) 55:2199–2211
DOI 10.1007/s10773-015-2859-9

Performance Improvement of Two-way Quantum Key Distribution by Using a Heralded Noiseless Amplifier

Chenyang Li[1] · Ruihang Miao[1] · Xinbao Gong[2] ·
Ying Guo[3] · Guangqiang He[1,4,5]

Received: 31 July 2015 / Accepted: 4 November 2015 / Published online: 18 November 2015

Abstract We show the successful use of a heralded noiseless linear amplifier on the detection stage in the two-way continuous-variable quantum key distribution to improve the performance. Due to the excess noise, the secret-key rate of the two-way protocol becomes negative for a certain distance of transmission. The use of a heralded noiseless linear amplifier increases this distance by the equivalent of $20\log_{10}\mathbf{g}$ dB of losses, and it also helps the two-way protocol tolerate more excess noise.

✉ Guangqiang He
gqhe@sjtu.edu.cn

Chenyang Li
5110809041@sjtu.edu.cn

Ruihang Miao
mrhcat@sjtu.edu.cn

Xinbao Gong
xbgong@sjtu.edu.cn

Ying Guo
yingguo@csu.edu.cn

[1] State Key Lab of Advanced Optical Communication Systems and Networks Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai, China

[2] Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai, China

[3] School of Information Science and Engineering, Central South University, Changsha, China

[4] State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai, China

[5] Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou, China

Keywords Continuous variable quantum key distribution · Noiseless amplifier · Two-way protocol

1 Introduction

Quantum key distribution (QKD) [1–5] allows the two legitimate partners to establish a secret key through an untrusted environment controlled by an eavesdropper. In recent years, continuous-variable quantum key distribution (CVQKD) has been promoted as an alternative to discrete-variable quantum key distribution, because CVQKD use the homodyne detection technique, which is widely used in classical optical communication, rather than dedicated photon-counting technology [6–8]. Generally speaking, CVQKD is usually demonstrated as the one-way protocol, which means the quantum states are transmitted through a noisy channel only once, but it is often limited to several tens of kilometers [9]. A recent experimental demonstration of the one-way protocol succeeds over 80 km of optical fiber [10].

In contrast to the one-way protocol, an idea of the two-way protocol is put forward to keep the high secure key rate and defend the attack by the eavesdropper [11, 12]. In the two-way protocol, the two partners, Alice and Bob, have two configurations in the protocol. The switching between the two configurations is used as a virtual principle against Eve, which is proved to effectively defend the collective entangling-cloner attack.

In this paper, we propose to use a heralded noiseless linear amplifier (NLA) [13–24] before the homodyne detection to improve the performance of the two-way protocol against losses and noise. Compared to other optical amplifier, a probabilistic NLA can amplify the amplitude of a coherent state while obtaining the original level of noise [13], and the correct operation is heralded, since only data from successful amplified states can be used to error correction to get the information. It has been demonstrated that the NLA can be applied in the one-way protocol to improve the maximum transmission distance [22]. It is useful for quantum communication by compensating the effect of losses [23]. Recent research has realized a heralded noiseless amplification of a photon polarization qubit [24].

The question arises if the NLA can be applied to the two-way protocol to improve the performance. Here we address this problem, by obtaining the equivalent parameters of the two-way protocol with the NLA and then transferring the circumstance into that without the NLA to compute the secret-key rate. We find the NLA can help the two-way protocol improve the maximum transmission distance and tolerate more excess noise. The security proofs about inserting the NLA before homodyne detector are similar to those concerning protocols with postselection.

This paper is organized as follows. In Section 2, we demonstrate the two-way protocol, and then make comparison with the one-way protocol, which reveals the reason why the two-way protocol can contribute to prefect the traditional one-way protocol. In Section 3, we calculate the equivalent parameters with the use of the NLA in the two-way protocol, based on the main communicational channel of the two-way protocol. In Section 4, we compare the secret key rate with the NLA and without the NLA in the two-way protocol, then we see the improvement of maximum transmission distance and endurable excess noise with the use of the NLA, where we can also see the better performance of the two-way protocol than the one-way protocol. The conclusion is drawn in Section 5.

2 Two-way QKD Protocol

2.1 Two-way QKD Protocol

The two-way protocol has been proposed to make some improvements to the traditional one-way protocol. As depicted in Fig. 1, Bob has an output quadrature $\hat{B}_1 = \hat{0}+b_1$, where a pure vacuum state with variance $V_0 = 1$ is modulated by Gaussian variable b_1 with variance $V_{b_1} := \mu$. Then through the insecure channel of the first quantum communication, mode B_1 is sent to Alice. After receiving the noisy mode A_1, Alice randomly switches between two configurations [12]:

(i) the ON configuration: Alice encodes a Gaussian variable a with variance $V_a = \mu$, and then sent the output mode A_2 with the quadrature $\hat{A}_2 = \hat{A}_1 + a$;
(ii) the OFF configuration: Alice homodynes the incoming mode A_1 with classical output a_1. After the detection, Alice sends another thermal state $\hat{A}_2 = \hat{0} + a_2$, with the same signal variances as Bob, i.e.$V_0 = 1$ and $V_{a_2} = \mu$.

In both cases, Bob receives the mode B_2 ,which is the output of the incoming mode A_2 back through the second noisy channel in the same circumstance of the first channel. At the end of the double quantum communication, Alice and Bob use the public channel to communicate which configuration, ON or OFF, was chosen in the protocol. For the OFF configuration, Bob directly homodynes the incoming mode B_2, resulting in the classical output $b_2 \approx a_2$ and $a_1 \approx b_1$, which is typical of the one-way QKD system. For the ON configuration, Bob performs the generic quadrature $\hat{B} = \hat{B}_2 - Tb_1$, and then homodynes the mode B with the output $b \approx a$.

Usually, the switching between the ON and OFF configuration is used as a virtual basis against Eve. If Eve performs the two-mode coherent attack, Alice and Bob use the OFF configuration to defend the attack,then obtaining a secret key from $b_2 \approx a_2$ and $a_1 \approx b_1$. On the contrary, if Eve performs the one-mode coherent attack, the ON configuration is

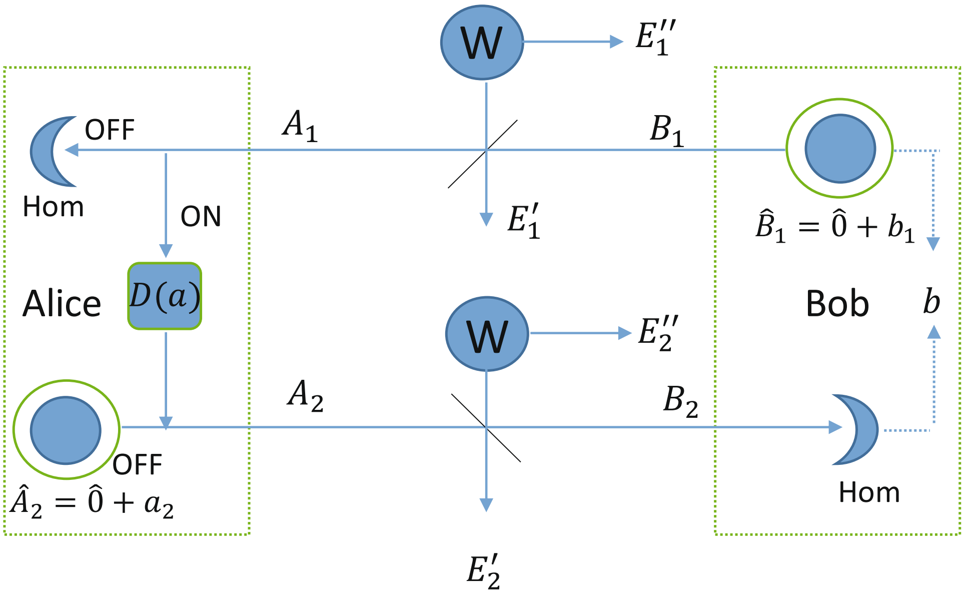

Fig. 1 Two-way QKD protocol. Eve uses the two Einstein-Podolsky-Rosen states to preform the collective entangling-cloner attack

undoubtedly an effective way to defend the attack to extract a secret key from $b_2 \approx a_2$. After obtaining a small subset of these variables, Alice and Bob can decide which configuration is useful to defend the attack, and then use the classical error correction and privacy amplification for their data to extract a secret key in direct or reverse reconciliation. In fact, the use of two-mode coherent attacks against the two-way protocol is also not advantageous for Eve. As discussed in Ref.[11], just using the ON configuration, Alice and Bob can reach security thresholds which are much higher than those of the one-way protocols.

Then let us describe the two-way protocol more precisely. As shown in Fig. 1, a collective entangling-cloner attack of an Einstein-Podolsky-Rosen(EPR) state with variance W against the two-way protocol consists of Eve performing two independent and identical beam-splitter attacks (transmission T), which is known as two-mode coherent attacks. So, the output mode quadrature A_1 can be expressed as:

$$\hat{A}_1 = \sqrt{T}\hat{B}_1 + \sqrt{1-T}\hat{E}_1. \tag{1}$$

After modulation of Alice, we get

$$\hat{A}_2 = \sqrt{T}\hat{B}_1 + \sqrt{1-T}\hat{E}_1 + a. \tag{2}$$

Then through the attack channel, the output mode B_2 can be expressed as:

$$\hat{B}_2 = T\hat{B}_1 + \sqrt{T}a + \sqrt{1-T}(\sqrt{T}\hat{E}_1 + \hat{E}_2). \tag{3}$$

Subtracting off the input modulation b_1 (known to only Bob), we get the processed quadrature $\hat{B} = \hat{B}_2 - Tb_1$ equal to

$$\hat{B} = T\hat{0} + \sqrt{T}a + \sqrt{1-T}(\sqrt{T}\hat{E}_1 + \hat{E}_1). \tag{4}$$

After changing the shape of the (4), we can get

$$\hat{B} = \sqrt{T}(\sqrt{T}\hat{0} + \sqrt{1-T}\hat{E}_1 + a) + \sqrt{1-T}\hat{E}_2, \tag{5}$$

with variance

$$V_B = T(TV_0 + (1-T)W + V_a) + (1-T)W = T(V_0 + (1-T)(W-V_0) + V_a) + (1-T)W. \tag{6}$$

For an actual channel, the excess noise ϵ can be expressed as

$$(1-T)W = 1 - T + T\epsilon, \tag{7}$$

and the V_0 represents the vacuum noise 1. Thus, we can get

$$V_B = T(1 + T\epsilon + V_a) + 1 - T + T\epsilon, \tag{8}$$

From the (8), we can see it is very similar to the output of the one-way protocol

$$V_{out} = T(1 + V_a) + 1 - T + T\epsilon, \tag{9}$$

and further consider that the two-way protocol is an improvement of the one-way protocol with a real modulate variance :

$$V_{real} = T\epsilon + V_a = (1-T)(W-1) + V_a. \tag{10}$$

Then the (8) can be transformed into

$$V_B = T(1 + V_{real}) + 1 - T + T\epsilon. \tag{11}$$

Although it makes sacrifice to the percentage of useful modulation variance, yet with the quadrature $\hat{B} = \hat{B}_2 - Tb_1$, in which b_1 is only known to Bob and then effectively defend the attacks by Eve, it also largely increases the secret-key rate and decreases the information of eavesdropping. The detailed calculation of the secret-key rate of the two-way protocol will be derived in the next part.

Thus, we can keep in mind that the two-way protocol is an improvement of the one-way protocol by using the secret knowledge about the states, and this is why $a \approx b$ in the ON configuration. Then all the measures to increase the quality of the one-way protocol, such as adding phase-insensitive amplifier, phase-sensitive amplifier or noiseless linear amplifier on the Bob's detection stage [8, 22], can be applied to improve the two-way protocol. First, it should be noted that while amplifiers can effectively recover classical signals, they only offer limited advantages when working on quantum signals, as amplification is bound to preserve the original signal to noise ratio (SNR) . This implies that ordinary linear amplifiers, such as phase insensitive amplifier and phase sensitive amplifier, can only find limited applications in the context of QKD. On the other hand, a probabilistic NLA can in principle amplify the amplitude of a coherent state while retaining the initial level of noise. Therefore, when only considering its successful runs, the NLA can compensate the effect of losses and therefore have better performance for quantum communication.

2.2 Secret-key Rate in Reverse Reconciliation

Here we study the security performance of the two-way protocol against collective entangling-cloner attacks of an EPR state with variance W. As discussed in Ref.[11], the reverse reconciliation(RR) is proved to have the best performance in the two-way protocol. Adopting the ON configuration, we derive the analytical expressions of the asymptotic secret-key rates on the condition of high modulation ($\mu \to +\infty$) to simplify computation.

In the collective attack, the secret key rate for RR is given by $R := I(a : b) - I(E : b)$ using the Holevo bound [25]. The mutual information between Alice and Bob is derived from the differential Shannon entropy [26] and is simply given by

$$I(a : b) = \frac{1}{2}\log_2 \frac{V_b}{V_{b|a}}, \tag{12}$$

where V_b is the variance of Bob's post-processed variable b, and $V_{b|a}$ its variance conditioned to Alice's encoding variable a. From the (6), where $V_B = V_b$ and we set $V_a = u$, we can know:

$$V_b = T^2 V_0 + T\mu + (1 - T^2)W, \tag{13}$$

which gives $V_b \to T\mu$ in the limit of high modulation. With the same limit and setting $\mu = 0$, the conditional variance $V_{b|a}$ is given by

$$V_{b|a} = T^2 V_0 + (1 - T^2)W, \tag{14}$$

Thus, the mutual information between Alice and Bob is given by

$$\begin{aligned} I(a : b) &= \tfrac{1}{2}\log_2 \tfrac{T^2 V_0 + T\mu + (1-T^2)W}{T^2 V_0 + (1-T^2)W} \\ &\to \tfrac{1}{2}\log_2 \tfrac{T\mu}{T^2 V_0 + (1-T^2)W}. \end{aligned} \tag{15}$$

Then we need to compute the Eve's Holevo information on Bob's processed variable:

$$I(E : b) = S(E) - S(E|b), \tag{16}$$

where $S(E)$is the von Neumann entopy of Eve's multimode output state ρ_E (modes $E_1' E_1'' E_2' E_2''$) and $S(E|b)$ is the entropy of the output state $\rho_{E|b}$ conditioned to the Bob's variable b. Because these states are Gaussian, their entropies can be computed from the symplectic spectra of their covariance matrices, $\mathbf{V}_E$ and $\mathbf{V}_{E|b}$, respectively [1].

After computation, we get the following expression of the Eve's covariance matrixes for the Gaussian state ρ_E of modes $E_1'E_1''E_2'E_2''$

$$\mathbf{V}_E = \begin{pmatrix} \varepsilon\mathbf{I} & \varphi\mathbf{Z} & \chi\mathbf{I} & \mathbf{0} \\ \varphi\mathbf{Z} & W\mathbf{I} & \theta\mathbf{Z} & \mathbf{0} \\ \chi\mathbf{I} & \theta\mathbf{Z} & \triangle(V_a, V_a) & \varphi\mathbf{Z} \\ \mathbf{0} & \mathbf{0} & \varphi\mathbf{Z} & W\mathbf{I} \end{pmatrix}, \tag{17}$$

where $\mathbf{0}$:=diag(0, 0), $\mathbf{I}$:=diag(1, 1), $\mathbf{Z}$:=diag(1, −1) and the parameters are defined as

$$\varepsilon := (1-T)V_{B_1} + TW, \tag{18}$$

$$\chi = -\sqrt{T}(1-T)(W - V_{B_1}), \tag{19}$$

$$\theta = -(1-T)(W^2-1), \tag{20}$$

$$\gamma = T(1-T)V_{B_1} + (1-T+T^2)W, \tag{21}$$

$$\varphi = \sqrt{T(W^2-1)}, \tag{22}$$

$$\triangle(V_a, V_a) = \gamma\mathbf{I} + (1-T)\text{diag}(V_a, V_a). \tag{23}$$

As for parameters, we set $V_{B_1} = V_0 + \mu$ and $V_a = \mu$, and we use the limit of high modulation($\mu \to \infty$) to simplify our computation. Therefore, we can calculate the asymptotic symplectic spectrum of the covariance matrices, and obtain the four eigenvalues $\nu_1 \to W$, $\nu_2 \to W$ and ν_3, ν_4 with the relationship $\nu_3\nu_4 \to (1-T)^2\mu^2$. Using these eigenvalues, we are able to compute the entropy of Eve's state ρ_E which is given by [27]:

$$S(E) = \sum_{k=1}^{4} h(\nu_k) \to 2h(W) + \log_2((\frac{e}{2})^2(1-T)^2\mu^2), \tag{24}$$

where

$$h(x) := \frac{x+1}{2}\log_2(\frac{x+1}{2}) - \frac{x-1}{2}\log_2(\frac{x-1}{2}), \tag{25}$$

and its asymptotic expansion $h(x) \simeq \log(\frac{ex}{2})$ for large x.

Now we consider to compute covariance matrices $\mathbf{V}_{E|b}$. First, we start to derive the global covariance matrices

$$\mathbf{V}_{EB} = \begin{pmatrix} \mathbf{V}_E & \mathbf{D} \\ \mathbf{D}^T & V_b\mathbf{I} \end{pmatrix},$$

where covariance matrices $\mathbf{V}_E$ given in (17) describe Eve's modes $E_1'E_1''E_2'E_2''$, and the covariance matrices $V_b\mathbf{I}$ computed in (13) represent Bob's virtual mode B. After applying the homodyne detection on mode B, we get the conditional covariance matrices $\mathbf{V}_{E|b} = \mathbf{V}_E - (1/V_b)\mathbf{D}\Pi\mathbf{D}^T$, where Π := diag(1, 0, 0, 0). Here the block $\mathbf{D}$ describes the correlations between Eve's and Bob's modes, and is given by

$$\mathbf{D}^T = (\xi_1\mathbf{I}.\phi_1\mathbf{Z}, \xi_2\mathbf{I}, \phi_2\mathbf{Z}), \tag{26}$$

where

$$\xi_1 = -T\sqrt{1-T}(V_0 - W), \tag{27}$$

$$\phi_1 = \sqrt{T(1-T)(W^2-1)}, \tag{28}$$

$$\xi_2 = -\sqrt{T(1-T)}(TV_0 + V_a) + TW\sqrt{T(1-T)}, \tag{29}$$

$$\phi_2 = \sqrt{(1-T)(W^2-1)}. \tag{30}$$

With the same parameters and limits, we can derive asymptotic expression of the conditional symplectic spectrum $\tilde{\nu}_1, \tilde{\nu}_2, \tilde{\nu}_3, \tilde{\nu}_4$, which is given by $\tilde{\nu}_1 \rightarrow W$,

$$\tilde{\nu}_2 \rightarrow \sqrt{\frac{W(1+T^2V_0W+T^3(1-V_0W))}{T^2V_0+W+T^3(W-V_0)}}, \tag{31}$$

$$\tilde{\nu}_3\tilde{\nu}_4 \rightarrow \sqrt{\frac{(1-T)^3(T^2V_0+W+T^3(W-V_0))\mu^3}{T}}. \tag{32}$$

Using these eigenvalues ,we are able to compute the conditional entropy $S(E|b)$. Thus, after we calculate $I(E:b) = S(E) - S(E|b)$ and $R = I(a:b) - I(E:b)$, the RR secret-key rate with asymptotic expression is given by

$$\begin{aligned} R(T, W) = &\tfrac{1}{2}\log_2\left(\tfrac{T^2V_0+W+T^3(W-V_0)}{(V_0T^2+(1-T^2)W)(1-T)}\right) \\ &+h(\tilde{\nu}_2) - h(W), \end{aligned} \tag{33}$$

where $V_0 = 1$ represents the vacuum noise.

3 Equivalent Channel with the NLA in Two-way Protocol

From the last section, we clearly see the two-way protocol is an improvement of the one-way protocol. Then let us consider the use of the NLA before Bob's homodyne detection in the two-way protocol of Fig. 2. Here we also build the system in the Gaussian quantum channel, in which Eve performs Gaussian attacks. In this modified version of the protocol, Alice and Bob implement the two-way protocol, but Bob adds a NLA to his stage before his homodyne detection, which is here assumed to be perfect. Then, only the events corresponding to a successful amplification will be used to extract a secret key. This scheme is therefore very similar to protocols with postselection. Besides, Alice adds a NLA before his homodyne detection in the one-way protocol to keep the symmetry.

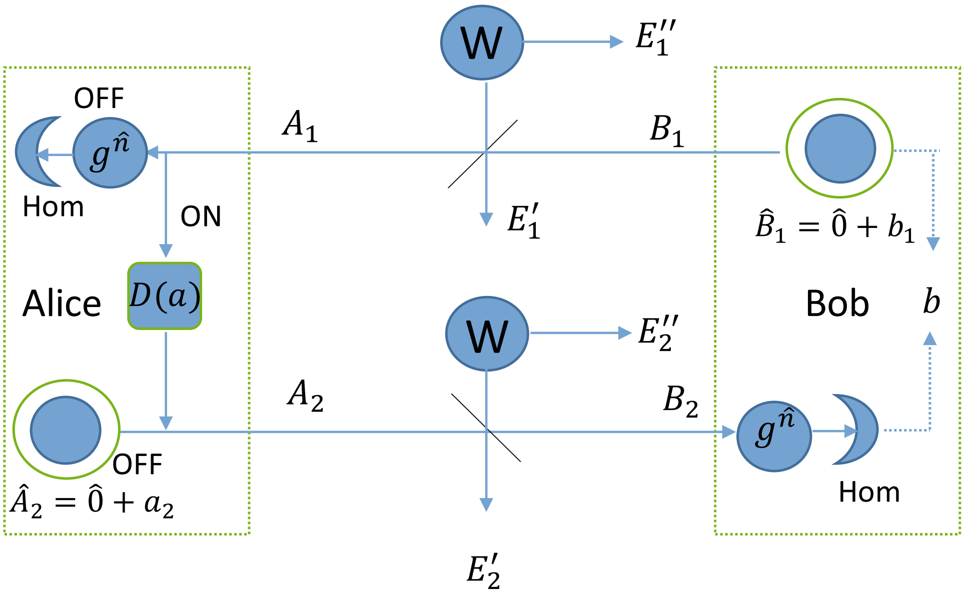

Fig. 2 Two-way QKD protocol with the NLA. Eve also use the two EPR states to preform the collective entangling-cloner attack

Since the two-way protocol is very similar to the one-way and the output of the NLA remains in the Gaussian regime, we can find equivalent parameters η, ζ and N of a thermal state sent through the double Gaussian noisy channel to help us keep the same Gaussian average value and variance, and then compute the secret key. Because the processed quadrature $\hat{B} = \hat{B}_2 - Tb_1$ is used to counterpart the Gaussian variable b_1 encoded by Bob, we can calculate the equivalent parameters without the function of both the Gaussian variable b_1 and the processed quadrature, which has no effect on the output of the NLA and helps us to simplify the computation.

First, the input state $\hat{\rho}$ before Bob's homodyne without the NLA is $\hat{\rho}_{th}(\lambda_{ch}) = (1 - \lambda_{ch}^2)\sum_{(n=0)}^{\infty} \lambda_{ch}^{2n}|n><n|$ displaced by $\beta = \beta_x + i\beta_y$, so it becomes

$$\hat{\rho} = \hat{D}(\beta)\hat{\rho}_{th}(\lambda_{ch})\hat{D}(-\beta). \tag{34}$$

As discussed in [22], when it passes through the NLA, the state is transformed to:

$$\hat{\rho}' \propto \hat{D}(\tilde{g}\beta)\hat{\rho}_{th}(g\lambda_{ch})\hat{D}(-\tilde{g}\beta), \tag{35}$$

where $\tilde{g} = g\frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}$ In order to keep a physical interpretation,we note that value of g must satisfy that $g\lambda_{ch} < 1$.

After Alice's encoding the Gaussian variable a, the amplitude of modulated thermal state is proportional to λ with variance $V = 1 + V_{real}$. This state is then sent through the quantum channel of transmittance T, which transforms its amplitude to $\propto \sqrt{T}\lambda$. The displacement β can thus be taken as

$$\beta = \sqrt{T}\lambda, \tag{36}$$

Then from the (11), we clearly see the incoming state before the homodyne detector with the variance $TV + (1 - T)W$. Then the variance $\frac{1+\lambda_{ch}^2}{1-\lambda_{ch}^2}$ of the thermal state corresponds to Bob's variance $T + (1 - T)W$ when $V_{real} = 0$, and then we get the expression

$$\begin{aligned} &\tfrac{1+\lambda_{ch}^2}{1-\lambda_{ch}^2} = T + (1-T)W \\ &\Rightarrow \lambda_{ch}^2 = \tfrac{T+(1-T)W-1}{T+(1-T)W+1}. \end{aligned} \tag{37}$$

Next, the action of the NLA on a displaced thermal state given by (35) produces the transformations:

$$\begin{aligned} &\sqrt{T}\lambda\alpha_A \xrightarrow{NLA} g\tfrac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}\sqrt{T}\lambda\alpha_A \\ &\tfrac{T+(1-T)W-1}{T+(1-T)W+1} \xrightarrow{NLA} g^2\tfrac{T+(1-T)W-1}{T+(1-T)W+1}. \end{aligned} \tag{38}$$

The next step is to consider the action of the NLA when Bob does not have any knowledge on the incoming states. In such a case, his state is a thermal state $\hat{\rho}_B = (1 - \lambda^{*2})\sum_{n=0}^{\infty}(\lambda^*)^{2n}|n><n|$

$$\begin{aligned} &\tfrac{1+\lambda^{*2}}{1-\lambda^{*2}} = TV + (1-T)W \\ &\Rightarrow \lambda^{*2} = \frac{T\frac{1+\lambda^2}{1-\lambda^2}+(1-T)W-1}{T\frac{1+\lambda^2}{1-\lambda^2}+(1-T)W+1}, \end{aligned} \tag{39}$$

$$\frac{T\frac{1+\lambda^2}{1-\lambda^2} + (1-T)W - 1}{T\frac{1+\lambda^2}{1-\lambda^2} + (1-T)W + 1} \xrightarrow{NLA} g^2\frac{T\frac{1+\lambda^2}{1-\lambda^2} + (1-T)W - 1}{T\frac{1+\lambda^2}{1-\lambda^2} + (1-T)W + 1}. \tag{40}$$

Now, there are all the equations required to find the expression of the effective parameter η, ζ and N. Using (38,40), those parameters can be solved as

$$\sqrt{\eta}\zeta = g\frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}\sqrt{T}\lambda, \tag{41}$$

$$\frac{\eta+(1-\eta)N-1}{\eta+(1-\eta)N+1} = g^2\frac{T+(1-T)W-1}{T+(1-T)W+1}, \tag{42}$$

$$\frac{\eta\frac{1+\zeta^2}{1-\zeta^2}+(1-\eta)N-1}{\eta\frac{1+\zeta^2}{1-\zeta^2}+(1-\eta)N+1} = g^2\frac{T\frac{1+\lambda^2}{1-\lambda^2}+(1-T)W-1}{T\frac{1+\lambda^2}{1-\lambda^2}+(1-T)W+1}. \tag{43}$$

The solution can be expressed as below

$$\zeta = \lambda\sqrt{\frac{TWg^2+Tg^2-Wg^2-TW+g^2-T+W+1}{TWg^2-Tg^2-Wg^2-TW+g^2+T+W+1}}, \tag{44}$$

$$\eta = \frac{4Tg^2}{(\nabla+(T+1)g^2+1-T)(\nabla+(1-T)g^2+T+1)}, \tag{45}$$

where $\nabla = ((T-1)g^2+1-T)W$,

$$N = \frac{((1-T)g^4+T-1)W^2-(2g^4+2)W+(T+1)g^4-T-1}{(g^2-1)^2(T-1)W^2+(2g^4-2)W-(1+T)g^4+(2T-2)g^2-T-1} \tag{46}$$

.

Then, we must pay attention to the equivalent parameters $0 \le \zeta < 1, 0 \le \eta \le 1$, and $N \ge 1$, so we can get:

$$0 \le \lambda < \left(\sqrt{\frac{TWg^2+Tg^2-Wg^2-TW+g^2-T+W+1}{TWg^2-Tg^2-Wg^2-TW+g^2+T+W+1}}\right)^{-1}, \tag{47}$$

$$g_{max}(T,W) = \sqrt{\frac{-2T\sqrt{\frac{(W^2-1)(T-1)^2}{T}}+4T\sqrt{\frac{(W+1)T}{W-1}}+((W+1)T-W+1)(W+1)(T-1)}{((W+1)T-W+1)^2}}. \tag{48}$$

Then we consider important comments about those equivalent parameters, which confirms the validity of their expression.

First of all, we degenerate to the real physical parameters without the NLA, for $g = 1$,

$$\begin{gathered} g = 1 \Rightarrow \\ \zeta = \lambda,\ \eta = T, N = W. \end{gathered} \tag{49}$$

Next, when there is no excess noise($W = 1$), they match previous result[13]:

$$\begin{gathered} W = 1 \Rightarrow \\ \zeta = \lambda\sqrt{1+(g^2-1)T},\ \eta = \frac{g^2T}{1+(g^2-1)T}, N = 1. \end{gathered} \tag{50}$$

After validity of the expression, we should pay attention to the equivalent parameters of the first channel. From (44,45), we can clearly see the equivalent transmittance η and variance of the attack N. However, we must keep in mind that the equivalent parameters just focus on the second back channel of information communication, because the actual function of the first channel is to prepare a vacuum state with additional modulated variance together with V_a to become V_{real}. Since the modified V_{real} is changed into the much larger value $V'_{real} = \frac{1+\zeta^2}{1-\zeta^2} - 1$, it doesn't matter for us to replace the first channel transmittance T with the equivalent parameter η, the Eve's attack W with the equivalent parameter N, which helps us to build the same channel of the two-way direction. Then, the equivalent V_a' can be expressed as:

$$V_a' = V_{real}' - (1-\eta)(N-1). \tag{51}$$

Through difficult calculation, we can clearly see the equivalent V_a' is closer to infinity compared to the original V_a, which makes the secret key rate calculation in the Section 2 closer to the real situation. Then using the equivalent parameters, we can extract the secret-key rate with the NLA in the two-way protocol from the (33).

4 Increase of the Maximum Transmission Distance

In the Section 2, we get the secret-key rate in the two-way QKD protocol. In the Section 3, we extract the equivalent parameters with the NLA before the Bob's homodyne detector. Then the analysis of the equivalent state allows us to get the secret key rate from the channel without the NLA. Then, we must pay attention to the successful amplification of the NLA with the probability of P_{ss}. Since we only care about the maximum distance and endurable excess noise which just depends on the positivity of the secret key rate, we can assume P_{ss} is a positive constant with the upper limitation of $1/g^2$ [22], which keeps the same positivity with the secret-key rate and does not have an effect on the results. Recent study shows its success in the one-way protocol in practice [28]. Although the NLA faithfully amplify low-energy input states and we use the large modulation for simplifying computation, it doesn't have the conflict in practice, since we can use the same modulated thermal states both in the one-way and two-way protocol and it cannot be modulation infinity. Then, we give the further discussion for the modified two-way protocol. The secret-key rate I_{NLA} is given by

$$I_{NLA} = P_{ss} I(\eta, N) = P_{ss} I'(T, W), \tag{52}$$

where $I'(T, W)$ represents the final secret-key rate with the parameter T and W. Next, we want to calculate the secret-key rate for an actual channel with transmittance T and excess noise ϵ, and we can demonstrate the relationship:

$$(1-T)W = 1 - T + T\epsilon. \tag{53}$$

Then we calculate the secret-key rate with the use of the NLA in the parameters of T and ϵ.

First, we find that the maximum of noiseless amplifier g_{max} depends on the value of the T and ϵ from the (48,53). In Fig. 3, we give the relationship between the g_{max} and the losses in dB, on the condition of $\epsilon = 0.1$. Due to the limitation of the g_{max}, we can't use a fixed noiseless amplifier to every value of T. For example, when $T = 1$, $g_{max} = 1$, which means we can't use the noiseless amplifier in the no-loss channel. But for the strong loss channel, the g_{max} becomes so large, then we can give a constant parameter g of the NLA to help improve the performance of the two-way protocol.

Because of excess noise, the secret key rate drops to zero for a certain distance. From the previous results [22], we know in the one-way QKD protocol, the use of the NLA can help to increase the maximum transmission distance. The equivalent losses for which the secret key rate is zero are increased by

$$\Delta\Sigma = 20\log_{10} \mathbf{g}\,\text{dB}. \tag{54}$$

Then after we use the equivalent parameters to compute the (33), we find the same increase of the permitted loss in the two-way, since the two-way protocol is an improvement of the one-way protocol. In Fig. 4, we compute the secret-key in two-way protocol without the NLA and with a NLA of $g = 2$. Then we can clearly see that the secret key rate remains

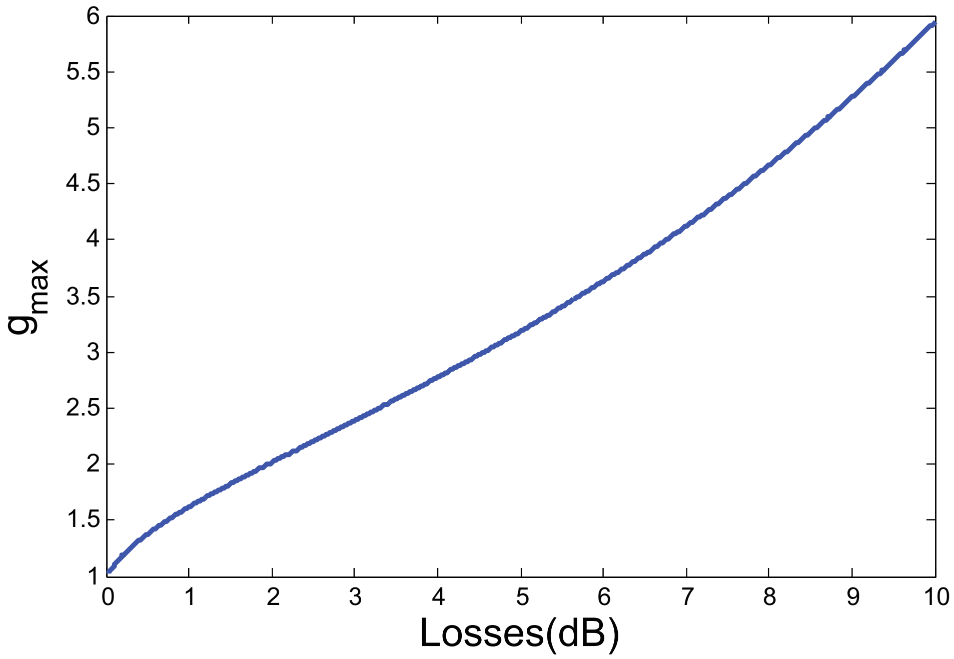

Fig. 3 Maximum value of the gain g_{max} as a function of the losses. we can clearly see g_{max} rises with the increase of the loss. In the curve, the excess noise $\epsilon = 0.1$

positive for losses increased by $\Delta\Sigma = 6$ dB. We also compute the circumstance with $g = 3$ and $g = 4$, where the increase on the permitted loss also satisfies the formula.

Another important quality for the two-way protocol with the NLA is to tolerate more excess noise. Because the probability of success chosen for the NLA don't change the positivity of the secret key rate, we can deduce the maximal tolerable excess noise for different

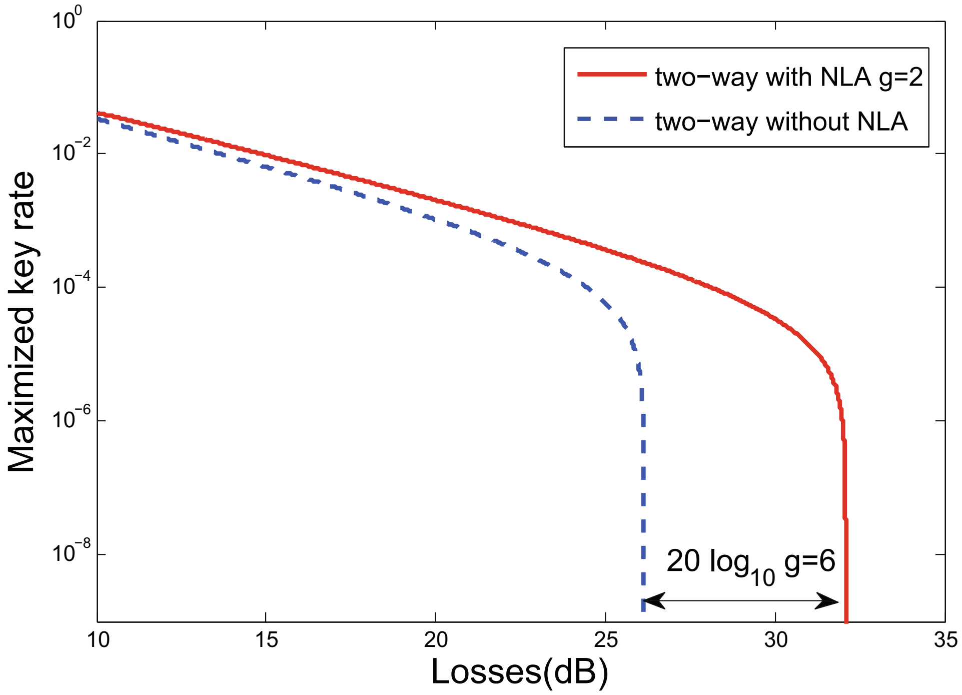

Fig. 4 Maximized secret key rate as a function of the losses in dB. Due to the probability of success, we can just keep the information on its positivity. we can clearly find the extended losses of the two-way protocol with the use of the NLA in the figure. The excess noise $\epsilon = 0.1$

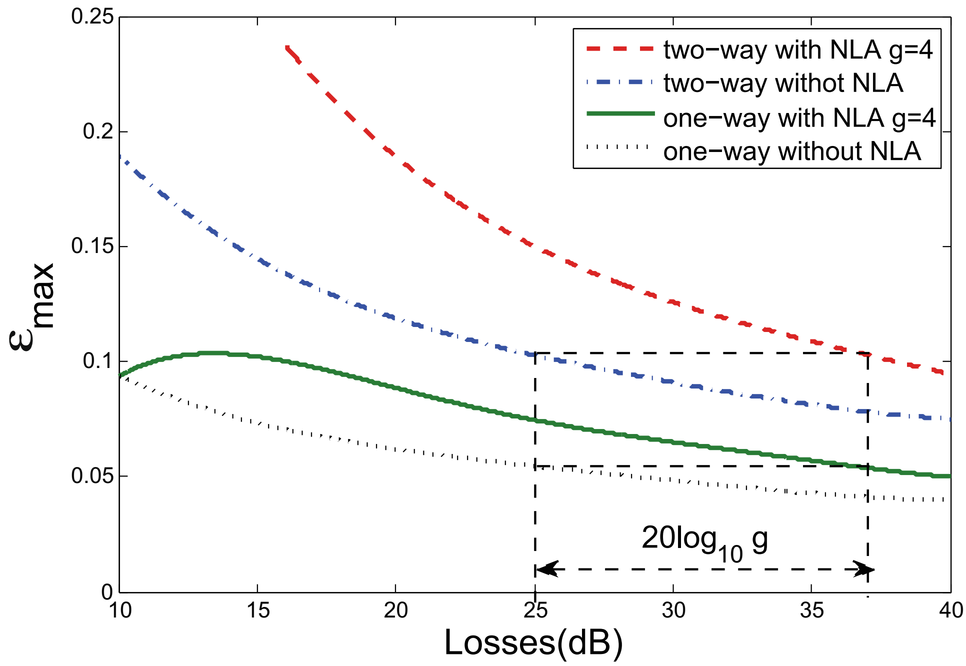

Fig. 5 Maximal excess noise as a function of the losses in dB. Because the maximal excess noise just depend on the the positivity of the secret key rate, it isn't related to specific probability of success of the NLA. From the figure we see that, the two-way can tolerate more excess noise in the channel than one-way protocol, and the NLA can help to improve the performance both in one-way and two-way protocol

losses. In Fig. 5, we compute the maximal excess noise in the two-way protocol, without the NLA and with a NLA of $g = 4$ and then compare with the one-way protocol in the same circumstances. We can see the two-way protocol is more robust than the one-way protocol. And the application of the NLA is helpful to improve the maximal tolerable excess noise of the two-way protocol as well as one way-protocol. We can also see that, with the same excess noise, the maximal permitted losses can be extended as $20\log_{10}$ **g** dB by using the NLA.

5 Conclusion

In this paper, we have shown the two-way protocol is an improvement of one-way protocol based on the confidential knowledge of the quantum states and then propose the use of a heralded noiseless linear amplifier before the homodyne detector as a way to improve the performance of the two-way protocol against losses and noise. The secret key rate becomes negative for a certain distance of transmission due to the excess noise, and we have demonstrated that a heralded noiseless linear amplifier can increase this distance by the equivalent of $20\log_{10}$ **g** dB of losses as well as its use in the one-way protocol, and it also helps the two-way protocol tolerate more excess noise. Our computation is based on an equivalent system with the function of the NLA, which can help us simplify the calculation.

Acknowledgments This work is supported by the National Natural Science Foundation of China (Grant Nos. 61475099, 61102053, 61379153), Program of State Key Laboratory of Quantum Optics and Quantum Optics Devices (NoKF201405), the Scientific Research Foundation for the Returned Overseas Scholars, State Education Ministry, SMC Excellent Young Faculty program, SJTU 2011, Chun-Tsung Program of SJTU, and PRP (Grant No. T03023051).

References

1. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: Rev. Mod. Phys. **84**, 621 (2012)
2. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: Rev. Mod. Phys. **81**, 1301 (2009)
3. Zhang, H., Fang, J., He, G.: Phys. Rev. A **86**, 022–338 (2012)
4. He, G., Zhu, J., Zeng, G.: Phys. Rev. A **73**, 012–314 (2006)
5. Qian, Y., Shen, Z., He, G., Zeng, G.: Phys. Rev. A **86**, 052–333 (2012)
6. Li, Z., Zhang, Y., Xu, F., Peng, X., Guo, H.: Phys. Rev. A **89**, 052–301 (2014)
7. Ma, X., Sun, S., Jiang, M., Gui, M., Zhou, Y., Liang, L.: Phys. Rev. A **89**, 032–310 (2014)
8. Fossier, S., Debuisschert, E., Tualle-Brouri, R., Grangier, P.: J. Phys. B **42**, 114–014 (2009)
9. Fossier, S., Diamanti, E., Debuisschert, T., Villing, A., Tualle-Brouri, R., Grangier, P.: New J. Phys. **11**, 040–523 (2009)
10. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., Diamanti, E.: Nat. Photonics **7**, 378 (2013)
11. Weedbrook, C., Ottaviani, C., Pirandola, S.: Phys. Rev. A **89**, 012–309 (2014)
12. Pirandola, S., Mancini, S., Lloyd, S., Braunstein, S.L.: Nat. Phys. **4**, 726 (2008)
13. Ralph, T.C., Lund, A.P.: In Quantum Communication Measurement and Computing Proceedings of 9th International Conference, edited by A. Lvovsky, AIP Conf. Proc. No. 1110(AIP,New York,2009), **pp.155-160**. arXiv:0809.0326
14. Ferreyrol, F., Blandino, R., Barbieri, M., Tualle-Brouri, R., Grangier, P.: Phys. Rev. A **83**, 063–801 (2011)
15. Zavatta, A., Fiurasek, J., Bellini, M.: Nat. Photon. Lett. **5**, 52 (2011)
16. Usuga, M.A., Muller, C.R., Wittmann, C., Marek, P., Filip, R., Marquardt, C., Leuchs, G., Andersen, U.L.: Nat. Phys. **6**, 767 (2010)
17. Barbieri, M., Ferreyrol, F., Blandino, R., Tualle-Brouri, R., Grangier, P.: Laser Phys. Lett. **8**, 411 (2011)
18. Xiang, G.Y., Ralph, T.C., Lund, A.P., Walk, N., Pryde, G.J.: Nat. Photon **4**, 316 (2010)
19. Ferreyrol, F., Barbieri, M., Blandino, R., Fossier, S., Tualle-Brouri, R., Grangier, P.: Phys. Rev. A **104**, 123–603 (2010)
20. Gagatsos, C.N., Fiurasek, J., Zavatta, A., Bellini, M., Cerf, N.J.: Phys. Rev. A **89**, 062–311 (2014)
21. Blandino, R., Barbieri, M., Grangier, P., Tualle-Brouri, R.: Phys. Rev. A **91**, 062–305 (2015)
22. Blandino, R., Leverrier, A., Barbieri, M., Etesse, J., Grangier, P., Tualle-Brouri, R.: Phys. Rev. A **86**, 012–327 (2012)
23. Ralph, T.C.: Rev, Phys. A **84**, 022–339 (2011)
24. Kocsis, S., Xiang, G.Y., Ralph, T.C., Pryde, G.J.: Nat. Phys. **9**, 23 (2012)
25. Holevo, A.S.: Probl. Inf. Transm. **9**, 177–183 (1973)
26. Shannon, C.E.: Bell Syst. Tech. J. **27**, 623–656 (2003)
27. Holevo, A.S., Sohma, M., Hirota, O.: Phys. Rev. A **59**, 1820–1828 (1999)
28. Chrzanowski, H.M., Walk, N., Assad, S.M., Janousek, J., Hosseini, S.: Nat. Photonics **8**, 333–338 (2014)