Security analysis of continuous-variable quantum key distribution under limited eavesdropping with practical fiber

Sheng Liu,[1] Lu Fan,[2] Zhengyu Li,[3] Qiang Zhou,[4] Yunbo Li,[1] Dong Wang,[1] Dechao Zhang,[1]
Yichen Zhang,[2,*] and Han Li[1]

[1] *Department of Fundamental Network Technology, China Mobile Research Institute, Beijing, China*
[2] *State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3] *Central Research Institute, 2012 Labs, Huawei Technologies Co., Ltd, Shenzhen 518129, Guangdong, China*
[4] *Institute of Fundamental and Frontier Sciences, University of Electronic Science and Technology of China, Chengdu 611731, China*

(Received 22 December 2023; revised 7 March 2024; accepted 7 May 2024; published 31 May 2024)

Research on optimal eavesdropping models under practical conditions will help to evaluate realistic risk when employing a quantum key distribution system for secure information transmission. Intuitively, fiber loss will lead to the optical energy leaking to the environment, rather than harvested by the eavesdropper, which also limits the eavesdropping ability while improving the quantum key distribution system performance in practical use. However, defining the optimal eavesdropping model in the presence of lossy fiber is difficult because the channel is beyond the control of legitimate partners and the leaked signal is undetectable. Here we investigate how the fiber loss influences the eavesdropping ability based on a teleportation-based collective attack model, which requires two distant stations and a shared entanglement source. We find that if the distributed entanglement is limited due to the practical loss, the optimal attack occurs when the two teleportation stations are merged to one and placed close to the transmitter site, which performs similar to the entangling-cloning attack but with a reduced wiretapping ratio. Assuming Eve uses the best available hollow-core fiber, the secret key rate in the practical environment can be 20–40% higher than that under ideal eavesdropping. While if the entanglement distillation technology is mature enough to provide high quality of distributed entanglement, the two teleportation stations should be distantly separated for better eavesdropping performance, where the eavesdropping can even approach the optimal collective attack. Under the current level of entanglement purification technology, the unavoidable fiber loss can still greatly limit the eavesdropping ability as well as enhance the secret key rate and transmission distance of the realistic system, which promotes the development of quantum key distribution systems in practical application scenarios.

DOI: 10.1103/PhysRevApplied.21.054065

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] generates secure keys between legitimate partners, which is one of the most promising quantum communication protocols to reach maturity for commercialization. Continuous-variable (CV) QKD [4–6] has received great attention, due to its better compatibility with classical optical communication devices [7] and potential high key-generation rates in metropolitan areas [8–21]. The theoretical security poof of CVQKD protocols with Gaussian states was performed in the asymptotic limit [22,23], and then extended to the finite-size situation [24–27].

QKD technology has attracted telecommunication operators' interests for a long time, and recently operators started to deploy QKD networks aimed at providing a quantum key to customers as a service. Therefore, besides the theoretical security, it is also useful to analyze the practical security of QKD systems in real application. This usually results in two categories of discussions.

The first is about side channels of QKD systems and the countermeasures. The main side-channel attacks against CVQKD are targeted at detectors, such as a local oscillator attack [28–30], wavelength attack [31,32], blind attack [33], polarization attack [34], and reference pulse attack [35,36]. Defending methods include adding system monitors such as local oscillator monitoring, as well as the CV measurement-device-independent (CVMDI) system [37–39] proposed to be immune to any detection attacks. The second is about limited eavesdropping under more realistic technology assumptions, such as individual attack

[*] Corresponding author: zhangyc@bupt.edu.cn

[40,41], the eavesdropping without quantum memory [42], and restricted wiretapping attack [43].

These discussions about practical security are helpful for understanding the real risks from the open channel, that one may face for a practically deployed QKD system. This may also be potentially linked to quality of service (QoS) classification of the QKD service in the future. A higher QoS level requires security under less constraints on an eavesdropper's abilities, and thus usually higher service pricing.

In this paper, we investigate the limitation and impact of fiber intrinsic loss introduced to the practical eavesdropping ability. In the theoretical security analysis, it is assumed that Eve can fully control the fiber channel by replacing it with lossless fiber or harvesting all the lost energy, whereas it is highly infeasible in practice. The generic eavesdropping models used for individual attack [40,41] and collective attack [22,23] are not enough for the discussion of limited eavesdropping with practical fibers. Recently, a teleportation-based collective attack [44] was proposed with two distant stations, in which Eve does not require lossless fibers, but relies on distributed entanglement. The attack strength varies between individual attack and optimal collective attack, according to the entanglement distributed between Eve's two stations.

Based on this teleportation-based attack model, we further investigate when the fiber loss limits the entanglement distribution and how the eavesdropping ability is. Thus it provides a baseline for the discussion of limited eavesdropping with nonzero fiber loss. We find that, when the entanglement distilled between Eve's two stations is limited due to the fiber loss, the optimal attack occurs when Eve's two stations are merged into one and placed close to the transmitter site, which performs similar to the entangling cloning attack [45] but with a reduced wiretapping ratio. With such an optimal attack in practical environment, the secret key rate will be much higher compared to the ideal eavesdropping situation. While if the entanglement distributed is large enough by applying the probabilistic noiseless linear amplifier, Eve's two stations should be separated distantly, with the performance still approaching the optimal collective attack.

The paper is structured as follows. In Sec. II, we introduce the optical teleportation-based attack model, and briefly analyze the limitations, including the fiber loss. In Sec. III, we analyze the limited eavesdropping model with practical fiber loss, in which we apply the noiseless linear amplifier to relax the limitation. We finally have a discussion in Sec. IV.

II. GENERAL EAVESDROPPING MODEL WITH OPTICAL TELEPORTATION

Traditional CV teleportation requires instant individual measurements for each transmission of quantum signal. While in all-optical CV teleportation, no instant measurements are required. Thus, the teleportation-based attack [44] with all optical teleportation architecture can reach optimal collective attack. For convenience, we briefly introduce the teleportation-based eavesdropping model and its limitations when practically used.

A. Eavesdropping model description

When discussing a specific eavesdropping model, it should be able to simulate the same channel parameters as the transmitter and receiver can estimate. In CVQKD, the most commonly used security analysis method is based on the Holevo bound [22,46] derived from the Gaussian extremity theorem [47], in which the channel parameters are mainly equivalent transmittance T_{equ} and equivalent excess noise ϵ_{equ}, defined from the covariance matrix.

The eavesdropping model with optical teleportation is shown in Fig. 1(a), where Eve has two attack stations and a shared Einstein-Podolsky-Rosen (EPR) entanglement source ρ_E. With this setup, Eve can simulate an equivalent Gaussian channel $\mathcal{G}_{\text{equ}}$ with parameters T_{equ} and

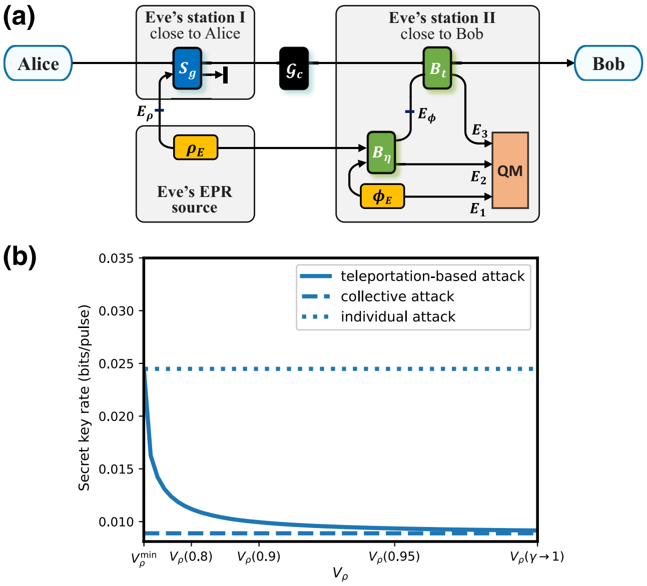

FIG. 1. (a) The teleportation-based collective attack. Eve prepares EPR state ρ_E shared by station I and II. In station I, S_g is the two-mode squeezing operation with gain $g > 1$. The output signal mode goes through a fiber channel to station II. In station II, Eve prepares the second EPR state ϕ_E to simulate channel noise. The beam splitters B_η and B_t have transmittances as η and t, respectively. (b) Simulation of the influence from the variance V_ρ of ρ_E on the secret key rate. The dotted line represents the individual attack, the dashed line describes the collective attack, and the solid line describes the teleportation-based attack. The simulated transmission channel $\mathcal{G}_{\text{equ}}$ is 50 km long with attenuation coefficient 0.275 dB/km, and the excess noise is $\epsilon = 0.04$. Other simulation parameters are, Alice's modulation variance $V_A = 4$, and reconciliation efficiency $\beta = 0.96$.

$\epsilon_{\rm equ}$, which gives the same covariance matrix that Alice and Bob have.

The first station (I) is close to Alice, in which Alice's quantum signal and one mode of EPR source ρ_E with the variance V_ρ go through a two-mode squeezing operation S_g. Then one output goes through a lossy noisy channel $\mathcal{G}_c$ to Eve's second station (station II). The channel $\mathcal{G}_c$ can be a normal fiber, or the best low-loss fiber that Eve can access. In the second station (II), Eve prepares the second EPR source ϕ_E with variance V_ϕ to help simulating channel noise $\epsilon_{\rm equ}$, by combing with the received mode through a beam splitter B_η with transmittance η. Then one output combines with the received signal from channel $\mathcal{G}_c$ through a second beam splitter B_t with transmittance t. One of its output is then sent to Bob. The modes E_1, E_2, and E_3 are stored in the quantum memory and later collectively measured.

Such a teleportation-based attack to simulating a fiber channel $\mathcal{G}_{\rm equ}$ needs to satisfy following constraints:

$$T_{\rm equ} = gT_c t, \tag{1}$$

$$\chi_{\rm equ} = t((g-1)T_c a + \chi_c) + (1-t)b - 2\sqrt{t(1-t)(g-1)T_c}c, \tag{2}$$

where $\chi_{\rm equ}$ and χ_c represent the channel output noise with $\chi_{\rm equ} = 1 - T_{\rm equ} + T_{\rm equ}\epsilon_{\rm equ}$ and $\chi_c = 1 - T_c + T_c\epsilon_c$, respectively. Here T_c and ϵ_c describe the Gaussian channel $\mathcal{G}_c$ as shown in Fig. 1(a). And a, b, c correspond to the components of the covariance matrix $\gamma_{E_\rho E_\phi}$ describing the modes E_ρ, E_ϕ in Fig. 1,

$$\gamma_{E_\rho E_\phi} = \begin{pmatrix} a \cdot I_2 & c \cdot \sigma_z \\ c \cdot \sigma_z & b \cdot I_2 \end{pmatrix} = \begin{pmatrix} V_\rho \cdot I_2 & \eta\sqrt{V_\rho^2 - 1} \cdot \sigma_z \\ \eta\sqrt{V_\rho^2 - 1} \cdot \sigma_z & \eta V_\rho + (1-\eta)V_\phi \cdot I_2 \end{pmatrix}, \tag{3}$$

where $I_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

In this model, the variation of eavesdropping strength is reflected in the preparation and distribution of Eve's EPR source ρ_E with variance $V_\rho(\gamma) = \frac{1+\gamma^2}{1-\gamma^2}$, where γ is the squeezing parameter. The minimum variance of ρ_E required to simulate the Gaussian channel $\mathcal{G}_{\rm equ}$ [48] is given by

$$V_\rho^{\rm min} = \frac{1+\gamma_{\rm min}^2}{1-\gamma_{\rm min}^2}, \tag{4}$$

with

$$\gamma_{\rm min} = \frac{-e - \sqrt{e^2 - 4df}}{2d}, \tag{5}$$

with the parameters

$$d = T_c t(g-1) + (1-t) + (t\chi_c + \chi_{\rm equ}), \tag{6}$$

$$e = -4\sqrt{t(1-t)(g-1)T_c}, \tag{7}$$

$$f = T_c t(g-1) + (1-t) + (t\chi_c + \chi_{\rm equ}). \tag{8}$$

Except for the parameter V_ρ, it is worth mentioning that the ideal model usually takes the two-mode squeezing gain $g \to \infty$, where the shared channel $\mathcal{G}_{\rm equ}$ is completely replaced by the standard teleportation protocol. While the parameters η, V_ϕ are usually optimized to maximize Eve's ability in the following simulation. Figure 1(b) illustrates the relationship between the model performance and the variance of Eve's EPR source. The simulation shows that the key rate gradually decreases as V_ρ increases. When V_ρ approaching infinity, the performance of this teleportation-based attack reaches the optimal collective attack. In this case, B_η has the same transmittance as the channel transmittance $\eta = T_{\rm equ}$, and $V_\phi = 1 + \frac{T_{\rm equ}\epsilon_{\rm equ}}{1-T_{\rm equ}}$. When V_ρ lies at the minimum $V_\rho^{\rm min}$, the model degrades to the individual attack. The transmittance of beam splitter B_η is $\eta = 1$, meaning no EPR ϕ_E is required.

When g takes a finite value as a more realistic situation, the simulated Gaussian channel $\mathcal{G}_{\rm equ}$ is noisier due to the presence of $\mathcal{G}_c$, usually means a weaker eavesdropping strength. The finite g leads to the increase of the required minimum variance $V_\rho^{\rm min}$ to simulate channel $\mathcal{G}_{\rm equ}$, which requires better entanglement generation and distribution ability. If Eve can prepare the EPR source with infinite entanglement, by taking $\eta = \frac{T_{\rm equ} - tT_c}{1-t}$, she can still achieve the optimal collective attack.

B. Limitation caused by fiber loss and entanglement distillation

The above analysis shows that it has requirement for the entanglement of the EPR source to achieve the optimal collective attack. However, various imperfections in the entanglement generation and distribution make remote distribution of the high-quality EPR source is a generic difficult problem in practical experiments.

Among all the imperfections, fiber loss matters the most since it will cause a huge entanglement degradation. Fiber loss consists of several parts, mainly including confinement loss, surface-scattering loss, Rayleigh scattering, macrobending loss, microbending loss, intrared absorption loss. Some of these loss are intrinsic, which is difficult to be eliminated by current fiber fabrication technologies. In most operators' deployed fiber, the attenuation coefficient is usually counted as 0.275 dB/km high. While standard G.652 fiber is 0.18–0.2 dB/km, low-loss fiber is of 0.15–0.17 dB/km. Furthermore, it is believed that in the not-too-distant future a hollow-core antiresonant optical fiber [49] can further lower the attenuation coefficient to

0.1 dB/km. Even with these best low-loss fibers, the attenuation can still easily reach 5–10 dB high in the 50–100 km range.

To overcome the entanglement degradation caused by the fiber loss, an additional entanglement distillation step is needed in station II. For the Gaussian EPR source like the commonly used two-mode squeezed state in CVQKD, the entanglement distillation usually consists of two steps [50, 51]. The first is to improve the entanglement degree with non-Gaussian operations, resulting in non-Gaussian output states. The second is Gaussification, which transform the non-Gaussian state back to a Gaussian state, while keeping the entanglement degree still improved.

There is an alternative method to distill the Gaussian EPR, which is probabilistic noiseless linear amplification (NLA) [52–54]. When amplification succeeds, NLA can amplify a coherent state $|\alpha\rangle$ to $|G\alpha\rangle$ without noise, where G is the gain factor of NLA. When applying NLA to one mode of a two-mode squeezed state, which passed through a lossy channel, the output state can be seen as another Gaussian state with larger initial entanglement and one mode passing through a channel with less loss.

In next section, we will analyze the limitation imposed by practical fiber loss on the eavesdropping ability. And we choose NLA as the entanglement distillation method for simplicity. Beside the fiber loss between Eve's two distant stations, the fiber transmission of signal state, including from Alice to station I and from station II to Bob, should be also taken into account.

III. LIMITED EAVESDROPPING WITH PRACTICAL FIBER

When considering practical fiber loss, the locations of Eve's two stations and how well the entanglement distributed between two stations will influence the eavesdropping strength. The eavesdropping model is described as Fig. 2. Assuming Eve's station I and station II are located at L_1 and L_2. There are four fiber channels, (1) from Alice to Eve's station I, (2) from Eve's station I to station II for transmitting amplified quantum signal, (3) from Eve's station I to station II for distributing EPR source, (4) from Eve's station II to Bob. For all these four channels, we assume that Eve can replace them with better quality fibers, but still having a loss, as discussed above $\alpha = 0.18 \sim 0.2$ dB/km for G.652 fiber, $0.15 \sim 0.17$ dB/km for low-loss fiber, 0.1 dB/km for hollow-core fiber.

Eve's distributed EPR is first generated in station I as ρ_E, and then one mode is sent to station II through a fiber channel. Then at station II, Eve employs a NLA for entanglement distillation, which means many copies will be consumed to generate one better EPR due to the probabilistic nature of NLA.

Intuitively, the better the distributed entanglement is, the more information Eve can access. This will put requirements on entanglement distillation, to reduce the entanglement reduction due to fiber loss.

We will first discuss the situation without NLA, to show the optimal attack strategy when remote entanglement distribution is limited by fiber loss. Then we discuss how NLA improves eavesdropping ability, which eventually can reach optimal collective attack, with two stations separated around Alice and Bob, respectively.

A. Eavesdropping without NLA

In the eavesdropping model without NLA, the locations of Eve's stations are the main consideration. In order to simulate the given channel $\mathcal{G}_{\text{equ}}$, the parameters of the model follow these constraints:

$$T_1T_2T_3tg = T, \tag{9}$$

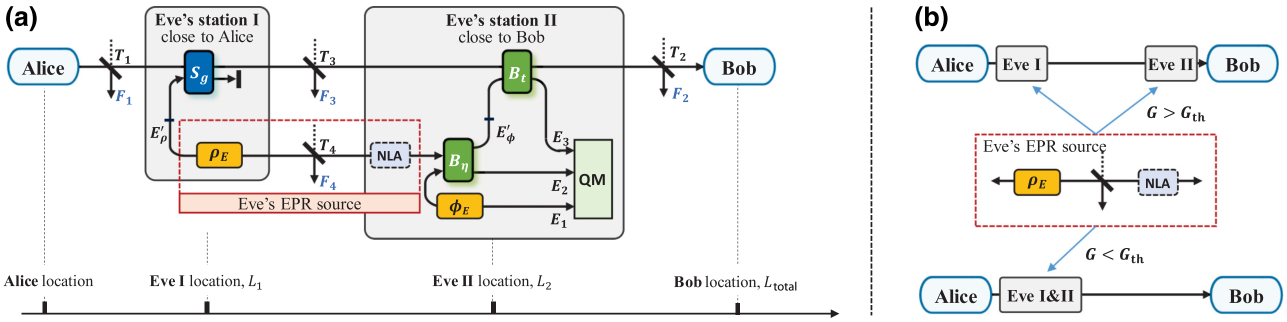

FIG. 2. (a) The EB scheme of the practical teleportation-based eavesdropping model with NLA. The four beam splitters with transmittances T_1, T_2, T_3, and T_4 describe the fiber losses for different fiber links. L_1 is the distance from Alice to station I, L_2 is the distance from Alice to station II, and L_{total} is the total distance from Alice to Bob. (b) The locations of Eve's stations that enable the optimal eavesdropping. If the gain of NLA is large enough, $G > G_{\text{th}}$, the optimal choice of station I and II are located close to Alice and Bob, respectively. If the gain of NLA is weak, $G < G_{\text{th}}$, the optimal choice will be station I and station II are placed together and close to Alice.

$$\chi_{\mathrm{equ}} = T_2(t(T_3(g(1-T_1)+(g-1)a')+(1-T_3))+(1-t)b' - 2\sqrt{t(1-t)(g-1)T_c c'}) + 1 - T_2. \tag{10}$$

And a', b', c' correspond the components of the covariance matrix $\gamma_{E'_\rho E'_\phi}$ describing the modes $E^{'}_{\rho}$, $E^{'}_{\phi}$ in Fig. 2,

$$\gamma_{E'_\rho E'_\phi} = \begin{pmatrix} a' \cdot I_2 & c' \cdot \sigma_z \\ c' \cdot \sigma_z & b' \cdot I_2 \end{pmatrix} = \begin{pmatrix} V_\rho \cdot I_2 & \sqrt{T_4 \eta (V_\rho^2 - 1)} \cdot \sigma_z \\ \sqrt{T_4 \eta (V_\rho^2 - 1)} \cdot \sigma_z & (\eta T_4 V_\rho + (1-T_4) + (1-\eta)V_\phi) \cdot I_2 \end{pmatrix}. \tag{11}$$

To focus on the influence of the locations of Eve's stations, we set the gain g of two-mode squeezing and the variance of prepared EPR state ρ_E to be sufficiently large in the following simulations. And we assume Eve exploits the hollow-core fiber with attenuation coefficient 0.1 dB/km.

Firstly, we change both the locations of Eve's two stations L_1 and L_2 ($L_1 \leq L_2 \leq L_{\mathrm{total}}$), to see how they influence the secret key rate. In Figs. 3(a) and 3(b), we fix the total distance to 50 and 100 km, respectively. It is shown that, when the location L_1 of station I is fixed, the secret key rate decreases as L_2 moves closer to L_1, which indicates that $L_2 = L_1$ gives the worst case. In this case, there is actually only one eavesdropping station, and it reduces to an entangling-cloning attack model with a reduced wiretapping ratio. Besides, when $L_2 = L_1$, the secret key rate decreases as L_1 moves closer to Alice, which shows the overall worst case is both Eve's stations are located close to Alice, $L_2 = L_1 = 0$. This follows the intuition that wiretapping at a location closer to the transmitter site is better, since more signal energy can be harvested. The simulation parameters for Figs. 3(a) and 3(b) can be found in the figure caption.

Secondly, we show the secret key rates when Eve chooses $L_2 = L_1 = 0$ and substitutes the rest of the fiber with different kinds of fibers, as in Figs. 4(a) and 4(b). Compared to the ideal collective attack (red line), Eve's practical eavesdropping ability is limited by the intrinsic fiber loss. The better fiber that Eve can use, the stronger eavesdropping ability she has. For a common QKD system with $\epsilon = 0.04$, under the 50-km transmission distance, the secret key rate could be increased by 20–40% when Eve uses the best-expected hollow-core fiber. When Eve has no choice but the commonly used G.652 fiber, the secret key rate could be increased even by 140%. It can be seen that if considering a practical eavesdropper with limited fiber technology, there will be a significant improvement in the secret key rate. The increase in transmission distance is more remarkable in the noisier system with $\epsilon = 0.1$. In (b), the transmission distance can be extended from the original 30 km to a maximum of 170 km and a minimum of 50 km, which is very meaningful for the practical application of QKD systems.

In the above analysis, even Eve can prepare the ideal EPR source with infinite entanglement, its practical ability is still limited due to the entanglement reduction caused by the transmission loss, when distributing one mode of the EPR to station II. And this is actually the reason that leads to the conclusion that both stations should locate at

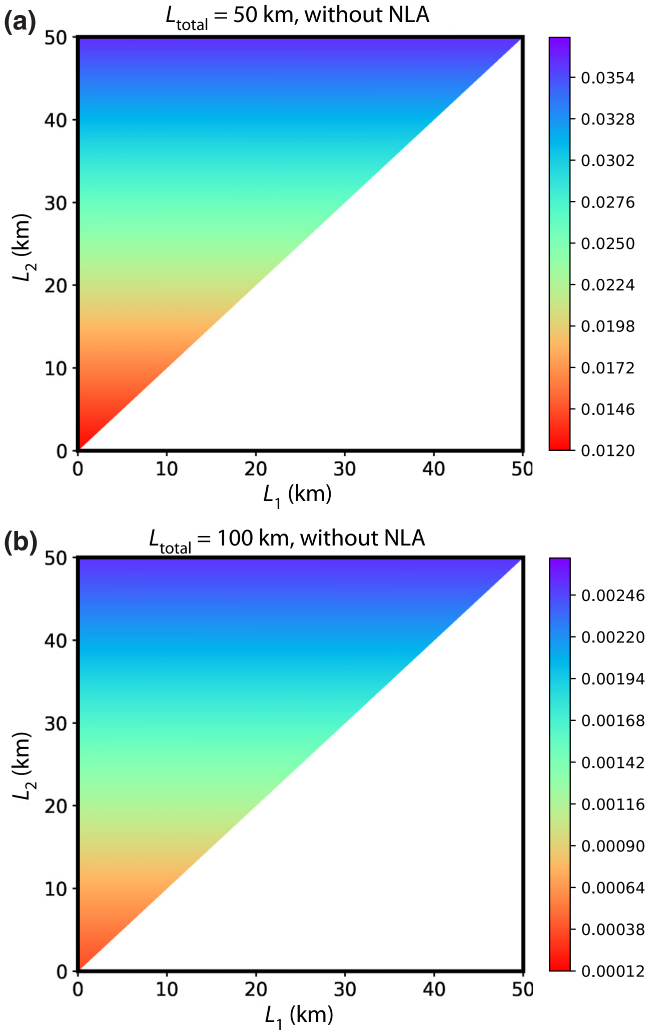

FIG. 3. The influence of Eve's two stations' locations on the secret key rate, when the total distance is 50 and 100 km, respectively. The simulated channel $\mathcal{G}_{\mathrm{equ}}$ has attenuation coefficient 0.275 dB/km, and the excess noise is $\epsilon = 0.04$. Other simulation parameters are Alice's modulation variance $V_A = 4$ and reconciliation efficiency $\beta = 0.96$.

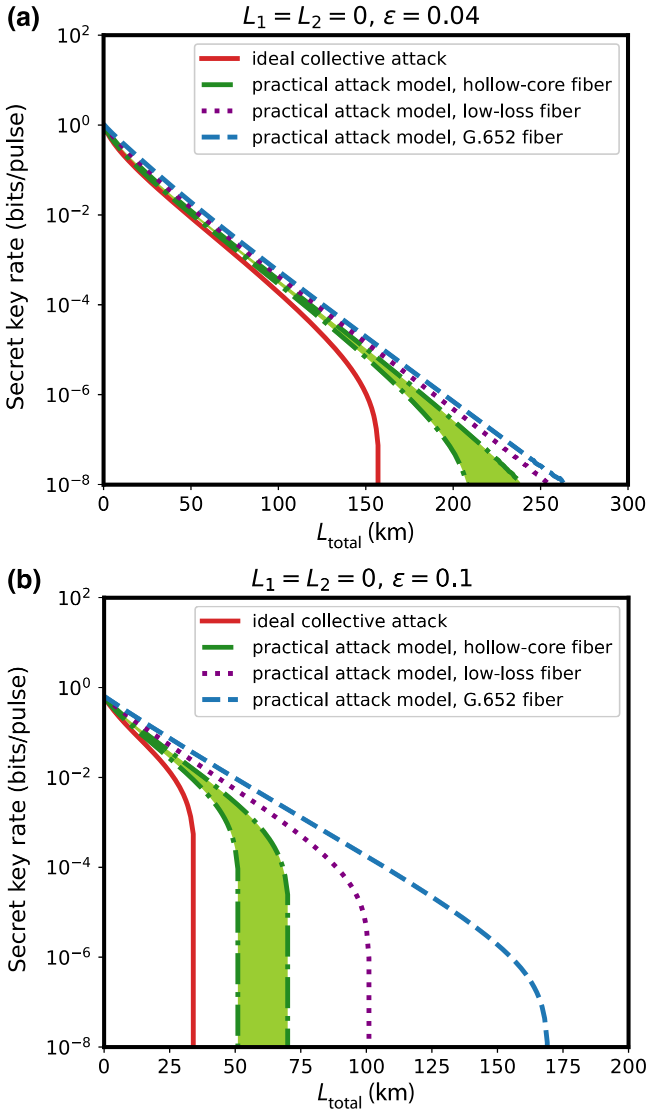

FIG. 4. Secret key rate versus transmission distance with different fibers when the system excess noise is 0.04 and 0.1, respectively. The red solid line represents the optimal collective attack case, where Eve can replace the channel with a lossless fiber. The blue dashed line represents the G.652 fiber with 0.2 dB/km, the purple dotted line represents the low-loss fiber with 0.15 dB/km, and the green dot-dashed line represents the best fiber predicted with current theory as attenuation coefficient is around 0.05∼0.1 dB/km. Other simulation parameters are Alice's modulation variance $V_A = 4$ and reconciliation efficiency $\beta = 0.96$.

the same site to achieve the optimal attack, under which the system performance still shows a great improvement compared with the ideal model. At the same time, Eve is also able to take many measures to resist the influence introduced by the fiber loss. One natural method to improve the eavesdropping ability is having entanglement distillation in station II, this will be discussed next.

B. Eavesdropping with NLA

We consider using NLA as the entanglement distillation method, which simplifies the analysis for the Gaussian channel while keeping the main conclusion.

NLA is a probabilistic operation, which can amplify a coherent state $|\alpha\rangle$ to $|G\alpha\rangle$ without noise when amplification succeeds, G is the gain factor of NLA. When applying NLA to one mode of a two-mode squeezed state ρ_E with squeezing parameter γ, which passed through a lossy channel with transmittance T_4, the output state's entanglement will be improved. When considering the output is still a Gaussian state for convenience, it is equivalent to an alternative two-mode squeezed state with squeezing parameter γ^G passing through a lossy channel with transmittance T_4^G [52], which fulfills the following conditions with

$$\gamma^G = \gamma\sqrt{1 + (G^2 - 1)T_4}, \tag{12}$$

$$T_4^G = \frac{G^2 T_4}{1 + (G^2 - 1)T_4}. \tag{13}$$

This gives an upper bound on the amplification gain, when keeping the output still in Gaussian form. Besides, in order to simulate the given channel $G_{\rm equ}$, the equivalent squeezing parameter γ^G also has a restriction as in Sec. II,

$$\gamma_{\min}^G \le \gamma^G \le 1. \tag{14}$$

Here the minimum squeezing parameter $\gamma_{\min}^G$ is redefined as

$$\gamma_{\min}^G = \frac{-e_G - \sqrt{{e_G}^2 - 4d_G f_G}}{2d_G}, \tag{15}$$

with the parameters

$$d_G = \frac{T_{\rm equ}}{T_2} + 2T_4^G - 1 + \frac{\chi_{\rm equ} - (1 - T_2)}{T_2}, \tag{16}$$

$$e_G = -4\sqrt{\frac{T_{\rm equ}}{T_1 T_2} T_4^G}, \tag{17}$$

$$f_G = 2\frac{T_{\rm equ}}{T_1 T_2} - \frac{T_{\rm equ}}{T_2} + 1 - \frac{\chi_{\rm equ} - (1 - T_2)}{T_2}. \tag{18}$$

We consider two cases for the rest of the simulations, (I) optimizing the initial EPR state ρ_E to make the equivalent source ρ_E^G with infinite entanglement ($\gamma^G \to 1$) to see the optimal distilled case, and (II) fixing the initial entanglement of ρ_E to see the influence of the gain of NLA.

First, we consider the simulation of case I. Optimizing initial EPR to make the distilled $\gamma_G \to 1$ actually means, for each NLA gain G, the distilled output state keeps the same EPR source and a different channel loss T_4^G. From Eq. (13), larger G means higher T_4^G, therefore better distributed EPR entanglement.

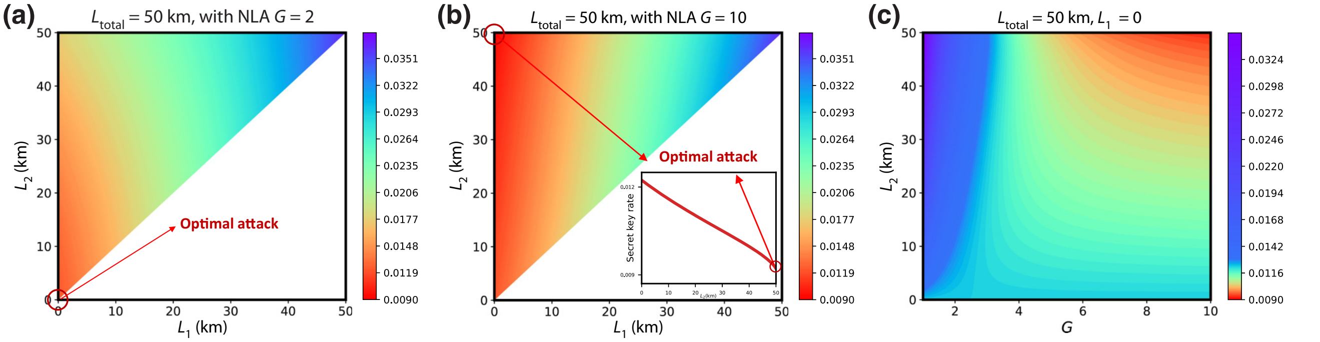

FIG. 5. (a),(b) The influence of Eve's two stations' locations on the secret key rate, when the gain of NLA are $G = 2$ and $G = 10$, respectively. Assume Eve uses the hollow-core fiber with an attenuation coefficient of 0.1 dB/km. (c) Secret key rate when changing the location of station II L_2 and the gain G of NLA, when station I is placed at the transmitter ($L_1 = 0$). For each G, the initial EPR state is optimized to make the equivalent source ρ_E^G with infinite entanglement ($\gamma^G \to 1$). Other parameters remain the same as before.

In Figs. 5(a) and 5(b), we move both locations of Eve's two stations simultaneously, with $G = 2$ in (a) and $G = 20$ in (b), while keeping the total distance $L_{\text{total}} = 50$ km unchanged. Both (a) and (b) show that the strongest eavesdropping happens when station I is located at Alice's end ($L_1 = 0$), while the situation is different regarding station II's location. As (a) has a weaker NLA gain, the worst-case secret key rate happens when Eve has both station I and II placed on the transmitter side, which is consistent with the previous discussion without NLA. While (b) has a larger NLA gain, one can find that, on opposite as (b), the optimal eavesdropping would preferably have station I and II placed on the transmitter and receiver side, respectively.

This conjecture is further verified in Fig. 5(c), where station I is placed at the sending side directly and only station II is moved. It shows that, for each NLA gain G, the secret key rate varies with different location of station II. And there exists a threshold G_{th}, when $G < G_{\text{th}}$, the optimal eavesdropping happens at the condition both Eve's stations locate at transmitter side ($L_2 = L_1 = 0$), while $G > G_{\text{th}}$, the optimal eavesdropping happens at the condition Eve's two stations separately locate at the transmitter side (station I, $L_1 = 0$) and the receiver side (station II, $L_2 = L_{\text{total}}$). This is because in the original model without NLA, placing Eve's stations at the transmitter means that she can collect more energy for eavesdropping before optical energy escapes into the environment. After applying the NLA, the gain G can improve the channel loss between two stations to optimize eavesdropping. When G exceeds a threshold, the impact of NLA on the optimal eavesdropping location dominates, and the two stations are placed separately on both sides of the communication for optimal eavesdropping. The conclusion is schematically illustrated in Fig. 2(b).

The above simulation is based on hollow-core fiber ($\alpha = 0.1$ dB/km). We also investigate different fibers with higher loss that Eve could use, which show the same feature as hollow-core fiber, as shown in Fig. 6. No matter how much worse the fiber loss is, as long as the gain of NLA is large enough, the optimal eavesdropping strategy is the same, i.e., Eve's two stations separately locate at transmitter side and receiver side. And when G is large

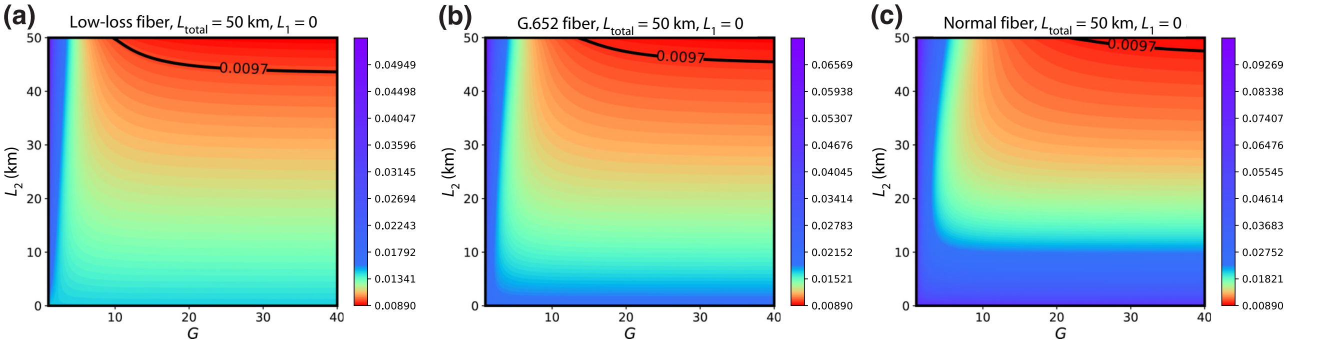

FIG. 6. Secret key rates when Eve uses different types of fibers, where the total distance is 50 km. (a) Low-loss fiber with 0.15 dB/km, (b) G.652 fiber with 0.2 dB/km and (c) normal fiber with 0.275 dB/km in the network. The upper right corner in each figure represents the case where the secret key rate is closing the worst case, which is the optimal collective attack. The simulation parameters remain the same as before.

enough, the eavesdropping ability is upgraded close to the optimal collective eavesdropping.

We next investigate the simulation case II with fixed initial EPR state ρ_E, which is more technologically reasonable since current two-mode squeezed state generation is not mature enough to easily generate arbitrary large entanglement. We still assume station I is located at the transmitter side. For each station II location L_2, the NLA gain will be limited by the condition $\gamma_{\min}^G \leq \gamma^G \leq 1$, derived from Eqs. (12) and (14). The simulation results are in Fig. 7, the left and right in (a) are determined by the restriction of γ_G as in Eq. (14) . When G takes the left boundary and γ_G takes the minimum value $\gamma_{\min}^G$, the channel is completely described by Eve's EPR source, and the eavesdropping model degenerates into the original individual attack. Taking the maximum value of 1 for γ_G will correspond to the right boundary of G. Moreover, the key rate of the right boundary decreases with the increase of L_2, indicating different kinds of collective attack. It is obvious that the optimal collective attack effect is almost achieved when $L_2 = L_{\text{total}}$.

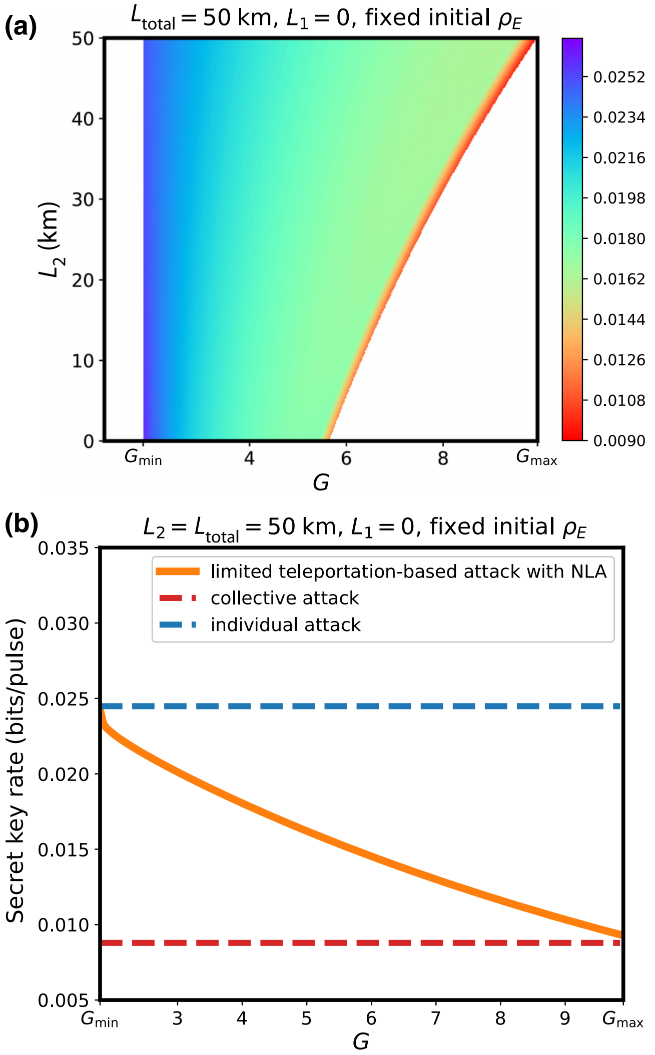

FIG. 7. (a) The influence of station II's location and the gain G on the secret key rate, when the variance V_ρ of initial EPR state ρ_E is fixed. (b) The secret key rate versus NLA gain G, when V_ρ is fixed. Other parameters remain the same as before.

This simulation shows that the location of eavesdropping will have an effect on the strength of the collective attack while the individual attack is not influential. Figure 7(b) clearly demonstrates the compensatory effect of the NLA for limited eavesdropping performance. Picking an appropriate EPR state, the entanglement of Eve's distributed EPR source can still be improved so that the limited eavesdropping with lossy fiber can be converted from the individual attack to the optimal collective attack, with specific NLA.

From the above simulations, it is clear that the distillation of entanglement source is the crucial factor that affects the eavesdropping ability. The presence of practical fiber loss will limit the distributed entanglement, resulting in the optimal attack occurring when Eve's two stations are merged and placed at the transmitter. The practical QKD system performance under such an optimal attack is better as the fiber loss is higher. When NLA is used to greatly optimize the distillation of the entanglement source, the optimal attack will occur when the two stations are separated on both the transmitting and receiving sides, where it can even approach the optimal collective attack when the NLA gain is large.

IV. DISCUSSION

An all-optical-teleportation-based attack model is of interest for allowing that Eve does not have to fully control the shared channel, in which the entanglement source is the key role to eavesdropping ability. In the ideal eavesdropping model, Eve is usually assumed to have an infinite power to prepare, distill, and distribute arbitrary entanglement sources. The gap between realistic and ideal scenarios will challenge the premise, among which the most inevitable imperfection is the practical fiber loss. Indeed, Eve can only replace the normal channel between the communicating parties with a low-loss channel as far as possible, such as hollow-core fiber. We have found that in the realistic environment, even if Eve can use the best available hollow-core fiber to perform eavesdropping, the key rate and transmission distance of the QKD system will still be improved to a greater extent. In addition to the amount of fiber loss, the location of fiber loss also has an impact on Eve's eavesdropping ability.

We also analyzed when NLA is used for entanglement distillation to improve the practical eavesdropping ability. Numerical simulations reveal that fiber loss will challenge Eve's ability, while the NLA can be used to improve her eavesdropping strength. After the compensation from NLA on the distributed entanglement, the eavesdropping ability could even be improved approaching the performance of optimal collective attack.

Despite this, we believe that other nonideal factors during entanglement distribution, such as finite entanglement generation, imperfect squeezing with limited gain, etc., should also be investigated in the future, further deepening the understanding of the realistic risk of a practical CVQKD system.

ACKNOWLEDGMENTS

This research was supported by the National Natural Science Foundation of China (Grants No. 62001044 and No. 61531003), the Basic Research Program of China (Grant No. JCKY2021210B059), the Equipment Advance Research Field Foundation (Grant No. 315067206), and the Fund of State Key Laboratory of Information Photonics and Optical Communications (Grant No. IPOC2021ZT02).

APPENDIX A: THE ENTANGLEMENT OF EVE'S SOURCE

In the entangling cloning eavesdropping model for the Gaussian CVQKD, Alice first prepares an EPR state $\hat{\Psi}_{AA'}$ whose covariance matrix has the form

$$\gamma_{AA'} = \begin{pmatrix} V\cdot I_2 & \sqrt{V^2-1}\cdot\sigma_z \\ \sqrt{V^2-1}\cdot\sigma_z & V\cdot I_2 \end{pmatrix}, \tag{A1}$$

with $V = V_A + 1$. One mode of the EPR state $\hat{\Psi}_{AA'}$ A' is transmitted through a given Gaussian channel $\mathcal{G}_{\text{equ}}(T_{\text{equ}}, \epsilon_{\text{equ}})$ as B to Bob, where its covariance matrix transform is described as

$$\Psi_{AB} = \mathcal{G}(\Psi_{AA'}) = \mathcal{T}\Psi_{AA'}(\mathcal{T})^T + \mathcal{N}. \tag{A2}$$

$\mathcal{T}$ and $\mathcal{N}$ characterize the transmittance and the excess noise, respectively. The covariance matrix γ_{AB} is given by

$$\gamma_{AB} = \begin{pmatrix} V\cdot I_2 & \sqrt{T_{\text{equ}}(V^2-1)}\cdot\sigma_z \\ \sqrt{T_{\text{equ}}(V^2-1)}\cdot\sigma_z & (T_{\text{equ}}V + (1-T_{\text{equ}})N)\cdot I_2 \end{pmatrix}, \tag{A3}$$

where $N = 1 + \frac{T_{\text{equ}}\epsilon_{\text{equ}}}{1-T_{\text{equ}}}$ represents the noise variance.

In the all-optical teleportation model, the signal mode A' will pass through S_g, Gaussian channel $\mathcal{G}_c$ and B_t successively with symplectic transformations as

$$S_g = \begin{pmatrix} \sqrt{g}\cdot I_2 & \sqrt{g^2-1}\cdot I_2 \\ -\sqrt{g^2-1}\cdot I_2 & \sqrt{g}\cdot I_2 \end{pmatrix}, \tag{A4}$$

$$B_t = \begin{pmatrix} \sqrt{t}\cdot I_2 & \sqrt{1-t}\cdot\sigma_z \\ \sqrt{1-t}\cdot\sigma_z & \sqrt{t}\cdot I_2 \end{pmatrix}. \tag{A5}$$

The covariance matrix of its output B' and mode A $\gamma_{AB'}$ is given as Eq. (A6).

$$\gamma_{AB'} = \begin{pmatrix} V\cdot I_2 & \sqrt{tT_cg(V^2-1)}\cdot\sigma_z \\ \sqrt{tT_cg(V^2-1)}\cdot\sigma_z & (T_{\text{equ}}V + t((g-1)T_ca+\chi_c) + (1-t)b - 2\sqrt{t(1-t)(g-1)T_c}c)\cdot I_2 \end{pmatrix}. \tag{A6}$$

In order to adequately describe the given Gaussian channel, the output of the all-optical teleportation model should be the same as the previous model, that is, Eq. (A6) should be equivalent to Eq. (A3), so there is

$$T_{\text{equ}} = gT_ct, \tag{A7}$$

$$\chi_{\text{equ}} = t((g-1)T_ca+\chi_c) + (1-t)b - 2\sqrt{t(1-t)(g-1)T_c}c. \tag{A8}$$

The EPR source ρ_E in the all-optical teleportation model has a minimum entanglement as $\eta = 1$ where the channel noise completely describes the EPR state source as the individual attack, then the covariance matrix $\gamma_{E_\rho E_\phi}$ describing the modes E_ρ, E_ϕ is converted to

$$\gamma_{E_\rho E_\phi} = \begin{pmatrix} V_\rho^{\text{min}}\cdot I_2 & \sqrt{{V_\rho^{\text{min}}}^2-1}\cdot\sigma_z \\ \sqrt{{V_\rho^{\text{min}}}^2-1}\cdot\sigma_z & \eta V_\rho\cdot I_2 \end{pmatrix}. \tag{A9}$$

V_ρ^{min} can be solved naturally. Correspondingly, when the EPR source has infinite entanglement where its variance is infinite, Eq. (A8) holds when $\eta = T_{\text{equ}}$ and $V_\phi = N$. At this point, the channel excess noise is fully characterized by Eve's station II as the collective attack.

APPENDIX B: THE SECRET KEY RATE OF LIMITED EAVESDROPPING WITH FIBER LOSSES

The secret key rate formula against the collective attack is given by the Devetak-Winter formula,

$$R = \beta I(a:b) - S(x:E), \tag{B1}$$

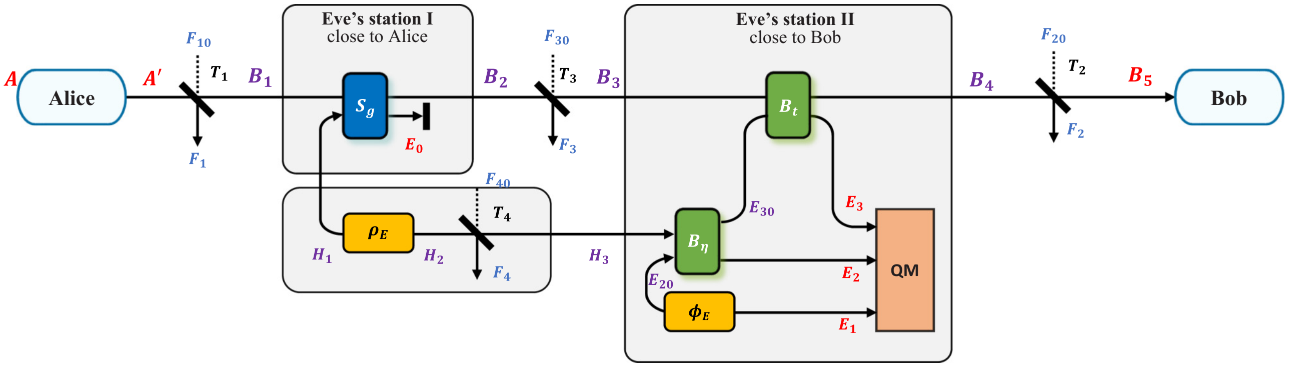

FIG. 8. The mode transformation of the all-optical teleportation with practical fiber loss. The mode A is reserved by Alice, while B_5 is the pattern received by Bob. Eve performs the collective attack on E_1, E_2, and E_3 in quantum memory to steal secret keys. It should be stressed that since the channel loss is not under the control of Eve, the channel modes F_1, F_2, F_3, and F_4 modeled by beam splitters with transmittances T_1, T_2, T_3, and T_4 are trusted, resulting in the increase of the secret key rate.

where β is the reconciliation efficiency [55]. $I(a:b)$ is the mutual information between Alice and Bob, and $S(x:E)$ is the mutual information between Alice and Eve. The amount of information Eve can extract $S(x:E) \leq \chi(x:E)$ where $\chi(x:E)$ represents the Holevo bound. The maximum amount of secret keys for Eve to perform the eavesdropping can be given by

$$S(x:E) = S(E) - S(E|x), \tag{B2}$$

which can be obtained through the symplectic eigenvalues of a N-mode state.

In the practical environments, the pure fiber losses are all modeled as a beam splitter, such as

$$B_{T_1} = \begin{pmatrix} \sqrt{T_1}\cdot I_2 & \sqrt{1-T_1}\cdot\sigma_z \\ \sqrt{1-T_1}\cdot\sigma_z & \sqrt{T_1}\cdot I_2 \end{pmatrix}. \tag{B3}$$

The parameters T_2, T_3, T_4 in the model are also described in this way.

The EB model with mode transformation is shown in Fig. 8. The output after the first channel loss is represented as B_1 where F_{10} is the vacuum state,

$$\gamma_{AB_1F_1} = B_{T_1}^{A'F_{10}}(\gamma_{AA'} \oplus I_2)(B_{T_1}^{A'F_{10}})^T, \tag{B4}$$

here $B_{T_1}^{A'B_1} = I_2 \oplus B_{T_1}$. After the two-mode squeezing operation S_g,

$$\gamma_{AB_2E_0H_3} = S_g^{B_1H_1}(\gamma_{AB_1} \oplus \gamma_{H_1H_3})(S_g^{B_1H_1})^T, \tag{B5}$$

$$\gamma_{H_1H_3} = \begin{pmatrix} V_\rho^{\text{min}}\cdot I_2 & \sqrt{T_4({V_\rho^{\text{min}}}^2-1)}\cdot\sigma_z \\ \sqrt{T_4({V_\rho^{\text{min}}}^2-1)}\cdot\sigma_z & (T_4V_\rho+1-T_4)\cdot I_2 \end{pmatrix}, \tag{B6}$$

and $S_g^{B_1H_1} = I_2 \oplus S_g \oplus I_2$. Further, the signal will undergo the pure loss with transmittance T_3,

$$\gamma_{AH_3B_3F_3} = B_{T_3}^{B_2F_{30}}(\gamma_{AH_3B_2} \oplus I_2)\left(B_{T_3}^{B_2F_{30}}\right)^T, \tag{B7}$$

where $B_{T_3}^{B_2F_{30}} = I_2 \oplus I_2 \oplus B_{T_3}$. On the other hand, the mode H_3 also passes through the B_η,

$$\gamma_{AB_3E_{30}E_2E_1} = B_\eta^{H_3E_{20}}(\gamma_{AB_3H_3} \oplus \gamma E_{20}E_1)\left(B_\eta^{H_3E_{20}}\right)^T, \tag{B8}$$

where $B_\eta^{H_3E_{20}} = I_2 \oplus I_2 \oplus B_\eta \oplus I_2$. Here

$$B_\eta = \begin{pmatrix} \sqrt{\eta}\cdot I_2 & \sqrt{1-\eta}\cdot\sigma_z \\ \sqrt{1-\eta}\cdot\sigma_z & \sqrt{\eta}\cdot I_2 \end{pmatrix} \tag{B9}$$

and

$$\gamma_{E_{20}E_1} = \begin{pmatrix} V_\phi\cdot I_2 & \sqrt{V_\phi^2-1}\cdot\sigma_z \\ \sqrt{V_\phi^2-1}\cdot\sigma_z & V_\phi\cdot I_2 \end{pmatrix}. \tag{B10}$$

The modes B_3 and E_{30} will together go through B_t,

$$\gamma_{AB_4E_3E_2E_1} = B_t^{B_3E_{30}}(\gamma_{AE_2E_1B_3E_{30}})\left(B_t^{B_3E_{30}}\right)^T, \tag{B11}$$

where $B_t^{B_3E_{30}} = I_2 \oplus I_2 \oplus I_2 \oplus B_t$. At last, there exists the fiber loss between station II and Bob,

$$\gamma_{AE_3E_2E_1B_5F_2} = B_{T_2}^{B_4F_{20}}(\gamma_{AE_3E_2E_1B_4} \oplus I_2)\left(B_{T_2}^{B_4F_{20}}\right)^T, \tag{B12}$$

where $B_{T_2}^{B_4F_{20}} = I_2 \oplus I_2 \oplus I_2 \oplus I_2 \oplus B_{T_2}$. The modes E_1, E_2, and E_3 are stored in quantum memory controlled by Eve, the secret key rate further can be calculated from

Eq. (B12). When $T_1, T_2, T_3, T_4 = 1$, γ_{AB_5} in Eq. (B12) degenerates to Eq. (A6), at which point the practical model also reduces to the ideal all-optical teleportation-based model.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[4] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. **88**, 057902 (2002).

[5] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum cryptography without switching, Phys. Rev. Lett. **93**, 170504 (2004).

[6] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: A review and perspective, Appl. Phys. Rev. **11**, 011318 (2024).

[7] H. Guo, Z. Li, S. Yu, and Y. Zhang, Toward practical quantum key distribution using telecom components, Fundam. Res. **1**, 96 (2021).

[8] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[9] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, *et al.*, Field test of classical symmetric encryption with continuous variables quantum key distribution, Opt. Express **20**, 14030 (2012).

[10] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Field demonstration of a continuous-variable quantum key distribution network, Opt. Lett. **41**, 3511 (2016).

[11] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, *et al.*, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[12] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[13] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, *et al.*, Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area, Commun. Phys. **5**, 162 (2022).

[14] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, *et al.*, Practical continuous-variable quantum key distribution with composable security, Nat. Commun. **13**, 4740 (2022).

[15] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber, Opt. Lett. **48**, 1766 (2023).

[16] H. H. Brunner, C.-H. F. Fung, M. Peev, R. B. Méndez, L. Ortiz, J. P. Brito, V. Martín, J. M. Rivas-Moscoso, F. Jiménez, A. A. Pastor, *et al.*, Demonstration of a switched CV-QKD network, EPJ Quantum Tech. **10**, 38 (2023).

[17] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution, preprint arXiv:2207.11702.

[18] A. A. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, and T. Gehring, Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver, preprint arXiv:2305.19642.

[19] M. Zhang, P. Huang, P. Wang, S. Wei, and G. Zeng, Experimental free-space continuous-variable quantum key distribution with thermal source, Opt. Lett. **48**, 1184 (2023).

[20] Y. Bian, Y. Pan, X. Xu, L. Zhao, Y. Li, W. Huang, L. Zhang, S. Yu, Y. Zhang, and B. Xu, Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip, preprint arXiv:2402.10411.

[21] X. Jiang, S. Xue, J. Tang, P. Huang, and G. Zeng, Low-complexity adaptive reconciliation protocol for continuous-variable quantum key distribution, Quantum Sci. Technol. **9**, 025008 (2024).

[22] R. García-Patrón and N. J. Cerf, Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[23] M. Navascués, F. Grosshans, and A. Acin, Optimality of Gaussian attacks in continuous-variable quantum cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[24] R. Renner and J. I. Cirac, de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography, Phys. Rev. Lett. **102**, 110504 (2009).

[25] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Security of continuous-variable quantum key distribution against general attacks, Phys. Rev. Lett. **110**, 030502 (2013).

[26] S. Pirandola, Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks, Phys. Rev. Res. **3**, 043014 (2021).

[27] S. Pirandola, Limits and security of free-space quantum communications, Phys. Rev. Res. **3**, 013279 (2021).

[28] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, Phys. Rev. A **87**, 062313 (2013).

[29] X. Ma, S. Sun, M. Jiang, and L. Liang, Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems, Phys. Rev. A **88**, 022339 (2013).

[30] L. Fan, Y. Bian, M. Wu, Y. Zhang, and S. Yu, Quantum hacking against discrete-modulated continuous-variable quantum key distribution using modified local oscillator

intensity attack with random fluctuations, Phys. Rev. Appl. **20**, 024073 (2023).

[31] J. Huang, C. Weedbrook, Z. Yin, S. Wang, H. Li, W. Chen, G. Guo, and Z. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, Phys. Rev. A **87**, 062329 (2013).

[32] X. Ma, S. Sun, M. Jiang, and L. Liang, Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol, Phys. Rev. A **87**, 052309 (2013).

[33] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Homodyne-detector-blinding attack in continuous-variable quantum key distribution, Phys. Rev. A **98**, 012312 (2018).

[34] Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, Polarization attack on continuous-variable quantum key distribution, J. Phys. B **52**, 015501 (2018).

[35] Y. Shao, H. Wang, Y. Pi, W. Huang, Y. Li, J. Liu, J. Yang, Y. Zhang, and B. Xu, Phase noise model for continuous-variable quantum key distribution using a local local oscillator, Phys. Rev. A **104**, 032608 (2021).

[36] Y. Shao, Y. Li, H. Wang, Y. Pan, Y. Pi, Y. Zhang, W. Huang, and B. Xu, Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator, Phys. Rev. A **105**, 032601 (2022).

[37] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052301 (2014).

[38] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photonics **9**, 397 (2015).

[39] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber, Optica **9**, 492 (2022).

[40] J. Lodewyck and P. Grangier, Tight bound on the coherent-state quantum key distribution with heterodyne detection, Phys. Rev. A **76**, 022332 (2007).

[41] J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching, Phys. Rev. A **76**, 052301 (2007).

[42] H. Bechmann-Pasquinucci, Eavesdropping without quantum memory, Phys. Rev. A **73**, 044305 (2006).

[43] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, Secret-key distillation across a quantum wiretap channel under restricted eavesdropping, Phys. Rev. Appl. **14**, 024044 (2020).

[44] S. Tserkis, N. Hosseinidehaj, N. Walk, and T. C. Ralph, Teleportation-based collective attacks in Gaussian quantum key distribution, Phys. Rev. Res. **2**, 013208 (2020).

[45] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, Quantum Info. Comput. **3**, 535 (2003).

[46] A. S. Holevo, Information-theoretical aspects of quantum measurement, Probl. Peredachi Inf. **9**, 31 (1973).

[47] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian quantum states, Phys. Rev. Lett. **96**, 080502 (2006).

[48] S. Tserkis, J. Dias, and T. C. Ralph, Simulation of Gaussian channels via teleportation and error correction of gaussian states, Phys. Rev. A **98**, 052335 (2018).

[49] E. N. Fokoua, S. A. Mousavi, G. T. Jasion, D. J. Richardson, and F. Poletti, Loss in hollow-core optical fibers: Mechanisms, scaling rules, and limits, Adv. Opt. Photonics **15**, 1 (2023).

[50] E. T. Campbell and J. Eisert, Gaussification and entanglement distillation of continuous-variable systems: A unifying picture, Phys. Rev. Lett. **108**, 020501 (2012).

[51] E. T. Campbell, M. G. Genoni, and J. Eisert, Continuous-variable entanglement distillation and noncommutative central limit theorems, Phys. Rev. A **87**, 042330 (2013).

[52] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier, Phys. Rev. A **86**, 012327 (2012).

[53] J. Fiurášek and N. J. Cerf, Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution, Phys. Rev. A **86**, 060302 (2012).

[54] S. Yang, S. Zhang, X. Zou, S. Bi, and X. Lin, Continuous-variable entanglement distillation with noiseless linear amplification, Phys. Rev. A **86**, 062321 (2012).

[55] G. Van Assche, J. Cardinal, and N. J. Cerf, Reconciliation of a quantum-distributed Gaussian key, IEEE Trans. Inf. **50**, 394 (2004).