Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection

Nedasadat Hosseinidehaj,[1,*] Andrew M. Lance,[2] Thomas Symul,[2] Nathan Walk,[3] and Timothy C. Ralph[1]

[1]*Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

[2]*QuintessenceLabs Pty. Ltd., Canberra ACT, Australia*

[3]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

(Received 30 December 2019; revised manuscript received 23 April 2020; accepted 27 April 2020; published 22 May 2020)

In a continuous-variable quantum key distribution (CV-QKD) protocol, which is based on heterodyne detection at the receiver, the application of a noiseless linear amplifier (NLA) on the received signal before the detection can be emulated by the postselection of the detection outcome. Such a postselection, which is also called a measurement-based NLA, requires a cutoff on the amplitude of the heterodyne-detection outcome to produce a normalizable filter function. Increasing the cutoff with respect to the received signals results in a more faithful emulation of the NLA and nearly Gaussian output statistics at the cost of discarding more data. While recent works have shown the benefits of postselection via an asymptotic security analysis, we undertake an investigation of such a postselection utilizing a composable security proof in the realistic finite-size regime, where this tradeoff is extremely relevant. We show that this form of postselection offers only a small fraction of the asymptotic improvement in the finite-size regime. This postselection can improve the secure range of a CV-QKD over lossy thermal channels if the finite block size is sufficiently large and the optimal value for the filter cutoff is typically in the non-Gaussian regime. The relatively modest improvement in the finite-size regime as compared to the asymptotic case highlights the need for new tools to prove the security of non-Gaussian cryptographic protocols. These results also represent a quantitative assessment of a measurement-based NLA with an entangled-state input in both the Gaussian and non-Gaussian regime.

DOI: 10.1103/PhysRevA.101.052335

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] is the most mature application of quantum information technologies, which allows two distant trusted parties, traditionally called Alice and Bob, to share a secret key, which is unknown to a potential eavesdropper, Eve. In the quantum communication part of QKD Alice encodes classical information (i.e., key information) into conjugate quantum basis states, which are then transmitted over an insecure quantum channel to Bob, who measures the received quantum states in a randomly chosen basis, to obtain classical information, which is correlated to Alice's data. Repeating this procedure many times, Alice and Bob end up with two sets of correlated data, known as the raw keys. In the classical postprocessing part of QKD Alice and Bob proceed with the sifting (if applicable), parameter estimation, reconciliation (or error correction), and privacy amplification over a public but authenticated classical channel to obtain a shared secret key [1–3]. QKD systems were first introduced using discrete-variable quantum systems, where the key information is encoded onto the degrees of freedom of single photons, and the measurement at the receiver is realized by single-photon detectors [4,5]. As an alternative, continuous-variable (CV) QKD systems were introduced [6–8], where the key information is encoded onto the amplitude and phase quadratures of the quantized electromagnetic field, and the measurement relies on coherent detection, either homodyne or heterodyne detectors [9–11], which are faster and more efficient than single-photon detectors. CV-QKD systems can potentially achieve higher secret key rates than their discrete-variable counterparts, and their practical implementation is also compatible with current telecommunication optical networks. Although, thanks to the reverse reconciliation [12] (where the receiver, i.e., Bob, is the reference of the error correction), a secret key can asymptotically be generated for a pure loss channel over an arbitrary large distance, the practical secure distance of CV-QKD systems is limited due to the excess noise, imperfect classical postprocessing, and finite-size effects.

In order to improve the transmission range of CV-QKD systems a postselection strategy was proposed [13–17] in which, following the measurement of all the received quantum states, Alice and Bob discard the classical data corresponding to those channels for which the resulting key rate is negative, keeping only the data corresponding to those channels with a positive key-rate contribution. In this technique the resulting postselected data has non-Gaussian statistics. Further, it has been shown that the application of an ideal noiseless linear amplifier (NLA), proposed in Ref. [18], on the received signal preceding the detection can probabilistically enhance the secure range of CV-QKD systems, while preserving the Gaussian statistics [19]. Also, the use of single quantum scissors [18] as a practical candidate for an NLA has been shown to

*n.hosseinidehaj@uq.edu.au

enhance the secure range of CV-QKD systems [20,21]. However, any physical realization of the NLA is very demanding, requiring state-of-the-art technology, such as single-photon sources. Moreover, the actual success probability of these experiments is much lower than the theoretical predictions. In Refs. [22–24] it has been shown that the physical implementation of the NLA can be substituted with a classical data postprocessing. In particular, where the NLA directly precedes a heterodyne detection, the noiseless amplifier can be emulated by a Gaussian postselection of the detection outcome via a probabilistic classical filter function [23,24]. This postselection scheme, which is also called measurement-based NLA [24], has experimentally been demonstrated in Ref. [24] and requires a cutoff (on the amplitude of the heterodyne-detection outcome) for the classical filter to emulate the NLA. The postselection scheme results in Gaussian statistics for the postselected data if the filter cutoff is chosen sufficiently large [23,24].

In the asymptotic regime it has been shown that the Gaussian postselection can extend the maximum transmission distance of CV-QKD systems [22–24]. However, in reality only a finite number of signals are exchanged between Alice and Bob. The finite-size issue becomes even more significant when the postselection is applied as it reduces the size of data. It is unclear whether the postselection can still improve the CV-QKD performance in the realistic finite-size regime.

In this work we investigate the finite-size effects in the security analysis of CV-QKD systems with the postselection (or the measurement-based NLA) at the receiver. We show that in the finite-size regime when the filter cutoff is large enough to make the postselected statistics Gaussian, the maximum transmission distance of the CV-QKD system can be improved providing that the block size is sufficiently large. Considering finite blocks in a practical regime, we illustrate that the postselection is effective when the CV-QKD system has undergone high values of excess noise. Since reducing the cutoff can increase the success probability of the postselection (at the expense of decreasing the classical mutual information between Alice and Bob), we also investigate the impact reducing the cutoff can have on the finite-size key rate, illustrating that if the filter cutoff is sufficiently reduced, the improvement of CV-QKD performance due to the postselection can further be increased. Note that in the recent works on measurement-based NLA [23,24], the security proof is based on the equivalent entanglement-based scheme where the classical filter is replaced with a quantum filter, as they assumed a sufficiently large cutoff to emulate an ideal NLA (with a Gaussian output). However, since reducing the cutoff can change the statistics of the postselected data from Gaussian to non-Gaussian regime, we analyze the security proof based on the equivalent entanglement-based scheme with a classical filter (and not a quantum filter). Thus, our results also provide a characterization of the measurement-based NLA, when it is applied to a mixed Gaussian entangled state, which is an extension to a recent work on the characterization of the measurement-based NLA with a pure coherent-state input [25].

The structure of the remainder of this paper is as follows. In Sec. II, the Gaussian CV-QKD system is described. In Sec. III, the security of the CV-QKD system is analyzed in both the asymptotic and composable finite-size regime. In Sec. IV, the postselection of Bob's detection outcome is discussed, and the security of the postselection protocol is analysed in the composable finite-size regime. In Sec. V, the numerical results, showing the impact of the Gaussian and non-Gaussian postselection on the CV-QKD performance in the finite-size regime, is provided. Finally, concluding remarks are provided in Sec. VI.

II. CV-QKD SYSTEM

Here we consider a Gaussian no-switching CV-QKD protocol [15,26], which relies on the preparation of coherent states and heterodyne detection. In a prepare-and-measure scheme Alice generates a pair of random real numbers, a_q and a_p, chosen from two independent Gaussian distributions of variance V_A. Alice prepares coherent states by modulating (displacing) a coherent laser source by amounts of a_q and a_p, such that the variance of the imposed signals is V_A. The variance of the beam after the modulator is $V_A + 1 = V$ (where the 1 is for the shot noise variance), hence we obtain an average output state, which is thermal of variance V. The prepared coherent states are then transmitted over an insecure quantum channel with transmissivity T and excess noise ξ (relative to the input of the quantum channel) to Bob. For each incoming state, Bob uses heterodyne detection and measures both the $\hat{q}$ and $\hat{p}$ quadratures for obtaining (b_q, b_p). In this protocol, sifting is not needed, since both of the real random variables generated by Alice are used for the generation of the key. When the quantum communication is finished and all the incoming quantum states have been measured by Bob, classical postprocessing including discretization, parameter estimation, error correction, and privacy amplification over a public but authenticated classical channel is commenced to produce a shared secret key.

This Gaussian CV-QKD system in the prepare-and-measure scheme can be represented by an equivalent entanglement-based scheme [9,10], where Alice generates a pure Gaussian entangled state, i.e., a two-mode squeezed vacuum state ρ_{AB} with the quadrature variance V, where $V = \frac{1+\chi^2}{1-\chi^2}$, and where $\chi = \tanh(r)$, with r being the two-mode squeezing parameter. Alice retains mode A, while sending mode B to Bob. In the entanglement-based scheme, if Alice applies a heterodyne detection to mode A, she projects mode B onto a coherent state. At the output of the channel, Bob applies a heterodyne detection to the received mode. As a result of Alice and Bob's heterodyne detection on all the shared entangled states, they end up with two sets of correlated classical data as the raw key, from which they can extract a shared secret key through the classical postprocessing.

III. ASYMPTOTIC AND FINITE-SIZE SECURITY ANALYSIS

In the asymptotic regime the secret key rate in the reverse reconciliation scenario, where Bob is the reference of reconciliation, is given by $K = \beta I(a{:}b) - \chi(b{:}E)$ against Gaussian collective attacks, where $I(a{:}b)$ is the mutual information shared between Alice and Bob limited by the Shannon bound, $\chi(b{:}E)$ is the maximum mutual information shared

between Eve and Bob limited by the Holevo bound, and $0 \leqslant \beta \leqslant 1$ is the reconciliation efficiency. Note that in the asymptotic regime collective attacks are as strong as coherent attacks [9,10,27]. Furthermore, for Gaussian CV-QKD protocols, where the key encoding is performed by a Gaussian modulation of Gaussian states and the decoding is performed by Gaussian measurement, i.e., homodyne or heterodyne detection, Gaussian attacks are asymptotically optimal among collective attacks [28–30].

In the composable finite-size regime, the Gaussian no-switching CV-QKD protocol acting on $2n$ coherent states sent from Alice to Bob (or $2n$ two-mode squeezed vacuum states in the equivalent entanglement-based scheme) is ϵ secure against Gaussian collective attacks in the reverse reconciliation scenario if $\epsilon{=}2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm cor}$ [31,32] and if the key length ℓ is chosen such that [31,32]

$$\ell \leqslant N[\beta I(a{:}b) - \chi(b{:}E)] - \sqrt{N}\Delta - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right), \quad (1)$$

where [31,32]

$$\Delta = (d+1)^2 + 4(d+1)\sqrt{\log_2\left(2/\epsilon_{\rm sm}^2\right)} + 2\log_2(2/(\epsilon^2\epsilon_{\rm sm})) + 4\epsilon_{\rm sm} d/(\epsilon\sqrt{N}), \quad (2)$$

and where $N{=}2n$, d is the discretization parameter, $\epsilon_{\rm sm}$ is the smoothing parameter, $\epsilon_{\rm cor}$ and $\epsilon_{\rm PE}$ are the maximum failure probabilities for the error correction and parameter estimation, respectively, and $\bar{\epsilon}$ comes from the leftover hash lemma [31,32].

The final key rate (in bits per mode) where the key is ϵ secure against Gaussian collective attacks is given by ℓ/N. Note that in Eq. (1) we have considered the same scenario as Ref. [31], where almost all the raw data can be utilized to distill the secret key (by performing the parameter estimation after the error correction[1]). However, if Alice and Bob are required to disclose a non-negligible number of data points of size k, during the parameter estimation, a classical data of size $N' = N - k$ is used for the key extraction. As a result, the final secure key rate is given by ℓ/N, where ℓ is given by Eq. (1), but now N in Eqs. (1) and (2) has to be replaced by N'.

Note that according to the approach introduced in Refs. [34,35], and numerically analyzed in Ref. [36], in order to analyze the composable finite-size security of the no-switching CV-QKD protocol against coherent attacks, the security of the protocol is first analyzed against Gaussian collective attacks with a security parameter ϵ [31], and then by applying the Gaussian de Finetti reduction [34] the security is obtained against coherent attacks with a polynomially larger security parameter $\tilde{\epsilon}$ [34], where the security loss due to the reduction from coherent attacks to collective attacks scales like $O(N^4)$ [34].

Note that if the security of two protocols are proven according to a composable security definition, then the security of the combination of these two protocols can be proved based on their individual functionalities. In fact, the security of the combination can be proved without the need for a separate security proof for the combined protocol. This is essential for the actual application of QKD since the secret key must be used in combination with the one-time pad protocol to achieve a secure communication [31,34].

[1]It has also been shown in Ref. [33] that in CV-QKD the whole raw keys can be used for both parameter estimation and secret key generation, without compromising the security, and without any requirements of doing error correction before parameter estimation.

IV. POSTSELECTION

A. Noiseless linear amplifier (quantum filter)

In contrast to classical optical channels, losses in quantum channels cannot be compensated for by usual deterministic phase-insensitive amplifiers, as the latter would inevitably introduce additional noise [37], making the quantum channel insecure. To avoid this noise penalty, the idea of heralded noiseless linear amplifier (NLA) was proposed in Ref. [18], which enables one to probabilistically amplify the amplitude of a coherent state without adding any extra noise. An NLA can be represented by the unbounded amplification operator $g^{\hat{n}}$ with the amplification gain $g > 1$ and the photon number operator $\hat{n}$, which realizes the following transformation on an input coherent state $|\alpha\rangle$ [18],

$$g^{\hat{n}}|\alpha\rangle = \exp\left[\tfrac{1}{2}(g^2-1)|\alpha|^2\right]|g\alpha\rangle. \quad (3)$$

For a Gaussian CV-QKD system it has been shown that the maximum transmission distance of the system can be increased by applying an ideal NLA on the received mode preceding Bob's detection [19]. Explicitly, in the equivalent entanglement-based scheme of the CV-QKD system Alice prepares a pure two-mode Gaussian entangled state, keeps one mode, while sending the second mode through an insecure quantum channel to Bob, who applies an NLA to noiselessly amplify the received mode, and distill the entanglement. Since the amplification is probabilistic, the successfully distilled entangled states are then used in an ordinary deterministic CV-QKD protocol, where Alice and Bob apply Gaussian measurements to their own shared modes.

An ideal NLA probabilistically converts a Gaussian state into another Gaussian state. The NLA distills the entanglement between Alice and Bob, hence effectively converts the initial channel into another channel with presumably higher associated performances. It has been shown in Ref. [19] that for an entanglement-based scheme with an initial pure entangled state with the two-mode squeezing parameter of χ, and a quantum channel with the transmissivity T and the excess noise ξ, the covariance matrix of the output amplified state is equal to the covariance matrix of an equivalent system with a two-mode squeezing parameter χ_g, sent through a channel of transmissivity T_g and excess noise ξ_g, without using the NLA. These effective parameters are given by [19]

$$\chi_g = \chi\sqrt{\frac{(g^2-1)(\xi-2)T-2}{(g^2-1)\xi T-2}}$$
$$T_g = \frac{g^2 T}{(g^2-1)T\left[\frac{1}{4}(g^2-1)(\xi-2)\xi T - \xi + 1\right] + 1}$$
$$\xi_g = \xi - \frac{1}{2}(g^2-1)(\xi-2)\xi T. \quad (4)$$

These effective parameters can be interpreted as physical parameters of an equivalent system if they satisfy the constraints $0 \leqslant \chi_g < 1$, $0 \leqslant T_g \leqslant 1$, and $\xi_g \geqslant 0$. Note that the first condition of Eq. (4) is always satisfied if χ is below a limit value [19]

$$0 \leqslant \chi_g < 1 \Rightarrow 0 \leqslant \chi < \left(\sqrt{\frac{(g^2-1)(\xi-2)T-2}{(g^2-1)\xi T-2}}\right)^{-1}. \tag{5}$$

Recall that Eq. (4) can only be utilized to calculate the covariance matrix of the output amplified state of an NLA, when the NLA can be ideally implemented to preserve the Gaussianity of the input state.

The improvement of the performance of Gaussian CV-QKD systems using an ideal NLA has been discussed for different protocols and in different scenarios [38–40]. However, in all of these works the success probability has been considered based on the theoretical predictions (which is much higher than the actual experimental success probability). Also, the use of quantum scissors as a practical candidate for an NLA has been investigated in CV-QKD systems [20,21,41,42]. Note that all of these works have focused on the CV-QKD performance in the asymptotic regime, which is an unrealistic scenario.

B. Measurement-based NLA (classical filter)

Since all optical implementations of NLA are extremely challenging, the method of Gaussian postselection or measurement-based NLA was proposed [22,23], and experimentally demonstrated [24], where the physical implementation of an NLA can be emulated with a suitable data processing. This represents a significant advantage as the difficulty of sophisticated physical operations can be moved from a hardware implementation to a software implementation. In particular, it has been shown in Refs. [23,24], when an NLA directly precedes a heterodyne detection, the NLA can be emulated by conditioning upon the heterodyne measurement outcome via a classical filter function. This means that in the no-switching CV-QKD system, the probabilistic noiseless amplification of the received signal before Bob's heterodyne detection can be emulated by the probabilistic postselection of Bob's heterodyne measurement data [23,24].

Considering the input state of an NLA as $\rho_{\rm in}$, the Husimi Q function of the amplified output state is given by

$$\begin{aligned} Q_{\rm out}(\alpha) &= \frac{1}{\pi}\langle\alpha|g^{\hat{n}}\rho_{\rm in}g^{\hat{n}}|\alpha\rangle \\ &= \exp[(g^2-1)|\alpha|^2]\frac{1}{\pi}\langle g\alpha|\rho_{\rm in}|g\alpha\rangle. \end{aligned} \tag{6}$$

Performing a change of variable, $\alpha_m = g\alpha$, we obtain

$$Q_{\rm out}(\alpha_m) = \exp\left[\left(1-\frac{1}{g^2}\right)|\alpha_m|^2\right]\frac{1}{\pi}\langle\alpha_m|\rho_{\rm in}|\alpha_m\rangle. \tag{7}$$

Having Eq. (7), we are able to determine the appropriate classical postselection filter to approximate an ideal NLA prior to a heterodyne detection.

Let us assume in the entanglement-based representation of the no-switching CV-QKD protocol, Alice and Bob share a mixed Gaussian entangled state ρ_{AB} [with a zero mean and covariance matrix $\mathbf{M} = [x\mathbf{I}_2, z\mathbf{Z}; z\mathbf{Z}, y\mathbf{I}_2]$ with $\mathbf{I}_2$ a 2×2 identity matrix, and $\mathbf{Z} = \mathrm{diag}(1,-1)$] before the detection. When Alice and Bob apply heterodyne detection to their own modes, obtaining the measurement values α_m and β_m, respectively, the joint probability distribution of the measurement outcomes is given by $Q_{\rm in}(\alpha_m, \beta_m)$, which is in fact the Husimi Q function of the mixed Gaussian entangled state ρ_{AB}. Note that the Husimi Q function of a Gaussian two-mode state with a zero mean and covariance matrix $\mathbf{M}$ can be expressed as [23],

$$\begin{aligned} Q_{\rm in}(\alpha_m, \beta_m) = \frac{\sqrt{\det(\mathbf{\Gamma})}}{\pi^2}\exp[-x'|\alpha_m|^2 - y'|\beta_m|^2 \\ - 2z'|\alpha_m||\beta_m|\cos(\phi_\alpha + \phi_\beta)], \end{aligned} \tag{8}$$

where $\mathbf{\Gamma} = [x'\mathbf{I}_2, z'\mathbf{Z}; z'\mathbf{Z}, y'\mathbf{I}_2] = 2(\mathbf{M}+\mathbf{I}_4)^{-1}$ with $\mathbf{I}_4$ a 4×4 identity matrix. Note that we have $\alpha_m = |\alpha_m|\exp(i\phi_\alpha)$ and $\beta_m = |\beta_m|\exp(i\phi_\beta)$.

Postselection in the CV-QKD protocol is performed by filtering of the raw key (i.e., the measurement outcomes) based on the value of the quadrature amplitudes detected by Bob. In fact, Bob applies a probabilistic filter to his measurement outcomes, β_m, to realize the prefactor, $\exp[(1-\frac{1}{g^2})|\beta_m|^2]$, in Eq. (7). Note that the filter is truncated by a real cutoff parameter γ_c to make the filter probability convergent. The filter function is [23–25]

$$F(\beta_m) = \begin{cases} \exp\left[\left(1-\frac{1}{g^2}\right)\left(|\beta_m|^2-\gamma_c^2\right)\right], & |\beta_m| < \gamma_c \\ 1, & |\beta_m| \geqslant \gamma_c \end{cases}, \tag{9}$$

where $\beta_m = b_q + ib_p$ is constructed from Bob's quadrature measurement outcomes b_q and b_p, and the first piece of $F(\beta_m)$ gives the acceptance probability, with which particular heterodyne measurement outcomes of Bob (outcomes with magnitude less than γ_c) are kept, while the others beyond the cutoff γ_c are kept with unity probability.

Considering $N_{\rm ps}$ as the number of accepted data points which are kept by Bob, and N is the total number of data points before the postselection, the success probability of the postselection is given by

$$\begin{aligned} P_s = \frac{N_{\rm ps}}{N} &= \int\int d^2\alpha_m \int\int d^2\beta_m \; F(\beta_m) Q_{\rm in}(\alpha_m, \beta_m) \\ &= \int_0^{2\pi}\int_0^{\infty} d\phi_\alpha d|\alpha_m| \int_0^{2\pi}\int_0^{\gamma_c} d\phi_\beta d|\beta_m| \\ &\quad \times \exp\left[\left(1-\frac{1}{g^2}\right)\left(|\beta_m|^2-\gamma_c^2\right)\right] Q_{\rm in}(\alpha_m, \beta_m)|\alpha_m||\beta_m| \\ &\quad + \int_0^{2\pi}\int_0^{\infty} d\phi_\alpha d|\alpha_m| \int_0^{2\pi}\int_{\gamma_c}^{\infty} d\phi_\beta d|\beta_m| \\ &\quad \times Q_{\rm in}(\alpha_m, \beta_m)|\alpha_m||\beta_m|. \end{aligned} \tag{10}$$

The final step to emulate an NLA is a linear rescaling on Bob's side that realizes $\beta_m = g\beta$. However, the rescaling is only applied to Bob's measurement outcomes with magnitude less than γ_c, while the others beyond the cutoff γ_c are kept unaffected. The final joint probability distribution of the mea-

surement outcomes after the rescaling is given by

$$Q_{\rm out}(\alpha,\beta) = \begin{cases} \frac{g^2}{P_s}\exp\left[\left(1-\frac{1}{g^2}\right)\left(|\beta_m|^2-\gamma_c^2\right)\right]Q_{\rm in}(\alpha_m,\beta_m), & |\beta_m|<\gamma_c \\ \frac{1}{P_s}Q_{\rm in}(\alpha_m,\beta_m), & |\beta_m|\geqslant\gamma_c \end{cases}, \tag{11}$$

where $\beta_m{=}g\beta$ for $|\beta_m|{<}\gamma_c$, and $\beta_m{=}\beta$ for $|\beta_m|{\geqslant}\gamma_c$, while Alice's measurement outcomes do not need rescaling, i.e., we always have $\alpha_m{=}\alpha$. Note that the Q function is normalized to unity, i.e., we require to have $\int\int d^2\alpha\int\int d^2\beta\ Q_{\rm out}(\alpha,\beta)=1$. The normalization requirement is realized by the multiplication factor $\frac{1}{P_s}$. Note also that for the first piece of $Q_{\rm out}(\alpha,\beta)$, the factor g^2 is further required for the normalization due to the linear rescaling.

Thus, in the postselection, Bob first applies the filter function, $\exp[(1-\frac{1}{g^2})(|\beta_m|^2-\gamma_c^2)]$, to his measurement outcomes β_m with magnitude less than γ_c, and then rescales his filtered outcomes such that $\beta_m=g\beta$, while his measurement outcomes beyond the cutoff γ_c are kept unaffected with unit probability. In the CV-QKD protocol with the postselection, for each measurement, Bob publicly reveals whether the outcome is kept or rejected, in order for Alice to keep or discard her corresponding measurement outcome. The filtered raw key of size $N_{\rm ps}$ is then treated as if it was the original raw key, which means the parameter estimation (to estimate the covariance matrix, $\mathbf{M}_{\rm ps}$, of the postselected state shared between Alice and Bob in the equivalent entanglement-based scheme) should be performed on the postselected data.

Having the final probability distribution of the postselected data, $Q_{\rm out}(\alpha,\beta)$, we are able to calculate the inferred covariance matrix of the amplified state before the heterodyne detection in the equivalent quantum-filter representation. The inferred covariance matrix $\mathbf{M}_{\rm ps}=[x_{\rm ps}\mathbf{I}_2, z_{\rm ps}\mathbf{Z}; z_{\rm ps}\mathbf{Z}, y_{\rm ps}\mathbf{I}_2]$ is given by

$$\begin{aligned} x_{\rm ps} &= \int\int d^2\alpha\int\int d^2\beta\ ([2{\rm Re}(\alpha)]^2-1)Q_{\rm out}(\alpha,\beta), \\ y_{\rm ps} &= \int\int d^2\alpha\int\int d^2\beta\ ([2{\rm Re}(\beta)]^2-1)Q_{\rm out}(\alpha,\beta), \\ z_{\rm ps} &= \int\int d^2\alpha\int\int d^2\beta\ (4{\rm Re}(\alpha){\rm Re}(\beta))Q_{\rm out}(\alpha,\beta). \end{aligned} \tag{12}$$

Note that in Eq. (12) only the second moment of Alice and Bob's quadratures has been calculated to compute the elements of the covariance matrix of the amplified state, since the first moment of Alice and Bob's quadratures remain zero after the postselection. The schematic of the postselection protocol in the entanglement-based representation has been shown in Fig. 1.

C. Security analysis for the postselection protocol

In the asymptotic security analysis of the CV-QKD system with the postselection (or the measurement-based NLA), the computed key rate must be multiplied by the success probability of the postselection, P_s, of Eq. (10). Explicitly, the asymptotic key rate of the postselection protocol, which is secure against Gaussian collective attacks in the reverse reconciliation scenario is given by $K_{\rm ps}=P_s[\beta I_{\rm ps}(a{:}b)-\chi_{\rm ps}(b{:}E)]$, where $I_{\rm ps}(a{:}b)$ is the classical mutual information between Alice and Bob following the postselection, and $\chi_{\rm ps}(b{:}E)$ is the Holevo bound, i.e., the upper bound on Eve's information on the postselected data (see Appendix A and Appendix B for the key-rate calculation).

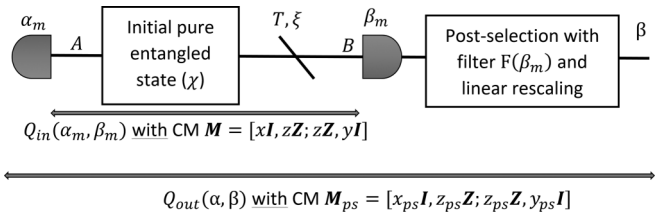

FIG. 1. The no-switching protocol with the postselection in the entanglement-based representation. Alice and Bob initially share a pure Gaussian entangled state with the squeezing parameter χ. The first mode A is kept by Alice for heterodyne detection to obtain the measurement value α_m. The second mode B is transmitted over the insecure channel, with parameters T and ξ, to Bob, who measures the received mode with heterodyne detection to obtain β_m. At this stage, the mixed entangled state shared between Alice and Bob is Gaussian, given with a covariance matrix $\mathbf{M}=[x\mathbf{I}_2, z\mathbf{Z}; z\mathbf{Z}, y\mathbf{I}_2]$, and the joint probability distribution of the measurement outcomes is given by $Q_{\rm in}(\alpha_m,\beta_m)$. Bob then applies the filter function, $F(\beta_m)$, to his measurement outcomes β_m with magnitude less than γ_c, and then rescales his filtered outcomes such that $\beta_m=g\beta$, while his measurement outcomes beyond the cutoff γ_c are kept unaffected with unit probability. Bob then publicly reveals whether the outcome is kept or rejected, in order for Alice to keep or discard her corresponding measurement outcome. The final probability distribution of the postselected data is now given by $Q_{\rm out}(\alpha,\beta)$, based on which we can calculate the inferred covariance matrix, $\mathbf{M}_{\rm ps}=[x_{\rm ps}\mathbf{I}_2, z_{\rm ps}\mathbf{Z}; z_{\rm ps}\mathbf{Z}, y_{\rm ps}\mathbf{I}_2]$, of the amplified state before the heterodyne detection in the equivalent quantum-filter representation.

In the finite-size security analysis of the CV-QKD protocol with the postselection, the size of the data contributing to the secret key is no longer N. In fact, only the accepted data of size $N_{\rm ps}=P_sN$ contributes to the final postselected key rate, hence, in order to compute the finite-size key length, the number N must be replaced by $N_{\rm ps}$. Explicitly, the finite-size key length of the postselection protocol, which is secure against Gaussian collective attacks in the reverse reconciliation scenario is given by

$$\ell_{\rm ps}\leqslant N_{\rm ps}[\beta I_{\rm ps}(a{:}b)-\chi_{\rm ps}(b{:}E)]-\sqrt{N_{\rm ps}}\Delta_{\rm ps}-2\log_2\left(\frac{1}{2\bar{\epsilon}}\right), \tag{13}$$

where $\Delta_{\rm ps}$ is calculated using Eq. (2) with N being replaced by $N_{\rm ps}$. Hence, the finite-size key rate of the postselection protocol is given by $K_{\rm ps}^{\rm FS}=\ell_{\rm ps}/N$ or

$$K_{\rm ps}^{\rm FS}\leqslant P_s[\beta I_{\rm ps}(a{:}b)-\chi_{\rm ps}(b{:}E)]-\sqrt{\frac{P_s}{N}}\Delta_{\rm ps} -\frac{2}{N}\log_2\left(\frac{1}{2\bar{\epsilon}}\right). \tag{14}$$

Note that in contrast to the asymptotic regime, the success probability of the postselection does not affect the finite-size key rate as only a proportional factor. Note also that in Eq. (13) we have again assumed almost the whole raw key of size $N_{\rm ps}$ after the postselection can be used for secret key generation.

However, if the data points of size k are disclosed after the postselection for the parameter estimation, a classical data of size $N'_{\rm ps} = N_{\rm ps} - k$ is used for the key extraction. In this case, the finite-size key rate is given by $\ell_{\rm ps}/N$, where $\ell_{\rm ps}$ is given by Eq. (13), but now $N_{\rm ps}$ in Eq. (13) has to be replaced by $N'_{\rm ps}$.

Note that in the entanglement-based representation of the no-switching protocol, which is used for the security analysis, the postselection protocol can be equivalently considered as a protocol without postselection, but with effective parameters for the initial entanglement and effective parameters for the channel. In this equivalent protocol without postselection Eve's Holevo information is obtained by holding a purification of Alice and Bob's effective system [22–24]. Also, given that the joint state of Alice, Bob, and Eve is pure before the postselection, and since the postselection is just a projective measurement, by definition, it cannot decrease the purity of the joint state [22]. Thus, Eve's Holevo information can be upper bounded based on the covariance matrix of the postselected data.

Note that for the no-switching protocol with the postselection we can still use the Gaussian de Finetti reduction of Ref. [34], to reduce coherent attacks to Gaussian collective attacks in the security analysis, since the postselection protocol in the entanglement-based representation is equivalent with an entanglement-based protocol without postselection with effective parameters for the initial entanglement, and effective parameters for the channel. This effective protocol with heterodyne detection by both Alice and Bob commutes with the action of the unitary group [34,35]. Thus, the Gaussian de Finetti reduction can be used for the security analysis of the equivalent protocol.

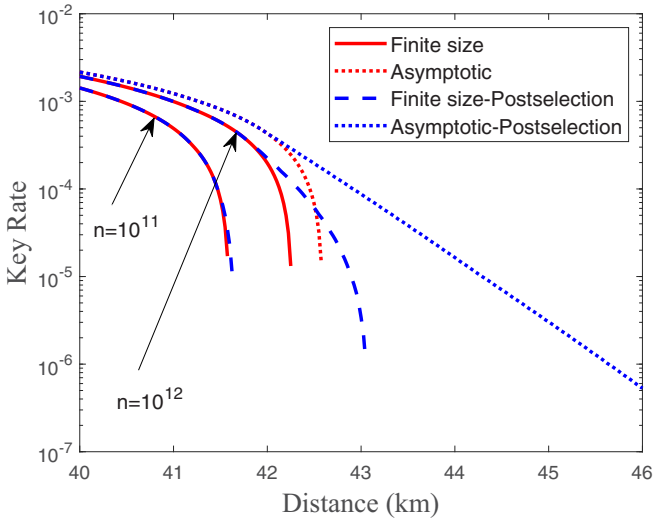

FIG. 2. The achievable secret key rate from reverse reconciliation as a function of channel distance (km) in the no-switching CV-QKD protocol over a lossy channel with $\xi = 0.1$ and with 0.2 dB losses per km, without the postselection (red lines) and with the Gaussian postselection, where $\gamma_c = 3g\sqrt{V_B}$ (blue lines) for the asymptotic and finite-size regime ($n = 10^{11}$ and $n = 10^{12}$) with the discretization parameter of $d = 5$ and $\beta = 0.95$. The modulation variance (or the squeezing parameter χ) and the gain g are optimised to maximize the key rate.

V. NUMERICAL RESULTS

A. Gaussian postselection

In the postselection scheme, when the cutoff γ_c is chosen sufficiently large such that the cutoff circle can embrace the amplified distribution, we can assume the distribution of the postselected data remains statistically Gaussian, and the postselection approximates an ideal NLA (which probabilistically converts a Gaussian state into another Gaussian state) [23,24]. Therefore, in the CV-QKD protocol with the Gaussian postselection, the security can be analyzed based on the equivalent scheme, where the classical filter is replaced with a quantum filter (or an ideal NLA) before Bob's heterodyne detection (as it has been analyzed in Ref. [23]), and the covariance matrix of the amplified state shared between Alice and Bob in the equivalent entanglement-based scheme can be calculated using the covariance matrix of the equivalent system with the effective parameters χ_g, T_g, ξ_g without the postselection. Note that the covariance matrix calculated based on the effective parameters χ_g, T_g, ξ_g of Eq. (4) is the same as the covariance matrix $\mathbf{M}_{\rm ps}$ of Eq. (12) when the cutoff γ_c is chosen sufficiently large.

Now we numerically simulate the effect of the Gaussian postselection on the performance of the CV-QKD protocol in the finite-size regime. In this work, we always consider a lossy quantum channel with 0.2 dB losses per kilometer, and the security parameter $\epsilon = 10^{-6}$. We consider different values of block size, $n = 10^{11}$ and $n = 10^{12}$. Note that the modulation variance (or the squeezing parameter χ in the equivalent entanglement-based scheme) and the gain g are optimized to maximize the key rate (see Fig. 7 in Appendix C). We also choose a sufficiently large cutoff, $\gamma_c = 3g\sqrt{V_B}$ (with V_B the quadrature variance of Bob's measurement outcome before the detection and postselection) to be able to assume the postselected state remains Gaussian. The measure we have used to make sure the chosen cutoff is sufficiently large is the elements of the covariance matrix. More precisely, for a chosen cutoff we calculate the covariance matrix using two approaches, the covariance matrix resulted from an ideal NLA, calculated based on the effective parameters χ_g, T_g, ξ_g of Eq. (4), and the covariance matrix resulted from the postselection, $\mathbf{M}_{\rm ps}$, calculated from Eq. (12) through the use of Q function. In our numerical simulations we found that by choosing $\gamma_c \geqslant 3g\sqrt{V_B}$ [25], the two approaches lead to the same elements for the covariance matrix (the difference is less than 0.01%), which means the chosen cutoff is large enough for the postselection to emulate an ideal NLA. Also note that if we consider $Q_{\rm in}(\beta_m)$ as the Q function of Bob's measurement outcome, the filtered data (before the linear rescaling) $F(\beta_m)Q_{\rm in}(\beta_m)$ is expected to have a distribution with variance g^2V_B, then one can choose the cutoff γ_c equal to a few standard deviations, i.e., $\gamma_c = rg\sqrt{V_B}$. Larger r decreases the success probability, while it results in a better approximation of an ideal NLA. Hence, a compromise should be made between the success probability and the fidelity with respect to an ideal NLA. Here, we choose $r = 3$ so that 99.7% of the amplified distribution lies within the cutoff circle [25].

In Fig. 2 the achievable secret key rate secure against Gaussian collective attacks is shown as a function of channel distance (km) without the postselection and with the Gaussian postselection for both the asymptotic and realistic finite-size regime ($n = 10^{11}$ and $n = 10^{12}$), and for the realistic reconciliation efficiency of $\beta = 0.95$ [43].

We can see from Fig. 2 that the Gaussian postselection (blue lines) can be useful when the protocol is operating close to its limit, i.e., in the waterfall region of the key rate versus distance graph, where modest increases in the correlation between Alice and Bob due to the postselection (or virtual amplification) can compensate for the sacrificed raw key, allowing the recovery of a secure key distribution from an initially insecure situation. According to Fig. 2, the Gaussian postselection is able to effectively extend the maximum transmission distance of the CV-QKD protocol in the unrealistic asymptotic regime as it has been previously illustrated in Refs. [23,24]. However, in the finite-size regime when the block size is reduced, the improvement of the maximum transmission distance due to the Gaussian postselection decreases, because increases in the correlation cannot compensate for the scarified raw key. In fact, in the finite-size regime, the improvement of maximum transmission distance due to the Gaussian postselection can only appear when the block size is sufficiently large (larger than $n = 10^{11}$ for the given parameters of Fig. 2), and the amount of such an improvement increases with increasing the block size. Note that in Fig. 2 we have considered a high-noise channel with $\xi = 0.1$. We have also performed a further numerical simulation for a lower-noise channel with $\xi = 0.05$ (with the other parameters the same as Fig. 2). In this case the maximum transmission distance of the protocol is 137.7 km, which can be improved by the Gaussian postselection for the block sizes larger than $n = 10^{15}$. Since we are more interested in a realistic finite-size regime with the block size in the range of $n = 10^8$–10^{12} [43–46], we will consider a higher-noise channel for the rest of our numerical results.

Note that in Fig. 2, we have considered the cutoff as $\gamma_c = 3g\sqrt{V_B}$, so that we can assume the postselected data has a Gaussian distribution, which can emulate an ideal NLA. However, if we choose higher values for the cutoff, the postselection provides a better estimation of the NLA, at the expense of lower success probability. As a result, a larger block size will be required for the CV-QKD performance to be improved by the Gaussian postselection.

B. Non-Gaussian postselection

In the measurement-based NLA the choice of the filter cutoff, γ_c, is critical. Larger cutoff will improve the approximation of the ideal NLA, however, a cutoff that is too high will unnecessarily sacrifice raw data, and decrease the success probability. On the other hand, a cutoff that is too low will increase the success probability, at the expense of reducing the mutual information between Alice and Bob. According to our numerical results for the Gaussian postselection, the success probability plays a significant role in the finite-size security analysis, since the success probability determines the size of data, which contributes to the postselected key. In this section we investigate whether a reduction of the postselection cutoff (which will increase the success probability) improves the postselection performance in the finite-size regime.

When the filter cutoff decreases from $\gamma_c = 3g\sqrt{V_B}$, the statistics of the postselected data start changing from Gaussian to non-Gaussian. However, based on the optimality of Gaussian attacks [28–30], for all bipartite quantum states ρ_{AB} with covariance matrix $\mathbf{M}_{AB}$, one can maximize Eve's information by considering ρ_{AB}^{G}, which is the Gaussian state having the same covariance matrix $\mathbf{M}_{AB}$. Hence, in order to analyze the security of the protocol in the non-Gaussian regime, we only require to calculate the covariance matrix of the non-Gaussian amplified state. Note that when the postselection is in the non-Gaussian regime, we cannot use Eq. (4) anymore to calculate the covariance matrix of the amplified state. Instead, we have to use the Q function of the postselected state, i.e., Eq. (12) to calculate the covariance matrix of the amplified state, and compute a lower bound on the postselected key rate. Note also that the technique of the measurement-based NLA with an entangled-state input has always been investigated in the Gaussian regime, where the filter cutoff is sufficiently large [23,24]. However, here we investigate the characterization of the measurement-based NLA with an entangled-state input in the non-Gaussian regime by decreasing the filter cutoff, and the impact this cutoff reduction can have on the related CV-QKD performance.

Let us consider a quantum channel equivalent with an optical fiber of 43 km, which, according to Fig. 2, is almost the maximum transmission distance of the CV-QKD system with the optimized Gaussian postselection, where we have the excess noise of $\xi = 0.1$, $\beta = 0.95$, and the block size of $n = 10^{12}$. For this channel the optimized Gaussian postselection (with $\gamma_c = 3g\sqrt{V_B}$) generates the finite-size key rate of $K_{\mathrm{ps}}^{\mathrm{FS}} = 3.4 \times 10^{-6}$ (in bits per mode). For this quantum channel we now investigate the effects a decrease in the postselection cutoff, γ_c, can have on the CV-QKD performance.

In Fig. 3, the three top plots show the elements of the covariance matrix, $\mathbf{M}_{\mathrm{ps}}$, of the amplified state [i.e., x_{ps}, y_{ps}, and z_{ps} in Eq. (12)] as a function of the postselection cutoff γ_c. As it can be seen, for $\gamma_c \geqslant 3g\sqrt{V_B} = 4.26$, the postselected state can be assumed to be Gaussian, as the elements of the covariance matrix $\mathbf{M}_{\mathrm{ps}}$ remain almost constant and equal to the covariance matrix elements of the amplified state resulted from an ideal NLA [calculated based on Eq. (4)]. We can see the covariance matrix elements of the amplified state decrease as the cutoff is reduced. As a result, the classical mutual information between Alice and Bob, $I_{\mathrm{ps}}(a{:}b)$, as well as Eve's information, i.e., the Holevo bound, $\chi_{\mathrm{ps}}(b{:}E)$ (with both being calculated based on the covariance matrix $\mathbf{M}_{\mathrm{ps}}$) decrease with the cutoff reducing (shown in the two bottom plots of Fig. 3). Although the raw key-rate term, $\beta I_{\mathrm{ps}}(a{:}b) - \chi_{\mathrm{ps}}(b{:}E)$, also drops with the decrease in the cutoff, the success probability of the postselection, P_s, exponentially increases with the cutoff decreasing according to the left plot of Fig. 4. As a result, both the asymptotic and finite-size key rates first increase with the cutoff decreasing up to an optimized value, and then decrease until they disappear (see Fig. 4, right plot). Therefore, our results show that there is an optimal value for the cutoff in the non-Gaussian regime, which maximizes the key rate. According to Fig. 4, the finite-size key rate can be

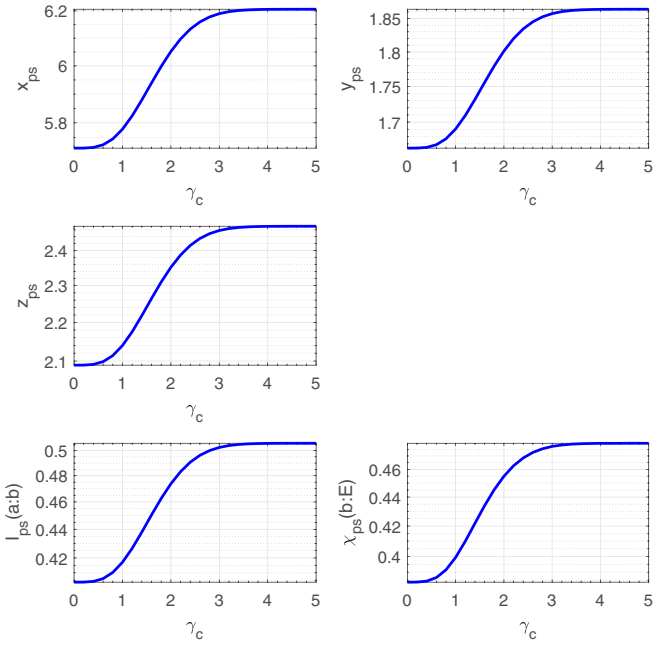

FIG. 3. The elements of the covariance matrix, $\mathbf{M}_{\rm ps}$, of the postselected state, (i.e., $x_{\rm ps}$, $y_{\rm ps}$, and $z_{\rm ps}$), the classical mutual information between Alice and Bob, $I_{\rm ps}(a{:}b)$, and Eve's information from reverse reconciliation (i.e., the Holevo bound), $\chi_{\rm ps}(b{:}E)$ as a function of the filter cutoff γ_c for a quantum channel equivalent with an optical fiber of 43 km, $\xi = 0.1$, $\beta = 0.95$, $\chi = 0.8379$, $g = 1.1$, and the block size of $n = 10^{12}$.

improved up to $K_{\rm ps}^{\rm FS} = 4.3 \times 10^{-5}$ (i.e., an improvement of more than one order of magnitude) by decreasing the cutoff from Gaussian regime to non-Gaussian regime, i.e., from $\gamma_c = 3g\sqrt{V_B} = 4.26$ to $\gamma_c = 3.4$. Note that in Figs. 3 and 4, for $\gamma_c \geqslant 3g\sqrt{V_B}$, the postselected state remains almost Gaussian and the postselection can emulate an ideal NLA, while $\gamma_c = 0$ corresponding to no postselection.

In principle, having the transmissivity and excess noise of the channel (which can be estimated by performing parameter estimation over the whole ensemble before the postselection), the optimal values of gain and cutoff can theoretically been

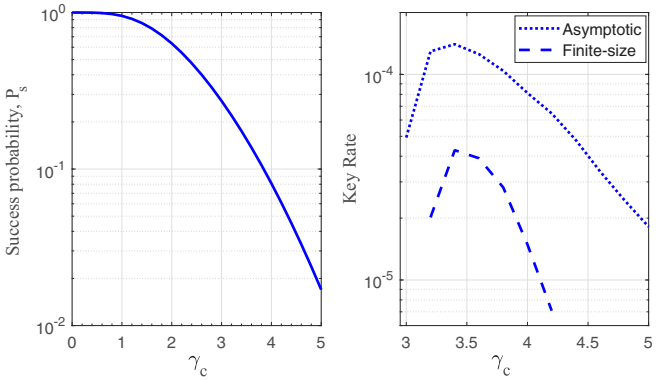

FIG. 4. The postselection success probability, P_s, and the finite-size and asymptotic key rate from reverse reconciliation as a function of the filter cutoff γ_c for a quantum channel and the protocol with the same parameters as Fig. 3.

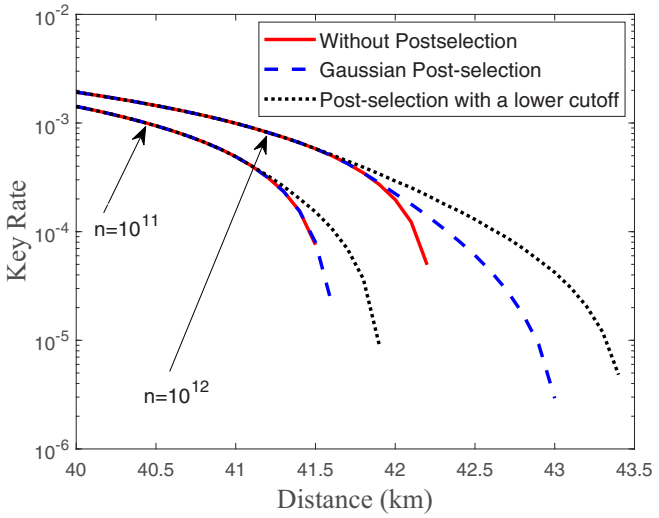

FIG. 5. The achievable secret key rate from reverse reconciliation as a function of channel distance (km) in the CV-QKD protocol over a lossy channel with $\xi = 0.1$ and with 0.2 dB losses per km, without postselection (red lines), with the Gaussian postselection, i.e., $\gamma_c = 3g\sqrt{V_B}$ (blue lines), and with the non-Gaussian postselection, i.e., choosing a lower cutoff $\gamma_c = 2.5g\sqrt{V_B}$ (black lines) for the finite-size regime ($n = 10^{11}$ and $n = 10^{12}$) with $\beta = 0.95$.

chosen to maximize the key rate. Note that the cutoff should be chosen depending on the variance of Bob's measurement results (which is also a function of the initial squeezing and the channel parameters), and the gain of the postselection filter (i.e., $\gamma_c = rg\sqrt{V_B}$). Increasing the gain and increasing the cutoff both increase the correlation between Alice and Bob on the postselected ensemble, at the expense of decreasing the success probability. While, decreasing the gain and decreasing the cutoff both decrease the correlation between Alice and Bob, at the advantage of higher success probability.

Note that the lower bound on the key rate, which we calculate for the postselection in the non-Gaussian regime is not tight, and it could likely be improved using the numerical approach of Ref. [47]. The bound is loose because it relies on Gaussian optimality proof [28–30], which means that $\chi_{\rm ps}(b{:}E)$ is computed for the Gaussian state with the same covariance matrix as the non-Gaussian amplified state, and $\chi_{\rm ps}(b{:}E)$ is therefore overestimated.

Now we repeat our numerical simulations for the postselection in Fig. 2, with a lower cutoff, $\gamma_c = 2.5g\sqrt{V_B}$, and compute the postselected finite-size key rate, with the results shown in Fig. 5. We can see that decreasing the cutoff from $\gamma_c = 3g\sqrt{V_B}$ to $\gamma_c = 2.5g\sqrt{V_B}$ has a positive impact on the CV-QKD performance, including the improvement of the finite-size key rate by up to an order of magnitude at the maximum transmission distance of the protocol, as well as the extension of the transmission distance up to a half kilometer. We can see that for $n = 10^{12}$ by decreasing the cutoff from $\gamma_c = 3g\sqrt{V_B}$ to $\gamma_c = 2.5g\sqrt{V_B}$ the improvement of the transmission distance due to the postselection increases. Furthermore, we can see that while for $n = 10^{11}$ there is no improvement in the transmission distance due to the postselection with $\gamma_c = 3g\sqrt{V_B}$, the transmission distance can be improved by decreasing the cutoff to $\gamma_c = 2.5g\sqrt{V_B}$. Recall

again that here in our numerical simulations for $\gamma_c = 2.5g\sqrt{V_B}$ the postselected state is not Gaussian (although it is close to the Gaussian regime), hence we use the output Q function, $Q_{\text{out}(\alpha,\beta)}$, to calculate the elements of the covariance matrix of the postselected state, $\mathbf{M}_{\text{ps}}$. Our results show the importance of the proper choice of the postselection cutoff in the CV-QKD system.

Additional calculations beyond those illustrated here have been carried out covering direct reconciliation, which results in similar trends to those indicated here. However, direct reconciliation is only successful when the channel loss is below 3 dB. In the direct reconciliation, Eve's information should be calculated based on the mutual information between Alice and Eve, i.e., $\chi_{\text{ps}}(a{:}E)$. For the numerical simulations of the direct reconciliation see Appendix D.

According to the numerical results the Gaussian postselection is not useful for extending the secure range of the protocol for data blocks of size 10^6–10^9 (as used in past CV-QKD experiments [43,44]) due to its small success probability, P_s. However, having sufficiently large data blocks of size 10^{10}–10^{12} (as used in recent CV-QKD experiments [45,46]), and optimally choosing the cutoff in the non-Gaussian regime (which increases P_s) allows a small fraction of the asymptotic improvement to be achieved, given current security-proof techniques. This small improvement might be useful for direct reconciliation protocols, where the secure distance of the protocol is limited to only few kilometers (see Fig. 8 in Appendix D).

Note that for both physical and measurement-based NLAs, there is a tradeoff between the success probability and the faithfulness with which an ideal NLA can be emulated. However, the tradeoff is not identical, since the cutoff is in photon number for a physical NLA, and in heterodyne amplitude for a measurement-based NLA [25]. In principle, using a physical NLA with higher success probability, such as a single quantum scissor [18,20,21] (where it can act as an ideal NLA in the regime of small χ and high loss) could be advantageous (over measurement-based NLA) in extending the transmission range of the finite-size CV-QKD protocol. However, the downside is that a physical NLA introduces experimentally demanding single-photon resources to CV-QKD systems. We should also note that because there is no free-propagating mode after the postselection, measurement-based NLA protocols cannot be used in CV quantum repeater setups such as Ref. [48]. As a result, CV repeater setups require a physical NLA.

C. Parameter estimation in the postselection protocol

Note that the no-switching CV-QKD protocol is experimentally implemented in the prepare-and-measure (PM) scheme, where for the postselection the classical filter is applied on Bob's heterodyne detection results, while for the security analysis we need to know the covariance matrix, $\mathbf{M}_{\text{ps}}$, of the amplified (or postselected) state shared between Alice and Bob in the equivalent entanglement-based (EB) scheme.

In the case of Gaussian postselection, we can consider a normal linear model for Alice and Bob's postselected variables in the PM scheme, $x_{\text{ps}}^{\text{PM}}$ and $y_{\text{ps}}^{\text{PM}}$, respectively, as $y_{\text{ps}}^{\text{PM}} = t_g x_{\text{ps}}^{\text{PM}} + z_{\text{ps}}^{\text{PM}}$, where $t_g = \sqrt{\frac{T_g}{2}}$, and $z_{\text{ps}}^{\text{PM}}$ follows a centered normal distribution with unknown variance $\sigma_g^2 = 1 + \frac{1}{2}T_g\xi_g$ (note that Alice's variable $x_{\text{ps}}^{\text{PM}}$ has the variance V_A^g). The maximum-likelihood estimators for the effective parameters, t_g, σ_g^2, and V_A^g are given by [49,50]

$$\begin{aligned}\hat{t}_g &= \frac{\sum_{i=1}^{k} x_i y_i}{\sum_{i=1}^{k} x_i^2},\\ \hat{\sigma}_g^2 &= \frac{1}{k}\sum_{i=1}^{k}(y_i - \hat{t}_g x_i)^2,\\ \hat{V}_A^g &= \frac{1}{k}\sum_{i=1}^{k} x_i^2,\end{aligned} \tag{15}$$

with the uncertainty in the effective parameters expressed as [49,50]

$$\begin{aligned}\Delta(t_g) &= z_{\epsilon_{\text{PE}}/2}\sqrt{\frac{\hat{\sigma}_g^2}{\sum_{i=1}^{k} x_i^2}},\\ \Delta\left(\sigma_g^2\right) &= z_{\epsilon_{\text{PE}}/2}\frac{\hat{\sigma}_g^2\sqrt{2}}{\sqrt{k}},\\ \Delta\left(V_A^g\right) &= z_{\epsilon_{\text{PE}}/2}\frac{\hat{V}_A^g\sqrt{2}}{\sqrt{k}},\end{aligned} \tag{16}$$

where x_i and y_i are the realizations of $x_{\text{ps}}^{\text{PM}}$ and $y_{\text{ps}}^{\text{PM}}$, respectively, and k is the number of data points randomly chosen from the postselected data for the parameter estimation.[2] As a result, the covariance matrix, $\mathbf{M}_{\text{ps}}$, of the amplified state shared between Alice and Bob in the EB scheme, which maximizes Eve's information [49] is given by $\hat{\mathbf{M}}_{\text{ps}} = [\hat{x}_{\text{ps}}\mathbf{I}_2, \hat{z}_{\text{ps}}\mathbf{Z}; \hat{z}_{\text{ps}}\mathbf{Z}, \hat{y}_{\text{ps}}\mathbf{I}_2]$, where

$$\begin{aligned}\hat{x}_{\text{ps}} &= V_{A,\max}^g + 1,\\ \hat{y}_{\text{ps}} &= 2\left(t_{g,\min}^2 V_{A,\max}^g + \sigma_{g,\max}^2\right) - 1,\\ \hat{z}_{\text{ps}} &= \sqrt{2}\,t_{g,\min}\sqrt{{V_{A,\max}^g}^2 + 2V_{A,\max}^g},\end{aligned} \tag{17}$$

and where

$$\begin{aligned}t_{g,\min} &= \hat{t}_g - \Delta(t_g)\\ \sigma_{g,\max}^2 &= \hat{\sigma}_g^2 + \Delta\left(\sigma_g^2\right),\\ V_{A,\max}^g &= \hat{V}_A^g + \Delta\left(V_A^g\right).\end{aligned} \tag{18}$$

However, in the case of non-Gaussian postselection, the relation between the cross-correlation term, z_{ps}, of the covariance matrix $\mathbf{M}_{\text{ps}}$ in the EB scheme is not directly related to the cross-correlation term of the data observed by Alice and Bob in the PM scheme, i.e., $\frac{1}{k}\sum_{i=1}^{k} x_i y_i$. Hence, instead of calculating $\mathbf{M}_{\text{ps}}$ from the data observed in the PM scheme, Alice and Bob can first reconstruct the equivalent data in the EB scheme based on the whole data from the PM scheme preceding the postselection. Considering Alice

[2]Note that $z_{\epsilon_{\text{PE}}/2}$ is such that $1 - \text{erf}(\frac{z_{\epsilon_{\text{PE}}/2}}{\sqrt{2}})/2 = \epsilon_{\text{PE}}/2$.

and Bob's variables in the PM scheme preceding the postselection as x^{PM} and y^{PM}, Alice and Bob's variables in the equivalent EB scheme preceding the postselection would be $x^{\mathrm{EB}} = \frac{\sqrt{V_A+2}}{\sqrt{2V_A}} x^{\mathrm{PM}}$ and $y^{\mathrm{EB}} = y^{\mathrm{PM}}$, with V_A is the initial modulation variance in the PM scheme preceding the postselection. Next, Bob applies the classical filter on his data and publicly reveals whether the data is kept or rejected. Finally, Alice and Bob perform parameter estimation over a randomly chosen subset (of size k) of their postselected data, $x_{\mathrm{ps}}^{\mathrm{EB}}$ as $y_{\mathrm{ps}}^{\mathrm{EB}}$, to directly estimate $\mathbf{M}_{\mathrm{ps}}$ via $\frac{1}{k}\sum_{i=1}^{k} x_i'^2$, $\frac{1}{k}\sum_{i=1}^{k} y_i'^2$, and $\frac{1}{k}\sum_{i=1}^{k} x_i' y_i'$, where x_i' and y_i' are the realizations of $x_{\mathrm{ps}}^{\mathrm{EB}}$ and $y_{\mathrm{ps}}^{\mathrm{EB}}$, respectively.

Note that an appropriate way to determine the optimized filter function (i.e., the optimized values of g and γ_c) in an experiment, is to perform parameter estimation over the whole ensemble before the postselection to estimate the parameters of the channel, based on which Alice and Bob can theoretically determine what would be the optimized values for the gain and cutoff.

VI. CONCLUSIONS

In this work we have investigated the impact postselection or measurement-based NLA can have on the performance of the no-switching CV-QKD protocol (when it is applied to the outcome of Bob's heterodyne detection) in the composable finite-size regime. We illustrated that the Gaussian postselection (with a sufficiently large cutoff in the heterodyne amplitude that can emulate an ideal NLA) can extend the maximum transmission distance of the CV-QKD protocol in the finite-size regime providing the finite block size is sufficiently large (10^{10}–10^{12}). We found Gaussian postselection offers a relatively modest improvement in the finite-size regime in comparison with improvement predicted by an asymptotic analysis. Further, we analyzed the performance of the measurement-based NLA on the entangled-state input in the non-Gaussian regime by decreasing the postselection cutoff (which increases the success probability at the expense of reducing the fidelity with respect to an ideal NLA), thereby illustrating that there is an optimal value for the postselection cutoff in the non-Gaussian regime that optimizes the CV-QKD performance in terms of both the finite key rate and transmission range. Future work could investigate numerical key estimation approaches such as in Ref. [47], which may lead to tighter bounds in the non-Gaussian regime. Techniques that provide tighter bounds for non-Gaussian statistics would therefore result in a smaller value for the optimal cutoff, which, given the exponential improvement in the fraction of data kept, could significantly improve the key rates.

ACKNOWLEDGMENTS

The authors acknowledge valuable discussions with Austin Lund. This research was supported by funding from the Australian Department of Defence. This research is also supported by the Australian Research Council (ARC) under the Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE170100012). N.W. acknowledges funding support from the European Unions Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement No. 750905 and Q.Link.X from the BMBF in Germany.

APPENDIX A: CALCULATION OF MUTUAL INFORMATION AND HOLEVO BOUND

In the entanglement-based scheme of the no-switching CV-QKD protocol, Alice generates a pure two-mode Gaussian entangled state, i.e., a two-mode squeezed vacuum state with the quadrature variance V. Alice keeps the first mode and transmits the second mode through a quantum channel with transmissivity T and excess noise ξ. The covariance matrix of the mixed state ρ_{AB} at the output of the channel before the detection is given by

$$\mathbf{M} = \begin{bmatrix} V\,\mathbf{I}_2 & \sqrt{T}\sqrt{V^2-1}\,\mathbf{Z} \\ \sqrt{T}\sqrt{V^2-1}\,\mathbf{Z} & (T(V+\chi_{\mathrm{line}}))\,\mathbf{I}_2 \end{bmatrix}, \tag{A1}$$

where $\chi_{\mathrm{line}} = \xi + \frac{1}{T} - 1$. Having the covariance matrix $\mathbf{M}$, we are able to compute the Q function, $Q_{\mathrm{in}}(\alpha_m, \beta_m)$, of the state shared between Alice and Bob preceding the postselection using Eq. (8). Then, following Eqs. (10) and (11) we can compute the postselection success probability P_s as well as the Q function, $Q_{\mathrm{out}}(\alpha, \beta)$, of the postselected state, from which we can compute the inferred covariance matrix, $\mathbf{M}_{\mathrm{ps}}$, of the amplified state using Eq. (12).

Following the postselection, the mutual information between Alice and Bob, $I_{\mathrm{ps}}(a{:}b)$, can be calculated as (see Appendix B for the actual mutual information)

$$I_{\mathrm{ps}}(a{:}b) = \log_2 \frac{x_{\mathrm{ps}}+1}{x_{\mathrm{ps}}+1-\frac{z_{\mathrm{ps}}^2}{y_{\mathrm{ps}}+1}}. \tag{A2}$$

In the collective attack, the Holevo mutual information $\chi(b{:}E)$ is given by $\chi(b{:}E) = S(\rho_E) - S(\rho_{E|b})$, where $S(\rho)$ is the von Neumann entropy of the state ρ. Note that $S(\rho_E)$ is given by the von Neumann entropy of the amplified state, which can be calculated through the symplectic eigenvalues $\lambda_{1,2}$ of covariance matrix $\mathbf{M}_{\mathrm{ps}}$[3]. The second entropy $S(\rho_{E|b})$ is given by the von Neumann entropy of Alice's state conditioned on Bob's detection, which can be calculated through the symplectic eigenvalue of the covariance matrix of the conditional state $\mathbf{M}_{A|b} = \mathbf{A}_{\mathrm{ps}} - \mathbf{C}_{\mathrm{ps}}\,(\mathbf{B}_{\mathrm{ps}} + \mathbf{I}_2)^{-1}\,\mathbf{C}_{\mathrm{ps}}^T$, where $\mathbf{A}_{\mathrm{ps}} = x_{\mathrm{ps}}\mathbf{I}_2$, $\mathbf{B}_{\mathrm{ps}} = y_{\mathrm{ps}}\mathbf{I}_2$, and $\mathbf{C}_{\mathrm{ps}} = z_{\mathrm{ps}}\mathbf{Z}$.

APPENDIX B: ACTUAL MUTUAL INFORMATION

In the case of Gaussian postselection, when the postselected state has Gaussian statistics, the actual mutual information between Alice and Bob can be calculated using the covariance matrix, $\mathbf{M}_{\mathrm{ps}}$, of the amplified (or postselected) state via Eq. (A2). However, in the case of non-Gaussian

[3]The von Neumann entropy of an n-mode Gaussian state ρ with the covariance matrix $\mathbf{M}$ is given by $S(\rho) = \sum_{i=1}^{n} G(\frac{\lambda_i - 1}{2})$, where λ_i are the symplectic eigenvalues of the covariance matrix $\mathbf{M}$, and $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$.

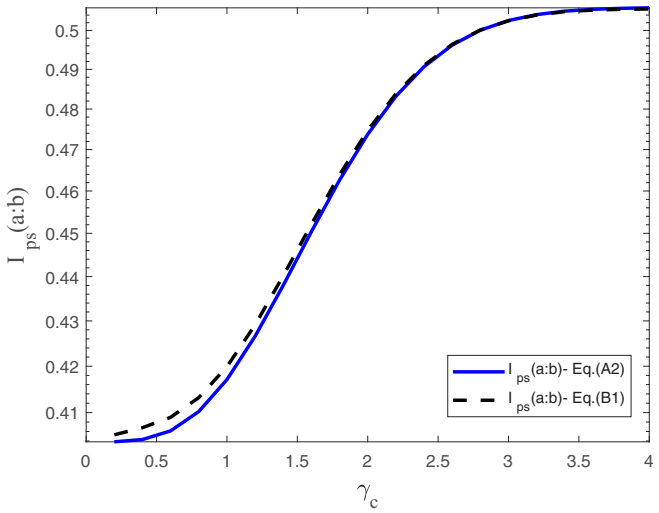

FIG. 6. The classical mutual information between Alice and Bob following the postselection, $I_{\rm ps}(a{:}b)$, using the covariance matrix, $\mathbf{M}_{\rm ps}$, of the amplified state via Eq. (A2) (solid line), and using the Q function of the postselected state via Eq. (B1) (dashed line), as a function of the filter cutoff γ_c for a quantum channel equivalent with an optical fiber of 43 km, $\xi = 0.1$, $\chi = 0.8379$, $g = 1.1$.

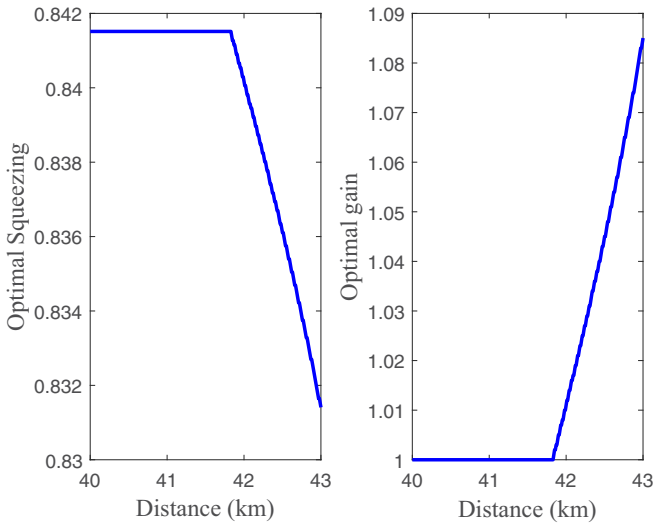

FIG. 7. The optimal value of the initial squeezing χ and the optimal value of gain g to maximize the finite-size key rate for the Gaussian postselection protocol with $n = 10^{12}$, $\xi = 0.1$, $\beta = 0.95$, and for the range of distance that the postselection is effective.

postselection, when the postselected state has non-Gaussian statistics, the actual mutual information can be calculated using

$$I_{\rm ps}(a{:}b) = H_{\rm ps}(a) + H_{\rm ps}(b) - H_{\rm ps}(a,b), \tag{B1}$$

where $H_{\rm ps}(a)$ is the Shannon entropy of Alice's classical variable (or Alice's heterodyne-measurement result in the entanglement-based scheme) following the postselection, $H_{\rm ps}(b)$ is the Shannon entropy of Bob's heterodyne-measurement result following the postselection, and $H_{\rm ps}(a,b)$ is the joint entropy of Alice and Bob's classical variables following the postselection. In Eq. (B1), $H_{\rm ps}(a,b)$ is calculated as

$$H_{\rm ps}(a,b) = -\int\int d^2\alpha \int\int d^2\beta \; Q_{\rm out}(\alpha,\beta)\log_2[Q_{\rm out}(\alpha,\beta)], \tag{B2}$$

where $Q_{\rm out}(\alpha,\beta)$ is the Q function of the postselected state given by Eq. (11). In Eq. (B1), $H_{\rm ps}(b)$ is calculated as

$$H_{\rm ps}(b) = -\int\int d^2\beta \; Q_{\rm out}(\beta)\log_2[Q_{\rm out}(\beta)], \tag{B3}$$

where $Q_{\rm out}(\beta)$ is the Q function of Bob's postselected state, given by

$$Q_{\rm out}(\beta) = \int\int d^2\alpha \; Q_{\rm out}(\alpha,\beta). \tag{B4}$$

In Eq. (B1), $H_{\rm ps}(a)$ is calculated as

$$H_{\rm ps}(a) = -\int\int d^2\alpha \; Q_{\rm out}(\alpha)\log_2[Q_{\rm out}(\alpha)], \tag{B5}$$

where $Q_{\rm out}(\alpha)$ is the Q function of Alice's postselected state, given by

$$Q_{\rm out}(\alpha) = \int\int d^2\beta \; Q_{\rm out}(\alpha,\beta). \tag{B6}$$

Note that while we can have analytical forms for $Q_{\rm out}(\alpha,\beta)$ and $Q_{\rm out}(\beta)$, from which we can calculate $H_{\rm ps}(a,b)$ and $H_{\rm ps}(b)$ using Eqs. (B2) and (B3), respectively, no closed-form solution for $Q_{\rm out}(\alpha)$ could be used, so Eqs. (B5) and (B6) should be numerically determined.

Now, we calculate the mutual information between Alice and Bob for the parameters of Fig. 3 using two approaches; first using the covariance matrix, $\mathbf{M}_{\rm ps}$, of the amplified (or postselected) state via Eq. (A2), and also using the Q function of the postselected state via Eq. (B1), with the results shown in

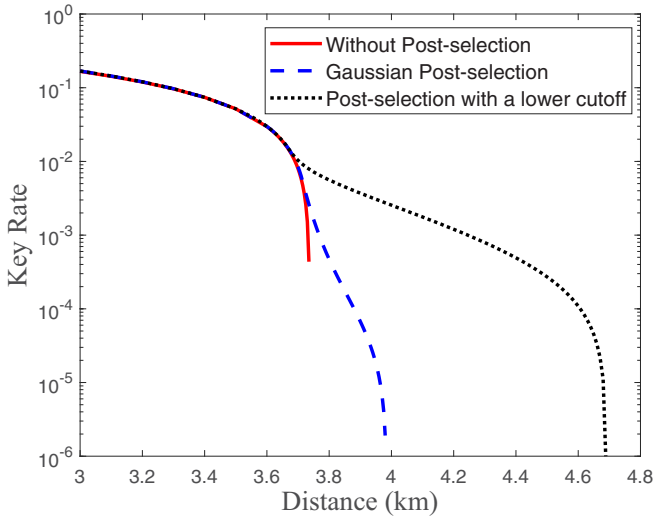

FIG. 8. The achievable secret key rate from direct reconciliation as a function of channel distance (km) in the CV-QKD protocol over a lossy channel with $\xi = 0.1$ and with 0.2 dB losses per km, without postselection (red lines), with the Gaussian postselection, i.e., $\gamma_c = 3g\sqrt{V_B}$ (blue lines), and with the non-Gaussian postselection, i.e., choosing a lower cutoff $\gamma_c = 2g\sqrt{V_B}$ (black lines) for the finite-size regime ($n = 10^{10}$) with $\beta = 0.95$.

Fig. 6. Note that for the numerical integration of Eqs. (B5) and (B6), we divide the integration interval into $m = 1000$ equal subintervals. As can be seen from Fig. 6, there is a very small gap between $I_{\rm ps}(a{:}b)$ calculated using the two approaches. More precisely, for $\gamma_c < 3$, the mutual information calculated using the covariance matrix, i.e., Eq. (A2) is less than that calculated using the output Q function, i.e., Eq. (B1), while for $\gamma_c > 3$, the mutual information calculated from Eq. (A2) is higher than that calculated from Eq. (B1). Note that by increasing the number of subintervals, the numerical integration becomes more precise, and the gap becomes smaller. Note also that since the gap between $I_{\rm ps}(a{:}b)$ calculated using the two approaches is very small (less than 0.8% even for $m = 1000$), for our numerical simulation we have calculated $I_{\rm ps}(a{:}b)$ using the covariance matrix, $\mathbf{M}_{\rm ps}$, of the amplified state via Eq. (A2).

APPENDIX C: OPTIMAL VALUES OF THE INITIAL SQUEEZING AND GAIN

Here we show in Fig. 7 the optimal value for the initial squeezing χ and the gain g, which maximizes the finite-size key rate for the Gaussian postselection protocol of Fig. 2 with $n = 10^{12}$, and for the transmission range that the postselection is effective.

APPENDIX D: POSTSELECTION IN THE DIRECT RECONCILIATION SCENARIO

Here, we show the effectiveness of the postselection in the finite-size regime for the direct reconciliation. Figure 8 shows the achievable secret key rate secure against Gaussian collective attacks in the direct reconciliation scenario as a function of channel distance without the postselection, and with the Gaussian postselection (where the cutoff is sufficiently large, i.e., $\gamma_c = 3g\sqrt{V_B}$) in the finite-size regime. We found if the block size is sufficiently large, here larger than $n = 10^{10}$, the transmission range of the direct reconciliation scheme can be improved by the postselection, with the improvement increasing with increasing the block size. Now, by keeping the block size fixed, we decrease the postselection cutoff to $\gamma_c = 2g\sqrt{V_B}$, where the postselected data has a non-Gaussian statistics. As it can be seen, this non-Gaussian postselection is more effective than the Gaussian postselection, increasing the transmission range from 3.7 km to 4.7 km.

[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 *et al.*, Advances in quantum cryptography, arXiv:1906.01645.

[3] F. Xu, X. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, arXiv:1903.09051.

[4] C. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[5] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[6] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

[7] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[8] M. D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, Phys. Rev. A **62**, 062308 (2000).

[9] R. Garcia-Patron, PhD thesis. Universite Libre de Bruxelles, 2007.

[10] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[11] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations, Entropy **17**, 6072 (2015).

[12] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[13] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit, Phys. Rev. Lett. **89**, 167901 (2002).

[14] S. Lorenz, N. Korolkova, and G. Leuchs, Continuous-variable quantum key distribution using polarization encoding and post selection, Appl. Phys. B **79**, 273 (2004).

[15] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light, Phys. Rev. Lett. **95**, 180503 (2005).

[16] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection, Phys. Rev. A **74**, 042326 (2006).

[17] M. Heid and N. Lütkenhaus, Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction, Phys. Rev. A **73**, 052316 (2006).

[18] T. C. Ralph and A. P. Lund, Nondeterministic noiseless linear amplification of quantum systems, in *Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing, Calgary, 2008*, edited by A. Lvovsky, AIP Conf. Proc. No. 1110 (AIP, Melville, 2009), p. 155.

[19] 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).

[20] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, Long-distance continuous-variable quantum key distribution with quantum scissors, IEEE Journal Selected Topics Quant. Electron. **26**, 1 (2020).

[21] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, Discrete-modulation continuous-variable quantum key

distribution enhanced by quantum scissors, IEEE Journal Selected Areas Commun. **38**, 506 (2020).

[22] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, Security of continuous-variable quantum cryptography with Gaussian postselection, Phys. Rev. A **87**, 020303(R) (2013).

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

[24] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, Measurement-based noiseless linear amplification for quantum communication, Nature Photon. **8**, 333 (2014).

[25] J. Zhao, J. Yan Haw, T. Symul, P. Koy Lam, and S. M. Assad, Characterization of a measurement-based noiseless linear amplifier and its applications, Phys. Rev. A **96**, 012319 (2017).

[26] 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).

[27] 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).

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

[29] M. Navascues, F. Grosshans, and A. Acin, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[30] R. García-Patron and N. J. Cerf, Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[31] A. Leverrier, Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, Phys. Rev. Lett. **114**, 070501 (2015).

[32] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, Phys. Rev. A **97**, 052327 (2018).

[33] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Parameter Estimation with Almost No Public Communication for Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **120**, 220505 (2018).

[34] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction, Phys. Rev. Lett. **118**, 200501 (2017).

[35] S. Ghorai, E. Diamanti, and A. Leverrier, Composable security of two-way continuous-variable quantum key distribution without active symmetrization, Phys. Rev. A **99**, 012311 (2019).

[36] N. Hosseinidehaj, N. Walk, and T. C. Ralph, Optimal realistic attacks in continuous-variable quantum key distribution, Phys. Rev. A **99**, 052336 (2019).

[37] C. Caves, Quantum limits on noise in linear amplifiers, Phys. Rev. D **26**, 1817 (1982).

[38] Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, S. Yu, and H. Guo, Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution, Entropy **17**, 4547 (2015).

[39] T. Wanga, S. Yu, Y.-C. Zhang, W. Gu, and H. Guo, Improving the maximum transmission distance of continuous-variable quantum key distribution with noisy coherent states using a noiseless amplifier, Phys. Lett. A **378**, 2808 (2014).

[40] F. Yang, R. Shi, Y. Guo, J. Shi, and G. Zeng, Continuous-variable quantum key distribution under the local oscillator intensity attack with noiseless linear amplifier, Quant. Info. Proc. **14**, 3041 (2015).

[41] Y. Zhang, S. Yu, and H. Guo, Application of practical noiseless linear amplifier in no-switching continuous-variable quantum cryptography, Quant. Info. Proc. **14**, 4339 (2015).

[42] E. Villasenor and R. Malaney, Improving QKD for Entangled States with Low Squeezing via Non-Gaussian Operations, arXiv:1911.00141.

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

[44] Y. Zhang *et al.*, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[45] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[46] Y.-C. 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 fiber, arXiv:2001.02555.

[47] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum key Distribution, Phys. Rev. X **9**, 041064 (2019).

[48] J. Dias and T. C. Ralph, Quantum repeaters using continuous-variable teleportation, Phys. Rev. A **95**, 022312 (2017).

[49] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).

[50] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, Phys. Rev. A **86**, 032309 (2012).