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

Author(s):

Nedasadat Hosseinidehaj, Andrew M. Lance, Thomas Symul, Nathan Walk, and Timothy C. Ralph

Citation:

"Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection:
Nedasadat Hosseinidehaj, Andrew M. Lance, Thomas Symul, Nathan Walk, and Timothy C. Ralph
Phys. Rev. A 101, 052335 ; https://doi.org/10.1103/PhysRevA.101.052335"

Finite-size effects in continuous-variable QKD with Gaussian post-selection

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

(Dated: December 23, 2019)

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 post-selection of the detection outcome. Such a post-selection, which is also called a measurement-based NLA, requires a cut-off to produce a normalisable filter function. Increasing the cut-off 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 post-selection via an asymptotic security analysis, we undertake the first investigation of such a post-selection utilising a composable security proof in the realistic finite-size regime, where this trade-off is extremely relevant. We show that this form of post-selection can improve the secure range of a CV-QKD over lossy thermal channels if the finite block size is sufficiently large and that the optimal value for the filter cut-off 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.

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 post-processing 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 post-processing, and finite-size effects.

In order to improve the transmission range of CV-QKD systems a post-selection 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 post-selected data has non-Gaussian statistics. Further, it has been shown that the application of a noiseless linear amplifier (NLA), proposed in [18], on the received signal preceding the detction can probabilistically enhance the secure range of CV-QKD systems, while preserving the Gaussian statistics [19]. However, any physical realization of the NLA is very demanding, requiring state-of-the art technology, such as single-photon sources, single-photon addition and subtraction. Moreover, the actual success probability of these experiments is much lower than the theoretical predictions. In [20–22] it has been shown that the physical implementation of the NLA can be substituted with a classical data post-processing. In particular, where the NLA directly precedes a heterodyne detection, the noise-

[*] n.hosseinidehaj@uq.edu.au

less amplifier can be emulated by a Gaussian post-selectin of the detection outcome via a probabilistic classical filter function [21, 22]. This post-selection scheme, which is also called measurement-based NLA [22], has experimentally been demonstrated in [22] and requires a cut-off on the classical filter to emulate the NLA. The post-selection scheme results in Gaussian statistics for the post-selected data if the filter cut-off is chosen sufficiently large [21, 22].

In the asymptotic regime it has been shown that the Gaussian post-selection can extend the maximum transmission distance of CV-QKD systems [20–22]. However, in reality a finite number of signals are exchanged between Alice and Bob. The finite-size issue becomes even more significant when the post-selection is applied as it reduces the size of data. It is unclear whether the post-selection 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 post-selection (or the measurement-based NLA) at the receiver. We show that in the finite-size regime when the filter cut-off is large enough to make the post-selected 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 post-selection is effective when the CV-QKD system has undergone high values of excess noise. Since reducing the cut-off can increase the success probability of the post-selection (at the expense of decreasing the classical mutual information between Alice and Bob), we also investigate the impact reducing the cut-off can have on the finite-size key rate, illustrating that if the filter cut-off is sufficiently reduced, the improvement of CV-QKD performance due to the post-selection can further be increased. Note that in the recent works on measurement-based NLA [21, 22], the security proof is based on the equivalent entanglement-based scheme where the classical filter is replaced with a quantum filter (or NLA), as they assumed a sufficiently large cut-off to emulate an ideal NLA (with a Gaussian output). However, since reducing the cut-off can change the statistics of the post-selected data from Gaussian to non-Gaussian regime, we analyse the security proof based on the equivalent entanglement-based scheme with a classical filter (and not a quantum filter). Thus, our results also provides 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 [23].

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 analysed in both the asymptotic and finite-size regime. In Sec. IV, the post-selection of Bob's detection outcome is discussed, and the security of the post-selection protocol is analysed. In Sec. V, the numerical results, showing the impact of the post-selection 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, 24], that 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 post-processing 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 post-processing.

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 maximum 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 $0 \leq \beta \leq 1$ is the reconciliation efficiency. Note that in the asymptotic regime collective attacks are as strong as coherent attacks [9, 10, 25]. 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 [26–28].

In the 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 $\epsilon{=}2\epsilon_{\rm sm}{+}\bar{\epsilon}{+}\epsilon_{\rm PE}{+}\epsilon_{\rm cor}$ [29, 30] and if the key length ℓ is chosen such that [29, 30]

$$\ell{\leq}N[\beta I(a{:}b){-}\chi(b{:}E)]{-}\sqrt{N}\Delta{-}2\log_2(\tfrac{1}{2\bar{\epsilon}}), \tag{1}$$

where [29, 30]

$$\begin{aligned}\Delta &= (d{+}1)^2{+}4(d{+}1)\sqrt{\log_2(2/\epsilon_{\rm sm}^2)}{+}\\ &2\log_2(2/(\epsilon^2\epsilon_{\rm sm})){+}4\epsilon_{\rm sm}d/(\epsilon\sqrt{N}),\end{aligned} \tag{2}$$

and where $N{=}2n$, d is the discretization parameter, $\epsilon_{\rm sm}$ is the smoothing parameter, and $\epsilon_{\rm cor}$ and $\epsilon_{\rm PE}$ are the maximum failure probabilities for the error correction and parameter estimation, respectively.

The final key rate 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 [29], 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 [32, 33], and numerically analysed in [34], in order to analyse the composable finite-size security of the no-switching CV-QKD protocol against coherent attacks, the security of the protocol is first analysed against Gaussian collective attacks with a security parameter ϵ [29], and then by applying the Gaussian de Finetti reduction [32] the security is obtained against coherent attacks with a polynomially larger security parameter $\tilde{\epsilon}$ [32], where the security loss due to the reduction from coherent attacks to collective attacks scales like $O(N^4)$ [32].

IV. POST-SELECTION

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 [35], making the quantum channel insecure. To avoid this noise penalty, the idea of heralded noiseless linear amplifier (NLA) was proposed in [18], which enables one to amplify probabilistically 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],

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

For a Gaussian CV-QKD system it has been shown that the maximum transmission distance of the system can be increased by applying an 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 [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

[1] It has also been shown in [31] 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.

NLA. These effective parameters are given by [19]

$$\begin{aligned}
\chi_g &= \chi\sqrt{\tfrac{(g^2-1)(\xi-2)T-2}{(g^2-1)\xi T-2}} \\
T_g &= \tfrac{g^2T}{(g^2-1)T\left[\frac{1}{4}(g^2-1)(\xi-2)\xi T-\xi+1\right]+1} \\
\xi_g &= \xi - \tfrac{1}{2}(g^2-1)(\xi-2)\xi T.
\end{aligned} \tag{4}$$

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

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

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 [36–38]. 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 [39–42]. Note that all of these works have focussed 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 post-selection or measurement-based NLA was proposed [20, 21], and experimentally demonstrated [22], 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 [21, 22], 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 post-selection of Bob's heterodyne measurement data [21, 22].

Considering the input state of an NLA as ρ_{in}, the Husimi Q-function of the amplified output state is given by

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

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

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

Having Eq. (7), we are able to determine the appropriate classical post-selection 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 $\mathbf{M} = [a\mathbf{I}_2, c\mathbf{Z}; c\mathbf{Z}, b\mathbf{I}_2]$ with $\mathbf{I}_2$ a 2×2 identity matrix, and $\mathbf{Z} = \text{diag}\,(1,-1)$) 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 $Q_{\text{in}}(\alpha_m, \beta_m)$, 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 [21],

$$\begin{aligned}
&Q_{\text{in}}(\alpha_m, \beta_m) = \tfrac{\sqrt{\det(\mathbf{\Gamma})}}{\pi^2}\times \\
&\exp\left[-a'|\alpha_m|^2 - b'|\beta_m|^2 - 2c'\left|\alpha_m\right|\left|\beta_m\right|\cos(\phi_\alpha+\phi_\beta)\right],
\end{aligned} \tag{8}$$

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

Post-selection 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 pre-factor, $\exp\left[(1-\frac{1}{g^2})|\beta_m|^2\right]$, in Eq. (7). Note that the filter is truncated by a real cut-off parameter γ_c to make the filter probability convergent. The filter function is [21–23]

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

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 cut-off γ_c are kept with unity probability.

Considering N_{ps} as the number of accepted data points which are kept by Bob, and N is the total number of data points before the post-selection, the success probability of the post-selection is given by

$$P_s = \frac{N_{\rm ps}}{N} = \int\!\!\int d^2\alpha_m \int\!\!\int d^2\beta_m \; F(\beta_m) Q_{\rm in}(\alpha_m, \beta_m) =$$

$$\int_0^{2\pi}\int_0^{\infty} d\phi_\alpha d\left|\alpha_m\right| \int_0^{2\pi}\int_0^{\gamma_c} d\phi_\beta d\left|\beta_m\right| \exp\left[(1-\tfrac{1}{g^2})\left(\left|\beta_m\right|^2-\gamma_c^2\right)\right]$$

$$\times Q_{\rm in}(\alpha_m, \beta_m)\left|\alpha_m\right|\left|\beta_m\right|$$

$$+\int_0^{2\pi}\int_0^{\infty} d\phi_\alpha d\left|\alpha_m\right| \int_0^{2\pi}\int_{\gamma_c}^{\infty} d\phi_\beta d\left|\beta_m\right| Q_{\rm in}(\alpha_m, \beta_m)\left|\alpha_m\right|\left|\beta_m\right|, \tag{10}$$

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 cut-off γ_c are kept unaffected. The final joint probability distribution of the measurement outcomes after the rescaling is given by

$$Q_{\rm out}(\alpha, \beta) =$$

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

where $\beta_m{=}g\beta$ for $|\beta_m|{<}\gamma_c$, and $\beta_m{=}\beta$ for $|\beta_m|{\geq}\gamma_c$, while Alice's measurement outcomes do not need rescaling, i.e., we always have $\alpha_m{=}\alpha$.

Thus, in the post-selection, Bob first applies the filter function, $\exp\left[(1-\frac{1}{g^2})\left(\left|\beta_m\right|^2-\gamma_c^2\right)\right]$, 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 cut-off γ_c are kept unaffected with unit probability. In the CV-QKD protocol with the post-selection, 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 post-selected state shared between Alice and Bob in the equivalent entanglement-based scheme) should be performed on the post-selected data.

Having the final probability distribution of the post-selected 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 $\mathbf{M}_{\rm ps} = [a_{\rm ps}\mathbf{I}_2, c_{\rm ps}\mathbf{Z}; c_{\rm ps}\mathbf{Z}, b_{\rm ps}\mathbf{I}_2]$ is given by

$$\begin{aligned} a_{\rm ps} &= \int\!\!\int d^2\alpha \int\!\!\int d^2\beta \; ([2{\rm Re}(\alpha)]^2 - 1) Q_{\rm out}(\alpha, \beta), \\ b_{\rm ps} &= \int\!\!\int d^2\alpha \int\!\!\int d^2\beta \; ([2{\rm Re}(\beta)]^2 - 1) Q_{\rm out}(\alpha, \beta), \\ c_{\rm ps} &= \int\!\!\int d^2\alpha \int\!\!\int d^2\beta \; (4{\rm Re}(\alpha){\rm Re}(\beta)) Q_{\rm out}(\alpha, \beta). \end{aligned} \tag{12}$$

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 post-selection.

C. Security analysis for the post-selection protocol

In the asymptotic security analysis of the CV-QKD system with the post-selection (or the measurement-based NLA), the computed key rate must be multiplied by the success probability of the post-selection, P_s, of Eq. (10). Explicitly, the asymptotic key rate of the post-selection 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 post-selection, and $\chi_{\rm ps}(b{:}E)$ is the Holevo bound, i.e., the upper bound on Eve's information on the post-selected data (see Appendix A and Appendix B for the key-rate calculation).

In the finite-size security analysis of the CV-QKD protocol with the post-selection, the size of the data contributing to the secret key is no longer N. In fact, only the accepted data of size $N_{\rm ps} = P_s N$ contributes to the final post-selected 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 post-selection protocol which is secure against Gaussian collective attacks in the reverse reconciliation scenario is given by

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

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 post-selection protocol is given by $K_{\rm ps}^{\rm FS} = \ell_{\rm ps}/N$ or

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

Note that in contrast to the asymptotic regime, the success probability of the post-selection 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 post-selection can be used for secret key generation. However, if the data points of size k are disclosed after the post-selection 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 $N'_{\rm ps}$.

V. NUMERICAL RESULTS

A. Gaussian post-selection

In the post-selection scheme, when the cut-off γ_c is chosen sufficiently large such that the cut-off circle can embrace the amplified distribution, we can assume the distribution of the post-selected data remains statistically Gaussian, and the post-selection approximates an ideal NLA (which probabilistically converts a Gaussian state into another Gaussian state) [21, 22]. Therefore, in the CV-QKD protocol with the Gaussian post-selection, the security can be analysed based on the equivalent scheme, where the classical filter is replaced with a quantum filter (or NLA) before Bob's heterodyne detection (as it has been analysed in [21]), 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 post-selection. 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 cut-off γ_c is chosen sufficiently large.

Now we numerically simulate the effect of the Gaussian post-selection 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 kilometre, 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 optimised to maximise the key rate. We also choose a sufficiently large cut-off [2], $\gamma_c = 3g\sqrt{V_B}$ (with V_B the quadrature variance of Bob's measurement outcome before the detection and post-selection) to be able to assume the post-selected state remains Gaussian. In Fig. 1 the achievable secret key rate secure against Gaussian collective attacks is shown as a function of channel distance (km) without the post-selection and with the Gaussian post-selection 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. 1 that the Gaussian post-selection (blue lines) can be useful when the protocol is operating close to its limit, i.e., in the "water-fall" region of the key-rate versus distance graph, where modest increases in the correlation between Alice and Bob due to the post-selection (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. 1, the Gaussian post-selection 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 [21, 22]. However, in the finite-size regime when the block size is reduced, the improvement of the maximum transmission distance due to the Gaussian post-selection 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 post-selection can only appear when the block size is sufficiently large (larger than $n = 10^{11}$ for the given parameters of Fig. 1), and the amount of such an improvement increases with increasing the block size. Note that in Fig. 1 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. 1). In this case the maximum transmission distance of the protocol is 137.7 km, which can be improved by the Gaussian post-selection 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 $n = 10^8 - 10^{12}$, we will consider a higher-noise channel for the rest of our numerical results.

Note that in Fig. 1, we have considered the cut-off as $\gamma_c = 3g\sqrt{V_B}$, so that 99.7% of the amplified distribution lies within the cut-off circle [23], and we can assume the post-selected data has a Gaussian distribution which can emulate an ideal NLA. However, if we choose higher values for the cut-off, the post-selection 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 post-selection.

B. Non-Gaussian post-selection

In the measurement-based NLA the choice of the filter cut-off, γ_c, is critical. Larger cut-off will improve the approximation of the ideal NLA, however, a cut-off that is too high will unnecessarily sacrifice raw data, and decrease the success probability. On the other hand, a cut-off 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 post-selection, 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 post-selected key. In this section we investigate whether a reduction of the post-selection cut-off (which will increase the success probability) improves the post-selection performance in the finite-size regime.

When the fiter cut-off decreases from $\gamma_c = 3g\sqrt{V_B}$, the statistics of the post-selected data start changing from Gaussian to non-Gaussian. However, based on the optimality of Gaussian attacks [26–28], for all bipartite quantum states ρ_{AB} with covariance matrix $\mathbf{M}_{AB}$, one can

[2] In our numerical simulations we found that by considering $\gamma_c \geq 3g\sqrt{V_B}$ [23], the covariance matrix of the amplified state, $\mathbf{M}_{\rm ps}$, calculated from Eq. (12) is the same as the covariance matrix calculated based on the effective parameters χ_g, T_g, ξ_g of Eq. (4).

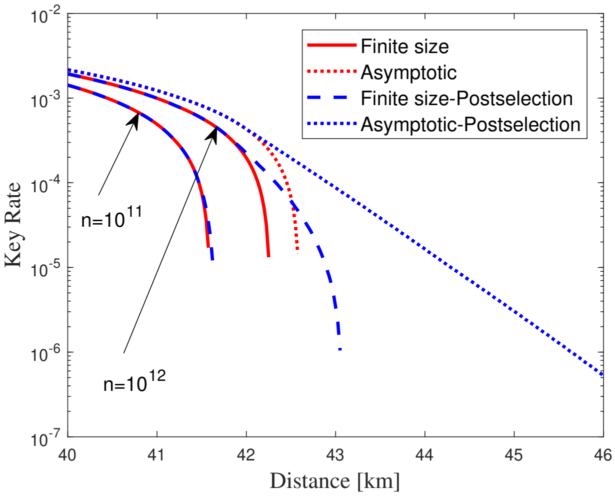

FIG. 1. The achievable secret key rate from reverse reconciliation as a function of channel distance (km) in the no-switching CV-QKD protocol over a lossy channel with $\xi = 0.1$ and with 0.2 dB losses per km, without the post-selection (red lines) and with the Gaussian post-selection, where $\gamma_c = 3g\sqrt{V_B}$ (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 maximise the key rate.

maximise Eve's information by considering ρ^G_{AB}, which is the Gaussian state having the same covariance matrix $\mathbf{M}_{AB}$. Hence, in order to analyse 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 post-selection 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 post-selected state, i.e., Eq. (12) to calculate the covariance matrix of the amplified state, and compute a lower bound on the post-selected 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 cut-off is sufficiently large [21, 22]. 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 cut-off, and the impact this cut-off 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. 1, is almost the maximum transmission distance of the CV-QKD system with the optimised Gaussian post-selection, 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 post-selection (with $\gamma_c = 3g\sqrt{V_B}$) generates the finite-size key rate of $K^{\rm FS}_{\rm ps} = 3.4 \times 10^{-6}$ (bits per symbol).

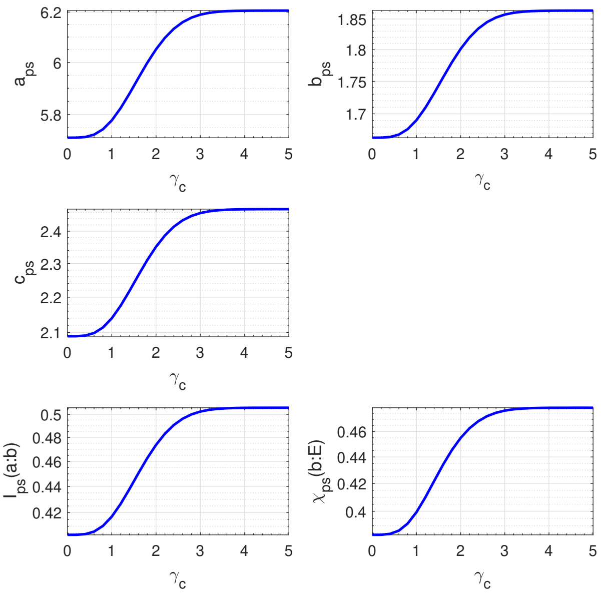

FIG. 2. The elements of the covariance matrix, $\mathbf{M}_{\rm ps}$, of the post-selected state, (i.e., $a_{\rm ps}$, $b_{\rm ps}$, and $c_{\rm ps}$), the classical mutual information between Alice and Bob, $I_{\rm ps}(a{:}b)$, and Eve's information from reverse reconciliation (i.e., the Holevo bound), $\chi_{\rm ps}(b{:}E)$ 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 $n = 10^{12}$.

For this quantum channel we now investigate the effects a decrease in the post-selection cut-off, γ_c, can have on the CV-QKD performance.

In Fig. 2, the three top plots show the elements of the covariance matrix, $\mathbf{M}_{\rm ps}$, of the amplified state (i.e., $a_{\rm ps}$, $b_{\rm ps}$, and $c_{\rm ps}$ in Eq. (12)) as a function of the post-selection cut-off γ_c. As it can be seen, for $\gamma_c \geq 3g\sqrt{V_B} = 4.26$, the post-selected state can be assumed to be Gaussian, as the elements of the covariance matrix $\mathbf{M}_{\rm ps}$ 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 cut-off is reduced. As a result, the classical mutual information between Alice and Bob, $I_{\rm ps}(a{:}b)$, as well as Eve's information, i.e., the Holevo bound, $\chi_{\rm ps}(b{:}E)$ (with both being calculated based on the covariance matrix $\mathbf{M}_{\rm ps}$) decrease with the cut-off reducing (shown in the two bottom plots of Fig. 2). Although the raw key-rate term, $\beta I_{\rm ps}(a{:}b) - \chi_{\rm ps}(b{:}E)$, also drops with the decrease in the cut-off, the success probability of the post-selection, P_s, exponentially increases with the cut-off decreasing according to the left plot of Fig. 3. As a result, both the asymptotic and finite-size key rates first increase with the cut-off decreasing up to an optimized value, and then de-

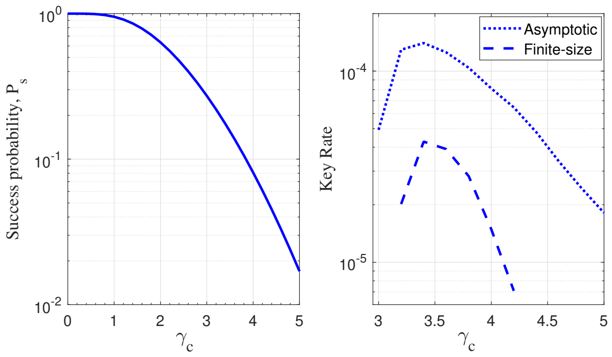

FIG. 3. The post-selection success probability, P_s, and the finite-size and asymptotic key rate from reverse reconciliation as a function of the filter cutoff γ_c for a quantum channel and the protocol with the same parameters as Fig. 2.

crease until they disappear (see Fig. 3, right plot). Therefore, our results show that there is an optimal value for the cut-off in the non-Gaussian regime which maximizes the key rate. According to Fig. 3, the finite-size key rate can be improved up to $K_{\mathrm{ps}}^{\mathrm{FS}} = 4.3\times10^{-5}$ (i.e., an improvement of more than one order of magnitude) by decreasing the cut-off 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. 2 and 3, for $\gamma_c \geq 3g\sqrt{V_B}$, the post-selected state remains almost Gaussian and the post-selection can emulate the ideal NLA, while $\gamma_c = 0$ corresponding to no post-selection.

Note that the lower bound on the key rate which we calculate for the post-selection in the non-Gaussian regime is not tight, and it could likely be improved using the numerical approach of [44]. The bound is loose because it relies on Gaussian optimality proof [26–28], which means that $\chi_{\mathrm{ps}}(b{:}E)$ is computed for the Gaussian state with the same covariance matrix as the non-Gaussian amplified state, and $\chi_{\mathrm{ps}}(b{:}E)$ is therefore overestimated. Techniques that provide tighter bounds for non-Gaussian statistics would therefore result in a smaller value for the optimal cut-off which, given the exponential improvement in the fraction of data kept, could significantly improve the key rates.

Now we repeat our numerical simulations for the post-selection in Fig. 1, with a lower cut-off, $\gamma_c = 2.5g\sqrt{V_B}$, and compute the post-selected finite-size key rate, with the results shown in Fig. 4. We can see that decreasing the cut-off 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 kilometre. We can see that for $n = 10^{12}$ by decreasing the cut-off from $\gamma_c = 3g\sqrt{V_B}$ to $\gamma_c = 2.5g\sqrt{V_B}$ the improvement of the transmission distance due to the post-selection becomes more significant. Furthermore, we can see that while for $n = 10^{11}$ there is no improvement in the transmission distance due to the post-selection with $\gamma_c = 3g\sqrt{V_B}$, the transmission distance can be improved by decreasing the cut-off 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 post-selected state is not Gaussian (although it is close to the Gaussian regime), hence we use the output Q-function, $Q_{\mathrm{out}(\alpha,\beta)}$, to calculate the elements of the covariance matrix of the post-selected state, $\mathbf{M}_{\mathrm{ps}}$. Our results show the importance of the proper choice of the post-selection cut-off in the CV-QKD system.

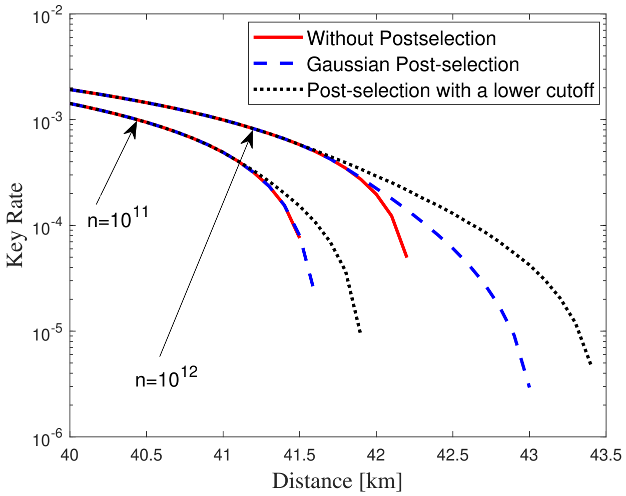

FIG. 4. The achievable secret key rate from reverse reconciliation as a function of channel distance (km) in the CV-QKD protocol over a lossy channel with $\xi = 0.1$ and with 0.2 dB losses per km, without post-selection (red lines), with the Gaussian post-selection, i.e., $\gamma_c = 3g\sqrt{V_B}$ (blue lines), and with the non-Gaussian post-selection, i.e., choosing a lower cut-off $\gamma_c = 2.5g\sqrt{V_B}$ (black lines) for the finite-size regime ($n = 10^{11}$ and $n = 10^{12}$) with $\beta = 0.95$.

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., $\chi_{\mathrm{ps}}(a{:}E)$. For the numerical simulations of the direct reconciliation see Appendix C.

C. Parameter estimation in the post-selection protocol

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

In the case of Gaussian post-selection, we can consider a normal linear model for Alice and Bob's post-selected variables in the PM scheme, $x_{\rm ps}^{\rm PM}$ and $y_{\rm ps}^{\rm PM}$, respectively as $y_{\rm ps}^{\rm PM} = t_g x_{\rm ps}^{\rm PM} + z_{\rm ps}$, where $t_g = \sqrt{\frac{T_g}{2}}$, and $z_{\rm ps}$ follows a centred normal distribution with unknown variance $\sigma_g^2 = 1 + \frac{1}{2}T_g\xi_g$ (note that Alice's variable $x_{\rm ps}^{\rm PM}$ 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 [45, 46]

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

with the uncertainty in the effective parameters expressed as [45, 46]

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

where x_i and y_i are the realizations of $x_{\rm ps}^{\rm PM}$ and $y_{\rm ps}^{\rm PM}$, respectively, and k is the number of data points randomly chosen from the post-selected data for the parameter estimation [3]. As a result, the covariance matrix , $\mathbf{M}_{\rm ps}$, of the amplified state shared between Alice and Bob in the EB scheme, which maximises Eve's information [45] is given by $\hat{\mathbf{M}}_{\rm ps} = [\hat{a}_{\rm ps}\mathbf{I}_2, \hat{c}_{\rm ps}\mathbf{Z}; \hat{c}_{\rm ps}\mathbf{Z}, \hat{b}_{\rm ps}\mathbf{I}_2]$, where

$$\begin{aligned} \hat{a}_{\rm ps} &= V_{A,\max}^g + 1, \\ \hat{b}_{\rm ps} &= 2(t_{g,\min}^2 V_{A,\max}^g + \sigma_{g,\max}^2) - 1, \\ \hat{c}_{\rm ps} &= \sqrt{2}\, t_{g,\min}\sqrt{{V_{A,\max}^g}^2 + 2V_{A,\max}^g}, \end{aligned} \tag{17}$$

and where

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

However, in the case of non-Gaussian post-selection, the relation between the cross-correlation term, $c_{\rm ps}$, of the covariance matrix $\mathbf{M}_{\rm ps}$ 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 $\mathbf{M}_{\rm ps}$ 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 post-selection. Considering Alice and Bob's variables in the PM scheme preceding the post-selection as $x^{\rm PM}$ and $y^{\rm PM}$, Alice and Bob's variables in the equivalent EB scheme preceding the post-selection would be $x^{\rm EB} = \frac{\sqrt{V_A+2}}{\sqrt{2V_A}}x^{\rm PM}$ and $y^{\rm EB} = y^{\rm PM}$, with V_A is the initial modulation variance in the PM scheme preceding the post-selection. 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 post-selected data, $x_{\rm ps}^{\rm EB}$ as $y_{\rm ps}^{\rm EB}$, to directly estimate $\mathbf{M}_{\rm ps}$ 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 $x_{\rm ps}^{\rm EB}$ and $y_{\rm ps}^{\rm EB}$, respectively.

VI. CONCLUSIONS

In this work we have investigated the impact post-selection or measurement-based NLA can have on the CV-QKD performance (when it is applied on the measurement outcome of Bob's detection) in the finite-size regime. We found that the post-selection can extend the maximum transmission distance of CV-QKD protocol in the finite-size regime providing the finite block size is sufficiently large. For finite blocks with a practical length, we found that the post-selection is effective for the protocols with high values of excess noise. Further, we analysed the performance of the measurement-based NLA on the entangled-state input in the non-Gaussian regime by decreasing the post-selection cut-off, thereby illustrating that there is an optimal value for the post-selection cut-off that optimises the CV-QKD performance in terms of both the finite key rate and transmission range.

VII. ACKNOWLEDGEMENTS

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). NW 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.

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

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

$$\mathbf{M} = \left[\begin{array}{cc} V\,\mathbf{I}_2 & \sqrt{T}\,\sqrt{V^2-1}\,\mathbf{Z} \\ \sqrt{T}\,\sqrt{V^2-1}\,\mathbf{Z} & (T(V+\chi_{\text{line}}))\,\mathbf{I}_2 \end{array} \right], \qquad \text{(A1)}$$

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

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

$$I_{\text{ps}}(a{:}b) = \log_2 \frac{a_{\text{ps}}+1}{a_{\text{ps}}+1-\frac{c_{\text{ps}}^2}{b_{\text{ps}}+1}}. \qquad \text{(A2)}$$

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 $\mathbf{M}_{\text{ps}}$[4]. 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 $\mathbf{M}_{A|b} = \mathbf{A}_{\text{ps}} - \mathbf{C}_{\text{ps}}\,(\mathbf{B}_{\text{ps}}+\mathbf{I}_2)^{-1}\,\mathbf{C}_{\text{ps}}^T$, where $\mathbf{A}_{\text{ps}} = a_{\text{ps}}\mathbf{I}_2$, $\mathbf{B}_{\text{ps}} = b_{\text{ps}}\mathbf{I}_2$, and $\mathbf{C}_{\text{ps}} = c_{\text{ps}}\mathbf{Z}$.

Appendix B: Actual mutual information

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

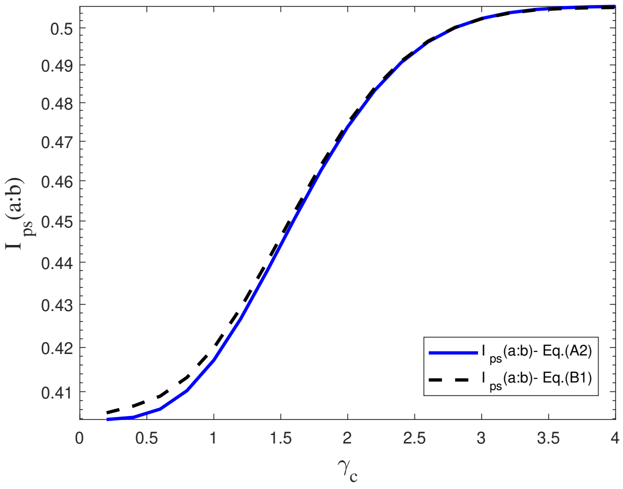

FIG. 5. The classical mutual information between Alice and Bob following the post-selection, $I_{\text{ps}}(a{:}b)$, using the covariance matrix, $\mathbf{M}_{\text{ps}}$, of the amplified state via Eq. (A2) (solid line), and using the Q-function of the post-selected state via Eq. (B1) (dashed line), as a function of the filter cutoff γ_c for a quantum channel equivalent with an optical fiber of 43 km, $\xi = 0.1$, $\chi = 0.8379$, $g = 1.1$.

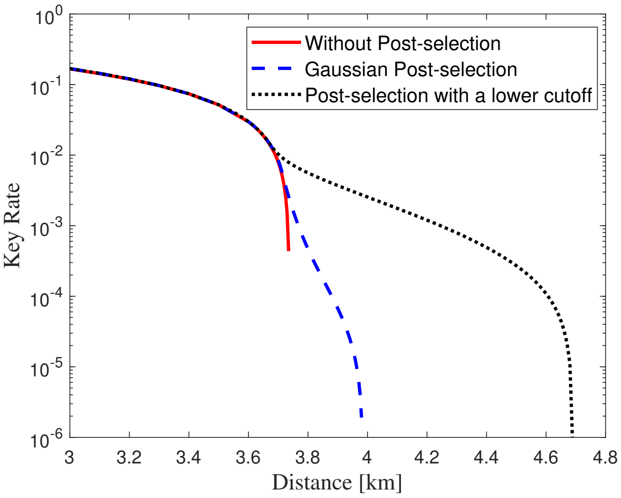

FIG. 6. The achievable secret key rate from direct reconciliation as a function of channel distance (km) in the CV-QKD protocol over a lossy channel with $\xi = 0.1$ and with 0.2 dB losses per km, without post-selection (red lines), with the Gaussian post-selection, i.e., $\gamma_c = 3g\sqrt{V_B}$ (blue lines), and with the non-Gaussian post-selection, i.e., choosing a lower cut-off $\gamma_c = 2g\sqrt{V_B}$ (black lines) for the finite-size regime ($n = 10^{10}$) with $\beta = 0.95$.

[4] 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 $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$.

formation 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 post-selection, $H_{\rm ps}(b)$ is the Shannon entropy of Bob's heterodyne-measurement result following the post-selection, and $H_{\rm ps}(a,b)$ is the joint entropy of Alice and Bob's classical variables following the post-selection. 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 post-selected 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 post-selected 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 post-selected 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. 2 using two approaches; first using the covariance matrix, $\mathbf{M}_{\rm ps}$, of the amplified (or post-selected) state via Eq. (A2), and also using the Q-function of the post-selected state via Eq. (B1), with the results shown in Fig. 5. 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. 5, 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 sub-intervals, 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: Post-selection in the direct reconciliation scenario

Here, we show the effectiveness of the post-selection in the finite-size regime for the direct reconciliation. Fig. 6 shows the achievable secret key rate secure against Gaussian collective attacks in the direct reconciliation scenario as a function of channel distance without the post-selection, and with the Gaussian post-selection (where the cut-off 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 post-selection, with the improvement increases with increasing the block size. Now, by keeping the block size fixed, we decrease the post-selection cut-off to $\gamma_c = 2g\sqrt{V_B}$, where the post-selected data has a non-Gaussian statistics. As it can be seen, this non-Gaussian post-selection is more effective than the Gaussian post-selection, increasing the transmission range from 3.7 km to 4.7 km.

[1] V. Scarani, et al., 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, J.-W. Pan, Quantum cryptography with realistic devices, arXiv:1903.09051.

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

[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, Rev. Mod. Phys. **84,** 621-699 (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 **421,** 238 (2003).

[13] C. Silberhorn, T. C. Ralph, N. Ltkenhaus, 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. Ltkenhaus, 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. Ltkenhaus, 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, Physical Review A **86,** 012327 (2012).

[20] 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).

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

[22] 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 Photonics **8,** 333 (2014).

[23] 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).

[24] 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).

[25] 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).

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

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

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

[29] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, Phys. Rev. Lett. **114,** 070501 (2015).

[30] 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).

[31] 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).

[32] A. Leverrier, Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction, Phys. Rev. Lett. **118,** 200501 (2017).

[33] 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).

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

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

[36] 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).

[37] 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, Physics Letters A **378,** 2808 (2014).

[38] 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, Quantum Inf. Process. **14,** 3041 (2015).

[39] Y. Zhang, S. Yu, and H. Guo, Application of practical noiseless linear amplifier in no-switching continuous-variable quantum cryptography, Quantum Inf. Process. **14,** 4339 (2015).

[40] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, Long-distance continuous-variable quantum key distribution with quantum scissors, arXiv:1808.01617.

[41] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors, arXiv:1907.13405.

[42] E. Villasenor and R. Malaney, Improving QKD for entangled states with low squeezing via non-Gaussian operations, arXiv:1911.00141.

[43] P. Jouguet1, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti1, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7,** 378 (2013).

[44] J. Lin, T. Upadhyaya, and N. Lutkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, arXiv:1905.10896.

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

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