
Article:
Wilkinson, Kieran N., Papanastasiou, Panagiotis, Ottaviani, Carlo orcid.org/0000-0002-0032-3999 et al. (2 more authors) (2020) Long-distance continuous-variable measurement-device-independent quantum key distribution with post-selection. Physical Review Research. 033424. ISSN 2643-1564

https://doi.org/10.1103/PhysRevResearch.2.033424

Long-distance continuous-variable measurement-device-independent quantum key distribution with postselection

Kieran N. Wilkinson,[1] Panagiotis Papanastasiou,[1] Carlo Ottaviani,[1] Tobias Gehring,[2] and Stefano Pirandola[1]
[1]*Department of Computer Science, University of York, York YO10 5GH, United Kingdom*
[2]*Department of Physics, Technical University of Denmark, Fysikvej, Kongens Lyngby 2800, Denmark*

(Received 8 June 2020; accepted 25 August 2020; published 16 September 2020)

We introduce a robust scheme for long-distance continuous-variable (CV) measurement-device-independent (MDI) quantum key distribution in which we employ postselection between distant parties communicating through the medium of an untrusted relay. We perform a security analysis that allows for general transmissivity and thermal noise variance of each link, in which we assume that an eavesdropper performs a collective attack and controls the excess thermal noise in the channels. The introduction of postselection enables the parties to sustain a secret key rate over distances exceeding those of existing CV MDI protocols. In the worst-case scenario in which the relay is positioned equidistant between them, we find that the parties may communicate securely over a range of 14 km in standard optical fiber. Our protocol helps to overcome the rate-distance limitations of previously proposed CV MDI protocols while maintaining many of their advantages.

DOI: 10.1103/PhysRevResearch.2.033424

I. INTRODUCTION

With the promise of provably secure communication built on the laws of physics, quantum key distribution (QKD) [1,2] is one of the most important results emerging from the field of quantum information theory [3,4]. Quantum key distribution allows two parties, conventionally named Alice and Bob, to generate a secret key by communicating via an untrusted quantum channel. An eavesdropper (Eve) may employ the most robust attack allowed by the laws of physics, however, she is always restricted by the inherent uncertainty of quantum mechanics and is forced to avoid overtampering with the signal as doing so will reveal her presence to the parties. By combining the attained secret key from a QKD protocol with the one-time pad algorithm, fully secure communication between the parties is guaranteed.

In recent years the field of QKD has evolved rapidly from the primitive BB84 protocol [5] to current state-of-the-art provably secure protocols allowing parties to communicate over hundreds of kilometers [6–8]. Furthermore, there exists a large body of work based on proof-of-principle experiments and in-field tests, including ground-to-satellite communications [9–11]. Most of the aforementioned work has focused on discrete-variable (DV) protocols. Continuous-variable (CV) protocols are promising alternatives that make use of readily available, inexpensive, and easily implementable equipment. CV protocols have been demonstrated to be capable of secret key rates close to the PLOB bound, which is the limit of repeaterless quantum communications in a lossy channel [12]. Many protocols have been proven secure and others have been demonstrated in a proof-of-concept experiment [13] and field tests [14,15]. Recently, experimental results for long-distance CV QKD over 202.81 km of ultralow-loss optical fiber have been achieved [16].

Many recent QKD protocols have focused on an end-to-end as opposed to point-to-point approach in which Alice and Bob communicate via remote relays. Introducing a single relay allows the parties to perform measurement-device-independent (MDI) QKD protocols, even if the relay is untrusted [17–22]. Measurement device independence removes the security threat of side-channel attacks attempted by Eve. Several MDI-inspired protocols have been devised that can achieve high rates and exceed the PLOB bound. The first of these protocols was the seminal twin-field protocol [23–25], followed by the phase-matching protocol [26,27] and the sending-or-not-sending protocol [28–31]. See Fig. 11 of Ref. [1] for a summary of their performances.

A CV MDI protocol was proposed and demonstrated in a proof-of-concept experiment to achieve very high secret key rates over relatively short distances [32] (see also Refs. [33–35] for other studies). Unfortunately, developing a protocol that allows exploitation of the practicality of the CV MDI regime at long distance is a difficult problem in recent QKD theory [36–39]. A great deal of effort has been directed at improving the performance of this type of protocol, with proposals based on virtual photon subtraction [40,41], unidimensional modulation [42], or discrete modulation [43]. While these protocols offered an improvement in the range of the asymmetric configuration, in which the relay is positioned within close range of one of the parties, their applicability in the symmetric configuration, in which the relay is positioned equidistance between the parties, was very limited. Only Refs. [40,41] offered any improvement over the original CV MDI protocol in the symmetric configuration.

In this work, we begin to bridge the rate-distance gap between DV and CV MDI protocols. In particular, we aim to improve the distance over which a rate is attainable in the symmetric configuration. In this case, a secret key rate under the original CV MDI protocol and ideal conditions is only attainable at very short distances corresponding to a 0.75-dB loss [33]. In order to extend this range, we employ a postselection regime. Postselection describes the ability of the parties to select only instances of the protocol in which they have an advantage over the eavesdropper, given a prescriptive map of the contribution of the possible signals. By discarding any other instances, the secret key rate is always positive, and the parties can communicate securely up to a distance at which the key rate drops below a minimum usability threshold.

Postselection of a CV protocol was first introduced by Silberhorn *et al.* [44] where it allowed a secret key to be constructed for losses exceeding the previous limit of 3 dB. Later, the technique was generalized to thermal loss channels [45,46] and the concept has been demonstrated in experimental settings [47,48]. In this work, we consider the postselection of an MDI protocol which includes a measurement at an untrusted relay. We perform postselection over the relay measurement outcome as well as Alice's and Bob's variables while assuming that Eve employs a collective attack in which she targets both the Alice-relay and Bob-relay links.

The paper is structured as follows. We begin by outlining the protocol in detail and follow the evolution of the modes. We then derive the mutual information between the parties and the Holevo bound in order to quantify Eve's information. Using these quantities, we can build the single-point rate, which serves as a prescriptive map for the parties to select the advantageous channel uses. Finally, we calculate the postselected secret key rate of the protocol.

II. PROTOCOL

Let us begin our analysis by outlining our protocol which is shown schematically in Fig. 1. The secure parties that we label Alice and Bob are each connected to a relay with fiber optic links. We assume that both parties have access to a general Gaussian distribution of the form

$$p(x,\sigma) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{x^2}{2\sigma}\right). \tag{1}$$

In each use of the protocol, Alice draws two random numbers q_A and p_A from her Gaussian distribution with variance σ_A. From these two numbers, she extracts absolute values $|q_A| = \mathbb{A}$ and $|p_A| = \mathbb{A}'$ and signs κ and κ', respectively. For both κ and κ', she records bit values 0 (1) if the sign is positive (negative). She proceeds to prepare a coherent state of the form $|\frac{1}{2}(\kappa\,\mathbb{A} + i\kappa'\,\mathbb{A}')\rangle$ and sends it to the relay via a quantum channel. Bob follows a similar procedure, generating two random numbers q_B and p_B using his Gaussian distribution with a generally different variance σ_B. He generates a state of the form $|\frac{1}{2}(\tilde{\kappa}\,\mathbb{B} + i\,\tilde{\kappa}'\,\mathbb{B}')\rangle$ and sends it to the relay.

After quantum communication ceases, the parties perform basis reconciliation. If the q quadrature is chosen, the variables κ' and $\tilde{\kappa}'$ are ignored. Alice publicly broadcasts $\mathbb{A}$ and p_A while Bob broadcasts $\mathbb{B}$ and p_B and attempts to reconcile his variable $\tilde{\kappa}$ with Alice's variable κ. Alternatively, if the p quadrature is chosen, the relevant variables become κ' and $\tilde{\kappa}'$. Alice broadcasts $\mathbb{A}'$ and q_A while Bob broadcasts $\mathbb{B}'$ and q_B.

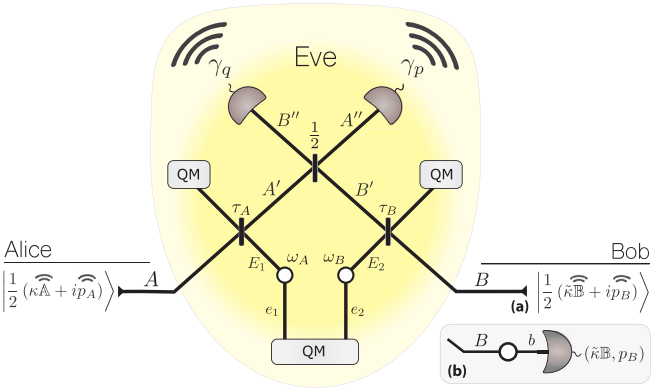

FIG. 1. Schematic of the protocol assuming the q quadrature is chosen by the parties for reconciliation. (a) Alice and Bob send their coherent states to the relay. Eve is in possession of two two-mode squeezed vacuum states, denoted by white circles. She employs dual entangling cloner attacks, interacting with Alice's and Bob's mode beam splitters of transmissivity τ_A and τ_B, respectively. The output modes A' and B' are mixed in the balanced beam splitter at the relay and the new output modes A'' and B'' are subsequently measured with homodyne p and q detection with corresponding outcomes γ_p and γ_q, respectively, that are publicly announced. After quantum communication ceases, Alice broadcasts $\mathbb{A}$ and p_A while Bob broadcasts $\mathbb{B}$ and p_B. (b) In the restricted eavesdropping scenario Bob's action is modeled in the entanglement-based representation. He measures, with heterodyne detection, one mode b of a two-mode squeezed vacuum state of variance μ obtaining the outcome $(\tilde{\kappa}\,\mathbb{B}, p_B)$. This action prepares coherent states in the conjugate mode B that is subsequently sent to the relay.

We assume that Eve employs dual entangling cloner attacks in which she inserts beam splitters of transmissivity τ_A and τ_B into lossless Alice-relay and Bob-relay channels, respectively. She uses the beam splitters to mix Alice's mode A with her mode E_1 and Bob's mode B with her mode E_2. The modes E_1 and E_2 each form one half of independent two-mode squeezed vacuum (TMSV) states with conjugate modes e_1 and e_2 and variances ω_A and ω_B, respectively. She stores the outputs from one port of each beam splitter in a quantum memory and sends the remaining outputs A' and B' to the relay, where they are mixed in a balanced beam splitter with outputs A'' and B'' that are subsequently measured with homodyne detection in the p and q quadratures, respectively. The corresponding outcomes γ_p and γ_q are publicly broadcast as $\boldsymbol{\gamma} = (\gamma_q, \gamma_p)$.

To model detector inefficiencies, we can treat the modes A'' and B'' as passing through beam splitters of transmissivity η where they are each mixed with one half of separate TMSV states with identical variance S before arriving at 100% efficient homodyne detectors. We may assume that the noise of the detectors is untrusted, in which case we assume the TMSV states are part of Eve's state and are included in the calculation of Eve's information, or trusted, in which case they are discarded. If $S = 1$ and $\tau_A = \tau_B = \tau$, the detector inefficiencies can be modeled without considering beam-splitter interactions at the relay by absorbing the detector efficiency parameter into

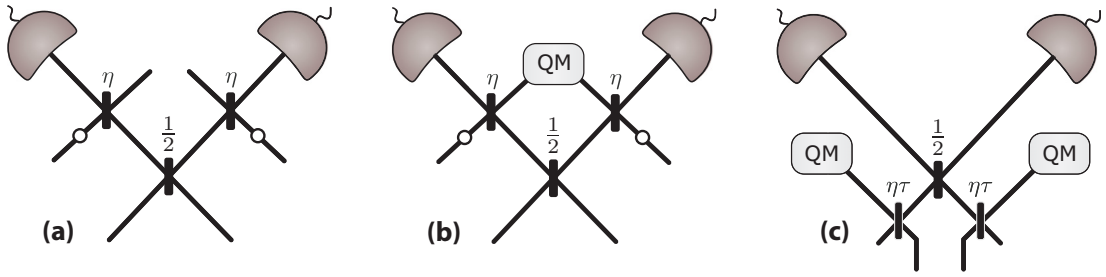

FIG. 2. Models of inefficiency in homodyne detection at the relay using beam splitters. (a) Trusted noise scenario in which it is assumed that Eve does not have access to the output of the beam splitters. (b) Outputs of the beam splitters are assumed to be added to Eve's quantum memory for later measurement. (c) Simplification in the symmetric case ($\tau_A = \tau_B = \tau$) and with $S = 1$ in which the transmissivities of the Alice-relay and Bob-relay links are scaled by a factor of η to model the effect of beam splitters at detectors.

the transmissivities of the links such that $\tau \to \eta\tau$. We outline each model schematically in Fig. 2.

In this paper, our goal is to establish the postselected asymptotic key rate of the protocol $R_{\rm PS}$. However, our initial objective is to obtain a formula for the standard asymptotic secret key rate R, which is given by the difference in the reconcilable information between the trusted parties βI_{AB}, where β is the reconciliation efficiency and I_{AB} is the mutual information between the parties, and the Holevo bound χ, which quantifies the maximum information Eve may attain about the secret variable depending on the particular attack,

$$R = \beta I_{AB} - \chi. \tag{2}$$

To this end, we follow the propagation of the covariance matrix (CM) of the total Alice-Bob-Eve system and its associated mean value. As each use of the protocol is Gaussian, these are the only tools we need to compute the probabilities and states needed to derive the key rate. After this step is complete, we explain the postselection procedure which allows us to extend the range of the protocol.

The initial covariance matrix of the total system is given by

$$\mathbf{V}_{AB\,\mathfrak{E}\,|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'} = \mathbf{I}_A \oplus \mathbf{I}_B \oplus \mathbf{V}_{\mathfrak{E}}, \tag{3}$$

where $\mathbf{V}_{\mathfrak{E}}$ is Eve's initial CM, which, assuming she controls the detector noise at the relay, is given by

$$\begin{aligned}\mathbf{V}_{\mathfrak{E}} = {}& \mathbf{V}_{\rm TMSV}(\omega_A) \oplus \mathbf{V}_{\rm TMSV}(\omega_B) \\ & \oplus \mathbf{V}_{\rm TMSV}(S) \oplus \mathbf{V}_{\rm TMSV}(S),\end{aligned} \tag{4}$$

with $\mathbf{V}_{\rm TMSV}(\mu)$ the CM of a TMSV state with variance μ given by

$$\mathbf{V}_{\rm TMSV}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I}\end{pmatrix}, \tag{5}$$

where $\mathbf{Z} = \mathrm{diag}(1, -1)$ and $\mathbf{I}$ is the 2×2 identity matrix. The mean value of the combined system of Alice and Bob is given by

$$\bar{\mathbf{x}}_{AB|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'} = (\kappa\,\mathbb{A}, \kappa'\,\mathbb{A}', \tilde\kappa\,\mathbb{B}, \tilde\kappa'\,\mathbb{B}')^{\mathsf{T}}, \tag{6}$$

while the mean value of Eve's system can be taken initially as zero. The action of all of the beam splitters can be encapsulated by a unitary operator $\hat{\mathbf{T}}$ that, when applied to the system, gives the postpropagation CM $\mathbf{V}_{A''B''\mathfrak{E}'|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'}$ and mean value $\bar{\mathbf{x}}_{A''B''\mathfrak{E}'|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'}$. Eve's CM with conditioning on γ is obtained by performing the homodyne measurements at the relay on the modes A'' and B'' in the p and q quadratures, respectively. The measurement outcome in the q quadrature γ_q with conditioning on the measurement outcome of the p quadrature γ_p is given by

$$\begin{aligned}&p(\gamma_q|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'\,\gamma_p) \\ &\quad = \frac{1}{\sqrt{2\pi\upsilon}}\exp\left[-\frac{1}{2\upsilon}\left(\gamma + \sqrt{\frac{\eta}{2}}(\kappa\,\mathbb{A}\,\sqrt{\tau_A} - \tilde\kappa\,\mathbb{B}\,\sqrt{\tau_B})\right)^2\right]\end{aligned} \tag{7}$$

and in the reverse case we have

$$\begin{aligned}&p(\gamma_p|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'\,\gamma_q) \\ &\quad = \frac{1}{\sqrt{2\pi\upsilon}}\exp\left[-\frac{1}{2\upsilon}\left(\gamma - \sqrt{\frac{\eta}{2}}(\kappa'\,\mathbb{A}'\,\sqrt{\tau_A} + \tilde\kappa'\,\mathbb{B}'\,\sqrt{\tau_B})\right)^2\right],\end{aligned} \tag{8}$$

where

$$\upsilon = (1-\eta)S + \frac{\eta}{2}[\tau_A + \tau_B + (1-\tau_A)\omega_A + (1-\tau_B)\omega_B]. \tag{9}$$

Noting that the two quadratures are independent, we have

$$p(\gamma_q|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'\,\gamma_p) = p(\gamma_q|\kappa\,\tilde\kappa\,\mathbb{A}\,\mathbb{B}), \tag{10}$$

$$p(\gamma_p|\kappa\,\tilde\kappa\,\kappa'\,\tilde\kappa'\,\mathbb{A}\,\mathbb{B}\,\mathbb{A}'\,\mathbb{B}'\,\gamma_q) = p(\gamma_p|\kappa'\,\tilde\kappa'\,\mathbb{A}'\,\mathbb{B}'). \tag{11}$$

This fact allows us to simplify our calculation of the rate by only considering one quadrature. The quadrature of importance is that which is chosen by Alice and Bob in the quadrature reconciliation step as it, at this point, becomes the quadrature that contains the relevant encoding variable. However, the rate is independent of this choice of quadrature. We will therefore arbitrarily choose the q quadrature for our forthcoming calculation of the rate and we will employ the refined notation $\gamma \equiv \gamma_q$ while ignoring the variables κ', $\tilde\kappa'$, $\mathbb{A}'$, and $\mathbb{B}'$.

Restricted eavesdropping

If Bob broadcasts the tuple $(\mathbb{B}, p_B)$ or $(q_B, \mathbb{B}')$, he ensures that both parties can independently establish which instances of the protocol should be included in the final key. Such a communication step is likely a necessity in any postselection protocol; however, there may be a more optimal strategy that reduces the amount of information Bob must broadcast and

therefore the amount of information Eve gains. As an example, it may be possible for Bob to reveal the string of good instances at the end of the protocol as opposed to broadcasting his measurement data in each use. A strategy such as this would yield a secret key rate that lies in between the achievable lower bound in which Bob broadcasts the aforementioned tuples in every use of the protocol and the upper bound in which no information is broadcast by Bob. An alternative way to think about the latter is to consider a *restricted eavesdropping* scenario in which Eve does not make use of the information broadcast by Bob in her attack. In this context, it is possible to compute the upper bound on the secret key rate by computing Eve's states without conditioning on Bob's measurement outcome. To establish Eve's states in this case, we need to consider an entanglement-based version of the protocol as shown in Fig. 1(b). Bob's action may be modeled as measuring one mode of a TMSV state with variance μ. The amplitude of the coherent states $|\tilde{\beta}\rangle$ remotely prepared as a result of this process is related to the measurement outcome $\boldsymbol{\beta}$ by

$$\tilde{\beta} = \xi \boldsymbol{\beta}^*, \quad \xi = \sqrt{\frac{\mu+1}{\mu-1}}. \tag{12}$$

We label Bob's heterodyne measurement outcome $(\tilde{\kappa}\,\mathbb{B}, \tilde{\kappa}'\,\mathbb{B}')$.

For our analysis, we again consider only the q quadrature using the fact that the quadratures are uncorrelated. After applying the beam-splitter operation to the CM and mean value, we obtain the relay measurement outcome $\gamma \equiv \gamma_q$ with probability

$$p(\gamma\,|\kappa\,\mathbb{A}) = \frac{1}{\sqrt{2\pi\tilde{\upsilon}}} \exp\left[-\frac{1}{2\tilde{\upsilon}}\left(\gamma + \kappa\,\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\right)^2\right], \tag{13}$$

where

$$\tilde{\upsilon} = (1-\eta)S + \frac{\eta}{2}[\tau_A + \tau_B\mu + (1-\tau_A)\omega_A + (1-\tau_B)\omega_B]. \tag{14}$$

After the relay measurements, the CM and mean value of the remaining system become $\mathbf{V}_{b\mathfrak{E}'|\kappa\,\mathbb{A}\,\boldsymbol{\gamma}}$ and $\bar{\mathbf{x}}_{b\mathfrak{E}'|\kappa\,\mathbb{A}\,\boldsymbol{\gamma}}$. Eve's CM and mean value are obtained by tracing out Bob's remaining mode b. In the final step, Bob performs a heterodyne measurement on his retained mode. With the associated probability distribution $p(\tilde{\kappa}\,\mathbb{B}, p_B|\kappa\,\mathbb{A}\,\gamma)$ and by integrating over p_B we obtain

$$p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma) = \frac{1}{\sqrt{2\pi V_b}} \times \exp\left[-\frac{1}{2V_b}\left(\tilde{\kappa}\,\mathbb{B} - \sqrt{(\mu^2-1)\frac{\eta\tau_B}{2}}\frac{\left(\gamma + \kappa\,\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\right)}{\upsilon}\right)^2\right], \tag{15}$$

where

$$V_b = (\mu+1)\left(1 - \frac{\mu-1}{\upsilon}\frac{\eta\tau_B}{2}\right). \tag{16}$$

In the following sections, we derive the secret key rate of the protocol for both eavesdropping scenarios based on the secret encoding variable κ and Bob's variable $\tilde{\kappa}$. We first compute the mutual information and then the Holevo bound and finally we introduce the postselection procedure and calculate the postselected rate.

III. MUTUAL INFORMATION

The first step in the calculations of the secret key rate is to establish the mutual information between Alice and Bob using the protocol outputs. The mutual information formula is given, independently of the eavesdropping strategy, by

$$I(\kappa : \tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B}\,\gamma) = H(\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma) - H(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma), \tag{17}$$

where, for random variables X and Y, $H(X|Y) = \int p(y)H_{X|y}dy$ is the conditional entropy of X given Y and $H_{X|y}$ is the entropy of X conditioned on Y taking the value y. The first term of the mutual information is therefore given by

$$H(\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma) = \int p(\mathbb{A}\,\mathbb{B}\,\gamma)H_{\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma}d\,\mathbb{A}\,d\,\mathbb{B}\,d\,\gamma, \tag{18}$$

while the second may be expressed as

$$H(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma) = \int p(\mathbb{A}\,\mathbb{B}\,\gamma)\sum_{\tilde{\kappa}} p(\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B}\,\gamma)H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma}d\,\mathbb{A}\,d\,\mathbb{B}\,d\,\gamma, \tag{19}$$

where $H_{\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma}$ and $H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma}$ reduce to the binary entropy of respective probabilities $p(\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma)$ and $p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma)$. We can derive the latter probability using Bayes's theorem as

$$\begin{aligned} p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma) &= \frac{p(\gamma\,|\kappa\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B})p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B})}{\sum_\kappa p(\gamma\,|\kappa\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B})p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B})} \\ &= \frac{1}{1+\exp\left[2\kappa\,\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\left(\gamma - \tilde{\kappa}\,\mathbb{B}\sqrt{\frac{1}{2}\eta\tau_B}\right)\upsilon^{-1}\right]}, \end{aligned} \tag{20}$$

where we have used the fact that κ, $\tilde{\kappa}$, $\mathbb{A}$, and $\mathbb{B}$ are independent variables. Using the same logic, we derive

$$p(\tilde{\kappa}\,|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma) = \frac{1}{1+\exp\left[-2\,\tilde{\kappa}\,\mathbb{B}\sqrt{\frac{1}{2}\eta\tau_B}\left(\gamma + \kappa\,\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\right)\upsilon^{-1}\right]}. \tag{21}$$

We also require the probabilities of each of κ and $\tilde{\kappa}$ with conditioning on $\mathbb{A}$, $\mathbb{B}$, and γ only. We have

$$\begin{aligned} p(\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma) &= \frac{\sum_{\tilde{\kappa}} p(\gamma\,|\kappa\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B})p(\kappa\,\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B})}{\sum_{\kappa,\tilde{\kappa}} p(\gamma\,|\kappa\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B})p(\kappa\,\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B})} \\ &= \frac{1}{1+\left(\frac{p(+|1\,\mathbb{A}\,\mathbb{B}\,\gamma)}{p(-|0\,\mathbb{A}\,\mathbb{B}\,\gamma)}\right)^\kappa \exp\left[2\kappa\sqrt{\frac{1}{2}\eta}(\mathbb{B}\sqrt{\tau_B} + \mathbb{A}\sqrt{\tau_A})\upsilon^{-1}\right]}, \end{aligned} \tag{22}$$

where we note that $p(\kappa\,\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B}) = 1/4$ for all combinations of κ and $\tilde{\kappa}$ due to the independence of the variables. Using the same logic, we obtain the remaining probability required for

the calculation of the conditional entropies,

$$p(\tilde{\kappa} \mid \mathbb{A}\,\mathbb{B}\,\gamma) = \frac{1}{1+\left(\frac{p(0|-\mathbb{A}\,\mathbb{B}\,\gamma)}{p(1|+\mathbb{A}\,\mathbb{B}\,\gamma)}\right)^{\tilde{\kappa}} \exp\left[-2\,\tilde{\kappa}\,\sqrt{\tfrac{1}{2}\eta}(\mathbb{B}\,\sqrt{\tau_B}+\mathbb{A}\,\sqrt{\tau_A})\upsilon^{-1}\right]}. \tag{23}$$

The final probability we require is the total probability of all of the postselection variables, which is given by

$$p(\mathbb{A}\,\mathbb{B}\,\gamma) = \sum_{\kappa,\tilde{\kappa}} p(\gamma\,|\kappa\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}) p(\kappa\,\mathbb{A}) p(\tilde{\kappa}\,\mathbb{B}). \tag{24}$$

The probabilities for the computation of the mutual information in the restricted eavesdropping scenario are slightly more complicated due to Bob's TMSV state; however, the first conditional probability is easily attainable as

$$\begin{aligned} p(\tilde{\kappa}\,|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma) &= \frac{p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma)}{\sum p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma)} \\ &= \frac{1}{1+\exp\left[-2\,\tilde{\kappa}\,\mathbb{B}\left(\gamma+\kappa\,\mathbb{A}\,\sqrt{\tfrac{1}{2}\eta\tau_A}\right)\Delta\;\tilde{\upsilon}'^{-1}\right]}, \end{aligned} \tag{25}$$

where we have defined

$$\tilde{\upsilon}' = (1-\eta)S + \frac{\eta}{2}[\tau_A+\tau_B+\omega_A(1-\tau_A)+\omega_B(1-\tau_B)] \tag{26}$$

and

$$\Delta = \sqrt{\frac{\eta}{2}\frac{1}{\tau_B}}\sqrt{\frac{\mu-1}{\mu+1}}. \tag{27}$$

In order to calculate the reverse probability $p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma)$, we first compute

$$\begin{aligned} p(\kappa|\,\mathbb{A}\,\gamma) &= \frac{p(\gamma|\kappa\,\mathbb{A})}{\sum_{\kappa} p(\gamma|\kappa\,\mathbb{A})} \\ &= \frac{1}{1+\exp\left(2\kappa\,\mathbb{A}\,\gamma\sqrt{\tfrac{1}{2}\eta\tau_A}\tilde{\upsilon}^{-1}\right)} \end{aligned} \tag{28}$$

and then the required probability can be derived as

$$\begin{aligned} p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma) &= \frac{p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma)p(\kappa|\,\mathbb{A}\,\gamma)}{\sum_{\kappa} p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma)p(\kappa|\,\mathbb{A}\,\gamma)} \\ &= \frac{1}{1+\exp\left[2\kappa\,\mathbb{A}\,\sqrt{\tfrac{1}{2}\eta\tau_A}(\gamma'-\tilde{\kappa}\,\mathbb{B}\,\Delta)\tilde{\upsilon}'^{-1}\right]}, \end{aligned} \tag{29}$$

where we have defined

$$\gamma' = \frac{1}{\tilde{\upsilon}}\left(\tilde{\upsilon}'+\frac{\eta}{2}\frac{1}{\tau_B}(\mu-1)\right)\gamma. \tag{30}$$

We can now compute the total probabilities of κ and $\tilde{\kappa}$ as

$$\begin{aligned} p(\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma) &= \frac{\sum_{\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma)p(\kappa|\,\mathbb{A}\,\gamma)}{\sum_{\kappa,\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma)p(\kappa|\,\mathbb{A}\,\gamma)} \\ &= \frac{1}{1+\Xi_{\kappa}\exp\left[2\kappa\,\mathbb{A}\,\sqrt{\tfrac{1}{2}\eta\tau_A}(\gamma'+\mathbb{B}\,\Delta)\tilde{\upsilon}'^{-1}\right]} \end{aligned} \tag{31}$$

and

$$p(\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B}\,\gamma) = \frac{1}{1+\Xi_{\tilde{\kappa}}\exp\left[-2\,\tilde{\kappa}\,\mathbb{B}(\gamma-\mathbb{A}\,\sqrt{\tfrac{1}{2}\eta\tau_A})\tilde{\upsilon}'^{-1}\Delta\right]}, \tag{32}$$

with

$$\Xi_m = \left(\frac{p(1|+\mathbb{A}\,\mathbb{B}\,\gamma)}{p(1|-\mathbb{A}\,\mathbb{B}\,\gamma)}\right)^{m}. \tag{33}$$

Finally, the total probability of the three postselection variables becomes

$$p(\mathbb{A}\,\mathbb{B}\,\gamma) = \sum_{\kappa,\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}\,|\kappa\,\mathbb{A}\,\gamma)p(\gamma|\kappa\,\mathbb{A})p(\kappa\,\mathbb{A}). \tag{34}$$

IV. HOLEVO BOUND

In our consideration of Eve's accessible information on the secret variable, we use the Holevo bound, which quantifies the maximum amount of information Eve may attain using any strategy permitted by the laws of quantum mechanics. We may write the bound as

$$\chi(\mathfrak{E}':\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma) = S(\mathfrak{E}'|\,\mathbb{A}\,\mathbb{B}\,\gamma) - S(\mathfrak{E}'|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma), \tag{35}$$

where $S(X|x) := \int p(x)S(\hat{\rho}_{X|x})dx$ is the conditional von Neumann entropy (VNE) of system X on variable x with corresponding probability distribution $p(x)$, and $S(\hat{\rho})$ is the VNE of state $\hat{\rho}$, defined as

$$S(\hat{\rho}) = -\sum_i \lambda_i \log_2 \lambda_i, \tag{36}$$

where $\{\lambda_i\}$ are the eigenvalues of $\hat{\rho}$.

The first term of the Holevo bound can be written as

$$S(\mathfrak{E}'|\,\mathbb{A}\,\mathbb{B}\,\gamma) = \int p(\mathbb{A}\,\mathbb{B}\,\gamma)S(\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\mathbb{B}\,\gamma})d\,\mathbb{A}\,d\,\mathbb{B}\,d\,\gamma, \tag{37}$$

where $\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\mathbb{B}\,\gamma}$ is Eve's total state, which can be derived from the output state of the protocol as

$$\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\mathbb{B}\,\gamma} = \sum_{\kappa,\tilde{\kappa}} p(\kappa\,\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B}\,\gamma)\hat{\rho}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\tilde{\kappa}\,\mathbb{B}\,\gamma}. \tag{38}$$

Similarly, the second (conditional) term is given by

$$S(\mathfrak{E}'|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma) = \int p(\mathbb{A}\,\mathbb{B}\,\gamma)\sum_{\kappa} p(\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma)S(\hat{\rho}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma})d\,\mathbb{A}\,d\,\mathbb{B}\,d\,\gamma, \tag{39}$$

where $\hat{\rho}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma}$ is Eve's conditional state given by

$$\hat{\rho}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma} = \sum_{\tilde{\kappa}} p(\tilde{\kappa}\,|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma)\hat{\rho}_{\mathfrak{E}'|\kappa\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma}. \tag{40}$$

Neither the total nor the condition states are Gaussian, and computing their entropy directly in the Fock basis is a difficult problem. Instead, we follow a method originating from Refs. [45,46] for one-way protocols with coherent states, and with little added complexity we derive the equivalent method for the MDI protocol with coherent states.

Let us first note that Eve's state emerging from the protocol is pure and can be written in the shorthand notation

$$\hat{\rho}_{\mathfrak{E}'|\kappa\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma} = \hat{\mathfrak{E}}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}} = \left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}}\right\rangle\!\left\langle\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}}\right|. \tag{41}$$

For convenience we also introduce the shorthand notation

$$p^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}} \equiv p(\kappa\,\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B}\,\gamma), \tag{42}$$

$$p^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\tilde{\kappa}\,|\kappa} \equiv p(\tilde{\kappa}\,|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma). \tag{43}$$

Using the broadcast values $\mathbb{A}$, p_A, $\mathbb{B}$, p_B, and γ, Eve knows that her total state is a convex combination of the four states $|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{0+}\rangle$, $|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{0-}\rangle$, $|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{1+}\rangle$, and $|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{1-}\rangle$ and her state can be expressed in a four-dimensional space. Note that in our notation we use Alice's assigned bit values 0 (1) to represent $\kappa = +\,(-)$ in order to aide distinguishability between κ and $\tilde{\kappa}$.

Let us rewrite the total state in Eq. (38) as

$$\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\mathbb{B}\,\gamma} = \sum_{\kappa,\tilde{\kappa}} p^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}} \left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}}\right\rangle\!\left\langle\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}}\right|. \tag{44}$$

To examine the information held by Eve in her state we can compute the matrix of all overlaps $\mathbf{S}$ whose elements S_{ij} are given by the overlaps $\langle\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa_1\,\tilde{\kappa}_1}|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa_2\,\tilde{\kappa}_2}\rangle$ of Eve's possible states. We may write the matrix of all overlaps as

$$\mathbf{S} = \begin{array}{c} \begin{matrix} 0+ & 0- & 1+ & 1- \end{matrix} \\ \begin{pmatrix} 1 & B & A & AB \\ B & 1 & AB & A \\ A & AB & 1 & B \\ AB & A & B & 1 \end{pmatrix} \end{array} \begin{matrix} 0+ \\ 0- \\ 1+ \\ 1- \end{matrix}, \tag{45}$$

where we have ignored phase factors that may always be removed by multiplying the states $|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}}\rangle$ by other appropriate phase factors. The matrix of overlaps reveals the interrelationship between the basis vectors in Eve's total state. It can be seen that the matrix is expressible in tensor-product form as

$$\mathbf{S} = \begin{pmatrix} 1 & A \\ A & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & B \\ B & 1 \end{pmatrix}, \tag{46}$$

which implies that Eve's state is the product of two states in two-dimensional Hilbert spaces, which we write as

$$\left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa\,\tilde{\kappa}}\right\rangle = \left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa}\right\rangle\left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\tilde{\kappa}}\right\rangle. \tag{47}$$

The individual states can be expanded as

$$\left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{0}\right\rangle = c_0\,|\Phi_0\rangle + c_1\,|\Phi_1\rangle, \tag{48}$$

$$\left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{1}\right\rangle = c_0\,|\Phi_0\rangle - c_1\,|\Phi_1\rangle \tag{49}$$

and

$$\left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{+}\right\rangle = c_+\,|\Phi_+\rangle + c_-\,|\Phi_-\rangle, \tag{50}$$

$$\left|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{-}\right\rangle = c_+\,|\Phi_+\rangle - c_-\,|\Phi_-\rangle, \tag{51}$$

where $\{|\Phi_0\rangle, |\Phi_1\rangle\}$ and $\{|\Phi_+\rangle, |\Phi_-\rangle\}$ are orthonormal basis sets for the Hilbert spaces spanned by $|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\kappa}\rangle$ and $|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{\tilde{\kappa}}\rangle$, respectively.

Our focus now turns to relating the coefficients to the overlaps A and B. We perform the inner products

$$\left\langle\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{0}|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{0}\right\rangle = |c_0|^2 + |c_1|^2 = 1, \tag{52}$$

$$\left\langle\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{0}|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{1}\right\rangle = |c_0|^2 - |c_1|^2 = A, \tag{53}$$

from which we obtain expressions for the absolute values of the coefficients c_0 and c_1 of

$$|c_0|^2 = \tfrac{1}{2}(1 + A), \tag{54}$$

$$|c_1|^2 = \tfrac{1}{2}(1 - A), \tag{55}$$

and following a similar calculation we arrive at the expressions for the absolute values of the remaining coefficients

$$|c_+|^2 = \tfrac{1}{2}(1 + B), \tag{56}$$

$$|c_-|^2 = \tfrac{1}{2}(1 - B). \tag{57}$$

The values A and B are computed from the overlap formula for Gaussian states [49], which, for two pure states $\hat{\rho}_1$ and $\hat{\rho}_2$ with the same CM $\mathbf{V}$ and different mean values $\bar{\mathbf{x}}_1$ and $\bar{\mathbf{x}}_2$, reduces to

$$\mathrm{Tr}(\hat{\rho}_1\hat{\rho}_2) = \exp[-\tfrac{1}{4}(\bar{\mathbf{x}}_1 - \bar{\mathbf{x}}_2)^{\mathsf{T}}\mathbf{V}^{-1}(\bar{\mathbf{x}}_1 - \bar{\mathbf{x}}_2)] \tag{58}$$

and our coefficients A and B become

$$A = \left\langle\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{0}|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{1}\right\rangle = \exp\left[-\frac{1}{2}\,\mathbb{A}^2\left(1 - \frac{\eta\tau_A}{\upsilon}\right)\right] \tag{59}$$

and

$$B = \left\langle\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{+}|\mathfrak{E}'^{\mathbb{A}\,\mathbb{B}\,\gamma}_{-}\right\rangle = \exp\left[-\frac{1}{2}\,\mathbb{B}^2\left(1 - \frac{\eta\tau_B}{\upsilon}\right)\right]. \tag{60}$$

We now have all of the tools required to compute Eve's total state using Eq. (44). We arrive at the matrix

$$\hat{\mathfrak{E}}'^{\mathbb{A}\,\mathbb{B}\,\gamma} = \begin{pmatrix} |c_0|^2|c_+|^2 & |c_0|^2c_+c_-^*\Lambda(+,-,+,-) & |c_+|^2c_0c_1^*\Lambda(+,+,-,-) & c_0c_+c_1^*c_-^*\Lambda(+,-,-,+) \\ |c_0|^2c_-c_+^*\Lambda(+,-,+,-) & |c_0|^2|c_-|^2 & c_0c_-c_1^*c_+^*\Lambda(+,-,-,+) & |c_-|^2c_0c_1^*\Lambda(+,+,-,-) \\ |c_+|^2c_1c_0^*\Lambda(+,+,-,-) & c_1c_+c_0^*c_-^*\Lambda(+,-,-,+) & |c_1|^2|c_+|^2 & |c_1|^2c_+c_-^*\Lambda(+,-,+,-) \\ c_1c_-c_0^*c_+^*\Lambda(+,-,-,+) & |c_-|^2c_1c_0^*\Lambda(+,+,-,-) & |c_1|^2c_0c_+^*\Lambda(+,-,+,-) & |c_1|^2|c_-|^2 \end{pmatrix}, \tag{61}$$

where we have defined

$$\Lambda(s_1, s_2, s_3, s_4) = s_1 p_{0+}^{\mathbb{A}\mathbb{B}\gamma} + s_2 p_{0-}^{\mathbb{A}\mathbb{B}\gamma} + s_3 p_{1+}^{\mathbb{A}\mathbb{B}\gamma} + s_4 p_{1-}^{\mathbb{A}\mathbb{B}\gamma}. \tag{62}$$

To obtain the entropy of the total state, we first compute the eigenvalues of Eq. (61), which amounts to solving a quartic equation in which the coefficients are combinations of the absolute values of the basis coefficients. We then compute their VNE using Eq. (36). This entropy is then substituted into Eq. (37) to obtain the first term of the Holevo bound.

In order to compute the conditional state and the second term of the Holevo bound, we construct the density matrices of the conditional states. First, we have

$$\hat{\mathfrak{E}}_0^{\prime\,\mathbb{A}\mathbb{B}\gamma} = |\mathfrak{E}_0^{\prime\,\mathbb{A}\mathbb{B}\gamma}\rangle\langle\mathfrak{E}_0^{\prime\,\mathbb{A}\mathbb{B}\gamma}| \otimes \big(p_{+|0}^{\mathbb{A}\mathbb{B}\gamma} |\mathfrak{E}_+^{\prime\,\mathbb{A}\mathbb{B}\gamma}\rangle\langle\mathfrak{E}_+^{\prime\,\mathbb{A}\mathbb{B}\gamma}| + p_{-|0}^{\mathbb{A}\mathbb{B}\gamma} |\mathfrak{E}_-^{\prime\,\mathbb{A}\mathbb{B}\gamma}\rangle\langle\mathfrak{E}_-^{\prime\,\mathbb{A}\mathbb{B}\gamma}|\big), \tag{63}$$

which has corresponding eigenvalues

$$\lambda_{1,2}^0 = \tfrac{1}{2}\Big(1 \pm \sqrt{1 - 16 p_{+|0}^{\mathbb{A}\mathbb{B}\gamma} p_{-|0}^{\mathbb{A}\mathbb{B}\gamma} |c_-|^2 |c_+|^2}\Big). \tag{64}$$

Then, for the counterpart state we have

$$\hat{\mathfrak{E}}_1^{\prime\,\mathbb{A}\mathbb{B}\gamma} = |\mathfrak{E}_1^{\prime\,\mathbb{A}\mathbb{B}\gamma}\rangle\langle\mathfrak{E}_1^{\prime\,\mathbb{A}\mathbb{B}\gamma}| \otimes \big(p_{+|1}^{\mathbb{A}\mathbb{B}\gamma} |\mathfrak{E}_+^{\prime\,\mathbb{A}\mathbb{B}\gamma}\rangle\langle\mathfrak{E}_+^{\prime\,\mathbb{A}\mathbb{B}\gamma}| + p_{-|1}^{\mathbb{A}\mathbb{B}\gamma} |\mathfrak{E}_-^{\prime\,\mathbb{A}\mathbb{B}\gamma}\rangle\langle\mathfrak{E}_-^{\prime\,\mathbb{A}\mathbb{B}\gamma}|\big), \tag{65}$$

with eigenvalues

$$\lambda_{1,2}^1 = \tfrac{1}{2}\Big(1 \pm \sqrt{1 - 16 p_{+|1}^{\mathbb{A}\mathbb{B}\gamma} p_{-|1}^{\mathbb{A}\mathbb{B}\gamma} |c_-|^2 |c_+|^2}\Big). \tag{66}$$

Using the eigenvalues of the two states, it is straightforward to compute the second term of the Holevo bound using Eq. (39).

A. Restricted eavesdropping

Let us now consider Eve's accessible information in the restricted eavesdropping scenario. In this case, Eve has to distinguish between two states corresponding to the two possible values of κ. Under these conditions, it is possible to consider both individual and collective attacks as we will outline in the following sections.

1. Individual attacks

Let us first examine the case in which Eve employs individual attacks and may not access a quantum memory. In this case the mutual information between Alice and Eve I_{AE} can be estimated by from Eve's error probability using the fidelity F of Eve's two possible states $\hat{\rho}_{\mathfrak{E}'|+\mathbb{A}\,\gamma}$ and $\hat{\rho}_{\mathfrak{E}'|-\mathbb{A}\,\gamma}$, which we compute using Eq. (58). We apply the lower bound

$$F_- = \frac{1 - \sqrt{1 - F}}{2} \tag{67}$$

in order to bound Eve's error probability from below, modeling a worst-case scenario for Alice and Bob [50]. The total expression for the mutual information I_{AB} becomes

$$I_{AE} = \int p(\mathbb{A}\,\gamma)[1 - H_2(F_-)] d\,\mathbb{A}\, d\gamma, \tag{68}$$

where $H_2(p)$ is the binary entropy.

2. Collective attacks

In the case of collective attacks we must compute the Holevo bound in order to establish an upper bound on Eve's accessible information. The Holevo bound is given by

$$\chi^{\mathrm{RE}}(\mathfrak{E}' : \kappa|\,\mathbb{A}\,\gamma) = S(\mathfrak{E}'|\,\mathbb{A}\,\gamma) - S(\mathfrak{E}'|\kappa\,\mathbb{A}\,\gamma), \tag{69}$$

where the first term can be written as

$$S(\mathfrak{E}'|\,\mathbb{A}\,\gamma) = \int p(\mathbb{A}\,\gamma) S(\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\gamma}) d\,\mathbb{A}\, d\,\gamma, \tag{70}$$

where $\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\gamma}$ is the total state, given by

$$\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\gamma} = \sum_\kappa p(\kappa|\,\mathbb{A}\,\gamma) \hat{\rho}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\gamma}. \tag{71}$$

As it is derived from the sum of two Gaussian states, the total state is non-Gaussian. To avoid the difficulty in obtaining the entropy of this state from its photon statistics, we may employ a non-Gaussian entropy approximation, which we derive in Appendix B. Using the main result, we may write the CM of the total state as

$$\mathbf{V}_{\mathfrak{E}'|\,\mathbb{A}} = \mathbf{V}_{\mathfrak{E}'|\kappa\,\mathbb{A}} + p(+|\,\mathbb{A}\,\gamma) p(-|\,\mathbb{A}\,\gamma) \Delta\bar{\mathbf{x}}_{\mathfrak{E}'} \cdot \Delta\bar{\mathbf{x}}_{\mathfrak{E}'}^{\mathsf{T}}, \tag{72}$$

where $\Delta\bar{\mathbf{x}}_{\mathfrak{E}'} = \bar{\mathbf{x}}_{\mathfrak{E}'|+\mathbb{A}\,\gamma} - \bar{\mathbf{x}}_{\mathfrak{E}'|-\mathbb{A}\,\gamma}$. Taking the entropy of this state via the symplectic eigenvalues $\{\nu_i\}$ of its CM provides an upper bound on the exact entropy of Eve's total state as it assumes this state to be Gaussian. We therefore have

$$S(\hat{\rho}_{\kappa\,\mathbb{A}\,\gamma}) < S(\mathbf{V}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\gamma}) = \sum_i h(\nu_i), \tag{73}$$

where

$$h(x) = \frac{x+1}{2} \log_2 \frac{x+1}{2} - \frac{x-1}{2} \log_2 \frac{x-1}{2}. \tag{74}$$

Meanwhile, the second term of the Holevo bound involves a Gaussian state and can be computed directly from the protocol output, independently of any measurement outcome. As described in Sec. II, Eve's CM $\mathbf{V}_{\mathfrak{E}'|\kappa\,\mathbb{A}}$ after the relay measurements is obtained by tracing out Bob's remaining mode. The entropy is then simply computed from the symplectic eigenvalues $\{\upsilon_i\}$ of the remaining CM by

$$S(\hat{\rho}_{\mathfrak{E}'|\kappa\,\mathbb{A}}) = S(\mathbf{V}_{\mathfrak{E}'|\kappa\,\mathbb{A}}) = \sum_i h(\upsilon_i). \tag{75}$$

The Holevo bound is then reduced to the expression

$$\chi(\mathfrak{E}' : \kappa|\,\mathbb{A}\,\gamma) \leqslant \int p(\mathbb{A}\,\gamma) S(\mathbf{V}_{\mathfrak{E}'|\,\mathbb{A}\,\gamma}) d\,\mathbb{A}\, d\,\gamma - S(\mathbf{V}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\gamma}). \tag{76}$$

V. APPLICATION OF POSTSELECTION

We have now computed all of the components required for the calculation of the secret key rate and we can now describe the postselection step that improves the range of our protocol. Let us first write the mutual information as a single integrand in the form

$$I_{AB} = \int p(\mathbb{A}\,\mathbb{B}\,\gamma) \tilde{I}_{AB}(\mathbb{A}, \mathbb{B}, \gamma) d\,\mathbb{A}\, d\,\mathbb{B}\, d\,\gamma, \tag{77}$$

where we defined the *single-point* mutual information $\tilde{I}_{AB}(\mathbb{A},\mathbb{B},\gamma) = H_{\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma} - \sum_{\tilde{\kappa}} p(\tilde{\kappa}\,|\,\mathbb{A}\,\mathbb{B}\,\gamma) H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\,\mathbb{B}\,\gamma}$. Similarly, we can write the Holevo bound as a single integrand

$$\chi = \int p(\mathbb{A}\,\mathbb{B}\,\gamma)\tilde{\chi}(\mathbb{A},\mathbb{B},\gamma) d\,\mathbb{A}\,d\,\mathbb{B}\,d\gamma, \tag{78}$$

with $\tilde{\chi}$ the single-point Holevo bound given by

$$\tilde{\chi} = S(\hat{\rho}_{\mathfrak{E}'|\,\mathbb{A}\,\mathbb{B}\,\gamma}) - \sum_{\kappa} p(\kappa|\,\mathbb{A}\,\mathbb{B}\,\gamma) S(\rho_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\mathbb{B}\,\gamma}). \tag{79}$$

In the same way, we define the single-point Holevo bound for restricted eavesdropping $\tilde{\chi}^{\mathrm{RE}}$ for collective attacks and the single-point mutual information between Alice and Eve $\tilde{I}_{AE}$ for individual attacks,

$$\chi^{\mathrm{RE}} \leqslant S(\mathbf{V}_{\mathfrak{E}'|\,\mathbb{A}\,\gamma}) - S(\mathbf{V}_{\mathfrak{E}'|\kappa\,\mathbb{A}\,\gamma}), \tag{80}$$

$$\tilde{I}_{AE} = 1 - H_2(F_-). \tag{81}$$

Using these definitions, we may define the single-point rate $\tilde{R} = \tilde{I}_{AB} - \tilde{\chi}$ for complete eavesdropping, $\tilde{R} = \tilde{I}_{AB} - \tilde{\chi}^{\mathrm{RE}}$ for restricted eavesdropping, and $\tilde{R} = \tilde{I}_{AB} - \tilde{I}_{AE}$ for individual attacks. We can then express the secret key rate in terms of the single-point rate as

$$R = \int p(\mathbb{A}\,\mathbb{B}\,\gamma)\tilde{R}(\mathbb{A},\mathbb{B},\gamma) d\,\mathbb{A}\,d\,\mathbb{B}\,d\,\gamma\,. \tag{82}$$

For postselection, we are interested in the region where the single-point rate is positive so that the parties can choose to only include instances of the protocol that contribute positively to the key rate. We can therefore define the postselected key rate as

$$R_{\mathrm{PS}} = \int p(\mathbb{A}\,\mathbb{B}\,\gamma)\max\{\tilde{R}(\mathbb{A},\mathbb{B},\gamma),0\} d\,\mathbb{A}\,d\,\mathbb{B}\,d\,\gamma\,. \tag{83}$$

We can also define the postselection area Γ, which is simply the region of the $\mathbb{A}$-$\mathbb{B}$-γ volume in which the single-point rate is positive. Computing the postselected rate amounts to integrating the single-point rate in this volume,

$$R_{\mathrm{PS}} = \int_{\Gamma} p(\mathbb{A}\,\mathbb{B}\,\gamma)\tilde{R}(\mathbb{A},\mathbb{B},\gamma) d\,\mathbb{A}\,d\,\mathbb{B}\,d\,\gamma\,. \tag{84}$$

VI. RESULTS

Let us now present numerical results for the rates of our protocol under a variety of parameters. In order to express the rates as a function of the distance between the parties, we first use the relation $\tau = 10^{-\mathrm{dB}/10}$ to express the transmissivity in terms of the loss in decibels. Then, if the protocol is performed with standard optical fiber, the length of the links can be expressed in kilometers, assuming a loss per kilometer of 0.2 dB/km. We use the excess noise to express the variances ω_A and ω_B in terms of the transmissivities of the channels. By considering each link to be a point-to-point channel we write

$$\omega_{A\,(B)} = 1 + \epsilon_{A\,(B)} \frac{\eta\tau_{A\,(B)}/2}{1 - \eta\tau_{A\,(B)}/2}, \tag{85}$$

where $\epsilon_{A\,(B)}$ is the excess noise in the Alice-relay (Bob-relay) links.

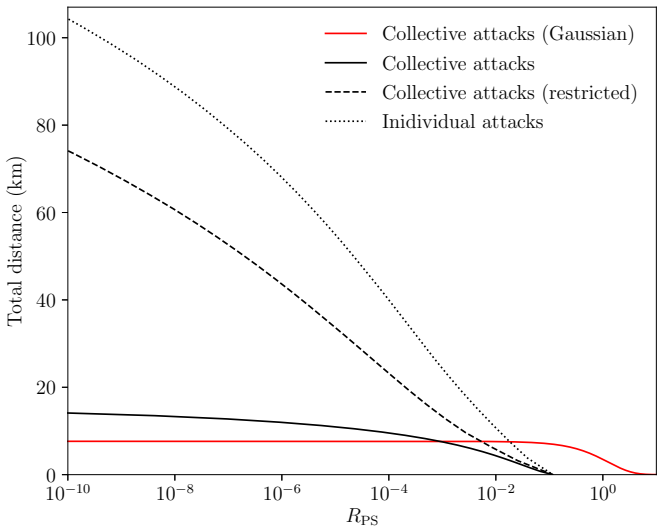

FIG. 3. Rates of the pure-loss symmetric protocol as a function of the total distance between Alice and Bob with σ_A, σ_B, and μ optimized. The red line represents the rate of the symmetric Gaussian MDI protocol.

Figure 3 shows the total distance between Alice and Bob as a function of the rates of all variations of the protocol in the symmetric configuration ($\tau_A = \tau_B$) and assuming a pure-loss attack ($\epsilon = \epsilon_A = \epsilon_B = 0$) with perfect detection efficiency. The rates are optimized over the variances σ_A and σ_B (σ_A and μ for restricted eavesdropping). For comparison we include the rate of the original Gaussian MDI protocol [32] with equivalent parameters. At the cost of a lower rate at short distances, our protocol improves the range at which the parties may communicate. It is important to note that a fully secure rate in which Bob broadcasts less information may lie anywhere between the rates of the complete and restricted eavesdropping cases, but despite being the worst-case scenario, the rate under complete eavesdropping offers a notable advantage over the Gaussian MDI protocol.

Figure 4 shows rates of protocol under complete eavesdropping as a function of the total distance between Alice and Bob. We show the pure-loss rate with ideal parameters $\eta = 1$ and $\beta = 1$ as well as a realistic rate with excess noise $\epsilon = 0.05$, detector efficiency of 98%, and reconciliation efficiency of 95%. Again, we also show the optimal rates of the Gaussian MDI protocol with identical parameters. Our protocol provides an advantage over the original MDI protocol under ideal as well as realistic parameters. In Fig. 5 we explore the asymmetric configuration of the protocol under complete eavesdropping. We see that our protocol offers the biggest advantage as the symmetry of the configuration increases. However, we still observe an advantage in the asymmetric regime up to very asymmetric configurations with less than 1 km separating Alice from the relay.

To explore the effect of the realistic parameters in more detail, we consider in Fig. 6, for individual and collective attacks with restricted eavesdropping, the rates with $\epsilon = 0.05$, $\eta = 0.8$, and $\beta = 0.95$ (these are typical choices [51]) in the symmetric configuration. For each rate, we have incorporated η by scaling the transmissivities on each link. This has a

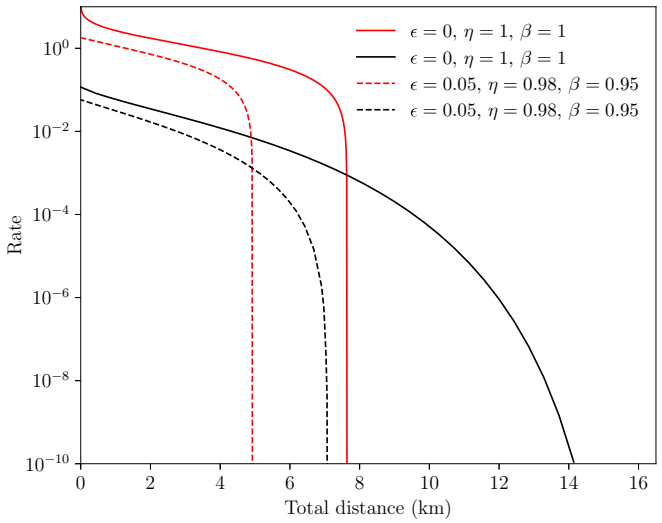

FIG. 4. Rates of the symmetric protocol function of the total distance between Alice and Bob with σ_A and σ_B optimized (black lines). For comparison, we include the original Gaussian MDI protocol with optimal parameters (red lines). The solid lines correspond to the pure-loss protocols with ideal parameters $\eta = 1$ and $\beta = 1$, while the dashed lines correspond to a realistic scenario in which $\epsilon = 0.05$, $\eta = 0.98$, and $\beta = 0.95$.

considerable effect on the rate but a distance exceeding 60 km with collective attacks is still possible. In Appendix A we consider the optimal parameters σ_A and μ for an experimental configuration.

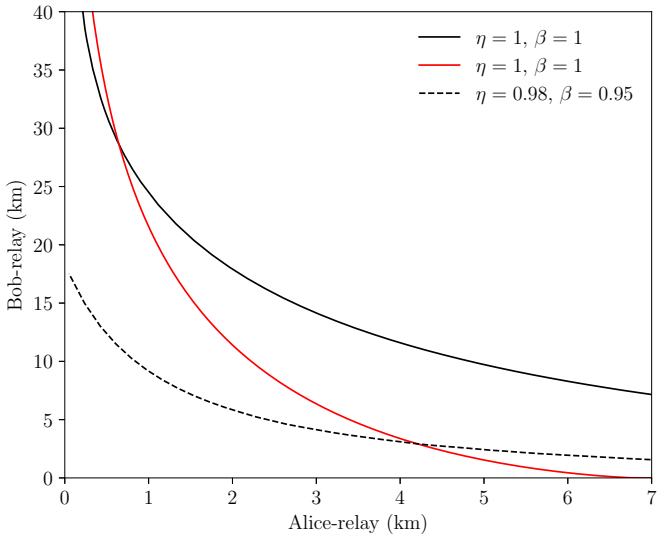

FIG. 5. Comparison of the maximum Bob-relay distance as a function of the Alice-relay distance under complete eavesdropping. The black lines represent our protocol with the solid line corresponding to the pure-loss case with ideal parameters $\eta = 1$ and $\beta = 1$ and the dashed line corresponding to case with $\epsilon = 0.05$ and imperfect parameters $\eta = 0.98$ and $\beta = 0.95$. For comparison, the red line represents the pure-loss Gaussian MDI protocol with ideal parameters.

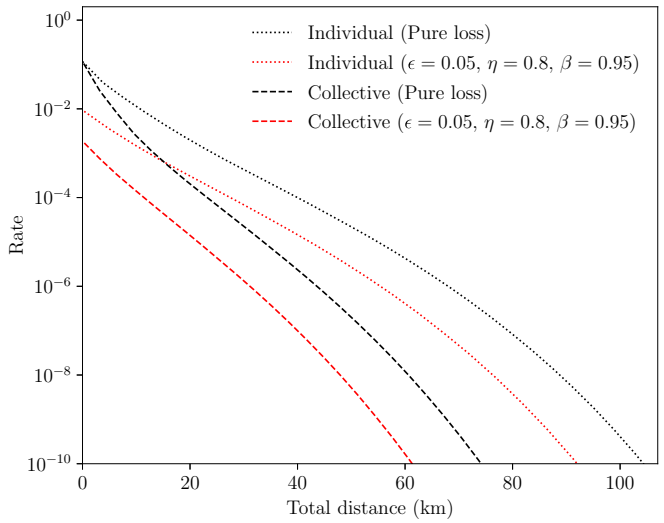

FIG. 6. Rates of the symmetric protocol with restricted eavesdropping as a function of the total distance between Alice and Bob with σ_A and μ optimized. The black lines correspond to the pure-loss case with perfect detection and reconciliation, while the red lines represent the rate with parameters $\epsilon = 0.05$, $\eta = 0.8$, and $\beta = 0.95$.

VII. CONCLUSION

In this work, we have introduced a long-distance CV MDI QKD protocol with a general mathematical formulation with collective attacks which can include excess noise and experimental inefficiencies. We have demonstrated that our protocol surpasses the range of the original Gaussian CV MDI QKD protocol in both symmetric and asymmetric configurations. This improvement exists in the most powerful eavesdropping scenario and is substantially increased to distances exceeding 50 km if restricted eavesdropping is considered with either individual or collective attacks. In future work, it would be beneficial to explore an achievable fully secure rate between these extremes if Bob can communicate all of the necessary information to Alice without broadcasting the absolute value of his measurement in each use of the protocol.

Our protocol is robust against excess noise as well as detection and reconciliation inefficiencies and it is therefore a significant step towards a realistic experimental implementation. We have demonstrated that CV MDI QKD need not be restricted to short distances. In fact, our protocol provides a theoretical framework for MDI QKD at distances previously achievable only with discrete variable protocols, obtainable with inexpensive and easily implementable equipment.

ACKNOWLEDGMENTS

This work was funded by the European Union via "Continuous Variable Quantum Communications" (Grant Agreement No. 820466) and the EPSRC via the "Quantum Communications hub" (Grants No. EP/M013472/1 and No. EP/T001011/1). S.P. would like to thank Y.-C. Zhang and X.-B. Wang for their useful suggestions about previous literature.

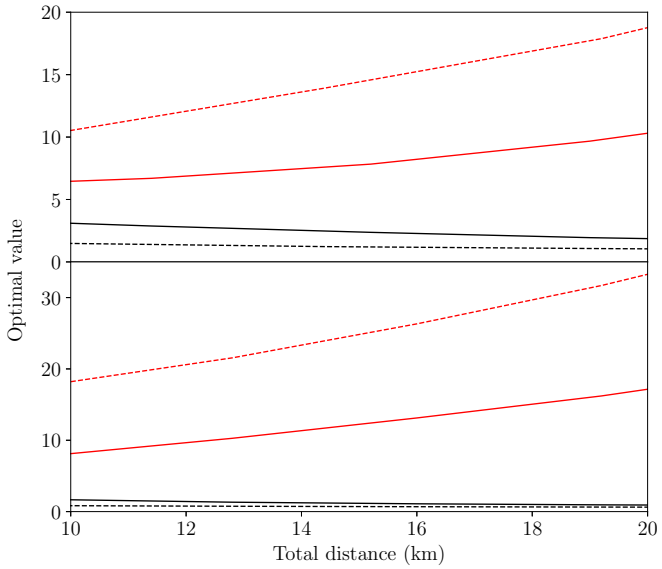

FIG. 7. Optimal parameters μ (red lines) and σ_A (black lines) for the protocol with restricted eavesdropping under individual attacks (top panel) and collective attacks (bottom panel). The solid lines represent the optimal parameters for the pure-loss case with ideal detection and the dashed lines represent the optimal parameters for $\epsilon = 0.05$, $\eta = 0.8$, and $\beta = 0.95$.

APPENDIX A: OPTIMAL PARAMETERS

For the purposes of a proof-of-concept experiment, we show in Fig. 7 the optimal parameters for the symmetric protocol with restricted eavesdropping under individual (top) and collective (bottom) attacks with the same parameters as those used for the rates in Fig. 6 between 10 and 20 km. The optimal values of μ are displayed with red lines, while black lines correspond to optimal values of σ_A. We note that the optimal parameters are small relative to the original Gaussian MDI protocol in which the optimal value of μ tends to infinity for perfect reconciliation efficiency.

APPENDIX B: ENTROPY APPROXIMATION OF A NON-GAUSSIAN STATE

To avoid a complex treatment of non-Gaussian states in the Fock basis, we introduce an approximation for the entropy of a particular type of non-Gaussian state that is composed of the average of two Gaussian states with the same CM and different mean values. We use the CM and mean values of the constituent states to write a formula for the CM of this state and then, by calculating the entropy of this CM, we obtain an estimate for its entropy. This approximation is most accurate for states with small higher-order moments, but it is an upper bound as it assumes the state to be Gaussian. This fact makes the approximation particularly useful in quantum key distribution when calculating the total entropy of an eavesdropper's non-Gaussian state in the Holevo bound.

We will label the constituent states of the state of interest as $\hat{\rho}_+$ and $\hat{\rho}_-$ with associated probabilities $p(+)$ and $p(-)$, respectively. The general non-Gaussian state can then be written as

$$\hat{\rho} = \sum_{\kappa=\pm} p(\kappa)\hat{\rho}_\kappa. \tag{B1}$$

Let us now recall the definitions of the mean value and CM of a Gaussian state $\hat{\rho}$. The mean value of an operator $\hat{x}_i$ for a state $\hat{\rho}$ is given by

$$\bar{x}_i = \langle \hat{x}_i \rangle = \mathrm{Tr}(\hat{x}_i \hat{\rho}) \tag{B2}$$

and the covariance matrix of a state is given by

$$V_{ij} = \tfrac{1}{2}\langle \{\Delta\hat{x}_i, \Delta\hat{x}_j\}\rangle = \tfrac{1}{2}\,\mathrm{Tr}[\{\hat{x}_i, \hat{x}_j\}\hat{\rho}] - \bar{x}_i\bar{x}_j. \tag{B3}$$

Using Eq. (B3), we can express the elements V_{ij} of the CM $\mathbf{V}$ of a constituent state $\hat{\rho}_\kappa$ with mean value $\bar{\mathbf{x}}^\kappa$ as

$$V_{ij}^\kappa + \bar{x}_i^\kappa \bar{x}_j^\kappa = \tfrac{1}{2}\,\mathrm{Tr}[\{\hat{x}_i, \hat{x}_j\}\hat{\rho}_\kappa] \tag{B4}$$

and we can also write the elements V'_{ij} of the CM $\mathbf{V}'$ of the total state $\hat{\rho}$ as

$$\begin{aligned} V'_{ij} &= \frac{1}{2}\,\mathrm{Tr}\left[\{\hat{x}_i, \hat{x}_j\}\left(\sum_{\kappa=\pm} p(\kappa)\hat{\rho}_\kappa\right)\right] - \bar{x}_i\bar{x}_j \\ &= \sum_{\kappa=\pm} p(\kappa)\tfrac{1}{2}\,\mathrm{Tr}[\{\hat{x}_i, \hat{x}_j\}\hat{\rho}_\kappa] - \bar{x}_i\bar{x}_j. \end{aligned} \tag{B5}$$

We then substitute into this expression the right-hand side of Eq. (B4) to obtain

$$\begin{aligned} V'_{ij} &= \sum_{\kappa=\pm} p(\kappa)\left(V_{ij}^\kappa + \bar{x}_i^\kappa \bar{x}_j^\kappa\right) - \bar{x}_i\bar{x}_j \\ &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)\bar{x}_i^\kappa \bar{x}_j^\kappa - \bar{x}_i\bar{x}_j, \end{aligned} \tag{B6}$$

where we have made use of the requirement that the CMs of the constituent states are identical. Now, by writing the mean values as $\bar{x}_i = \mathrm{Tr}(\hat{x}_i\hat{\rho}) = \sum_\kappa p(\kappa)\,\mathrm{Tr}(\hat{x}_i\hat{\rho}_k)$ and substituting into Eq. (B6), we obtain

$$V'_{ij} = V_{ij} + \sum_{\kappa=\pm} p(\kappa)\bar{x}_i^\kappa \bar{x}_j^\kappa - \sum_{\kappa=\pm}\sum_{\kappa'=\pm} p(\kappa)p(\kappa')\bar{x}_i^\kappa \bar{x}_j^{\kappa'} \tag{B7}$$

and by factoring out one of the sums we obtain

$$\begin{aligned} V'_{ij} &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)\left[\bar{x}_i^\kappa \bar{x}_j^\kappa - \sum_{\kappa'=\pm} p(\kappa')\bar{x}_i^\kappa \bar{x}_j^{\kappa'}\right] \\ &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)\left[\bar{x}_i^\kappa \bar{x}_j^\kappa - p(\kappa)\bar{x}_i^\kappa \bar{x}_j^\kappa - p(-\kappa)\bar{x}_i^\kappa \bar{x}_j^{-\kappa}\right] \\ &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)p(-\kappa)\bar{x}_i^\kappa\left(\bar{x}_j^\kappa - \bar{x}_j^{-\kappa}\right), \end{aligned} \tag{B8}$$

where we have used $1 - p(\kappa) = p(-\kappa)$. Note that $p(\kappa)p(-\kappa) = p(+)p(-)$ for either value of κ, and $\sum_\kappa \bar{x}_i^\kappa(\bar{x}_j^\kappa - \bar{x}_j^{-\kappa}) = (\bar{x}_j^+ - \bar{x}_j^-)\sum_\kappa \kappa\bar{x}_i^\kappa$. Therefore, we obtain

$$\begin{aligned} V'_{ij} &= V_{ij}^+ + p(+)p(-)(\bar{x}_j^+ - \bar{x}_j^-)\sum_{\kappa=\pm}\kappa\bar{x}_i^\kappa \\ &= V_{ij}^+ + p(+)p(-)(\bar{x}_j^+ - \bar{x}_j^-)(\bar{x}_i^+ - \bar{x}_i^-). \end{aligned} \tag{B9}$$

We can write this in compact outer product form as

$$\mathbf{V}' = \mathbf{V} + p(+)p(-)\Delta\bar{\mathbf{x}}\cdot\Delta\bar{\mathbf{x}}^{\mathsf{T}}, \tag{B10}$$

where $\Delta\bar{\mathbf{x}} = \bar{\mathbf{x}}^+ - \bar{\mathbf{x}}^-$.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, arXiv:1906.01645.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2002).

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

[5] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).

[6] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photon. **9**, 163 (2015).

[7] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, *Proceedings of the International Symposium on Information Theory* (IEEE, Piscataway, 2004), p. 136.

[8] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, Phys. Rev. Lett. **119**, 200501 (2017).

[9] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. Lita, A. Miller, and J. Nordholt, New J. Phys. **8**, 193 (2006).

[10] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, Opt. Express **16**, 18790 (2008).

[11] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, Phys. Rev. Lett. **120**, 030501 (2018).

[12] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

[13] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).

[14] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Opt. Lett. **41**, 3511 (2016).

[15] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang *et al.*, Quantum Sci. Technol. **4**, 035006 (2019).

[16] Y.-C. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Phys. Rev. Lett. **125**, 010502 (2020).

[17] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[18] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[19] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[20] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).

[21] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).

[22] H.-L. Yin and Y. Fu, Sci. Rep. **9**, 3045 (2019).

[23] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).

[24] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, arXiv:1805.05511.

[25] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Nat. Photon. **13**, 334 (2019).

[26] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X **8**, 031043 (2018).

[27] J. Lin and N. Lütkenhaus, Phys. Rev. A **98**, 042332 (2018).

[28] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Phys. Rev. A **98**, 062323 (2018).

[29] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sci. Rep. **9**, 3080 (2019).

[30] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Phys. Rev. Appl. **12**, 024061 (2019).

[31] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, Phys. Rev. A **101**, 042330 (2020).

[32] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).

[33] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).

[34] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).

[35] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Phys. Rev. A **90**, 052325 (2014).

[36] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).

[37] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Phys. Rev. A **96**, 042334 (2017).

[38] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A **97**, 052327 (2018).

[39] Z. Chen, Y. Zhang, G. Wang, Z. Li, and H. Guo, Phys. Rev. A **98**, 012314 (2018).

[40] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, Phys. Rev. A **97**, 042328 (2018).

[41] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Rev. A **97**, 042329 (2018).

[42] L. Huang, Y. Zhang, Z. Chen, and S. Yu, Entropy **21**, 1100 (2019).

[43] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Rev. A **99**, 022322 (2019).

[44] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[45] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

[46] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[47] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303(R) (2007).

[48] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[49] L. Banchi, S. L. Braunstein, and S. Pirandola, Phys. Rev. Lett. **115**, 260501 (2015).

[50] S. Pirandola and S. Lloyd, Phys. Rev. A **78**, 012331 (2008).

[51] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, Phys. Rev. Appl. **12**, 054013 (2019).