Continuous-variable quantum key distribution in fast fading channels

Panagiotis Papanastasiou,[1] Christian Weedbrook,[2] and Stefano Pirandola[1]

[1] *Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom*

[2] *Xanadu, 372 Richmond St W, Toronto, M5V 2L7, Canada*

We investigate the performance of several continuous-variable quantum key distribution protocols in the presence of fading channels. These are lossy channels whose transmissivity changes according to a probability distribution. This is typical in communication scenarios where remote parties are connected by free-space links subject to atmospheric turbulence. In this work, we assume the worst-case scenario where an eavesdropper has full control of a fast fading process, so that she chooses the instantaneous transmissivity of a channel, while the remote parties can only detect the mean statistical process. In our study, we consider coherent-state protocols run in various configurations, including the one-way switching protocol in reverse reconciliation, the measurement-device-independent protocol in the symmetric configuration and a three-party measurement-device-independent network. We show that, regardless of the advantage given to the eavesdropper (full control of fading), these protocols can still achieve high rates.

I. INTRODUCTION

The purpose of quantum key distribution (QKD) [1, 2] is to establish a secret key between two authenticated parties based on the laws of quantum mechanics [3]. This key can then be used for cryptographic tasks such as the one-time pad [4]. In QKD, the effect of eavesdropping on the exchanged quantum systems between the parties can be detected and quantified so that a shared secret key can be extracted. This is achieved by implementing the correct amount of error correction and privacy amplification after communicating via a public channel. Significant advantages have been provided by the use of continuous variable (CV) systems [5], in particular, with Gaussian states [6]. CV systems can transfer higher amounts of information per signal with respect to qubit-based approaches and they rely on cheaper technological implementations. A number of CV-QKD protocols have been studied [7–18] and experimentally implemented [19–25].

In this scenario, another concept that needs to be treated carefully is that of side channel attacks, where the eavesdropper (Eve) creates an alternate channel with the aim of directly attacking the setups where the signal states are prepared and measured. A practical but partial solution was proposed in 2012 and known as measurement-device-independent (MDI) QKD [26, 27], later extended to the CV setting [28–30]. An MDI-QKD protocol can be seen as a "prepare and measure" version of entanglement swapping [31] where the middle Bell detection is performed by an untrusted relay. Recently, a suitable generalization of the Bell detection to many parties has led Ref. [32] to introduce a multipartite CV-MDI-QKD star network with an arbitrary number of users.

Today the field of CV-QKD needs to accomplish two main complementary tasks. The first one is the invention of practical protocols that can achieve the high secret key rates that are ideally accessible with CV systems. When implemented with ideal reconciliation efficiencies, low-loss couplings and highly-efficient detectors, CV-QKD protocols are not so far from the ultimate Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound for private communications over a lossy channel [33] (see also extensions of this bound to multiple users [34], repeaters and networks [35], and other developments [36–38]). The other task is improving the security analysis of CV-QKD protocols so as to include realistic issues associated with their practical realization, e.g., finite-size effects [39, 40], and other aspects such as composability [41, 42].

In terms of realistic implementations, one should also consider the possibility of temporal variations of the communication line between two remote users as modeled by the so-called fading channel. In this case, the transmissivity η of the link between the two parties is not constant and may take values according to some probability distribution [43]. This description usually emerges from the fact that the parties use a free-space link [44] that is susceptible to the atmospheric turbulence [45–51]. Previous studies (e.g., see Ref. [52]) have considered the symmetric situation where both users and eavesdropper are subject to truly environmental fading. In this manuscript, we consider a different situation, i.e., the worst-case scenario where the eavesdropper is in complete control of the quantum channel, so that she may choose different instantaneous values of the transmissivity for each use of the channel.

This type of fading is fast so that the users are only able to estimate the statistical distribution of the transmissivity but not its instantaneous values. This is in contrast to slow fading where the transmissivity of the channel remains constant for sufficiently many uses allowing the remote users to estimate its actual value. In mathematical terms, for some fixed transmissivity η consider the key rate as given by the difference between the mutual information $I_{\rm AB}$ of the remote parties and the accessible information $I_{\rm E}$ of the eavesdropper, i.e., $R(\eta) = I_{AB} - I_E$. In slow fading, the key rate is averaged over the distribution of the transmissivity. In fast fading, this is not the most conservative approach. While we may still consider the average $\tilde{I}_{\rm E}$ for the eavesdropper, we need to assume the

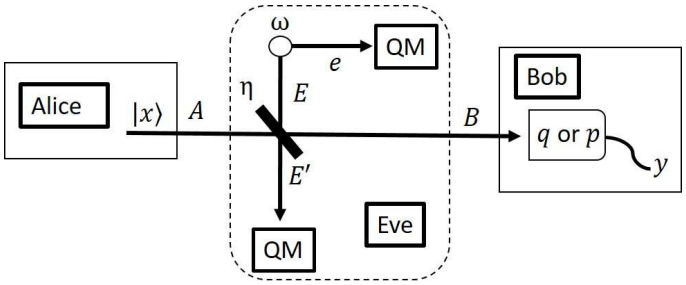

FIG. 1: One-way switching protocol. Alice prepares a coherent state on mode A whose mean value $\mathbf{x}$ is modulated according to a Gaussian with variance ϕ. This state is sent through the channel with transmissivity η whose value may be changed by Eve in each use of the channel. Bob gets an output mode B, which is homodyned randomly in the q or p quadratures, with outcome y. Eve's attack also comprises of her sending mode E of an EPR state to interact with mode A in a beam splitter interaction with instantaneous transmissivity η, and injecting thermal noise ω. After the interaction she stores mode E' and the other EPR mode e in a quantum memory to be measured at the end of the quantum communication (collective attack).

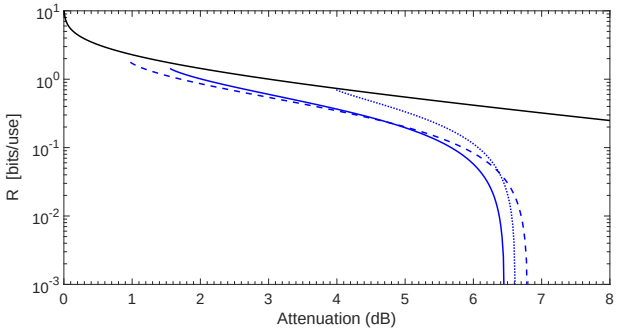

FIG. 2: Fast fading channel. Secret key rates are plotted for $\Delta\eta = 0.2$ (dashed blue line), $\Delta\eta = 0.5$ (solid blue line) and $\Delta\eta = 0.6$ (dotted blue line). We have set $\omega = 1$ (passive eavesdropping), $\beta = 1$ (ideal reconciliation) and $\mu = 10^6$. We compare the results with the PLOB bound for repeaterless private communications over a lossy channel (black line) [33]. We can see that high rates can be achieved up to losses of about $6 - 7$dB, where the rates start to rapidly decrease.

lower transmissivity for the users, i.e., $I_{\rm AB}^{\eta_{\rm min}}$ [53]. Therefore, the secret key rate will be given by

$$R_{\rm fast} = \beta I_{\rm AB}^{\eta_{\rm min}} - \tilde{I}_{\rm E}, \tag{1}$$

where $\beta \in [0, 1]$ is a reconciliation parameter.

In this work, we adopt a basic model of fading channel where the transmissivity is uniformly distributed over some interval. Then, we study the performance of several CV-QKD protocols in the worst-case scenario. We first investigate the effects in the case of the one-way coherent-state switching protocol [7] in reverse reconciliation (Sec. II). In Sec. III, we then study the CV-MDI-QKD protocol [28] in the symmetric configuration [30]. Finally, in Sec. IV, we focus on the case of a CV-MDI-QKD network [54] considering three remote users. In all cases we show that high key rates are achievable within reasonable distances, even in the presence of fast-fading attacks.

II. ONE-WAY QKD UNDER FAST FADING

Consider a sender (Alice) preparing a bosonic mode A using coherent states whose mean values $\mathbf{x} = (x_q, x_p)$ are chosen according to a zero-mean Gaussian distribution with variance ϕ. These states are sent through a channel with transmissivity η to Bob, who then applies a homodyne measurement to either the q or p quadrature of his output mode B, with the outcome being described by a random variable y (see Fig. 1). For each use of the channel, Eve has a two-mode squeezed vacuum state [6] with thermal variance $\omega \geq 1$, which represents a realistic version of an Einstein-Podolsky-Rosen (EPR) pair in CV systems. This state describes modes e and E as depicted in Fig. 1. Then Eve's remote mode E is made to interact with Alice's mode A via a beam splitter with transmissivity η which takes values from a uniform distribution P_η with extremal values $\eta_{\rm min}$ and $\eta_{\rm max} = \eta_{\rm min} + \Delta\eta$. Thus, Eve receives mode E' and stores both e and E' in a quantum memory, to be measured at the end of the entire quantum communication.

An arbitrary input signal state ρ undergoes a transformation via a thermal-loss channel $\mathcal{E}_{\eta,\omega}(\rho)$ for a specific η randomly chosen by Eve (while ω is kept as fixed). The asymptotic key rate will be given by Eq. (1). Here, Eve's information on Bob's variable (reverse reconciliation) is given by the averaged Holevo bound

$$\tilde{I}_{\rm E} = \int d\eta P_\eta \chi({\rm E} : y), \tag{2}$$

where

$$\chi({\rm E} : y) = S(\rho_{E'e}) - S(\rho_{E'e|y}) \tag{3}$$

with $S(\cdot)$ being the von Neumann entropy computed over Eve's output state $\rho_{E'e}$ and her conditional output state $\rho_{E'e|y}$ (given Bob's outcome y).

The derivation is simplified by using the entanglement-based (EB) representation of the protocol [6], where, for each use of the channel, Alice holds an EPR pair with parameter $\mu = \phi + 1$ and sends one of the modes through the channel. By heterodyning her kept mode a, Alice projects the other travelling mode A into a modulated coherent state. This allows us to exploit purification arguments and write $S(\rho_{E'e}) = S(\rho_{aB})$ and $S(\rho_{E'e|y}) = S(\rho_{a|y})$. Furthermore, because the states involved are all Gaussian, we may write the von Neumann entropy in terms of the symplectic eigenvalues of the covariance matrices (CMs) of ρ_{AB} and $\rho_{A|y}$. In fact, for a Gaussian state whose CM has symplectic spectrum $\{z\}$,

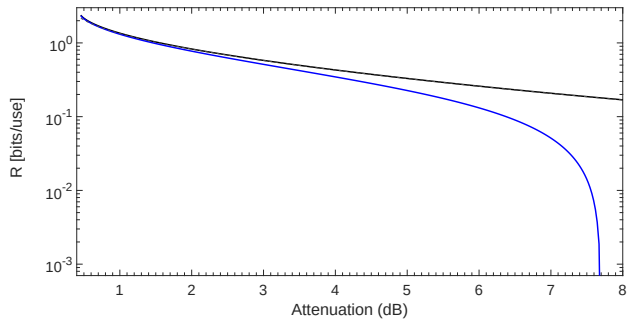

FIG. 3: Comparison between fast and slow fading. We plot the secret key rate for the fast fading channel (lower blue line) and slow fading channel (upper black line) for $\Delta\eta = 0.1$. We also set $\mu = 10^6$, $\omega = 1$ (passive eavesdropping) and $\beta = 1$ (ideal reconciliation). Performances are comparable within the range between 0 and 6 dB.

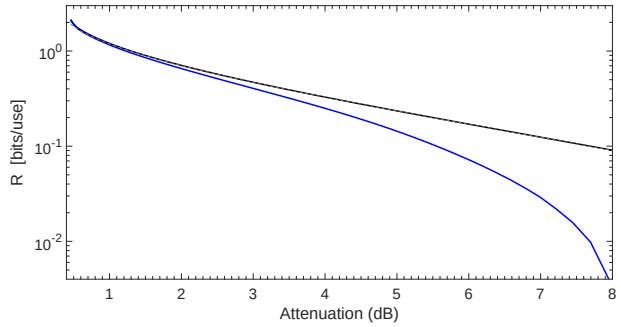

FIG. 4: Comparison between fast and slow fading. As in Fig. 3 but for $\omega = 1.01$, $\beta = 0.98$, and optimized over μ.

we may write

$$S = \sum_z h(z), \tag{4}$$

where

$$h(z) = \frac{z+1}{2}\log_2\frac{z+1}{2} - \frac{z-1}{2}\log_2\frac{z-1}{2}. \tag{5}$$

In Eq. (1), the term $I_{\rm AB}^{\eta_{\rm min}}$ represents the mutual information between Alice and Bob, who does not know the instantaneous value of the transmissivity but only the uniform distribution P_η with minimum transmissivity $\eta_{\rm min}$. Therefore, they need to choose the worst-case scenario associated with the minimum possible transmissivity. As a result, their mutual information turns out to be $I_{\rm AB}^{\eta_{\rm min}} := I_{\rm AB}(\eta_{\rm min})$ where

$$I_{\rm AB}(\eta) = \frac{1}{2}\log_2\frac{V_B}{V_{B|x_q}}. \tag{6}$$

Here V_B is the variance of Bob's variable y, and $V_{B|x_q}$ is the conditional variance given Alice's input x_q (or x_p), computed for a generic value of the transmissivity η.

In the regime of $\mu \gg 1$ we may compute

$$\chi({\rm E}:y) = \frac{1}{2}\log_2\frac{\eta(1-\eta)\mu}{\omega} + h(\omega), \tag{7}$$

and

$$I_{\rm AB}(\eta) = \frac{1}{2}\log_2\frac{\eta\mu}{\eta+(1-\eta)\omega}. \tag{8}$$

Thus, the secret key rate for a fast fading channel is given by

$$R_{\rm fast} = \beta I_{\rm AB}(\eta_{\rm min}) - \frac{1}{\Delta\eta}\int_{\eta_{\rm min}}^{\eta_{\rm max}} d\eta\chi({\rm E}:y). \tag{9}$$

In particular, if we restrict ourselves to a pure-loss channel and we set $\beta = 1$ then the rate above simplifies to

$$\begin{aligned} R_{\rm fast}^{\rm loss} =& \frac{1}{2\Delta\eta}\left[g(\bar{\eta}_{\rm min}-\Delta\eta) - g(\bar{\eta}_{\rm min})\right] \\ &-\frac{1}{2\Delta\eta}(\eta_{\rm min}+\Delta\eta)\log_2\frac{\eta_{\rm min}+\Delta\eta}{\eta_{\rm min}} \\ &+\log_2 e, \end{aligned} \tag{10}$$

where $g(x) = x\log_2 x$ and $\bar{x} = 1-x$. Note that, for slow fading, both Alice and Bob's mutual information and Eve's Holevo information need to be averaged so that

$$R_{\rm slow} = \frac{1}{\Delta\eta}\int_{\eta_{\rm min}}^{\eta_{\rm max}} d\eta[\beta I_{\rm AB}(\eta) - \chi({\rm E}:y)]. \tag{11}$$

In Fig. 2 we show the secret key rate for a fast-fading channel with $\Delta\eta = 0.2$, $\Delta\eta = 0.5$ and $\Delta\eta = 0.6$, also compared with the PLOB bound, which sets the limit for repeaterless private communication over a lossy channel [33]. In Fig. 3 we compare the key rates for slow and fast fading considering $\Delta\eta = 0.1$. In Fig. 4, we consider the secret key rates for $\Delta\eta = 0.1$ but including extra thermal noise $\omega = 1.01$ and assuming a non-ideal reconciliation parameter $\beta = 0.98$ (rates are optimized over μ). As we can see from the plots, the key rate is high up to losses of the order of $6-7$dB, even in the presence of fast fading attacks.

III. CV-MDI-QKD UNDER FAST FADING

The detailed calculations for the CV-MDI-QKD protocol can be found in the Supplementary Material of Ref. [28, 30]. Here we consider the symmetric configuration, so that each link with the untrusted relay is a fading channel whose transmissivity (η_A and η_B) follows a uniform probability distribution, while the thermal noise ω is equal and fixed. For fast fading, we have

$$\begin{aligned} R_{\rm fast}^{\rm MDI} =& \beta I_{\rm AB}(\eta_{\rm min}) - \\ &- \frac{1}{(\Delta\eta)^2}\int_{\eta_{\rm min}}^{\eta_{\rm min}+\Delta\eta}\int_{\eta_{\rm min}}^{\eta_{\rm min}+\Delta\eta} d\eta_A d\eta_B \chi(\eta_A,\eta_B), \end{aligned} \tag{12}$$

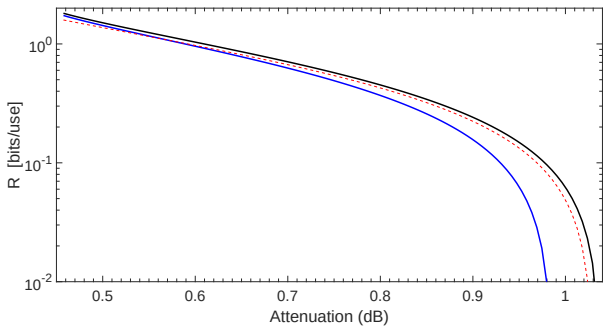

FIG. 5: Performances of the CV-MDI-QKD protocol in symmetric configuration assuming two fading channels in the links with $\Delta\eta = 0.1$ and no excess noise ($\omega = 1$). We plot the secret key rate for fast fading (lower blue line), slow fading (upper black line), and also for the standard case of a non-fading lossy channel (middle red dashed line) over the expectation value of η, i.e., $\bar{\eta} = \eta_{\min} + \frac{\Delta\eta}{2}$. We set $\beta = 1$ and $\mu = 10^6$.

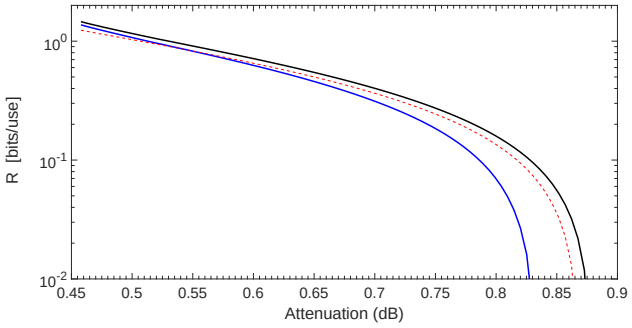

FIG. 6: We plot the same cases as in Fig. 5, but assuming a two-mode correlated attack with noise $\omega = 1.01$, imperfect reconciliation $\beta = 0.98$ and optimization over μ. As expected, the key rates deteriorate.

where $I_{\rm AB}(\eta)$ and $\chi(\eta_A, \eta_B)$ are given in Refs. [28, 30].

In Fig. 5, we present secret key rates for $\beta = 1$, $\omega = 1$ and very large modulation $\mu \simeq 10^6$, while we set $\Delta\eta = 0.1$. We see that the performance for fast fading is not so far from that related to slow fading and that is achievable with a standard lossy channel. In Fig. 6, we then present the same instances but for $\beta = 0.98$, optimizing over μ and setting $\omega = 1.01$. In this latter case, the eavesdropper may also optimize her attack by exploiting correlations in the injected environmental state [28].

IV. CV-MDI-QKD THREE-USER NETWORK UNDER FAST FADING

Let us start with investigating the protocol assuming lossy channels. We consider a three-party network where Alice, Bob and Charlie prepare coherent states for their modes A, B and C. The mean values are Gaussian variables x_1, x_2, and x_3 with the same variance ϕ. Then they send these states to an untrusted relay through three links described by lossy channels with transmissivities η_A, η_B and η_C respectively. The relay is assumed to operate in a certain way in each channel use. In particular, as illustrated in Fig. 7, it mixes Alice's and Bob's modes in a beam splitter with transmissivity $\tau_1 = 1/2$ and homodynes the q quadrature of the output mode R_1^-, while the mode R_1^+ is mixed with Charlie's mode in a beam splitter with transmissivity $\tau_2 = 2/3$. Then, the output modes R_2^- and R_2^+ are homodyned with respect to the q and p quadrature, respectively. All the measurement results $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \gamma_3)$ are then broadcast (see Fig. 7). This is the three-party realization of the multipartite CV Bell detection recently introduced in Ref. [54]. The distributed classical correlations can be processed by the three parties to derive a common secret key for secure quantum conferencing. See Ref. [54] for a CV-MDI-QKD quantum conferencing network with arbitrary number of parties (and Ref. [55] for a recent fully device-independent quantum conferencing network in discrete variables).

Although the relay is assumed to be under the control of the eavesdropper, we can always assume an attack that is described by an attack restricted in the links according to the discussion in Ref. [28]. More specifically, a correlated attack among all the three links is described by a covariance matrix. Here each of the modes are interacting by a beam splitter with each of the modes that the parties send through the channel. This CM is given by

$$\mathbf{V}_{E_A E_B E_C} = \begin{pmatrix} \omega_A \mathbf{I} & \mathbf{G}_1 & \mathbf{G}_3 \\ \mathbf{G}_1 & \omega_B \mathbf{I} & \mathbf{G}_2 \\ \mathbf{G}_3 & \mathbf{G}_2 & \omega_C \mathbf{I} \end{pmatrix}, \tag{13}$$

where ω_A, ω_B and ω_C are the vectors of the noise injected by the eavesdropper in each link whereas $\mathbf{G}_i = \mathrm{diag}(g_i, g_i')$ describes the correlations between the modes. When g_i and g_i' are equal to zero, the attack is reduced to an uncorrelated attack, which is the case that we investigate in this study.

In terms of the security analysis, we adopt the EB representation of the protocol, where the (traveling) modes A, B and C are each one half of an EPR pair with parameter $\mu = \phi + 1$. Then heterodyne measurements are applied to the ancillary EPR modes a, b, and c so that the traveling modes are projected onto modulated coherent states. In this representation, Eve's Holevo bound χ is given by the symplectic eigenvalues of the total CM $\mathbf{V}_{abc|\boldsymbol{\gamma}}$ and the conditional CM $\mathbf{V}_{bc|\boldsymbol{\gamma},x_1}$ following the reasoning in Sec. II. In particular, the total CM is defined as the CM of the parties' local modes after the application of the three relay measurements with outcomes $\boldsymbol{\gamma}$, and the conditional CM is derived by the total CM after applying a heterodyne detection on mode a (we assume that Alice's variable is the one to reconciliate with).

The mutual information in the case of the three parties is defined as the minimum of the mutual information between Alice-Bob and Alice-Charlie, i.e., $I_{\min} = \min\{I_{AB}, I_{AC}\}$. Each of the terms are evaluated by the formula $I_{AB(C)} = \frac{1}{2}\log_2 \boldsymbol{\Sigma}_{b(c)}$, where we have the follow-

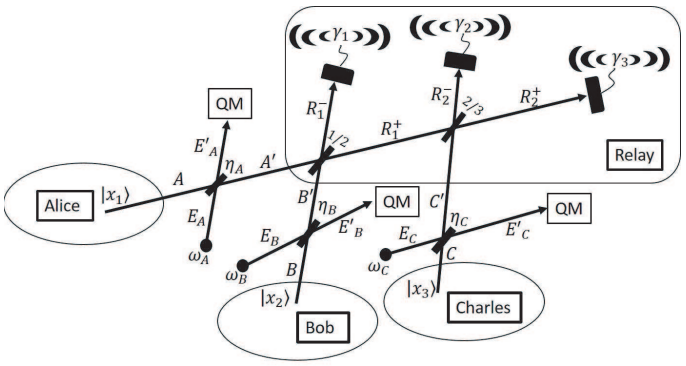

FIG. 7: Three-party CV-MDI-QKD network. The parties prepare coherent states in the modes A, B and C whose mean values are Gaussian variables $\mathbf{x}_1$, $\mathbf{x}_2$ and $\mathbf{x}_3$, with variance ϕ. Then the parties send these states to the relay using links with transmissivities η_A, η_B and η_C respectively. After traveling through the links the modes arrive at the relay as modes A', B' and C' and processed by the relay. Although the relay is under the full control of the eavesdropper, we can assume without loss of generality that it operates consistently in each use of the channel: (a) firstly it mixes Alice's and Bob's modes in a beam splitter with transmissivity 1/2 and measures the q-quadrature of mode R_1^- with a homodyne detection, (b) subsequently mixes Charlie's mode with R_1^+ and then measures the q-quadrature and p-quadrature of modes R_2^- and R_2^+ respectively, (c) finally the results of the measurements γ_1, γ_2 and γ_3 are broadcast. As in Ref. [28], any general attack affecting both the links and the relay can be reduced to an attack tampering only with the links. In this case, Eve is injecting thermal noise ω_1, ω_2 and ω_3 in each of the links by means of the modes E_A, E_B and E_C interacting with modes A, B, C. In a general Gaussian attack, Eve's modes are described by a correlated Gaussian state whose covariance matrix is specified in Eq. (13).

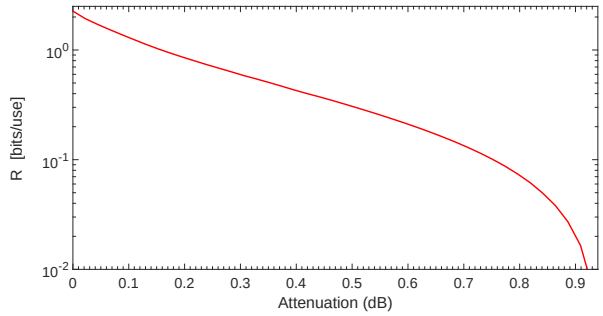

FIG. 8: The rate for the three-party star configuration protocol based on the CV-MDI-QKD scheme, optimized over μ.

ing (for $m = b$ or c)

$$\mathbf{\Sigma}_m = \frac{\det(\mathbf{V}_{m|\boldsymbol{\gamma}}) + \mathrm{tr}(\mathbf{V}_{m|\boldsymbol{\gamma}}) + 1}{\det(\mathbf{V}_{m|\boldsymbol{\gamma},x_1}) + \mathrm{tr}(\mathbf{V}_{m|\boldsymbol{\gamma},x_1}) + 1}, \tag{14}$$

in terms of the covariance matrices of the local mode m.

As a result, the secret conferencing key rate is given

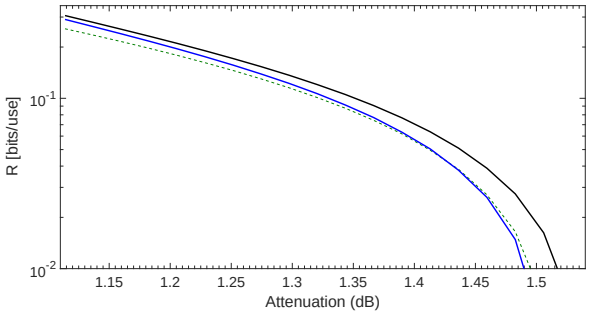

FIG. 9: The secret conferencing key rate in a star configuration of the three-party CV-MDI-QKD network assuming fast-fading channels (blue solid line) and slow-fading channels (black solid line) with the same variance $\Delta\eta = 0.05$. We also include the rate of the protocol in the presence of lossy channels with transmissivity $\bar{\eta} = \eta + \frac{\Delta\eta}{2}$. For all the plots we have optimized over $\mu \in [2, 20]$ and set $\omega = 1$.

by

$$R(\mu, \boldsymbol{\omega}, \boldsymbol{\eta}) = \beta I_{\min}(\mu, \boldsymbol{\omega}, \boldsymbol{\eta}) - \chi(\mu, \boldsymbol{\omega}, \boldsymbol{\eta}), \tag{15}$$

where $\boldsymbol{\omega} = (\omega_A, \omega_B, \omega_C)$ is the vector of the noise injected by the eavesdropper in each link with corresponding transmissivity $\boldsymbol{\eta} = (\eta_A, \eta_B, \eta_C)$. Numerically, we have checked that, even for ideal reconciliation $\beta = 1$, the largest value of μ is not the optimal and we have therefore to optimize the rate over μ. In the case of a star configuration, the previous rate simplifies to

$$R^{\mathrm{star}}(\mu, \omega, \eta) = \beta I_{\min}(\mu, \omega, \eta) - \chi(\mu, \omega, \eta), \tag{16}$$

where $\eta_A = \eta_B = \eta_C := \eta$ and $\omega_A = \omega_B = \omega_C := \omega$. This is plotted in Fig. 8 for passive eavesdropping ($\omega = 1$).

Consider the star configuration in the presence of fading channels affecting the links, with uniform distribution between $\eta_{\min}$ and $\eta_{\min} + \Delta\eta$. We need to integrate the Holevo bound with respect to the three transmissivities of the channels and compute the mutual information assuming the minimum transmissivity (worst-case scenario). Thus, we write

$$R^{\mathrm{star}}_{\mathrm{fast}} = \beta I_{\min}(\mu, \omega, \eta_{\min}) - \iiint_{\eta_{\min}}^{\eta_{\min}+\Delta\eta} \frac{\chi(\mu, \omega, \boldsymbol{\eta})}{(\Delta\eta)^3} d\boldsymbol{\eta}, \tag{17}$$

The rate for $\Delta\eta = 0.05$ and $\omega = 1$ is optimized over μ and shown in Fig. 9. From the figure, we can see that the performance is comparable to the case of slow-fading where the parties' mutual information is averaged over the statistical distribution.

V. CONCLUSION

In this work we have investigated the effects of fading channels in the links used by authorized parties in various quantum key distribution protocols. More specifically,

we have studied the one-way switching protocol with coherent states in reverse reconciliation, the symmetric configuration of continuous-variable measurement-device-independent quantum key distribution protocol, and its extension to a three-user network for quantum conferencing. Fading describes channels with randomly varying transmissivity according to a probability distribution that encompasses effects present in free-space communications where the links are under the influence of atmospheric turbulence. Here, we have considered the most random scenario where the distribution is uniform between two extremal values.

In particular, our work considers the worst-case scenario where the eavesdropper is assumed to have the full control of the fading channel. In other words, it is Eve who fixes the instantaneous value of the transmissivity, not just the environment. When this value is changed very fast, e.g., for each transmission, then we have a fast fading attack which makes the honest user in a particularly disadvantage situation. They can only access the probability distribution of fading at the end of the quantum communication and they therefore need to assume the minimum transmissivity (compatible with that distribution) for the extraction of their secret key.

As we discussed in our paper, this is clearly different from a slow fading attack where the action of the eavesdropper is slow with respect to the quantum communication so that the transmissivity is approximately constant over a large block size. This allows the honest user to make an estimate of the transmissivity to be used in the extraction of part of the key. In any case, our work shows that the performance achievable in the worst-case scenario in the presence of fast fading is not so far from the performance under slow fading. In particular, sufficiently high rates can be achieved within ranges of distance which are typical of the various protocols analyzed. Such results prove the robustness of continuous-variable quantum key distribution protocols under conditions of turbulence which may be typical in realistic free-space scenarios.

VI. ACKNOWLEDGEMENTS

C.W. would like to acknowledge the Office of Naval Research program Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST), awarded to Raytheon BBN Technologies under prime contract number N00014-16-C-2069. The content of this paper does not necessarily reflect the position or policy of the Government and no official endorsement should be inferred. P. P. acknowledges support from the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2008).
[3] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
[4] B. Schneier, *Applied Cryptography* (John Wiley & Sons, New York, 1996).
[5] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[6] 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).
[7] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[8] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[9] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **95**, 052310 (2017).
[10] R. Filip, Phys. Rev. A **77**, 022310 (2008).
[11] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. Lett **105**, 110501 (2010).
[12] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[13] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
[14] C. Weedbrook, C. Ottaviani, and S. Pirandola, Phys. Rev. A **86**, 012309 (2014).
[15] V. Usenko and R. Filip, Entropy **18**, (2016)
[16] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. **4**, 726 (2008).
[17] C. Ottaviani and S. Pirandola, Sci. Rep. **6**, 22225 (2016).
[18] V. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).
[19] T. Gehring, C. S. Jacobsen, and U. L. Andersen, Quantum Information and Computation, **16**, 1081 (2016).
[20] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).
[21] F. Grosshans, G. Van Ache, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[22] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013)
[23] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, Phys. Rev. A **76** (4), 042305 (2007).
[24] C. S. Jacobsen, T. Gehring, and U. L. Andersen, Entropy **17**, 4654 (2015).
[25] Y.-C. Zhang *et al.*, *Continuous-variable QKD over 50km commercial fiber*, arXiv:1709.04618 (2017)
[26] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[27] M.Curty, B. Qi, H.K. Lo, Phys. Rev. Lett. **108**, 130503 (2012).
[28] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook,

S. L. Braunstein, S. Lloyd, T. Ghering, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).
[29] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Ghering, C.S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 773 (2015).
[30] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).
[31] S. Pirandola, C. Weedbrook, J. Eisert, A. Furusawa, and S. L. Braunstein, Nat. Photon. **9**, 641–652 (2015).
[32] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, arXiv:1709.06988.
[33] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017). See also arXiv:1510.08863 and arXiv:1512.04945 (2015).
[34] R. Laurenza, and S. Pirandola, Phys. Rev. A **96**, 032318 (2017).
[35] S. Pirandola, *Capacities of repeater-assisted quantum communications*, arXiv:1601.00966 (2016).
[36] T. P. W. Cope, L. Hetzel, L. Banchi, and S. Pirandola, Phys. Rev. A **96**, 022323 (2017).
[37] R. Laurenza, S. L. Braunstein, and S. Pirandola, *Finite-resource teleportation stretching for continuous-variable systems*, arXiv:1706.06065 (2017).
[38] S. Pirandola, and C. Lupo, Phys. Rev. Lett. **118**, 100502 (2017).
[39] L. Ruppert, V. C. Usenko, and R. Filip, Phys. Rev. A **90**, 062310 (2014).
[40] P. Papanastasiou, C. Ottaviani, and S. Pirandola, *Finite size analysis of measurement device independent quantum cryptography with continuous variables*, arXiv:1707.04599 (2017).
[41] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).
[42] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, *CV MDI QKD: Composable Security against Coherent Attacks*, arXiv:1704.07924 (2017).
[43] V. C. Usenko, B. Heim, C. Peuntinger, C Wittmann, C. Marquardt, G. Leuchs, and R. Filip, New J. Phys. **14**, 093048 (2012).
[44] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media* (SPIE, Bellingham, WA, 2005) 2nd ed. Vol. PM152.
[45] C. Peuntinger, B. Heim, C. R. Mueller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).
[46] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 113018 (2014).
[47] N. Hosseinidehaj and R. Malaney, Phys. Rev. A **91**, 022304 (2015).
[48] D. Vasylyev, A. A. Semenov, and W. Vogel, Phys. Rev. Lett. **117**, 090501 (2016).
[49] M. Bohmann, A. A. Semenov, J. Sperling, and W. Vogel, Phys. Rev. A **117**, 010302(R) (2016).
[50] N. Hosseinidehaj and R. Malaney, Phys. Rev. A **94**, 010302 (2015).
[51] M. Bohmann, J. Sperling, A. A. Semenov, and W. Vogel, Phys. Rev. A **95**, 012324 (2017).
[52] N. Hosseinidehaj and R.Malaney, *CV-MDI Quantum Key Distribution via Satellite*, arXiv:1605.05445 (2016).
[53] The approach is similar to what happens in a finite-size security analysis [39, 40], where the step of parameter estimation provides a statistical distribution for the values of the channel parameters. From this statistical distribution, the parties choose worst-case values for the parameters, e.g., a minimum value of the transmissivity that is compatible with the observed distribution. In the same fashion, in the presence of a fast fading channel, there is a probability distribution associated with the transmissivity and the most conservative strategy for Alice and Bob is to choose the worst-case value. In particular, for a uniform distribution, this means to pick the minimum value in the interval of possible transmissivities.
[54] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, *High-rate quantum conferencing and secret sharing*, arXiv:1709.06988 (2017).
[55] J. Ribeiro, G. Murta, and S. Wehner, *Fully device independent Conference Key Agreement*, arXiv:1708.00798 (2017).