ARTICLE OPEN

Check for updates

Composable end-to-end security of Gaussian quantum networks with untrusted relays

Masoud Ghalaii[1,2]✉, Panagiotis Papanastasiou[1,2] and Stefano Pirandola[1]

Gaussian networks are fundamental objects in network information theory. Here many senders and receivers are connected by physically motivated Gaussian channels, while auxiliary Gaussian components, such as Gaussian relays, are entailed. Whilst the theoretical backbone of classical Gaussian networks is well established, the quantum analog is yet immature. Here, we theoretically tackle composable security of arbitrary Gaussian quantum networks, with generally untrusted nodes, in the finite-size regime. We put forward a general methodology for parameter estimation, which is only based on the data shared by the remote end-users. Taking a chain of identical quantum links as an example, we further demonstrate our study. Additionally, we find that the key rate of a quantum amplifier-assisted chain can ideally beat the fundamental repeaterless limit with practical block sizes. However, this objective is practically questioned leading the way to future network/chain designs.

npj Quantum Information (2022)8:105 ; https://doi.org/10.1038/s41534-022-00620-5

INTRODUCTION

$-\log_2(1-\eta)$, where η is the channel's transmissivity, is the maximum fundamental rate, in bits, at which two distant parties can distribute quantum bits, entanglement bits, or secret bits. This is known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound and holds for any point-to-point protocol of quantum communication[1]. Since the discovery of PLOB, vast efforts have been made to break its hindrance, e.g., by using quantum repeater chains[2,3]. In fact to outclass the PLOB bound, it is necessary to insert in-the-middle quantum stations, which can also be set out in a non-chain configuration to build a quantum network withal. Thus, one ultimate goal is not only to surpass the PLOB bound, but also to branch out a network of quantum links that would enable simultaneous secure communication or key distribution between more than just a few pairs of users[4]. Such telecommunication networks can further develop to provide us with a future quantum internet for quantum-secure communications[2,3] and distributing quantum computing[5–8].

Gaussian networks, inter alia, are at the core of classical information theory, upon which concepts of communication networks have been developed[9]. Such networks, e.g., a large network of optical fiber links, have been studied and evolved in response to our continuous demand for data communications. They, as the name suggests, enjoy Gaussian signal assumptions and Gaussian links, where random variables with Gaussian probability density functions describe the channel noise. In addition, any other component, e.g., repeater relays, that makes the process of data communications possible or alleviates it is Gaussian, such that none of the shared variables/distributions between users of the network becomes non-Gaussian. In this work, we put our focus on Gaussian quantum networks that benefit from Gaussian input signals, Gaussian quantum channels, and auxiliary Gaussian quantum devices. In particular, we study end-to-end security between two arbitrary users of a Gaussian quantum network who are generally linked via untrusted nodes (see Fig. 1). More weakly, as we explain later, we also admit some post-selection operations that are conditionally Gaussian, i.e., projecting into a Gaussian state when they are successful (discarding their output otherwise).

While examining a quantum network, not only is it fundamental to compute the relevant communication rates between arbitrary users, namely upper, lower and achievable rates, but it is crucial to evaluate composable key rates with a finite number of uses of the network. Evaluating the rate is possible by analyzing the data statistics that the parties would obtain through the so-called parameter estimation (PE)[10–12]. For a typical single link, PE analysis, which commonly refers to estimating channel parameters (loss and noise), is relatively straightforward[13,14]. However, PE can become very challenging in large-scale quantum networks. For these reasons, we do not consider estimating channel parameters; instead, we use PE in a more general sense by directly estimating measurable quantities, e.g., the covariance matrix (CM) of the end parties.

In the context of continuous-variable (CV) quantum key distribution (QKD), we show that any two users of a Gaussian quantum network can successfully extract composable secret keys from their local shared data, together with any classical public data that they might receive from other stations of the network. As mentioned above, an important point to remark is that we allow the network to deviate from being Gaussian, including the possibility to be conditionally Gaussian, i.e., described by a Gaussian state only after the success of a non-Gaussian, post-selection mechanism (feature which is needed for effective entanglement distillation[15–19]). In particular, this happens when non-deterministic quantum amplifiers are in use, where they sporadically fail to amplify[20–25]. We further investigate the use of such amplifiers in a linear quantum chain.

RESULTS AND DISCUSSION

Gaussian quantum networks

We consider the scenario where Alice and Bob are two arbitrary users of a quantum network, as sketched in Fig. 1; their objective is to remotely share a secret key. Let us assume that there are

[1]Department of Computer Science, University of York, York YO10 5GH, UK. [2]These authors contributed equally: Masoud Ghalaii, Panagiotis Papanastasiou.
✉email: masoud.ghalaii@york.ac.uk

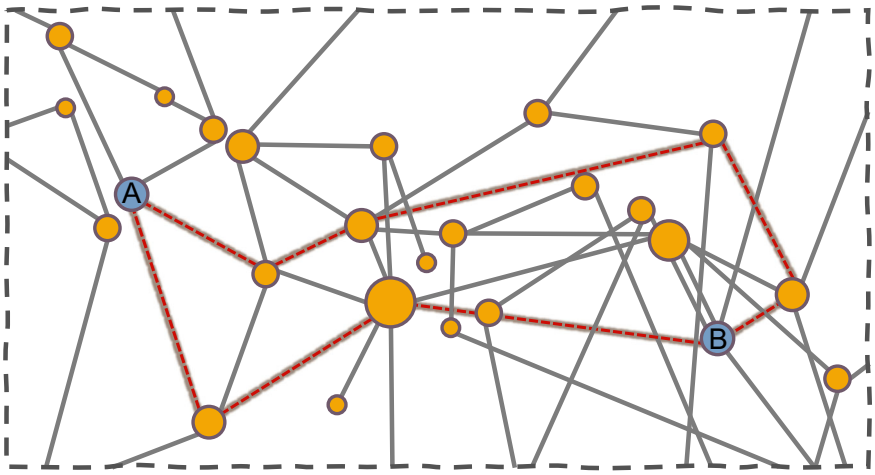

Fig. 1 Quantum communication network. Two arbitrary end-users, Alice (A) and Bob (B), can communicate through diverse, not necessarily direct, routes that extend across intermediate untrusted sender-receiver pairs that act as relays (yellow nodes). Two possible routes are highlighted in red. The quantum network is Gaussian if the operations at the nodes and the channels associated with links are all Gaussian, so that the final state shared by Alice and Bob is Gaussian. More weakly, we also include the possibility of non-Gaussian post-selection operations which however project into a Gaussian state when they are successful (see text for more details).

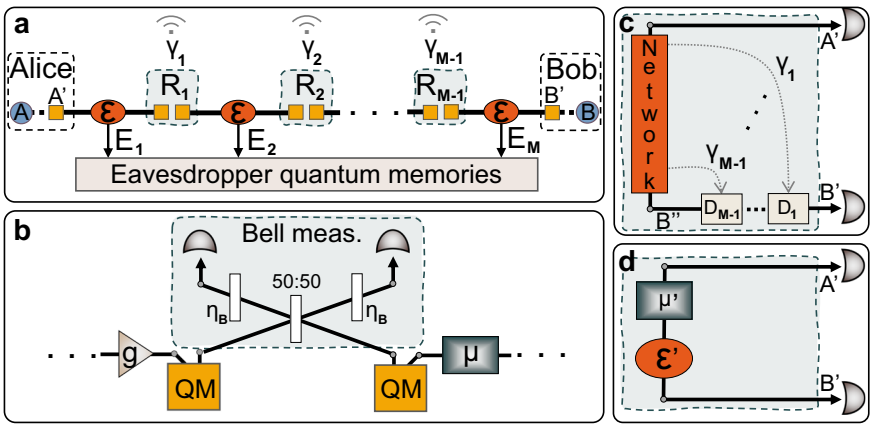

Fig. 2 Quantum communication chain within a network. a An arbitrary route between Alice and Bob can be seen as a linear chain between them that consists of M links and $M-1$ stations (R_i's). **b** Each station can encompass a noiseless linear amplifier (NLA, g), a bipartite entanglement TMSV source (μ), a couple of QMs, and a non-ideal Bell detection, whose loss is simulated by a couple of beam splitters with transmissivity η_B. **c** A Gaussian quantum network provides the end parties with a Gaussian bipartite state, called the network state $\rho_{A'B'}$. Displacement operations need to be applied according to the information received form the stations, as shown in **a**. **d** The effect of the Gaussian quantum network in **c** can be simulated via a one-way Gaussian protocol with an equivalent source μ', and an equivalent channel, $\mathcal{E}'$, with loss η' and excess noise ξ'.

$M-1$ stations that relay signals from Alice to Bob through a specific route that is made of M basic links. As Fig. 2a schematically illustrates, an arbitrary route can be seen as a chain of quantum links. It is also assumed that a powerful eavesdropper (Eve) may operate the intermediate stations and also store all the lost portion of the signals into her quantum memories (QMs). The relay stations may consist of several components. For instance, they can be equipped with entanglement sources, such as two-mode squeezed vacuum (TMSV), quantum amplifiers, QMs, and a classical communication system; see Fig. 2b. Nonetheless, the key role of the relays is to connect adjacent links via joint Bell measurements, whose outcomes γ_i (for $i=1,\ldots,M-1$) are aired to Alice and Bob for local data processing. Note that, in case the relays operate differently from expected, this would reflect in high amount of noise in Alice and Bob's shared data.

Figure 2c captures the role of the network in terms of quantum teleportation-stretching formalism[1]. The network provides end-parties, Alice and Bob, with a bipartite (entangled) Gaussian state, which we call the network state $\rho_{A'B''|\{\gamma_i\}}$, before γ_i's corrections are applied. We conventionally assume that the initial single links are of zero mean. However, execution of a relay, e.g., R_1, displaces the mean value of the state by an amount $f(\gamma_1)$ proportional to γ_1. In order to "correct" this a displacement operation, e.g., $\widehat{D}_1$, should be applied accordingly. Similar displacement operations are applied due to other relay outcomes that can all be postponed to one end. Thus, in this way, the mean value of the network state after γ_i corrections, now described by $\rho_{A'B'}$, becomes independent of the γ_i's (in fact we balance it to zero). Further, since displacements are local operations, the network state will have a CM $\mathbf{V}_{A'B'}=\mathbf{V}_{A'B''|\{\gamma_i\}}$, which is described in the normal form:

$$\mathbf{V}_{A'B'}=\begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}\end{pmatrix},\quad \begin{cases}\mathbf{I}:=\mathrm{diag}(1,1),\\ \mathbf{Z}:=\mathrm{diag}(1,-1).\end{cases} \tag{1}$$

Therefore, the network state supplies Alice and Bob with an overall two-mode Gaussian state that can be used to implement different one-way-like communication protocols.

We remark that the Gaussianity assumption can be weakened because of conditioning, or post-selection, where relays can

actually impose non-Gaussianity on the entire network, yet the system can be assumed conditionally Gaussian. This situation occurs because measurable quantities, such as CM elements, depend on relay measurement outcomes, which may vary for different sets of $\{\gamma_i\}$. This is similar to post-selection[26,27] or discrete-alphabet protocols[28,29] where, for example, the outcome set #1 gives $\mathbf{V}_{A'B'}^{\#1}$, while the outcome set #2 gives $\mathbf{V}_{A'B'}^{\#2}$ that differs from the CM associated to that of set #1. Thus, one needs to build an average rate over all possible outcome sets. Therefore, the average state/CM would be non-Gaussian. Nevertheless, if in such situations we choose to discard the unsuccessful events, then the post-selected state between Alice and Bob is Gaussian.

Security reduction

It is conceivable that the types of attack that eavesdroppers may apply on a multi-link quantum network can be more complex than the way they would attack conventional one-link protocols. For instance, in a quantum network a subset of the links that form the route from Alice to Bob may have correlations. In fact, Eve may adapt her attack on a link based on the information she has gained while attacking other, previous links. This generally defines a collective network attack, which has memory between the links but is memory-less between different uses of the network. Such inter-link correlations are taken into account in the network state or, alternatively, its corresponding CM. This is due to the fact that we consider only the end-to-end Gaussian CM for the analysis. As a requirement for our analysis, it is important to note that the CM of the network state is in normal form of Eq. (1). Note that we assume that the route is fixed. In the case it changes use-by-use, a more general attack would involve correlations between all the links that are overall used over multiple uses of the network.

Nevertheless, there may also be correlations between subsequent uses of a route, which defines an even more powerful and general, coherent attack. Hence, we need to prove the security when the eavesdroppers develop inter-use correlations, i.e., when they apply a coherent attack. Our solution is to tackle this problem by reducing the Gaussian quantum network security to that of one-way protocols, for which optimality of collective Gaussian attacks has been proven[30]. In this way, we reduce the complexity of the problem and extend the security analysis under collective attacks to coherent attacks.

Assume that the end-nodes of the network, A' and B', remain in the Gaussian regime. We can seek for equivalent parameters of a single Gaussian channel that does the same job. In fact, the overall function of a Gaussian quantum network can be reduced to, and modeled by, a one-way Gaussian channel, with loss η' and excess noise ξ', applied to an equivalent source with modulation μ'. See Fig. 2d, where we have that such equivalent parameters builds up a CM in normal form:

$$\mathbf{V}_{A'B'}^{\text{eqv}}=\begin{pmatrix}\mu'\mathbf{I} & \sqrt{\eta'(\mu'^2-1)}\mathbf{Z}\\ \sqrt{\eta'(\mu'^2-1)}\mathbf{Z} & \eta'\mu'+1-\eta'+\xi'\mathbf{I}\end{pmatrix}. \tag{2}$$

It is straightforward to find the elements of the CM of the equivalent state, given by Eq. (2), in the terms of the triplet (a, b, c) in Eq. (1) that describes the network state $\rho_{A'B'}$; one can obtain:

$$\begin{cases}\mu'=a,\\ \eta'=c^2(a^2-1)^{-1},\\ \xi'=(a+1)(b-1)-c^2.\end{cases} \tag{3}$$

Note that $\mathbf{V}_{A'B'}^{\text{eqv}}$ is bona fide, i.e., $\mu'\geq 1$, $\eta'\leq 1$, and $\xi'\geq 0$, when the CM in Eq. (1) is bona fide, i.e., $a, b\geq 1$ and $c\leq \min\{\sqrt{a^2-1},\sqrt{(a+1)(b-1)}\}$[31].

This means that the original collective network attacks can be extended to coherent network attacks where correlations could happen between different uses of the network. Consequently, the optimality of Gaussian attacks in typical one-way Gaussian protocols is extended to Gaussian quantum networks. It is therefore a reasonable assumption to consider Gaussian eavesdropping which is the optimal strategy in the presence of protocols based on Gaussian resources. For this reason, for our security analysis and composable study we consider network attacks that are collective and Gaussian.

Emulation of sending- and receiving-only relays

It is conceivable that a node in a quantum network is exploited to only send/share or only receive/measure quantum signals. In order to keep our study as general as possible, especially when it comes to PE, we shall simulate such specific relays that include either a relay with some outcome γ or a source with some variance μ to feed its adjacent relays; see Fig. 3a1. Assume three single links that are connected via two Bell detection modules. The emulation can be performed by (1) applying the second relay on modes B and c, which produces the outcome γ_2, (2) applying a correction/displacement, $\widehat{D}_2$, at the first relay on mode b, which subsequently teleports mode c to b', and (3) taking the limit $v\to\infty$. As sketched in Fig. 3a2, we show that the above steps would reduce the two "full" relays, which include a Bell measurement as well as a TMSV source, to a receiving-only and a sending-only relays.

For convenience, let us describe the situation in terms of the teleportation-stretching technique, developed in ref. [1], as shown in Fig. 3b1, b2. We shall show that in both cases, after taking the limit $v\to\infty$, the resultant CM for modes $b'C'$ is the same. By assuming that $\mathcal{E}$ is a thermal-loss with transmissivity η and noise at channel output ξ, we see that the scheme in Fig. 3b2 gives:

$$\mathbf{V}_{b'C'}^{\text{b2}}=\begin{pmatrix}\mu\mathbf{I} & \sqrt{\eta(\mu^2-1)}\mathbf{Z}\\ \sqrt{\eta(\mu^2-1)}\mathbf{Z} & \eta\mu+1-\eta+\xi\mathbf{I}\end{pmatrix}. \tag{4}$$

With a bit of math one can show that the execution of the relay in Fig. 3b1 gives:

$$\mathbf{V}_{b'C'}^{\text{b1}}=\begin{pmatrix}\mu-\frac{\mu^2-1}{\mu+v}\mathbf{I} & \frac{\sqrt{\eta(\mu^2-1)(v^2-1)}}{\mu+v}\mathbf{Z}\\ \frac{\sqrt{\eta(\mu^2-1)(v^2-1)}}{\mu+v}\mathbf{Z} & F\mathbf{I}\end{pmatrix},\qquad F=\frac{\mu(\eta\mu+1-\eta+\xi)+(1-\eta+\xi)+\eta}{\mu+v}. \tag{5}$$

One can then verify that $\mathbf{V}_{b'C'}^{\text{b1}}$ equals the CM in Eq. (4) in the limit $v\to\infty$.

In Fig. 3c1, c2, we further verify that corrections based on broadcasted γ_i's can be postponed to one end (here to the end-mode "a"). We do so by checking the equivalence when the displacement operator $\widehat{D}_2$ can be postponed and performed along with $\widehat{D}_1$. The equivalence can be verified through checking both CMs and mean values. From upper and lower panels in Fig. 3c, it is clear that the equality holds for CMs since both scenarios start with the same resources and channels, on which only local displacement operations, which do not change the CMs, are applied.

For mean values, we start by the fact that initial mean value vector for the four involved modes is zero, i.e., $\bar{\mathbf{x}}_{B'bAa}=\mathbf{0}$. Let us start from Fig. 3c1. The displacement $\gamma_2:=(q_{\gamma_2}+ip_{\gamma_2})/\sqrt{2}$ implies that $\bar{\mathbf{x}}'=(0\,0\,q_{\gamma_2}\,p_{\gamma_2}\,0\,0\,0\,0)^{\mathsf{T}}$, which after applying the balanced beam splitter of the Bell detection varies to:

$$\bar{\mathbf{x}}''_{B'bAa}=\left(0\,0\,\frac{q_{\gamma_2}}{\sqrt{2}}\,\frac{p_{\gamma_2}}{\sqrt{2}}\,\frac{-q_{\gamma_2}}{\sqrt{2}}\,\frac{-p_{\gamma_2}}{\sqrt{2}}\,0\,0\right)^{\mathsf{T}}. \tag{6}$$

Next, it can be shown that the execution of homodyne detection modules, with the outcomes q_{γ_1} and p_{γ_1} that forms

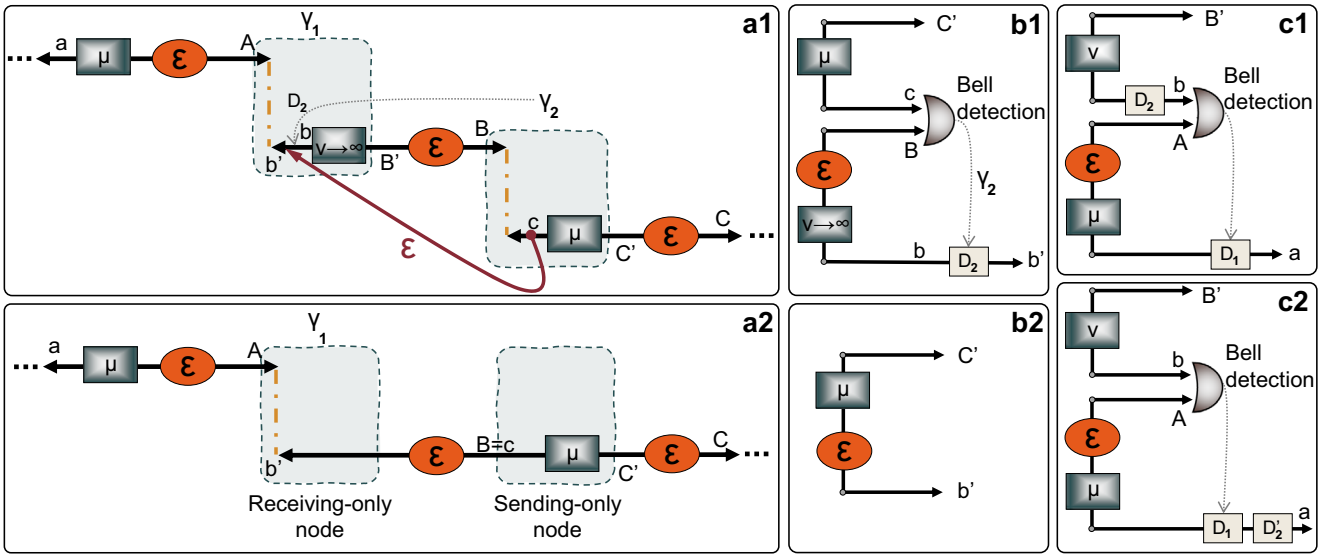

Fig. 3 Emulation of specific nodes of a quantum network. **a**1, **a**2 We emulate receiving-only and sending-only nodes. **b**1, **b**2 We sketch the teleportation stretching form of **a**1 and **a**2, respectively. **c**1, **c**2 We show that all displacement operations can be postponed to one, receiver end (see main text). Here, $\mathcal{E}$ and $\widehat{D}$ represent a thermal-loss channel and single-mode displacement operation, respectively. (see main text for explanation).

$\gamma_1 := q_{\gamma_1} + ip_{\gamma_1}$, gives the mean value vector for the mode a:

$$\bar{\mathbf{x}}_a''' = \Gamma\begin{pmatrix} q_{\gamma_2} + \sqrt{2}q_{\gamma_1} \\ p_{\gamma_2} - \sqrt{2}p_{\gamma_1} \end{pmatrix}, \text{with } \Gamma := \frac{\sqrt{\eta(\mu^2-1)}}{\nu+\eta(\mu-1)+1+\xi}. \tag{7}$$

Then the parties apply the following displacement dependent on the outcomes:

$$D_1(q_{\gamma_1}, p_{\gamma_1}) = \Gamma\begin{pmatrix} -\sqrt{2}q_{\gamma_1} \\ +\sqrt{2}p_{\gamma_1} \end{pmatrix}, \tag{8}$$

and obtain the mean of mode b (rescaled by the factor Γ):

$$\bar{\mathbf{x}}_a^{\text{up}} = \Gamma\begin{pmatrix} q_{\gamma_2} \\ p_{\gamma_2} \end{pmatrix}. \tag{9}$$

In Fig. 3c2, after applying the Bell detection module, with outcomes q'_{γ_1} and p'_{γ_1}, we have that:

$$\bar{\mathbf{x}}_a = \sqrt{2}\Gamma\begin{pmatrix} q'_{\gamma_1} \\ p'_{\gamma_1} \end{pmatrix}; \tag{10}$$

hence, we apply the displacement $D'_1(q'_{\gamma_1}, p'_{\gamma_1})$ to obtain:

$$\bar{\mathbf{x}}'_a = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{11}$$

One can show that the mean value vector for the mode a after the displacement $D'_2(q'_{\gamma_2}, p'_{\gamma_2})$ is given by:

$$\bar{\mathbf{x}}_a^{\text{down}} = \begin{pmatrix} q'_{\gamma_2} \\ p'_{\gamma_2} \end{pmatrix}, \tag{12}$$

whose entries can be tuned so that $\bar{\mathbf{x}}_a^{\text{down}} = \bar{\mathbf{x}}_a^{\text{up}}$.

Note that we can define a "network number," S_{net}, which tells us how a generic network is different from a fully designed network whose nodes are all sending-receiving. Precisely, the number S_{net} accounts for the number of only-receiving plus only-sending nodes. A fully designed network then has $S_{\text{net}} = 0$. Note also that, as described in Fig. 3, such nodes always appear in pairs, such that S_{net} is an even number, the reason being directionality of the generated signals as well as network's symmetry. In fact, like an entanglement source that feeds the two ends of a single link, the function of the network is to distribute entanglement toward both far-ends. Installing nodes that result in S_{net} being an odd number, would break the directionality, and the symmetry, which therefore breaks off the links of the network.

Parameter estimation

The outcomes of the relays are bi-dimensional Gaussian variables $\gamma_i = (q_{\gamma_i}, p_{\gamma_i})^T$, which are taken into account by Alice and Bob to post-process their local variables. Let us focus on the q-quadrature for the next derivations since equivalent steps hold for the p-variable. To simplify the derivations, we in fact assume that q and p quadratures are not mixed by the eavesdropper so that they can be treated as independent variables. (This is a reasonable protocol assumption; extension is just a matter of technicalities).

In this work we assume that both Alice and Bob apply heterodyne measurements on the end-to-end modes A' and B' with outcomes $z_A := (q_A, p_A)$ and $z_B := (q_B, p_B)$, respectively, to establish a secure key. By assuming that the relays work properly and that the quadratures follow a normal distribution, we can write the variables that build the raw key for Alice and Bob, respectively, as:

$$q_x = q_A - \sum_{i=1}^{M-1} u_i q_{\gamma_i}, \tag{13}$$

$$q_y = q_B - \sum_{i=1}^{M-1} v_i q_{\gamma_i}, \tag{14}$$

where u_i's and v_i's are real numbers. In a prepare and measure variant, where Alice prepares coherent states, she generates variable $\bar{z}_A = \left(\sqrt{\frac{\mu-1}{\mu+1}}q_A, \sqrt{\frac{\mu-1}{\mu+1}}p_A\right)$, with $\mu = \sigma_A^2 - 1$, where σ_A^2 is the variance of the Gaussian modulation of $\bar{z}_A$. Hence, before applying Eqs. (13) and (14), one needs to apply a transformation, $\mathbf{L} = \sqrt{\frac{\mu-1}{\mu+1}}\mathbf{I}$, on $\bar{z}_A$ in order to obtain z_A.

For security reasons, we require q_x and q_y to be uncorrelated with the public variables q_{γ_i}'s that are known to Eve, i.e., $\langle q_x q_{\gamma_i}\rangle = 0$, which imposes the following constraints:

$$\left\langle q_A q_{\gamma_i} \right\rangle = \sum_{k=1}^{M-1} u_k \langle q_{\gamma_i} q_{\gamma_k} \rangle, \tag{15}$$

from which one can calculate the weights u_i's (similar relations hold for q_y, q_B and v_i's).

Now, let us consider and study the sampled data $[q_A]_j$ and $[q_{\gamma_i}]_j$, for $j = 1, \ldots, N$, associated with variables q_A and q_{γ_i}, respectively. From these, Alice can calculate the corresponding maximum likelihood estimators:

$$\widehat{\langle q_A q_{\gamma_i}\rangle} = N^{-1}\sum_{j=1}^{N}[q_A]_j\left[q_{\gamma_i}\right]_j, \tag{16}$$

$$\widehat{\langle q_{\gamma_i} q_{\gamma_k}\rangle} = N^{-1}\sum_{j=1}^{N}\left[q_{\gamma_i}\right]_j\left[q_{\gamma_k}\right]_j. \tag{17}$$

Next, to obtain values of the weights u_i's, she replaces these values in the set of M equalities in Eq. (15). She then continues with calculating $[q_x]_j$ by replacing the u_i's, and the data points $[q_A]_j$ and $[q_{\gamma_i}]_j$, in Eq. (13). Indeed, Bob obtains similar relations for q_y and v_i's.

At this stage the parties are in a position to compute the classical CM associated to their post-processed data:

$$\widehat{\boldsymbol{\Sigma}} = \begin{pmatrix} \widehat{\mathbf{V}}_x & \widehat{\mathbf{C}}_{xy} \\ \widehat{\mathbf{C}}_{xy} & \widehat{\mathbf{V}}_y \end{pmatrix}, \tag{18}$$

where $\widehat{\mathbf{V}}_x = \mathrm{diag}\left(\widehat{\langle q_x^2\rangle}, \widehat{\langle p_x^2\rangle}\right)$, $\widehat{\mathbf{V}}_y = \mathrm{diag}\left(\widehat{\langle q_y^2\rangle}, \widehat{\langle p_y^2\rangle}\right)$, and $\widehat{\mathbf{C}}_{xy} = \mathrm{diag}\left(\widehat{\langle q_x q_y\rangle}, \widehat{\langle p_x p_y\rangle}\right)$.

For the q-quadrature we have that (not to mention that the parties repeat the same process for the p-quadrature):

$$\widehat{\langle q_x^2\rangle} = m_{\mathrm{pe}}^{-1}\sum_{j=1}^{m_{\mathrm{pe}}}[q_x]_j^2, \tag{19}$$

$$\widehat{\langle q_y^2\rangle} = m_{\mathrm{pe}}^{-1}\sum_{j=1}^{m_{\mathrm{pe}}}\left[q_y\right]_j^2, \tag{20}$$

$$\widehat{\langle q_x q_y\rangle} = m_{\mathrm{pe}}^{-1}\sum_{j=1}^{m_{\mathrm{pe}}}[q_x]_j\left[q_y\right]_j, \tag{21}$$

when m_{pe} is the number of signals sacrificed for PE.

Note that, in principle, the parties can locally calculate the values from the estimators $\widehat{\mathbf{V}}_x$ and $\widehat{\mathbf{V}}_y$ using N data points while $\widehat{\langle q_x q_y\rangle}$ demands sharing m_{pe} data points through the public classical channel. These data can be easily acquired by Eve and thus must not contribute to the key generation. In general, the parties optimize the amount of shared data, m_{pe}, so as to limit the uncertainty of terms such as $\widehat{\langle q_x q_y\rangle}$ while still keeping as many samples as possible for the secret key.

The parties can compute an interval, with confidence $1-\varepsilon_{\mathrm{pe}}$, for the estimated CM from which they derive the worst-case scenario CM, i.e., the CM that minimizes the key rate according to the sampled data with a probability larger than $1-\varepsilon_{\mathrm{pe}}$. This CM is given by:

$$\boldsymbol{\Sigma}_{\mathrm{wc}} = \widehat{\boldsymbol{\Sigma}} + \sqrt{\frac{4\kappa}{m_{\mathrm{pe}}}}\begin{pmatrix} \widehat{\mathbf{V}}_x & -\frac{\widehat{\mathbf{v}}_x+\widehat{\mathbf{v}}_y}{2}\mathbf{Z} \\ -\frac{\widehat{\mathbf{v}}_x+\widehat{\mathbf{v}}_y}{2}\mathbf{Z} & \widehat{\mathbf{V}}_y \end{pmatrix}, \tag{22}$$

with $\kappa = (8\varepsilon_{\mathrm{pe}}^{-1})$. This is calculated by using suitable tail bounds for the chi-squared distribution (see Methods). It is valid for any CM of two correlated systems even if the entries are given theoretically via a model, e.g., $y = \sqrt{\tau}x + \epsilon$, with scale factor $\sqrt{\tau}$ and variance σ_ϵ^2 for the normal variable ϵ.

Asymptotic key rate

We define the asymptotic secret key rate of sharing a key between two arbitrary users of a quantum network based on the Devetak-Winter rate[32]:

$$K = \beta I(z_A : z_B|\{\gamma_i\}) - \chi(E : z_r|\{\gamma_i\}), \tag{23}$$

where $I(z_A{:}\, z_B|\{\gamma_i\})$ is the mutual information between z_A and z_B and $S(E{:}\, z_r)$ is the Holevo information between Eve's system and the reconciliation variable z_r, with $r = A(B)$ indicating direct (reverse) reconciliation. In this work, we focus on the reverse reconciliation $r = B$. By definition, we have:

$$\chi(E : z_B|\{\gamma_i\}) = S(E|\{\gamma_i\}) - S(E|z_B\{\gamma_i\}), \tag{24}$$

where:

$$S(E|\{\gamma_i\}) = -\mathrm{tr}\left(\rho_{E|\{\gamma_i\}}\log_2\rho_{E|\{\gamma_i\}}\right) \tag{25}$$

is the von Neumann entropy of Eve's state, ρ_E (conditioned on the knowledge of the γ's), and:

$$S(E|z_B\{\gamma_i\}) = \int \mathrm{d}z_B p(z_B|\{\gamma_i\}) \times\left[-\mathrm{tr}\left(\rho_{E|z_B\{\gamma_i\}}\log_2\rho_{E|z_B\{\gamma_i\}}\right)\right], \tag{26}$$

where $\rho_{E|z_B\gamma_i}$ is the state conditioned on Bob's variable z_B (after the γ's).

With this in mind, the parties neither know the explicit description of Eve's system nor how she interacts with the links. However, by assuming that Eve purifies the system between Alice and Bob, such that $\rho_{ABE|\{\gamma_i\}}$ is a pure state, it holds that $S(E|\{\gamma_i\}) = S(AB|\{\gamma_i\})$ and $S(E|z_B\{\gamma_i\}) = S(A|z_B\{\gamma_i\})$[33], where the later equality also exploits the fact that Bob performs a rank-1 measurement (like heterodyne detection) therefore projecting the global pure state $\rho_{ABE|\{\gamma_i\}}$ into a reduced pure state $\rho_{AB|z_B\{\gamma_i\}}$. Since the state $\rho_{AB|\{\gamma_i\}}$ is Gaussian, it is characterized by its CM, $\mathbf{V}_{AB|\{\gamma_i\}}$. In practice, this can be estimated by the worst-case quantum CM, $\mathbf{V}_{\mathrm{wc}}$ (compatible with the classical data shared by the parties):

$$\mathbf{V}_{AB|\{\gamma_i\}} \simeq \mathbf{V}_{\mathrm{wc}} = \boldsymbol{\Sigma}_{\mathrm{wc}} - \mathbf{I}\oplus\mathbf{I}. \tag{27}$$

By setting:

$$\mathbf{V}_{AB|\{\gamma_i\}} := \begin{pmatrix} \mathbf{V}_{A|\{\gamma_i\}} & \mathbf{C}_{AB|\{\gamma_i\}} \\ \mathbf{C}_{AB|\{\gamma_i\}} & \mathbf{V}_{B|\{\gamma_i\}} \end{pmatrix}, \tag{28}$$

we have that the conditional CM after Bob's heterodyne is given by:

$$\mathbf{V}_{A|z_B\{\gamma_i\}} = \mathbf{V}_{A|\{\gamma_i\}} - \mathbf{C}_{AB|\{\gamma_i\}}^{\top}\left[\mathbf{V}_{B|\{\gamma_i\}} + \mathbf{I}\right]^{-1}\mathbf{C}_{AB|\{\gamma_i\}}. \tag{29}$$

Next, from the symplectic spectra $\boldsymbol{\nu}_{AB|\{\gamma_i\}}$ and $\boldsymbol{\nu}_{A|z_B\{\gamma_i\}}$, of $\mathbf{V}_{AB|\{\gamma_i\}}$ and $\mathbf{V}_{A|z_B\{\gamma_i\}}$, we compute the Holevo information:

$$\chi(E : z_B|\gamma_i) = \sum_l h([\boldsymbol{\nu}_{AB|\{\gamma_i\}}]_l) - \sum_k h([\boldsymbol{\nu}_{A|z_B\{\gamma_i\}}]_k), \tag{30}$$

where $h(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$. In addition, the mutual information is given by[34]:

$$I(z_A : z_B|\{\gamma_i\}) = \frac{1}{2}\log_2\frac{1+\det\mathbf{V}_{A|\{\gamma_i\}}+\mathrm{tr}\mathbf{V}_{A|\{\gamma_i\}}}{1+\det\mathbf{V}_{A|z_B\{\gamma_i\}}+\mathrm{tr}\mathbf{V}_{A|z_B\{\gamma_i\}}}. \tag{31}$$

Therefore, the parties have calculated a modified asymptotic key rate that encompasses the worst-case scenario given the sampled data. This is correct up to an error $\varepsilon_{\mathrm{pe}}$ and is calculated from Alice's and Bob's remote, shared, data that account for the relay outputs γ_i's without any assumption on the structure of the intermediate channels. To put it more precisely, the rate should be re-scaled in a way to account for the number of uses sacrificed for PE. We discuss this and other aspects in detail shortly.

Let us also remark that in all the derivation above, we assume that the conditioning associated with the γ_i's create the same conditional CM for the shared state regardless of the actual values

of γ_i's. This makes sense only under the Gaussian assumptions for the network, but this is still true even in the presence of NLAs, where the network is conditionally Gaussian.

Composable finite-size key rate

The security of Gaussian quantum networks can be further extended by considering finite-size correction terms dependent on small failure probabilities of different processes of the protocol. Over a chosen route of the network, Alice and Bob would share the following classical-quantum state between themselves and Eve, who is assumed to perform a collective Gaussian attack:

$$\rho_{ABE} = \sum_{k,l} p(k,l)|k\rangle_A\langle k| \otimes |l\rangle_B\langle l| \otimes \rho_E(k,l), \tag{32}$$

where $E \equiv E_1E_2 \ldots E_M$ are Eve's systems; see Fig. 2a. Thus, at the end of the error correction (EC), Alice and Bob possess correlated discretized variables k^n and l^n respectively associated with $\rho_{ABE}^{\otimes n}$.

As we discussed, the end-to-end CM, either built from sampled data or given by means of a proper model, would suffice to derive the secret key rate or suitable bounds by using the notions of coherent information and reverse coherent information of bosonic channels[35,36], as well as the relative entropy of entanglement[37]. Since in a real-world scenario the parties exchange only a finite number of signal states, here the focus is put on composable finite-size analysis, which has become the touchstone for QKD security, rather than the ultimate bounds. The security of a QKD protocol is desired to be composable, i.e., the protocol must not be distinguished from an ideal protocol which is secure by construction[2]. Mathematically, a composable security proof can be provided by incorporating proper error parameters, ε's, for each segment of the protocol, namely, EC, privacy amplification, smoothing, and hashing[10,11].

We assume that a total number of N Gaussian signals are measured by Alice and Bob. An amount n of these would be used for key extraction, while the rest $m_{\rm pe} = N - n$ are left for PE, i.e., the evaluation of the CM. Upon successful completion of the EC procedure, with probability $p_{\rm ec}$, the composable finite-size secret key rate is given by[38]:

$$K \geq \frac{np_{\rm ec}}{N}\left(K_{\rm pe} - \frac{\Delta_{\rm aep}}{\sqrt{n}} + \frac{\Theta}{n}\right), \tag{33}$$

where the higher-order terms read:

$$\Delta_{\rm aep} := 4\log_2(\sqrt{d}+2)\sqrt{\log_2(18p_{\rm ec}^{-2}\varepsilon_{\rm s}^{-4})}, \tag{34}$$

$$\Theta := \log_2\left[p_{\rm ec}\left(1-\frac{\varepsilon_{\rm s}^2}{3}\right)\right] + 2\log_2(\sqrt{2}\varepsilon_{\rm h}), \tag{35}$$

The above equation is valid for a protocol with overall security $\varepsilon = \varepsilon_{\rm cor} + \varepsilon_{\rm s} + \varepsilon_{\rm h} + p_{\rm ec}\varepsilon_{\rm pe}$, where $\varepsilon_{\rm pe}$ is the total error probability associated with PE. Assuming reverse reconciliation, the hash comparison stage of the finite-key analysis requires Bob sending $\lceil \log_2(1-\varepsilon_{\rm cor})\rceil$ bits to Alice for some proper $\varepsilon_{\rm cor}$ (called $\varepsilon_{\rm cor}$-correctness) and bounds the probability that Alice's and Bob's sequences are different even if their hashes coincide. $\varepsilon_{\rm h(s)}$ is the hashing (smoothing) parameter. Conveniently one can also define the frame error rate FER $= 1 - p_{\rm ec}$. It is also assumed that by using an analog-to-digital conversion, each CV symbol is encoded with d bits of precision.

The value of $K_{\rm pe}$ in Eq. (33) can be computed in different ways depending on the level of reliability. In practice, one would use the sampled data to compute $K_{\rm pe}$ using Eq. (23) and the worst-case CM shared by the end-users. Remarkably this is practically the most appropriate choice in the case of multi-hop quantum networks with untrusted relays. In the presence of a conditionally Gaussian network, the rate in Eq. (33) modifies by setting $m \to mp_{\rm s}$ where $p_{\rm s}$ is the probability of successful post-selection. As an example, in the following, we study a quantum repeater chain and compute the composable finite-size key rate considering the worst-case parameters for the end-to-end shared CM.

Numerical results

As we mentioned earlier, a route between two nodes in a quantum network can be seen as a chain of quantum links. We here apply our general techniques for quantum networks to study a quantum chain of identical links and generally-untrusted stations. We note that this is a mere example and that our methodology is generic that can be applied to any chain. Subsequently, by assuming the illustration in Fig. 2, we find the end-to-end CM and compute the composable finite-size key rate.

Let us assume the chain is made of $M = 2^m$ identical links (we call m the repeater depth), each described by a standard CM:

$$\mathbf{V}_0 = \begin{pmatrix} a_0\mathbf{I} & c_0\mathbf{Z} \\ c_0\mathbf{Z} & b_0\mathbf{I} \end{pmatrix}. \tag{36}$$

For a typical link (without an NLA), with a TMSV source μ, channel loss η and excess noise ϵ (referred to the channel's input), we have that $\mathrm{a}_0 = \mu$, $\mathrm{b}_0 = \eta\mu + 1 - \eta + \eta\epsilon$, and $c_0 = \sqrt{\eta(\mu^2-1)}$. By using similar techniques introduced in ref. [39], the end-to-end CM between Alice and Bob, in the case of non-ideal Bell measurements, is found to have the standard form:

$$\mathbf{V}_{AB} = \begin{pmatrix} a_m\mathbf{I} & c_m\mathbf{Z} \\ c_m\mathbf{Z} & b_m\mathbf{I} \end{pmatrix}, \tag{37}$$

with the following parameters:

$$\begin{cases} a_m = a_{m-1} - \frac{\eta_{\rm B}c_{m-1}^2}{\eta_{\rm B}(a_{m-1}+b_{m-1})+1-\eta_{\rm B}}, \\ b_m = b_{m-1} - \frac{\eta_{\rm B}c_{m-1}^2}{\eta_{\rm B}(a_{m-1}+b_{m-1})+1-\eta_{\rm B}}, \\ c_m = \frac{\eta_{\rm B}c_{m-1}^2}{\eta_{\rm B}(a_{m-1}+b_{m-1})+1-\eta_{\rm B}}. \end{cases} \tag{38}$$

As expected, for $\eta_{\rm B} = 1$ the above equations reduce to the previous results in ref. [39]. Next, we can apply the formula for finite-size key rate, given in Eq. (33).

In Fig. 4, we plot the secret key rate versus the overall distance between Alice and Bob. Assuming the CV QKD protocol with heterodyne detection, we compute $K_{\rm pe}$ for the worst-case scenario

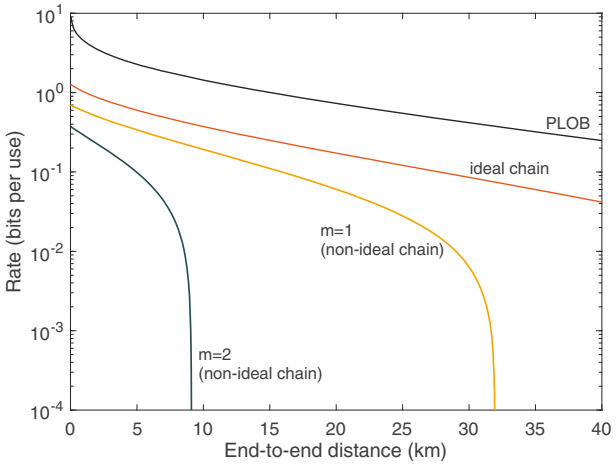

Fig. 4 Composable key rate per chain use. We consider a heterodyne-based CV-QKD protocol implemented over a quantum chain with depths $m = 1$ and $m = 2$. Here, we assume non-ideal Bell detection modules with $\eta_{\rm B} = 0.95$ and excess noise $\epsilon = 0.005$ SNU for each single link. Other parameters are $\beta = 0.98$, $N = 10^{10}$, $m_{\rm pe} = 0.1N$, $d = 2^5$, FER $= 0.1$, $\varepsilon_{\rm s} = \varepsilon_{\rm h} = \varepsilon_{\rm pe} = 10^{-10}$, $w = 6.34$ and $\varepsilon = 4.5 \times 10^{-10}$. Rates are compared with an ideal chain (with $\eta_{\rm B} = 1$, $\epsilon = 0$ and $\beta = 1$) and the repeaterless capacity, i.e., PLOB bound[1].

CM. The links are thermal-loss channels, which we simulate by considering optical fibers with the loss factor of 0.2 dB/km and noise parameter ϵ. Here, we choose an initial modulation at the input of each link, μ, such that the maximum distance is achieved. It was observed that the composable rate is highly sensitive to the relay loss, η_B, as well as channel excess noise, ϵ. This can be seen in Fig. 4 where we compare the rates for $m = 1$ and $m = 2$ with that of ideal chain, with $\eta_B = 1$ and $\epsilon = 0$.

It is known that Gaussian-only nodes cannot act as quantum repeaters[40,41]. Expectedly, Fig. 4 verifies that the end-to-end rate cannot reach/beat the repeaterless PLOB limit. This is because, in our example, the relays are Gaussian operation and as such they cannot do so. That being said, we emphasize that references[40,41] are more about entanglement distribution than QKD. The quantum repeater chain in our paper has an element of non-Gaussianity in the concept of being post-selectively Gaussian, e.g., via NLAs.

One can also compare a part of our results to the well-studied measurement-device-independent (MDI) QKD protocols[42]. In the case where $m = 1$ our chain includes two links and one intermediate node, which very much resembles a MDI setup. It is known that the so-called symmetric MDI, wherein the links are identical and the node sits exactly at the middle, is poor in delivering a secret key at long distances, especially for non-zero excess noise and non-ideal relay[43]. Whereas an asymmetric MDI, wherein the node is closer to one end, can reach longer distances. In our example, we assumed identical links and as such, comparing with symmetric MDI, we do not expect to reach longer distances.

Now let us revamp the quantum chain to design a quantum repeater. Considering the class of CV quantum repeaters[39,44–48], several proposals have been suggested to increase the reach of single-link CV QKD protocols, e.g., by utilizing NLAs[49], which nevertheless can improve the secure distance for only a few tens of kilometers[49–51]. One idea is that a quantum repeater can essentially be built by a concatenation of such NLA-improved links. Key elements of any repeater chain include entanglement distribution, entanglement distillation or purification, and entanglement swapping. An NLA-based quantum repeater uses TMSV sources as an entanglement distribution source and CV Bell measurements as entanglement swapper device. Other components such as QMs[52,53] can help to improve the performance of quantum repeaters, though they are not essential[54–56]. But due to the non-deterministic nature of NLAs, using QMs in the structure of amplifier-based repeaters seems indispensable.

To continue, we shall first account for the probabilistic (post-selection) nature of the NLAs. Take that in total N signals are transmitted, i.e., assume N runs. The meaning of "run" is well understood in a single-link protocol. It however may be slightly more complex in a repeater setup with essentially probabilistic links. Here, by each run we mean that TMSV sources at all stations simultaneously transmit a signal. Each signal then has the chance to be successfully amplified by an NLA placed at the other end of the link. In the following, we account for the post-selection effect of the NLAs by referring to ref. [57], which has studied a similar post-selection problem in the scope of free-space quantum communications.

Of the overall N runs of the protocol $p_s N$, where p_s is success probability of the repeater system, will be post-selected by NLAs. In other words, they post-select a portion $p_s N$ of the signals. Hence, assuming that EC is successful with probability p_{ec}, an average number of $np_s p_{ec}$ signals contribute to the final key and, therefore, Eq. (33) takes the form:

$$K \geq \frac{np_s p_{ec}}{N}\left(K_{pe} - \frac{\Delta_{aep}}{\sqrt{np_s}} + \frac{\Theta}{np_s}\right). \tag{39}$$

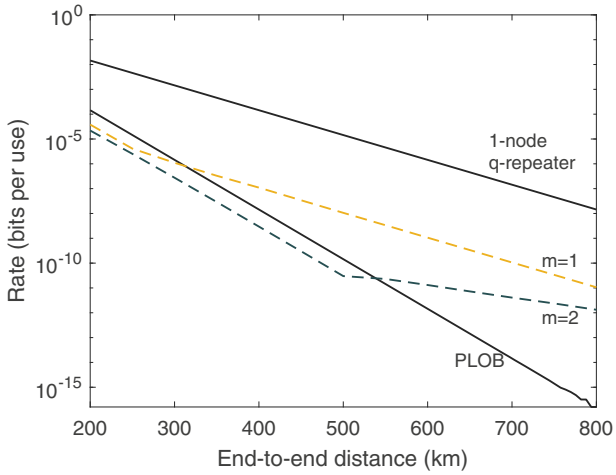

Fig. 5 Asymptotic key rate per use of quantum repeater chain. We consider a heterodyne-based CV-QKD protocol implemented over a quantum repeater chain with depths $m = 1$ and $m = 2$. Here, we assume reconciliation efficiency $\beta = 0.98$, ideal Bell detection modules with $\eta_B = 1.0$, and zero excess noise $\epsilon = 0$ for each single link. Rates are compared with the repeaterless capacity, i.e., PLOB bound[1], and the single-repeater capacity[4].

Before we present numerical results, let us briefly weigh up the action of NLAs. Firstly, to see if such devices can be practically useful, we allow some weakening of the Gaussian assumption. This is because the NLA-assisted relays can actually impose non-Gaussianity, which as pointed out earlier, is necessary to (possibly) outdistance the PLOB. As a well-known realization, we can take the action of quantum scissors (QSs), as non-deterministic NLAs, as a guide. QSs were introduced in ref. [20], and were studied further in refs. [24,25]. While the ideal NLA operation is unphysical, in the sense that it works only with zero probability of success, QSs can act as almost-ideal NLAs under weak signal assumptions. More precisely, it has been shown that a QS can almost-noiselessly amplify an input coherent state $|\alpha\rangle$ to $|g\alpha\rangle$ with the success probability of a QS $p_s = 1/g^2$, assuming that $g^2|\alpha|^2 \ll 1$[21,22,24]. In the prepare-and-measure (P&M) protocol, where each link has an initial Gaussian modulation variance V_A, a similar assumption holds: $\eta g^2 V_A \ll 1$, where we have also take into account the channel loss (We note that the P&M and entanglement-based protocols are related via $\mu = V_A + 1$).

In Fig. 5, by using the recursive equations, we plot the asymptotic secret key rate versus the overall distance between Alice and Bob. Here we have assumed that an ideal chain with $\eta_B = 1$ and $\epsilon = 0$. We encounter a dual optimization problem, which we solve numerically by optimizing over input modulation μ and amplification gain g, while making sure that $\eta g^2 V_A < 10^{-2}$.

We interpret the results as follows. The curves show that a quantum repeater chain with $m = 1$ ($m = 2$) can outperform the ultimate benchmarks at about 300 km (500 km), before which the optimized amplification gain is $g = 1$, meaning that no amplification in needed. Although these results look interesting, when we deviate from the ideal case, i.e., relay loss $\eta < 1$ and excess noise $\epsilon > 0$ (specifically we could not find a positive rate for, e.g., $\eta_B = 0.999$ and $\epsilon = 0.001$ SNU). As discussed for a chain without NLAs, this is partly due to the absolutely symmetric (MDI-like) design that we assumed through our example. With a different, possibly asymmetric, design of the repeater links, it may be possible that one can obtain positive rates (nevertheless, the methodology remains the same as presented in this manuscript). From this prospective, our results are the starting point for future studies on NLA-based quantum repeaters.

In summary, we have analyzed the composable end-to-end security of Gaussian quantum networks in the presence of generally-untrusted nodes. Assuming two arbitrary end-users of the network, we established a methodology that enables them to complete the crucial task of PE based only on the data remotely possessed. We have further investigated how they can use the estimated parameters and compute the composable key rate in the finite-size regime. Our study does not need to estimate channel parameters of the individual links that make the route between the two users. In fact, other than being Gaussian, it does not make any assumptions about the communication links, stations, and/or any other components involved.

Furthermore, we backed up our theory by considering the specific case of a chain of identical quantum links, both with and without NLAs. In our NLA-assisted design, we assumed ideal NLAs for two reasons. Firstly, under weak signal assumptions, they can be assumed Gaussian operations[20,24,25] (a good example of these NLAs are QSs[20]). Secondly, since they are ideal, in the sense that they do not add extra noise to the system, they help to obtain the ultimate performance that can be achieved by means of such designs. While we could show that an NLA-assisted chain can beat the repeaterless limit, we question its practicality. Compared with MDI protocols, we conclude that, apart from noise and loss, this is mostly due to symmetric design of the chain. In addition, for achieving a real-world analysis one can replace the ideal NLAs with realistic ones. This can nevertheless obsolete the Gaussianity of the network so this next step will have to be investigated cautiously.

METHODS

The worst-case scenario covariance matrix

In the following, we discuss the confidence intervals for $\widehat{\boldsymbol{\Sigma}}$. Despite the fact that this procedure is based on the shared data, it can have a direct application on a theoretical CM as in Eq. (37) defined through a specific model of the links between the parties. Our analysis relies on tail bounds for the chi-squared distribution. Assume that random data variables $[q]_1, \ldots, [q]_N$ from the variable q which follows a normal distribution with unit variance and zero mean value. Then, the random variable:

$$Q = \sum_{i=1}^{m_{\rm pe}} [q]_i^2 \sim \chi^2(m_{\rm pe}, 0) \tag{40}$$

follows a chi-squared distribution and allows for the following tail bounds [ref. [58], Lemma 6]:

$$P[Q \geq m_{\rm pe} + 2\sqrt{m_{\rm pe}\kappa} + 2\kappa] \leq \exp(-\kappa), \tag{41}$$

$$P[Q \leq m_{\rm pe} - 2\sqrt{m_{\rm pe}\kappa}] \leq \exp(-\kappa), \tag{42}$$

where κ is related to the error of PE, $\varepsilon_{\rm pe}$, as we shall see shortly.

From the samples $[q_x]_i$ and $[q_y]_i$, one can define standard normal variables $[q_x]_i = [q_x]_i/\sqrt{\sigma_x^2}$ and $[p_y]_i = [p_y]_i/\sqrt{\sigma_y^2}$ so the estimators of $\langle q_x^2\rangle$ and $\langle q_y^2\rangle$ can be expressed as:

$$\widehat{\langle q_x^2\rangle} := m_{\rm pe}^{-1} \sum_{i=1}^{m_{\rm pe}} [q_x]_i^2 = \sigma_x^2 m_{\rm pe}^{-1} \sum_{i=1}^{m_{\rm pe}} [q_x]_i^2, \tag{43}$$

$$\widehat{\langle q_y^2\rangle} := m_{\rm pe}^{-1} \sum_{i=1}^{m_{\rm pe}} \left[q_y\right]_i^2 = \sigma_x^2 m_{\rm pe}^{-1} \sum_{i=1}^{m_{\rm pe}} \left[q_y\right]_i^2, \tag{44}$$

where $\sum_{i=1}^{m_{\rm pe}} [q_x]_i^2$ and $\sum_{i=1}^{m_{\rm pe}} [q_y]_i^2$ are chi-square variables following the tail bounds:

$$\min\left[\sum_{i=1}^{m_{\rm pe}} [q_x]_i^2, \sum_{i=1}^{m_{\rm pe}} \left[q_y\right]_i^2\right] > m_{\rm pe} + 2\sqrt{m_{\rm pe}\kappa} + 2\kappa. \tag{45}$$

This guarantees that maximum noise is considered based on the data, and implies that:

$$\widehat{\langle q_x^2\rangle} \geq \langle q_x^2\rangle_{\rm wc}, \widehat{\langle q_y^2\rangle} \geq \langle q_y^2\rangle_{\rm wc}, \tag{46}$$

with probability:

$$\Pr\left[\widehat{\langle q_x^2\rangle} \geq \langle q_x^2\rangle_{\rm wc}\right] \leq \exp(-\kappa), \tag{47}$$

$$\Pr\left[\widehat{\langle q_y^2\rangle} \geq \langle q_y^2\rangle_{\rm wc}\right] \leq \exp(-\kappa), \tag{48}$$

for the worst-case scenario values:

$$\begin{aligned}\langle q_x^2\rangle_{\rm wc} &= \sigma_x^2 m_{\rm pe}{}^{-1}(m_{\rm pe} + 2\sqrt{m_{\rm pe}\kappa}) + \mathcal{O}(1/m_{\rm pe}) \\ &= \sigma_x^2(1 + 2\sqrt{\kappa/m_{\rm pe}}),\end{aligned} \tag{49}$$

$$\begin{aligned}\langle q_y^2\rangle_{\rm wc} &= \sigma_y^2 m_{\rm pe}{}^{-1}(m_{\rm pe} + 2\sqrt{m_{\rm pe}\kappa}) + \mathcal{O}(1/m_{\rm pe}) \\ &= \sigma_y^2(1 + 2\sqrt{\kappa/m_{\rm pe}}).\end{aligned} \tag{50}$$

To find the worst-case scenario values for the covariance term $\langle xy\rangle$ we make the following calculations: Combining the samples $[x]_i$ and $[y]_i$ accordingly, we have that:

$$([q_y]_i - [q_x]_i)^2 = [q_y]_i^2 + [q_x]_i^2 - 2[q_y]_i[q_x]_i, \tag{51}$$

$$([q_y]_i + [q_x]_i)^2 = [q_y]_i^2 + [q_x]_i^2 + 2[q_y]_i[q_x]_i, \tag{52}$$

which leads to the relation:

$$[q_y]_i[q_x]_i = \frac{1}{4}[([q_y]_i + [q_x]_i)^2 - ([q_y]_i - [q_x]_i)^2]. \tag{53}$$

The variables $[q_y]_i \pm [q_x]_i$ are zero-mean Gaussian variables with variances $V_\pm$ since $[q_x]_i$ and $[q_y]_i$ are assumed to be Gaussian. More specifically, the variables $[q_{z_\pm}]_i = ([q_y]_i \pm [q_x]_i)/\sqrt{V_\pm}$ are standard normal variables. Thus by summing over all the samples and dividing by $m_{\rm pe}$, we may express the estimator of $\langle q_x q_y\rangle$ as:

$$\begin{aligned}\widehat{\langle q_x q_y\rangle} &:= m_{\rm pe}{}^{-1} \sum_{i=1}^{m_{\rm pe}} \left[q_y\right]_i [q_x]_i \\ &= \tfrac{1}{4}\left(V_+ m_{\rm pe}{}^{-1} \sum_{i=1}^{m_{\rm pe}} \left[q_{z_+}\right]^2 - V_- m_{\rm pe}{}^{-1} \sum_{i=1}^{m_{\rm pe}} \left[q_{z_-}\right]^2\right),\end{aligned} \tag{54}$$

where $\sum_{i=1}^{m_{\rm pe}} [q_{z_\pm}]^2$ are chi-square distributions following the tail bounds of Eqs. (41) and (42).

We then impose that the estimator is smaller than its worst-case scenario value $\langle q_x q_y\rangle_{\rm wc}$, i.e.:

$$\widehat{\langle q_x q_y\rangle} < \langle q_x q_y\rangle_{\rm wc}, \tag{55}$$

where $\langle q_x q_y\rangle_{\rm wc}$ is computed by replacing $\sum_{i=1}^{m_{\rm pe}} [q_{z_\pm}]^2$ with the tail bounds in Eqs. (41) and (42), i.e., using:

$$\sum_{i=1}^{m_{\rm pe}} \left[q_{z_+}\right]^2 < m_{\rm pe} - 2\sqrt{m_{\rm pe}\kappa}, \tag{56}$$

and:

$$\sum_{i=1}^{m_{\rm pe}} \left[q_{z_-}\right]^2 > m_{\rm pe} + 2\sqrt{m_{\rm pe}\kappa} + 2\kappa. \tag{57}$$

Therefore, up to $\mathcal{O}(1/m_{\rm pe})$, we have:

$$\begin{aligned}\left\langle q_x q_y\right\rangle_{\rm wc} &= \tfrac{1}{4}\Big(V_+ \tfrac{1}{m_{\rm pe}}(m_{\rm pe} - 2\sqrt{m_{\rm pe}\kappa}) \\ &\quad - V_- \tfrac{1}{m_{\rm pe}}(m_{\rm pe} + 2\sqrt{m_{\rm pe}\kappa} + 2\kappa)\Big) \\ &= \tfrac{1}{4}\left((V_+ - V_-) - 2\sqrt{\kappa/m_{\rm pe}}(V_+ + V_-)\right) \\ &= \langle q_x q_y\rangle - \sqrt{k/m_{\rm pe}}(\langle q_x^2\rangle + \langle q_y^2\rangle).\end{aligned} \tag{58}$$

Note that a necessary condition for $\langle \widehat{q_x p_y} \rangle < \langle q_x q_y \rangle_{\text{wc}}$ to be valid is that either Eq. (56) or Eq. (57) is valid. Therefore:

$$\begin{aligned}
&\Pr\left[\langle \widehat{q_x p_y} \rangle < \langle q_x q_y \rangle_{\text{wc}}\right] \\
&\leq \Pr\left[\left(\sum_{i=1}^{m_{\text{pe}}} \left[q_{Z_+}\right]^2 < m_{\text{pe}} - 2\sqrt{m_{\text{pe}}\kappa}\right)\right. \\
&\left.\vee\left(\sum_{i=1}^{m_{\text{pe}}} \left[q_{Z_-}\right]^2 > m_{\text{pe}} + 2\sqrt{m_{\text{pe}}\kappa} + 2\kappa\right)\right] \\
&\leq \Pr\left[\left(\sum_{i=1}^{m_{\text{pe}_{\text{pe}}}} \left[q_{Z_+}\right]^2 < m_{\text{pe}} - 2\sqrt{m_{\text{pe}}\kappa}\right)\right] \\
&\quad + \Pr\left[\left(\sum_{i=1}^{m_{\text{pe}}} \left[q_{Z_-}\right]^2 > m_{\text{pe}} + 2\sqrt{m_{\text{pe}}\kappa} + 2\kappa\right)\right] \\
&\leq 2\exp(-\kappa).
\end{aligned} \tag{59}$$

Similarly, the parties calculate equivalent relations for the data from the p-quadrature. They obtain corresponding equations for $\langle p_x^2 \rangle_{\text{wc}}$, $\langle p_y^2 \rangle_{\text{wc}}$, and $\langle p_x p_y \rangle_{\text{wc}}$ following Eqs. (49), (50), and (58). In particular, since $\langle p_x p_y \rangle_{\text{wc}}$ is a negative quantity, the corresponding probability of Eq. (59) will have as an argument an inequality with a different direction and the minus sign in the corresponding Eq. (58) will be replaced by a plus sign.

All the worst-case parameters $\langle \ldots \rangle_{\text{wc}}$ define the worst-case scenario CM $\mathbf{\Sigma}_{\text{wc}}$ which has the form of Eq. (18) of the main text but with the replacements $\langle \ldots \rangle \to \langle \ldots \rangle_{\text{wc}}$. From the previous derivations, we see that:

$$\mathbf{\Sigma}_{\text{wc}} = \widehat{\mathbf{\Sigma}} + \sqrt{\frac{4\kappa}{m_{\text{pe}}}} \begin{pmatrix} \widehat{\mathbf{V}}_x & -\frac{\widehat{\mathbf{V}}_x + \widehat{\mathbf{V}}_y}{2}\mathbf{Z} \\ -\frac{\widehat{\mathbf{V}}_x + \widehat{\mathbf{V}}_y}{2}\mathbf{Z} & \widehat{\mathbf{V}}_y \end{pmatrix}, \tag{60}$$

where $\widehat{\mathbf{\Sigma}}$ is exactly the one defined in Eq. (18) of the main text, together with the associated $\widehat{\mathbf{V}}_x$ and $\widehat{\mathbf{V}}_y$. As we see, the diagonal (noise) terms are increased whereas the off-diagonal (correlation) terms are decreased in modulus. This vanishes in the asymptotic case where $m_{\text{pe}} \to \infty$.

Now, let us assume that at least one of the inequalities in Eqs. (46) or (55) is true which happens with total probability $\leq 4\exp(-\kappa)$. Considering the p quadrature, the total probability of failure is $\leq 8\exp(-\kappa)$. The latter is therefore a bound on the probability that the CM is worse than the worst-case expression $\mathbf{\Sigma}_{\text{wc}}$ (in which case the rate would be less than the worst-case value). The parties can only allow this to happen with a very small probability that is less than ε_{pe}. Therefore, by bounding the previous relation we have that:

$$8\exp(-\kappa) \leq \varepsilon_{\text{pe}}, \tag{61}$$

which defines $\kappa = (8/\varepsilon_{\text{pe}})$.

Finally, for calculating the secret key rate of Eq. (39) from the theoretical CM $\mathbf{V}$ in Eq. (37) we apply the inverse transformation of Eq. (27). In this way, we obtain a theoretical version of the classical CM:

$$\mathbf{\Sigma}^{\text{thr}} = [\mathbf{V} + (\mathbf{I} \oplus \mathbf{I})] := \begin{pmatrix} \mathbf{V}_x^{\text{thr}} & \mathbf{C}_{xy}^{\text{thr}} \\ \mathbf{C}_{xy}^{\text{thr}} & \mathbf{V}_y^{\text{thr}} \end{pmatrix}. \tag{62}$$

By using this CM, we can calculate the worst-case scenario theoretical CM:

$$\mathbf{\Sigma}_{\text{wc}}^{\text{thr}} = \mathbf{\Sigma}^{\text{thr}} + \sqrt{\frac{4\kappa}{m_{\text{pe}}}} \begin{pmatrix} \mathbf{V}_x^{\text{thr}} & -\frac{\mathbf{V}_x^{\text{thr}} + \mathbf{V}_y^{\text{thr}}}{2}\mathbf{Z} \\ -\frac{\mathbf{V}_x^{\text{thr}} + \mathbf{V}_y^{\text{thr}}}{2}\mathbf{Z} & \mathbf{V}_y^{\text{thr}} \end{pmatrix}. \tag{63}$$

Then, we calculate the worst-case scenario theoretical quantum CM using:

$$\mathbf{V}_{\text{wc}}^{\text{thr}} = \mathbf{\Sigma}_{\text{wc}}^{\text{thr}} - (\mathbf{I} \oplus \mathbf{I}). \tag{64}$$

The latter is finally used to compute K_{pe} of the composable secret key rate in Eq. (39) by following the steps (28)–(31).

DATA AVAILABILITY

All data in this paper can be reproduced by using the methodology described.

CODE AVAILABILITY

The code used in this study is available from the corresponding author upon reasonable request.

Received: 5 April 2022; Accepted: 16 August 2022;
Published online: 08 September 2022

REFERENCES

1. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
3. Cao, Y. et al. The evolution of quantum key distribution networks: on the road to the qinternet. *IEEE Commun. Surv. Tutor.* **24**, 839–894 (2022).
4. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019). See also preprint arXiv:1601.00966 (2016).
5. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
6. Pirandola, S. & Braunstein, S. L. Unite to build the quantum internet. *Nature* **532**, 169 (2016).
7. Razavi, M. *An Introduction to Quantum Communications Networks*. 2053–2571 (Morgan & Claypool Publishers, 2018).
8. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photon.* **9**, 641–652 (2015).
9. Cover, T. M. & Thomas, J. A. *Elements of Information Theory* 2nd edn (John Wiley & Sons, 2006).
10. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
11. Furrer, F. et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **109**, 100502 (2012).
12. Leverrier, A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **118**, 200501 (2017).
13. Papanastasiou, P., Ottaviani, C. & Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **96**, 042332 (2017).
14. Pirandola, S. Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.* **3**, 043014 (2021).
15. Eisert, J., Scheel, S. & Plenio, M. B. Distilling Gaussian states with Gaussian operations is impossible. *Phys. Rev. Lett.* **89**, 137903 (2002).
16. Eisert, J., Browne, D., Scheel, S. & Plenio, M. Distillation of continuous-variable entanglement with optical means. *Ann. Phys.* **311**, 431–458 (2004).
17. Ourjoumtsev, A., Dantan, A., Tualle-Brouri, R. & Grangier, P. Increasing entanglement between Gaussian states by coherent photon subtraction. *Phys. Rev. Lett.* **98**, 030502 (2007).
18. Takahashi, H. et al. Entanglement distillation from Gaussian input states. *Nat. Photon.* **4**, 178–181 (2010).
19. Kurochkin, Y., Prasad, A. S. & Lvovsky, A. I. Distillation of the two-mode squeezed state. *Phys. Rev. Lett.* **112**, 070402 (2014).
20. Ralph, T. C. & Lund, A. P. Nondeterministic noiseless linear amplification of quantum systems. *AIP Conf. Proc.* **1110**, 155–160 (2009).
21. Xiang, G. Y., Ralph, T. C., Lund, A. P., Walk, N. & Pryde, G. J. Heralded noiseless linear amplification and distillation of entanglement. *Nat. Photon.* **4**, 316–319 (2009).
22. McMahon, N. A., Lund, A. P. & Ralph, T. C. Optimal architecture for a non-deterministic noiseless linear amplifier. *Phys. Rev. A* **89**, 023846 (2014).
23. Chrzanowski, H. M. et al. Measurement-based noiseless linear amplification for quantum communication. *Nat. Commun.* **8**, 333–338 (2014).
24. Pandey, S., Jiang, Z., Combes, J. & Caves, C. M. Quantum limits on probabilistic amplifiers. *Phys. Rev. A* **88**, 033852 (2013).
25. Caves, C. M., Combes, J., Jiang, Z. & Pandey, S. Quantum limits on phase-preserving linear amplifiers. *Phys. Rev. A* **86**, 063802 (2012).
26. Fiurášek, J. & Cerf, N. J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **86**, 060302 (2012).

27. Li, Z. et al. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. *Phys. Rev. A* **93**, 012310 (2016).
28. Wilkinson, K. N., Papanastasiou, P., Ottaviani, C., Gehring, T. & Pirandola, S. Long-distance continuous-variable measurement-device-independent quantum key distribution with postselection. *Phys. Rev. Res.* **2**, 033424 (2020).
29. Papanastasiou, P. & Pirandola, S. Continuous-variable quantum cryptography with discrete alphabets: composable security under collective Gaussian attacks. *Phys. Rev. Res.* **3**, 013047 (2021).
30. García-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
31. Pirandola, S., Serafini, A. & Lloyd, S. Correlation matrices of two-mode bosonic systems. *Phys. Rev. A* **79**, 052327 (2009).
32. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **461**, 207–235 (2005).
33. Araki, H. & Lieb, E. H. Entropy inequalities. *Commun. Math. Phys.* **18**, 160–170 (1970).
34. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **9**, 397–402 (2015).
35. García-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J. H. Reverse coherent information. *Phys. Rev. Lett.* **102**, 210501 (2009).
36. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
37. Vedral, V. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.* **74**, 197–234 (2002).
38. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **3**, 013279 (2021).
39. Ghalaii, M. & Pirandola, S. Capacity-approaching quantum repeaters for quantum communications. *Phys. Rev. A* **102**, 062412 (2020).
40. Niset, J., Fiurášek, J. & Cerf, N. J. No-go theorem for Gaussian quantum error correction. *Phys. Rev. Lett.* **102**, 120501 (2009).
41. Namiki, R., Gittsovich, O., Guha, S. & Lütkenhaus, N. Gaussian-only regenerative stations cannot act as quantum repeaters. *Phys. Rev. A* **90**, 062316 (2014).
42. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **9**, 397–402 (2015).
43. Papanastasiou, P., Ottaviani, C. & Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **96**, 042332 (2017).
44. Dias, J. & Ralph, T. C. Quantum repeaters using continuous-variable teleportation. *Phys. Rev. A* **95**, 022312 (2017).
45. Dias, J., Winnel, M. S., Hosseinidehaj, N. & Ralph, T. C. Quantum repeater for continuous-variable entanglement distribution. *Phys. Rev. A* **102**, 052425 (2020).
46. Furrer, F. & Munro, W. J. Repeaters for continuous-variable quantum communication. *Phys. Rev. A* **98**, 032335 (2018).
47. Seshadreesan, K. P., Krovi, H. & Guha, S. Continuous-variable quantum repeater based on quantum scissors and mode multiplexing. *Phys. Rev. Res.* **2**, 013310 (2020).
48. Dias, J., Munro, W. J., Ralph, T. C. & Nemoto, K. Comparison of entanglement generation rates between continuous and discrete variable repeaters. Preprint at https://arxiv.org/abs/1906.06019 (2019).
49. Blandino, R. et al. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **86**, 012327 (2012).
50. Ghalaii, M., Ottaviani, C., Kumar, R., Pirandola, S. & Razavi, M. Long-distance continuous-variable quantum key distribution with quantum scissors. *IEEE J. Sel. Top. Quantum Electron.* **26**, 1–12 (2020).
51. Ghalaii, M., Ottaviani, C., Kumar, R., Pirandola, S. & Razavi, M. Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors. *IEEE J. Sel. Areas Commun.* **38**, 506–516 (2020).
52. Lvovsky, A. I., Sanders, B. C. & Tittel, W. Optical quantum memory. *Nat. Photon.* **3**, 706–714 (2009).
53. Simon, C. et al. Quantum memories. *Eur. Phys. J. D* **58**, 1–22 (2010).
54. Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A. & Nemoto, K. Quantum communication without the necessity of quantum memories. *Nat. Photon.* **6**, 777–781 (2012).
55. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6**, 6787 (2015).
56. Winnel, M. S., Guanzon, J. J., Hosseinidehaj, N. & Ralph, T. C. Overcoming the repeaterless bound in continuous-variable quantum communication without quantum memories. Preprint at https://arxiv.org/abs/2105.03586 (2021).
57. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **3**, 013279 (2021).
58. Kolar, M. & Liu, H. Marginal regression for multitask learning. *Proceedings of the Fifteenth International Conference on Artificial Intelligence and Statistics, PMLR* **22**, 647–655 (2012).

ACKNOWLEDGEMENTS

This work has been funded by the European Union via "Continuous Variable Quantum Communications" (CiViQ, Grant Agreement No. 820466) and the EPSRC via the UK Quantum Communications Hub (Grant No. EP/T001011/1).

AUTHOR CONTRIBUTIONS

All authors contributed to the scientific discussions and the theoretical developments of the study. M.G. wrote the manuscript except for the Parameter Estimation part, which was written by P.P., with the entire manuscript being revised by S.P.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Masoud Ghalaii.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.