Article:
Fletcher, Alasdair I. and Pirandola, Stefano orcid.org/0000-0001-6165-5615 (2022) Continuous variable measurement device independent quantum conferencing with post-selection. npj Quantum Information. 17329. ISSN: 2056-6387

https://doi.org/10.1038/s41598-022-22251-8

scientific reports

Check for updates

OPEN

Continuous variable measurement device independent quantum conferencing with postselection

Alasdair I. Fletcher✉ & Stefano Pirandola

A continuous variable (CV), measurement device independent (MDI) quantum key distribution (QKD) protocol is analyzed, enabling three parties to connect for quantum conferencing. We utilise a generalised Bell detection at an untrusted relay and a postselection procedure, in which distant parties reconcile on the signs of the displacements of the quadratures of their prepared coherent states. We derive the rate of the protocol under a collective pure-loss attack, demonstrating improved rate-distance performance compared to the equivalent non-post-selected protocol. In the symmetric configuration in which all the parties lie the same distance from the relay, we find a positive key rate over 6 km. Such postselection techniques can be used to improve the rate of multi-party quantum conferencing protocols at longer distances at the cost of reduced performance at shorter distances.

Quantum Key Distribution (QKD) promises provably secure communication[1] based on fundamental physical principles. Relying on the inability to clone arbitrary quantum states[2] and by utilising non-orthogonal states or entanglement[3], two distant parties are able to agree symmetric cryptographic keys, secure against any attack possible within the laws of quantum mechanics. The technology has rapidly matured, advancing from the first proposed protocols based on transmission of discrete single qubit states[4,5] and proof of principle of experiments to practical deployments over long distances[6–8] and networks and network protocols enabling multiple users to communicate securely across metropolitan sized areas and beyond[9–11].

However, whilst QKD offers ultimate security against channel attacks, its practical implementation remains challenging. Many approaches require trusted experimental devices and detectors and therefore suffer from the possibility of so-called *side-channel attacks* against such devices. Fully Device-Independent approaches to QKD are possible, which entirely eliminate such attacks[12–14] but these are practically limited by low rates and poor distance scaling. Instead Measurement Device Independent (MDI) QKD[15,16] provides a middle ground, offering higher rates[17] and various practical implementations[18–20], by relaxing the assumptions on the protocol to having distant parties send states to a central detector relay which may be controlled by an Eavesdropper (Eve). Malicious behaviour by Eve may be detected by the parties in the reconciliation and parameter estimation stage of the protocol.

Moreover, point-to-point quantum communications are known to be inherently distance limited by the PLOB bound[21] expressed by the formula $\mathcal{C} = -\log_2(1-\eta)$ with the transmissivity η decaying exponentially with distance. Continuous variable (CV) QKD protocols are able to reach rates approaching the PLOB bound, outperforming discrete state protocols; furthermore their experimental implementation is more straightforward[1,22]. Naively, there was thought to be a 3db (corresponding to $\eta = \frac{1}{2}$) loss-limit on CV QKD, however this has since been exceeded with reverse reconciliation, twin-field QKD[23–26] and postselection techniques. Postselection techniques rely on the fact that even beyond 3db loss there are regions in parameter space in which the rate remains positive[27]. By announcing the absolute values of the quadratures of their prepared coherent states the two end parties are able to select only these regions, reconciling the signs of their quadratures into a key with a positive rate even beyond 3db loss. Such post selection techniques have been implemented experimentally[28] and have recently been exploited in the MDI setting to extend the maximum distance of two-party CV MDI QKD[29]. Other similar postselection techniques are also possible and have recently been utilised in[30,31] for discrete modulation CV QKD protocols to improve their distance scaling and tolerance to excess noise.

Whilst such postselection techniques have been shown to improve the distance scaling for typical QKD protocols with two end users; it is also frequently desirable, particularly within a network setting, for multiple users to be able to establish a common secret key. Quantum conferencing[32] enables the secure distribution of such keys from a single QKD protocol rather than via the composition of multiple bipartite protocols. Such protocols rely on establishing multipartite entangled states between the users such as GHZ states[33] in the discrete variable

Department of Computer Science, University of York, York YO10 5GH, UK. ✉email: alasdair.fletcher@york.ac.uk

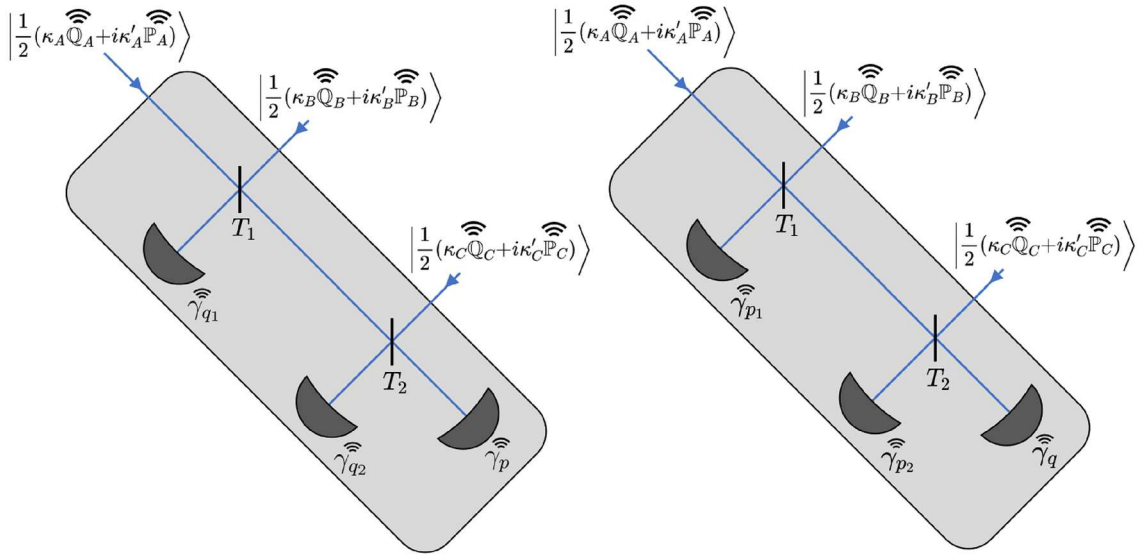

Figure 1. Structure of the detector, demonstrating the two possible orientations. Input modes are mixed by two beamsplitters with transmissivities $T_1 = \frac{1}{2}$ and $T_2 = \frac{2}{3}$. In the first configuration (pictured left) the states undergo two q homodyne detections and one p homodyne detection. The parties will attempt reconciliation between $\kappa'_A, \kappa'_B, \kappa'_C$. In the second orientation (pictured right) the states undergo two p homodyne detections and one q homodyne detection. In this case the parties attempt reconciliation on $\kappa_A, \kappa_B, \kappa_C$.

case. Quantum conferencing has attracted a great deal of interest and a variety of protocols have been proposed, including MDI protocols with discrete variables[34], twin field protocols[35–37], consideration of the effect of finite sized keys[38] and recently a continuous variable MDI protocol[39].

In this work, we provide the first demonstration that the same post selection techniques typically applied to two party QKD can also be utilised to increase the effective range at which CV MDI quantum conferencing can occur. We utilise the same generalised Bell detection from the CV MDI quantum conferencing protocol introduced in[39] to establish multipartite correlations between the user's variables and a similar postselection procedure to that used in[29] to extend the effective range of the protocol. Whilst we are restricted by the need to perform numerical integration in large number of dimensions to consider only three parties and pure loss attacks, the protocol presented here is in principle readily extended to N users and entangling cloner attacks.

The structure of the paper is as follows: in "Protocol and detector" we introduce the protocol and explain the structure of the detector; "Rate" explains how the rate of the protocol is calculated; "Results" provides results and "Conclusion" is for conclusions.

Protocol and detector

In this paper, we consider the case of three users undertaking quantum conferencing. The three parties: Alice, Bob and Charlie individually prepare Gaussian modulated coherent states. Each party individually has access to an independent zero-mean Gaussian distribution with standard deviations $\sigma_A, \sigma_B, \sigma_C$ respectively. Each party then draws two independent values from their respective distributions for the value of the q and p quadratures of their coherent state. They encode the absolute values in the variables $\mathbb{Q}_i$ and $\mathbb{P}_i$ respectively and the signs in κ_i and κ'_i. Thus they prepare coherent states of the form:

$$|\alpha_i\rangle = |\frac{1}{2}(\kappa_i\mathbb{Q}_i + \kappa'_i\mathbb{P}_i)\rangle \quad \text{for } i = A, B, C\,. \tag{1}$$

Each state is sent through a lossy channel to the detector which may be attacked by an eavesdropper (Eve). This is modelled as a beamsplitter attack in which Eve inserts a beamsplitter into each channel, storing the outputs in a quantum memory. In a pure loss attack, Eve does not actively inject any state at the beamsplitter and thus each coherent state is instead mixed with the vacuum state $|0\rangle$.

The structure of the detector is illustrated in Fig. 1 and was devised in[39] to perform a generalised Bell detection on the incoming coherent states. It is comprised of a cascade of beamsplitters, each having transmissivity $T_i = \frac{i}{i+1}$. In the case of three parties, which we consider, this corresponds to $T_1 = 1/2$ and $T_2 = 2/3$. The beamsplitters are followed by two q (p) homodyne detections and a final homodyne detection in the p (q) quadrature and the results of all the measurements are publicly broadcast. Operated correctly, in the entanglement based representation[1] the detector has the effect of projecting the Alice-Bob-Charlie state into a symmetric state with GHZ-like correlations between each parties state[39]. The two possible configurations are switched between randomly and are announced during the basis reconciliation stage of the protocol. If the first configuration (two q and one p detection) was selected, the parties will attempt to reconcile their values of $\kappa'_A, \kappa'_B, \kappa'_C$ into a secure key. Conversely, if the second configuration is utilised, the parties will attempt to reconcile their values of $\kappa_A, \kappa_B, \kappa_C$. At this point each party reveals their values of $\mathbb{Q}_i$ and $\mathbb{P}_i$, and publicly broadcasts them to every other user. Using

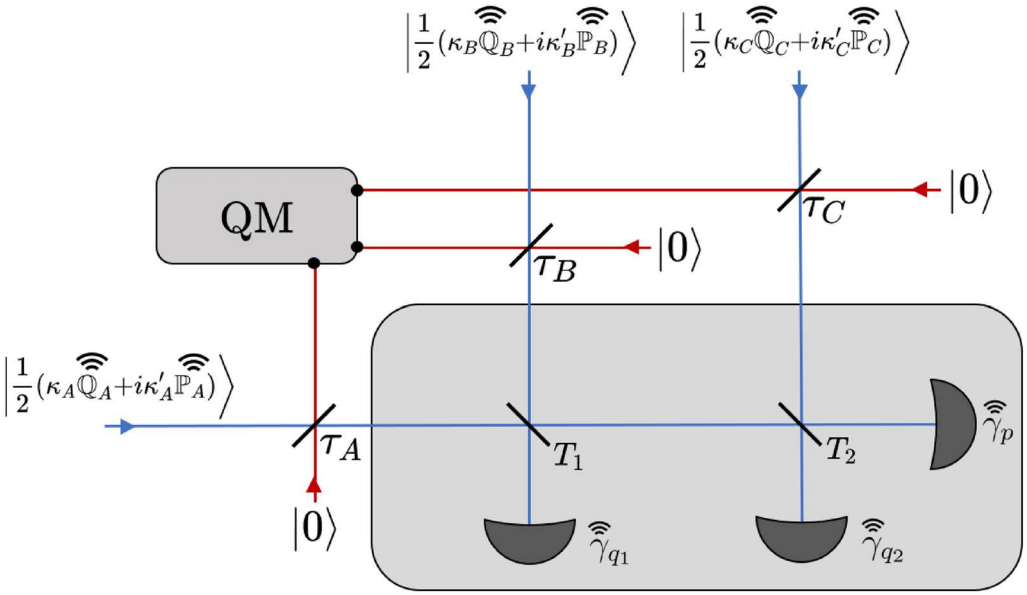

Figure 2. Operation of the detector under a collective pure loss attack. Eve attacks each of the incoming channels by inserting beamsplitters with transmissivities τ_A, τ_B, τ_C, which combine the incoming signals with vacuum states $|0\rangle$. Eve stores her output modes in a quantum memory (QM). The remaining modes are mixed in the cascade of beamsplitters and then undergo homodyne detection. The results of the homodyne detections $\gamma_{q_1}, \gamma_{q_2}, \gamma_p$ are publicly announced. Alice, Bob and Charlie also publicly announce the absolute values of the quadratures of their prepared coherent states $\mathbb{Q}_A, \mathbb{Q}_B, \mathbb{Q}_C, \mathbb{P}_A, \mathbb{P}_B, \mathbb{P}_C$. In this configuration the parties attempt to reconcile their values of $\kappa'_A, \kappa'_B, \kappa'_C$.

their knowledge of $\mathbb{Q}_i$ and $\mathbb{P}_i$, the parties can perform postselection, only retaining instances of the protocol where their mutual information exceeds Eve's Holevo information. Figure 2 depicts the protocol being performed under the pure loss attack assumed throughout this paper.

Rate

We first sketch the method used to determine the rate. At the end of the protocol the parties perform pairwise reconciliation between $\kappa_A, \kappa_B, \kappa_C$ or $\kappa'_A, \kappa'_B, \kappa'_C$ depending on the orientation of the detector. In the asymptotic limit of a large number of uses the rate of the protocol is given by:

$$R_{ij} = I_{ij} - \chi \tag{2}$$

where I_{ij} is the binary mutual information between the sign variables κ_i and κ_j or κ'_i and κ'_j. χ is the Holevo information. The mutual information can be found by utilising Bayes' Theorem and the distribution of measurement outcomes as detailed in "Mutual information". The Holevo information is calculated by carefully considering Eve's state at the end of the protocol as explained in "Holevo bound". Additionally, since we ultimately wish to perform postselection to increase the performance of the protocol we work with *single-point* versions of the above quantities $\tilde{I}_{ij}$ and $\tilde{\chi}$ which are the values conditioned upon the quadratures and measurement outcome. To this end we start by considering the initial covariance matrix of the Alice–Bob–Charlie–Eve system, which is given by:

$$\mathbf{V}_{ABCE} = \mathbf{I}_A \oplus \mathbf{I}_B \oplus \mathbf{I}_C \oplus \mathbf{V}_E \tag{3}$$

where $\mathbf{I}$ is the two-by-two identity matrix and for a pure loss attack $\mathbf{V}_E = \mathbf{I} \oplus \mathbf{I} \oplus \mathbf{I}$. The mean value of the Alice–Bob–Charlie system is:

$$\bar{\mathbf{x}}_{ABC} = (\kappa_A\mathbb{Q}_A, \kappa'_A\mathbb{P}_A, \kappa_B\mathbb{Q}_B, \kappa'_B\mathbb{P}_B, \kappa_C\mathbb{Q}_C, \kappa'_C\mathbb{P}_C)^T . \tag{4}$$

The mean value of Eve's system is zero. After propagation through the detector's array of beamsplitters and the homodyne detections, the distribution of measurement outcomes is given by:

$$p(\gamma_p|\kappa'_A, \kappa'_B, \kappa'_C, \mathbb{P}_A, \mathbb{P}_B, \mathbb{P}_C) = \frac{1}{\sqrt{2\pi\nu_p}} \exp\left(\frac{-(\gamma_p - \bar{p})^2}{2}\right) \tag{5}$$

where

$$\bar{p} = \sqrt{T_1 T_2 \tau_A}\, \kappa'_A\mathbb{P}_A + \sqrt{(1-T_1)T_2\tau_B}\, \kappa'_B\mathbb{P}_B + \sqrt{(1-T_2)\tau_C}\, \kappa'_C\mathbb{P}_C . \tag{6}$$

We have implicitly removed the conditioning on the modulus and absolute value of the q quadratures from the notation as there is no dependence upon them. Similarly for the opposite detector configuration:

$$p(\gamma_q|\kappa_A,\kappa_B,\kappa_C,\mathbb{Q}_A,\mathbb{Q}_B,\mathbb{Q}_C)=\frac{1}{\sqrt{2\pi\nu_q}}\exp\left(\frac{-(\gamma_q-\bar{q})^2}{2}\right) \tag{7}$$

where

$$\bar{q}=\sqrt{T_1T_2\tau_A}\,\kappa_A\mathbb{Q}_A+\sqrt{(1-T_1)T_2\tau_B}\,\kappa_B\mathbb{Q}_B+\sqrt{(1-T_2)\tau_C}\,\kappa_C\mathbb{Q}_C\,. \tag{8}$$

Finally, we have implicitly assumed throughout that the homodyne detectors have perfect efficiency.

Mutual information. We first introduce the following compact notation $\boldsymbol{\kappa'}=(\kappa'_A,\kappa'_B,\kappa'_C);\mathbb{P}=(\mathbb{P}_A,\mathbb{P}_B,\mathbb{P}_C)$, $\boldsymbol{\kappa}'_{\setminus A}=(\kappa'_B,\kappa'_C)$ which simplifies the following expressions. Let us recall the definition of the single point mutual information between the two binary variables κ'_i and κ'_j. This is clearly just the mutual information conditioned on the announced variables γ_p and $\mathbb{P}$:

$$\tilde{I}_{ij}=H_{\kappa'_i|\mathbb{P},\gamma_p}-\sum_{\kappa'_j}p(\kappa'_j|\,\mathbb{P},\gamma_p)\,H_{\kappa'_i|\kappa'_j\mathbb{P},\gamma_p} \tag{9}$$

where H is the binary entropy so that:

$$H_{\kappa'_i|\mathbb{P},\gamma_p}=-p(\kappa'_i|\mathbb{P},\gamma_p)\log_2\left(p(\kappa'_i|\mathbb{P},\gamma_p)\right)-\left(1-p(\kappa'_i|\mathbb{P},\gamma_p)\right)\log_2\left(1-p(\kappa'_i|\mathbb{P},\gamma_p)\right) \tag{10}$$

and

$$H_{\kappa'_i|\kappa'_j,\mathbb{P},\gamma_p}=-p(\kappa'_i|\kappa'_j,\mathbb{P},\gamma_p)\log_2(p(\kappa'_i|\kappa'_j,\mathbb{P},\gamma_p))-\left(1-p(\kappa'_i|\kappa'_j,\mathbb{P},\gamma_p)\right)\log_2\left(1-p(\kappa'_i|\kappa'_j,\mathbb{P},\gamma_p)\right). \tag{11}$$

From the symmetry of the detector we have $I_{AB}=I_{AC}=I_{BC}$ and for simplicity we consider only I_{AB} from this point onwards. Using Eq. (5) and Bayes' theorem we first calculate the probability of positive and negative values for κ'_A conditioned on κ'_B,κ'_C, the magnitudes of the p quadratures $\mathbb{P}$ and the measurement outcome γ_p:

$$p(\kappa'_A|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P},\gamma_p)=\frac{p(\gamma_p|\boldsymbol{\kappa}',\mathbb{P})\,p(\kappa'_A|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P})}{p(\gamma_p|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P})} \tag{12}$$

Noting that,

$$p(\gamma_p|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P})=\sum_{\kappa'_A}p(\gamma_p|\boldsymbol{\kappa}',\mathbb{P})\,p(\kappa'_A|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P}) \tag{13}$$

and $p(\kappa'_A|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P})=1/2$ we reach:

$$p(\kappa'_A|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P},\gamma_p)=\frac{p(\gamma_p|\boldsymbol{\kappa}',\mathbb{P})}{\sum_{\kappa'_A}p(\gamma_p|\boldsymbol{\kappa}',\mathbb{P})}. \tag{14}$$

We may then remove the conditioning on κ'_C to find $p(\kappa'_A|\kappa'_B,\mathbb{P},\gamma_p)$ for the second term in the single point mutual information.

$$p(\kappa'_A|\kappa'_B,\mathbb{P},\gamma_p)=\sum_{\kappa'_C}p(\kappa'_A|\boldsymbol{\kappa}'_{\setminus A},\mathbb{P}\gamma_p)\,p(\boldsymbol{\kappa}'_{\setminus b}|\kappa'_B,\mathbb{P}), \tag{15}$$

so that we may write

$$p(\kappa'_A|\kappa'_B,\mathbb{P})=\frac{\sum_{\kappa'_C}p(\gamma_p|\boldsymbol{\kappa}',\mathbb{P})}{\sum_{\kappa'_A\kappa'_C}p(\gamma_p|\boldsymbol{\kappa},'\mathbb{P})}. \tag{16}$$

Similarly to further remove the dependence from κ'_B:

$$p(\kappa'_A|\mathbb{P},\gamma_p)=\frac{\sum_{\kappa'_B\kappa'_C}p(\gamma_p|\boldsymbol{\kappa}',\mathbb{P})}{\sum_{\kappa'_A\kappa'_B\kappa'_C}p(\gamma_p|\boldsymbol{\kappa}',\mathbb{P})}. \tag{17}$$

By the same approach we can also find $p(\kappa'_B|\mathbb{P},\gamma_p)$, enabling the sum in Eq. (9) to be taken. Finally in order to take the integral over the single point mutual information we require the probability of all the variables

$$p(\gamma_p,\mathbb{P})=\sum_{\boldsymbol{\kappa}'}p(\gamma_p|\boldsymbol{\kappa'}\mathbb{P})\,p(\kappa'_A\mathbb{P}_A)\,p(\kappa'_B\mathbb{P}_B)\,p(\kappa'_C\mathbb{P}_C). \tag{18}$$

Holevo bound. At the end of the protocol Eve is left with the state $\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p}$ which is her total state conditioned on the announced absolute values of the p quadratures $\mathbb{P}$ and the measurement outcome γ_p. This state is a convex combination of pure Gaussian states corresponding to given values of $\kappa'_A,\kappa'_B,\kappa'_C$ and hence Eve's total state may be written:

$$\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p} = \sum_{\boldsymbol{\kappa}'} p(\boldsymbol{\kappa}'|\mathbb{P},\gamma_p)\ \hat{\rho}_{\mathfrak{E}|\boldsymbol{\kappa}',\mathbb{P},\gamma_p}. \tag{19}$$

It is important to note that whilst the conditional states, $\hat{\rho}_{\mathfrak{E}|\boldsymbol{\kappa}',\mathbb{P},\gamma_p}$, are pure and Gaussian the total state, $\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p}$ is not, which complicates our analysis. Nonetheless, assuming that Eve performs a collective attack on the protocol the relevant quantity to calculate is the Holevo information χ. We can again write this as a single point quantity in the following way.

$$\tilde{\chi}(\mathfrak{E}:\kappa_i'|\,\mathbb{P},\gamma_p) = S(\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p}) - S(\hat{\rho}_{\mathfrak{E}|\kappa_i',\mathbb{P},\gamma_p}) \tag{20}$$

where $\tilde{\chi}(\mathfrak{E}:\kappa_i'|\,\mathbb{P},\gamma_p)$ is the single point Holevo information and S is the von Neumann entropy which we recall is calculated from the eigenvalues $\{\lambda_i\}$ of a density matrix $\hat{\rho}$ by:

$$S(\hat{\rho}) = -\sum_i \lambda_i \log_2(\lambda_i). \tag{21}$$

First let us write the conditional states $\hat{\rho}_{\mathfrak{E}|\boldsymbol{\kappa}'\mathbb{P}\gamma_p}$ as:

$$\hat{\rho}_{\mathfrak{E}|\boldsymbol{\kappa}'\mathbb{P}\gamma_p} = |\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_A'\kappa_B'\kappa_C'}\rangle\langle\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_A'\kappa_B'\kappa_C'}| \tag{22}$$

We consider the matrix of overlaps O of this state for all the combinations of $\kappa_A', \kappa_B', \kappa_C'$.

$$O = \begin{pmatrix} 1 & C & B & BC & A & AC & AB & ABC \\ C & 1 & BC & B & AC & A & ABC & AB \\ B & BC & 1 & C & AB & ABC & A & AC \\ BC & B & C & 1 & ABC & AB & AC & A \\ A & AC & AB & ABC & 1 & C & B & BC \\ AC & A & ABC & AB & C & 1 & BC & B \\ AB & ABC & A & AC & B & BC & 1 & C \\ ABC & AB & AC & A & BC & B & C & 1 \end{pmatrix} \begin{matrix} (-1 & -1 & -1) \\ (-1 & -1 & 1) \\ (-1 & 1 & -1) \\ (-1 & 1 & 1) \\ (1 & -1 & -1) \\ (1 & -1 & 1) \\ (1 & 1- & 1) \\ (1 & 1 & 1) \end{matrix} \tag{23}$$

The values in the far column denote the row values of $\kappa_A', \kappa_B', \kappa_C'$. The columns may be similarly labelled. O is clearly separable as:

$$O = \begin{pmatrix} 1 & A \\ A & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & B \\ B & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & C \\ C & 1 \end{pmatrix} \tag{24}$$

which implies:

$$|\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_A'\kappa_B'\kappa_C'}\rangle = |\mathfrak{E}'^{\mathbb{P},\gamma_p}_{\kappa_A'}\rangle \otimes |\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_B'}\rangle \otimes |\mathfrak{E}'^{\mathbb{P},\gamma_p}_{\kappa_C'}\rangle\,. \tag{25}$$

Each of these states lies in a two-dimensional Hilbert space. Using x to index the parties A, B, C we may expand the states as:

$$|\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_i=-1}\rangle = c_0\,|\Phi_0^{(x)}\rangle + c_1\,|\Phi_1^{(x)}\rangle \tag{26}$$

$$|\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_i=1}\rangle = c_0\,|\Phi_0^{(x)}\rangle - c_1\,|\Phi_1^{(x)}\rangle \tag{27}$$

and find the following relation for the coefficients:

$$|c_0^{(x)}|^2 = \frac{1}{2}(1+X) \tag{28}$$

$$|c_1^{(x)}|^2 = \frac{1}{2}(1-X) \tag{29}$$

where X labels the corresponding values A, B, C from Eq. (23). For two Gaussian states with the same covariance matrix $\mathbf{V}$ and mean values $\bar{\mathbf{x}}_1$ and $\bar{\mathbf{x}}_2$ the following relation holds[40]:

$$\mathrm{Tr}(\hat{\rho}_1\hat{\rho}_2) = \exp\left(-\frac{1}{4}(\bar{\mathbf{x}}_1-\bar{\mathbf{x}}_2)\mathbf{V}^{-1}(\bar{\mathbf{x}}_1-\bar{\mathbf{x}}_2)\right) \tag{30}$$

which we use to calculate

$$A = \langle\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_A=-1}|\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_A=1}\rangle, \tag{31}$$

$$B = \langle\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_B=-1}|\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_B=1}\rangle, \tag{32}$$

$$C = \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_C=-1} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_C=1} \rangle. \tag{33}$$

We are now able to give $\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p}$ in the $\{|\Phi_0^{(A)}\rangle, |\Phi_1^{(A)}\rangle\} \otimes \{|\Phi_0^{(B)}\rangle, |\Phi_1^{(B)}\rangle\} \otimes \{|\Phi_0^{(C)}\rangle, |\Phi_1^{(C)}\rangle\}$ basis. Describing the row position with the binary string (i, j, k) and similarly the column position with (i', j', k') each component of the density matrix can be calculated by:

$$(\hat{\rho}_{\mathfrak{E}|\mathbb{P}\gamma_p})_{(ijk)(i'j'k')} = \sum_{\boldsymbol{\kappa'}} p(\boldsymbol{\kappa'}|\mathbb{P},\gamma_p) \langle \Phi_i^{(A)} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_A} \rangle \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_A} | \Phi_{i'}^{(A)} \rangle \langle \Phi_j^{(B)} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_B} \rangle \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_B} | \Phi_{j'}^{(2)} \rangle \langle \Phi_k^{(C)} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_C} \rangle \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_C} | \Phi_{k'}^{(C)} \rangle. \tag{34}$$

By calculating the following inner products:

$$\langle \Phi_0^{(x)} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_x=-1} \rangle = c_0^{(x)} \tag{35}$$

$$\langle \Phi_0^{(i)} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_x=1} \rangle = c_0^{(x)} \tag{36}$$

$$\langle \Phi_1^{(i)} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_x=-1} \rangle = c_1^{(x)} \tag{37}$$

$$\langle \Phi_1^{(i)} | \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa_x=1} \rangle = -c_1^{(x)} \tag{38}$$

we can therefore immediately find the diagonal components of the density matrix:

$$(\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p})_{(ijk)(ijk)} = |c_i^{(A)}|^2 \, |c_j^{(B)}|^2 \, |c_k^{(C)}|^2. \tag{39}$$

The off diagonal terms are given by:

$$(\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p})_{(ijk)(i'j'k')} = c_i^{(A)} \left(c_{i'}^{(A)}\right)^* c_j^{(B)} \left(c_{j'}^{(B)}\right)^* c_k^{(C)} \left(c_{k'}^{(C)}\right)^* \Lambda(i, j, k, i', j', k') \tag{40}$$

where $\Lambda(i, j, k, i', j', k')$ is given by

$$\Lambda(i, j, k, i', j', k') = \sum_{\boldsymbol{\kappa'}} (-1)^{f(\kappa'_A)|i-i'| + f(\kappa'_B)|j-j'| + f(\kappa'_C)|k-k'|} \, p(\boldsymbol{\kappa'}|\mathbb{P},\gamma_p) \tag{41}$$

where f is a function such that $f(\kappa_i = -1) = 0$ and $f(\kappa_i = 1) = 1$. We therefore have all the components of $\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p}$ from which we may numerically find the eigenvalues and compute the first term in the Holevo bound (Eve's conditional output state following the protocol $\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p}$ has dimension 2^N. Therefore for $N \geq 3$, including the tri-partite case considered in this paper, the eigenvalues of this state cannot be given in closed form. Therefore the entropy of the state and consequently the single point Holevo information $\tilde{\chi}$ can only be evaluated numerically for given values of the protocol's parameters. This greatly complicates numerical integration in Eq. (47) as no explicit expression for the single point rate can be given. It is for this reason that our analysis is limited to pure loss attacks and three users, even though the analysis is readily extended to an arbitrary number of users and entangling cloner attacks.). For the second term in the Holevo bound we need Eve's state conditioned on κ_A. If $\kappa'_A = -1$:

$$\hat{\rho}_{\mathfrak{E}|\kappa'_A=-1,\mathbb{P}} = |\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_A=-1}\rangle \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_A=-1}| \otimes \left(\sum_{\kappa'_B\kappa'_C} p(\kappa'_B, \kappa'_C|\kappa'_A = -1, \mathbb{P}, \gamma_p) \, |\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_B\kappa'_C|\kappa'_A=-1}\rangle \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_B\kappa'_C|\kappa'_A=-1}| \right); \tag{42}$$

if $\kappa'_A = 1$:

$$\hat{\rho}_{\mathfrak{E}|\kappa'_A=1,\mathbb{P}} = |\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_A=1}\rangle \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_A=1}| \otimes \left(\sum_{\kappa'_B\kappa'_C} p(\kappa'_B, \kappa'_C|\kappa'_A = 1, \mathbb{P}, \gamma_p) \, |\mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_B\kappa'_C|\kappa'_A=1}\rangle \langle \mathfrak{E}^{\mathbb{P},\gamma_p}_{\kappa'_B\kappa'_C|\kappa'_A=1}| \right). \tag{43}$$

The same method explained above may be used to determine components of these density matrices in the $\{|\Phi_0^{(B)}\rangle, |\Phi_1^{(B)}\rangle\} \otimes \{|\Phi_0^{(C)}\rangle, |\Phi_1^{(C)}\rangle\}$ basis. The eigenvalues may then be used to calculate the second term in the Holevo bound.

Postselection. We now demonstrate how the single point quantities may be used to calculate the postselected rate R_{PS}. The mutual information I_{AB} may be found by integrating the single point mutual information $\tilde{I}_{AB}$

$$I_{AB} = \int p(\mathbb{P}, \gamma_p) \, \tilde{I}_{AB}(\mathbb{P}, \gamma_p) \, d\mathbb{P} \, d\gamma_p \tag{44}$$

Similarly we do the same for the Holevo information:

$$\chi = \int p(\mathbb{P}, \gamma_p) \, \tilde{\chi}(\mathbb{P}, \gamma_p) \, d\mathbb{P} \, d\gamma_p \tag{45}$$

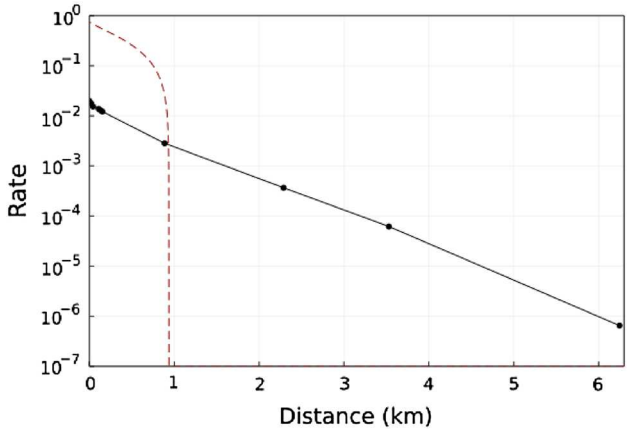

Figure 3. Post-selected rate of the protocol for the symmetric party configuration. Rate plotted with perfect detector efficiency and the variance in all prepared quadratures satisfy $\sigma_A = \sigma_B = \sigma_C = 1$. The rate of the equivalent 3-party protocol from[39] with optimised parameters, under a pure loss attack from is shown for comparison (red dashed line).

By defining the single point rate as $\tilde{R} = \tilde{I}_{AB} - \tilde{\chi}$. Thus the overall rate becomes:

$$R = \int p(\mathbb{P}, \gamma_p)\, \tilde{R}(\mathbb{P}, \gamma_p)\, d\mathbb{P}\, d\gamma_p. \tag{46}$$

The postselection ensures the parties only use instances of the protocol where the single point rate is positive. Hence the postselected rate R_{PS} becomes:

$$R_{PS} = \int p(\mathbb{P}, \gamma_p)\, \max\left[\tilde{R}(\mathbb{P}, \gamma_p), 0\right]\, d\mathbb{P}\, d\gamma_p \tag{47}$$

$$= \int_{\Gamma} p(\mathbb{P}, \gamma_p)\, \tilde{R}(\mathbb{P}, \gamma_p)\, d\mathbb{P}\, d\gamma_p \tag{48}$$

where Γ denotes the region in which the single point rate is positive.

Results

We now present the numerical results for the post-selected rate of the protocol. By utilising the relation $\tau = 10^{-\gamma d}$ and setting $\gamma = 0.02$/km (equivalent to 0.2 db/km), which corresponds to state of the art fibre optics, the rate of the protocol is expressed in terms of distances (d) of the parties from the detector. In particular, we consider the symmetric configuration in which each of the parties is located the same distance from the detector. Other asymmetric configurations can be considered within the same framework, by mapping the distance of the user furthest away into the transmissivity of each incoming channel. Thus the results presented here represent the worst case scenario for any other asymmetric configuration of the parties.

Figure 3 shows the rate-distance performance of the protocol in the asymptotic limit, assuming that a pure-loss attack is undertaken by Eve. We work with perfect detector efficiency and with the variance of each prepared quadrature $\sigma_A = \sigma_B = \sigma_B = 1$. We note that in general it may be possible to optimise the performance of the protocol over these parameters. Our results demonstrate that a positive rate can be maintained over a greater distance than in the corresponding 3-party case (shown for comparison in Fig. 3, albeit at the cost of lower rates at short distances). In particular the new protocol outperforms the equivalent protocol without postselection for distances greater than $\sim$ 1 km.

Conclusion

We have demonstrated a 3-party CV-MDI-QKD protocol that combines a generalised Bell detection with a post-selection regime based on performing reconciliation on the signs of prepared quadratures of coherent states. We show that improved rate-distance performance is possible compared to the equivalent 3-party protocol without postselection, allowing a rate in excess of 10^{-4} bits per use at greater than 3 km and a positive rate for distances of up to $\sim$ 6 km. Our protocol also outperforms the equivalent protocol without postselection for distances greater than $\sim$ 1 km. Moreover since these protocols have exactly the same structure in terms of state preparation and the detector relay, it is possible to use one such relay to perform either protocol, choosing whichever will give the higher rate. That is, if the users are able to establish their distances from the detector, they choose whether or not to announce the absolute values of their quadratures and undertake postselection depending on whether or not this will produce a better rate. Whilst $\sigma_A, \sigma_B, \sigma_C$ are preset so any optimisation over these parameters must consider both protocols simultaneously it is still possible to retain the advantages of higher rate at shorter distances from the non-postselected protocol in addition to the improved long distance performance from our protocol.

The need to undertake a high-dimensional numerical integral given in Eq. (47), for a function that cannot be given in closed form (Eve's conditional output state following the protocol $\hat{\rho}_{\mathfrak{E}|\mathbb{P},\gamma_p}$ has dimension 2^N. Therefore for $N \geq 3$, including the tri-partite case considered in this paper, the eigenvalues of this state cannot be given in closed form. Therefore the entropy of the state and consequently the single point Holevo information $\tilde{\chi}$ can only be evaluated numerically for given values of the protocol's parameters. This greatly complicates numerical integration in Eq. (47) as no explicit expression for the single point rate can be given. It is for this reason that our analysis is limited to pure loss attacks and three users, even though the analysis is readily extended to an arbitrary number of users and entangling cloner attacks.) to compute the post-selected key rate, limits our analysis to the 3-party case and pure-loss attacks. Nonetheless it may be possible to extend the study to the general N party case, maintaining the same structure of detector as in[39] and considering entangling cloner attacks. Thus, our new protocol demonstrates that secure, multi-party conferencing can be achieved over improved distances, while retaining the security advantages of an MDI QKD protocol.

Data availability

The datasets used and analysed during the current study are available from the corresponding author on reasonable request.

Received: 12 May 2022; Accepted: 12 October 2022
Published online: 15 October 2022

References

1. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012. https://doi.org/10.1364/aop.361502 (2020).
2. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802. https://doi.org/10.1038/299802a0 (1982).
3. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661. https://doi.org/10.1103/PhysRevLett.67.661 (1991).
4. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pp. 175–179 (1984).
5. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121. https://doi.org/10.1103/PhysRevLett.68.3121 (1992).
6. Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11**, 075003. https://doi.org/10.1088/1367-2630/11/7/075003 (2009).
7. Pittaluga, M. *et al.* 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photon.* **15**, 530. https://doi.org/10.1038/s41566-021-00811-0 (2021).
8. Zhang, Y. *et al.* Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **125**, 10502. https://doi.org/10.1103/PhysRevLett.125.010502 (2020) arXiv:2001.02555.
9. Joshi, S. K. *et al.* A trusted node-free eight-user metropolitan quantum communication network. *Sci. Adv.*https://doi.org/10.1126/sciadv.aba0959 *(2020).*
10. Dynes, J. F. *et al.* Cambridge quantum network. *NPJ Quantum Inf.* **5**, 101. https://doi.org/10.1038/s41534-019-0221-4 (2019).
11. Solomons, N. R. *et al.* Scalable authentication and optimal flooding in a quantum network. *PRX Quantum* **3**, 020311. https://doi.org/10.1103/PRXQuantum.3.020311 (2022).
12. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503. https://doi.org/10.1103/PhysRevLett.95.010503 (2005).
13. Schwonnek, R. *et al.* Device-independent quantum key distribution with random key basis. *Nat. Commun.* **12**, 2880. https://doi.org/10.1038/s41467-021-23147-3 (2021).
14. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021. https://doi.org/10.1088/1367-2630/11/4/045021 (2009).
15. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502. https://doi.org/10.1103/PhysRevLett.108.130502 (2012).
16. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503. https://doi.org/10.1103/PhysRevLett.108.130503 (2012).
17. Pirandola, S. *et al.* High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **9**, 397. https://doi.org/10.1038/nphoton.2015.83 (2015).
18. Tang, G.-Z., Li, C.-Y. & Wang, M. Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution. *Quantum Eng.* **3**, e79. https://doi.org/10.1002/que2.79 (2021).
19. Kwek, L.-C. *et al.* Chip-based quantum key distribution. *AAPPS Bull.* **31**, 15. https://doi.org/10.1007/s43673-021-00017-0 (2021).
20. Cui, Z. X., Zhong, W., Zhou, L. & Sheng, Y. B. Measurement-device-independent quantum key distribution with hyper-encoding. *Sci. China Phys. Mech. Astron.*https://doi.org/10.1007/s11433-019-1438-6 *(2019).*
21. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043. https://doi.org/10.1038/ncomms15043 (2017).
22. Laudenbach, F. *et al.* Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations (Adv. Quantum Technol. 1/2018). *Adv. Quantum Technol.* **1**, 1870011. https://doi.org/10.1002/qute.201870011 (2018).
23. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400. https://doi.org/10.1038/s41586-018-0066-6 (2018).
24. Chen, J. P. *et al.* Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photon.* **15**, 570. https://doi.org/10.1038/s41566-021-00828-5 (2021) arXiv:2102.00433.
25. Wang, S. *et al.* Twin-field quantum key distribution over 830-km fibre. *Nat. Photon.* **16**, 154. https://doi.org/10.1038/s41566-021-00928-2 (2022).
26. Yin, H. L. & Fu, Y. Measurement-device-independent twin-field quantum key distribution. *Sci. Rep.* **9**, 1. https://doi.org/10.1038/s41598-019-39454-1 (2019).
27. Silberhorn, C., Ralph, T. C., Lütkenhaus, N. & Leuchs, G. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Phys. Rev. Lett.* **89**, 167901. https://doi.org/10.1103/PhysRevLett.89.167901 (2002).
28. Symul, T. *et al.* Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. *Phys. Rev. A Atom. Mol. Opt. Phys.* **76**, 030303. https://doi.org/10.1103/PhysRevA.76.030303 (2007).
29. 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. https://doi.org/10.1103/physrevresearch.2.033424 (2020).

30. Lin, J., Upadhyaya, T. & Lütkenhaus, N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X* **91**, 41064. https://doi.org/10.1103/PhysRevX.9.041064 (2019) arXiv:1905.10896.
31. Liu, W. B. *et al.* Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. *PRX Quantum* **2**, 1. https://doi.org/10.1103/PRXQuantum.2.040334 (2021) arXiv:2104.11152.
32. Murta, G., Grasselli, F., Kampermann, H. & Bruß, D. Quantum conference key agreement: A review. *Adv. Quantum Technol.* **3**, 2000025. https://doi.org/10.1002/qute.202000025 (2020) arXiv:2003.10186.
33. Chen, K. & Lo, H.-K. Multi-partite quantum cryptographic protocols with noisy GHZ States. *Quantum Inf. Comput.* **7**, 689 (2007).
34. Fu, Y., Yin, H. L., Chen, T. Y. & Chen, Z. B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 1. https://doi.org/10.1103/PhysRevLett.114.090501 (2015) arXiv:1412.0832.
35. Zhao, S. *et al.* Phase-matching quantum cryptographic conferencing. *Phys. Rev. Appl.* **14**, 024010. https://doi.org/10.1103/PhysRevApplied.14.024010 (2020).
36. Cao, X.-Y. *et al.* High key rate quantum conference key agreement with unconditional security. *IEEE Access* **9**, 128870. https://doi.org/10.1109/ACCESS.2021.3113939 (2021).
37. Li, Z. *et al.* Finite-key analysis for quantum conference key agreement with asymmetric channels. *Quantum Sci. Technol.*https://doi.org/10.1088/2058-9565/ac1e00 *(2021) arXiv:2109.11163.*
38. Grasselli, F., Kampermann, H. & Bruß, D. Finite-key effects in multipartite quantum key distribution protocols. *N. J. Phys.*https://doi.org/10.1088/1367-2630/aaec34 *(2018) arXiv:1807.04472.*
39. Ottaviani, C., Lupo, C., Laurenza, R. & Pirandola, S. Modular network for high-rate quantum conferencing. *Commun. Phys.* **2**, 118. https://doi.org/10.1038/s42005-019-0209-6 (2019).
40. Banchi, L., Braunstein, S. L. & Pirandola, S. Quantum fidelity for arbitrary Gaussian states. *Phys. Rev. Lett.* **115**, 260501. https://doi.org/10.1103/PhysRevLett.115.260501 (2015).

Acknowledgements

A.I.F. acknowledges funding from the EPSRC via a Doctoral Training Partnership (EP/R513386/1). S. P. acknowledges funding from the European Union via the flagship project "Continuous Variable Quantum Communications" (CiViQ, Grant agreement No. 820466) and the EPSRC via the UK Quantum Communications Hub (Grant No. EP/T001011/1). The authors would like to thank Kieran Wilkinson for helpful discussions.

Author contributions

A.I.F. performed the analysis of the rate of the protocol, collected the numerical results and wrote the manuscript. S.P. devised the protocol and supervised the project. Both authors reviewed the manuscript and contributed to improving it.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.I.F.

Reprints and permissions information is available at www.nature.com/reprints.

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