Article:
Ottaviani, Carlo orcid.org/0000-0002-0032-3999, Lupo, Cosmo orcid.org/0000-0002-5227-4009, Laurenza, Riccardo et al. (1 more author) (2019) Modular network for high-rate quantum conferencing. Communications Physics. 118. ISSN 2399-3650

https://doi.org/10.1038/s42005-019-0209-6

COMMUNICATIONS PHYSICS

ARTICLE

https://doi.org/10.1038/s42005-019-0209-6 OPEN

Modular network for high-rate quantum conferencing

Carlo Ottaviani [1], Cosmo Lupo[2], Riccardo Laurenza[3] & Stefano Pirandola [1,4]

One of the main open problems in quantum communication is the design of efficient quantum-secured networks. This is a challenging goal, because it requires protocols that guarantee both unconditional security and high communication rates, while increasing the number of users. In this scenario, continuous-variable systems provide an ideal platform where high rates can be achieved by using off-the-shelf optical components. At the same time, the measurement-device independent architecture is also appealing for its feature of removing a substantial portion of practical weaknesses. Driven by these ideas, here we introduce a modular design of continuous-variable network where each individual module is a measurement-device-independent star network. In each module, the users send modulated coherent states to an untrusted relay, creating multipartite secret correlations via a generalized Bell detection. Using one-time pad between different modules, the network users may share a quantum-secure conference key over arbitrary distances at constant rate.

[1] Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK. [2] Department of Physics and Astronomy, University of Sheffield, Hounsfield Road, Sheffield S3 7RH, UK. [3] QSTAR, INO-CNR and LENS, Largo Enrico Fermi 2, 50125 Firenze, Italy. [4] Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA. Correspondence and requests for materials should be addressed to C.O. (email: carlo.ottaviani@york.ac.uk) or to S.P. (email: stefano.pirandola@york.ac.uk)

Quantum communication[1–3] with continuous variables (CV) systems[4–6] has attracted increasing attention over the past years. In particular, quantum key distribution (QKD) has been a rapidly developing field[7]. Theoretical studies have considered one-way protocols with coherent states[8–10], thermal protocols[11–16], and two-way protocols[17–21], with a number of experimental demonstrations[22–32]. It is known that CV-QKD protocols may achieve very high rates. As a matter of fact, ideal coherent-state protocols[9] may achieve rates as high as half of the Pirandola-Laurenza-Ottaviani-Banchi bound[33,34] for private communication over a lossy channel, i.e., $-\log_2(1-\eta)$ bits per use, with η being the channel transmissivity (see ref. [35] for a recent review on bounds for private communication).

In addition to point-to-point protocols, there has been effort towards network implementations[36–38]. An important step is the design of a scalable QKD network whose rate is high enough to compete with the classical infrastructure. Another feature to achieve is an end-to-end architecture where middle nodes may be untrusted. The first steps in this direction were moved in 2012 with the introduction of a swapping protocol based on an untrusted relay[39,40], a technique that became known as "measurement-device independence" (MDI), and recently extended to CV-QKD[41–46]. However, until today, MDI protocols have been limited to a small number of remote users, e.g., 2 in ref. [39], and 3 in ref. [47].

In this work we remove these limitations. In particular, we introduce a modular architecture that combines trusted and untrusted nodes, as well as quantum and classical communication methods, allowing secure quantum conferencing among an arbitrary number of users. At the core of our design there are MDI star-network modules, interconnected by shared nodes, which can run one-time pad protocols between different modules. Each module consists of a central (untrusted) relay performing a general N-mode Bell detection that allows an arbitrary number of users to share the same quantum conference key. The security of the protocol is first proven in the asymptotic limit of many signals exchanged, and then extended to the composable setting which incorporates finite-size effects. This modular design is scalable, because it allows us to increase arbitrarily the number of users and the achievable distance between them, while maintaining a high and constant rate. Moreover, it can be implemented using linear optical elements, and it allows to add extra modules resorting just on classical communication protocols. From this point of view the scheme is very flexible and represents a good prototype to be developed into a large scale CV-QKD network.

Results

Modular network for quantum conferencing. In our modular architecture (see Fig. 1), each individual module is a star network running a multipartite MDI-QKD quantum conferencing protocol based on the generalization of symmetric CV-MDI-QKD[43]. Each star-network module M_i is labeled by $i = 1, \ldots, N^\star$ and hosts N_i users. The generic user k in module M_i sends bright coherent states[4] $|\alpha_k^i\rangle$ to a central untrusted relay, whose amplitude α_k^i is Gaussianly modulated with variance μ_k^i. With no loss of generality we may assume that μ_k^i is the same for any k, so that we may associate a single variance parameter μ_i to module M_i. The eavesdropping is assumed to be performed by entangling cloners[7], so that the link connecting the arbitrary user k to the relay in module M_i is described by two parameters: the transmissivity η_k^i of the link, and its thermal noise $\bar{n}_k^i$.

Within module M_i the untrusted relay performs a multipartite Bell detection on the incoming N_i modes; this consists of a suitable cascade of beam-splitters followed by N_i homodyne detections, as shown in Fig. 2. The homodynes on the left measure quadratures $\hat{q}_2, \ldots, \hat{q}_{N_i}$, while the single one on the right measures $\hat{p}$. The outcomes of the measurements are combined into the global outcome $\gamma_i := (q_2, \ldots, q_{N_i}, p)$. After γ_i is broadcast to the users of the module, their individual variables α_k^i share correlations that can be post-processed into a secret key K_i via classical error correction and privacy amplification. All the users in module M_i reconcile their data with respect to a trusted user which is shared with another module M_j.

To reduce the parameters of the problem we may introduce the minimum transmissivity $\eta_i = \min_{k\in[1,N_i]} \eta_k^i$ and maximum thermal noise $\bar{n}_i = \max_{k\in[1,N_i]} \bar{n}_k^i$ associated to module M_i. From a physical point of view this is a symmetrization of the star network to the worst-case scenario, assuming all its links to have the worst combination of parameters. This condition clearly provides a lower bound $K(\mu_i, N_i, \eta_i, \bar{n}_i)$ to the actual key rate K_i of the module. By optimizing over the Gaussian modulation, we may consider the value $K(N_i, \eta_i, \bar{n}_i) := \max_{\mu_i} K(\mu_i, N_i, \eta_i, \bar{n}_i)$. Once each module has generated its key, the shared nodes run sessions of one-time pad where the keys from different modules are composed to generate a common key for all the network, with rate

$$K_{\rm net} = \min_{i\in[1,N^\star]} K(N_i, \eta_i, \bar{n}_i). \quad (1)$$

Therefore, the entire network can work at the rate of the least performing module. However, if this rate is high then the lego-like structure of the network allows all the users to communicate at the same high rate no matter how far they are from each other (see Fig. 1).

Detailed description the MDI star-network module. In this section we describe the modus operandi of a single module. To simplify the notation we omit the label i. In a single module, we consider an arbitrary number N of users (or "Bobs") sending Gaussian-modulated coherent states $|\alpha_k\rangle$ to a middle untrusted relay, as depicted in Fig. 2. Each of the coherent states is affected

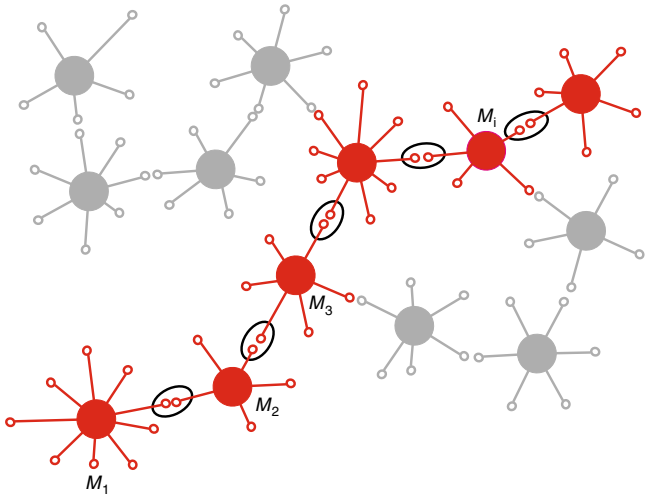

Fig. 1 Modular network for secure quantum conferencing. Each module M_i is a continuous-variable (CV) measurement-device-independent (MDI) quantum key-distribution (QKD) star network, composed by a central untrusted relay and N_i trusted users, whose connections are independently affected by loss and noise. Each module M_i first runs an independent protocol of quantum conference key-agreement. Because two different modules have a shared trusted user, we may implement classical one-time pad sessions where the keys from each module are processed into a final common key for the entire network

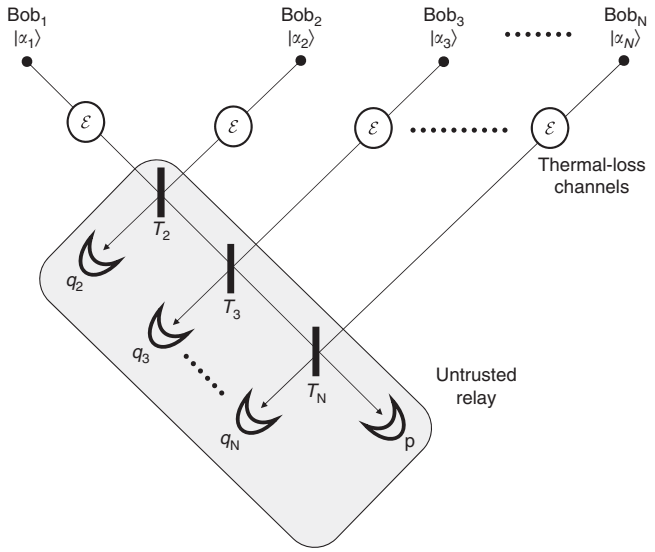

Fig. 2 Each Bob sends a Gaussian-modulated coherent state $|\alpha_k\rangle$ to an untrusted relay through a link which is described by a thermal-loss channel $\mathcal{E}$ with transmissivity η and thermal noise $\bar{n}$. At the relay, the incoming states are subject to a multipartite continuous-variable (CV) Bell detection, by using a cascade of beam-splitters with transmissivities $T_k = 1 - k^{-1}$ for $k = 2, ..., N$, followed by homodyne detectors in the $\hat{q}$ or $\hat{p}$ quadrature as shown in the figure. The global outcome $\gamma = (q_2, ..., q_N, p)$ is broadcast to the Bobs, so that a posteriori correlations are created in their local variables $\alpha_1, ..., \alpha_N$. These correlations are used to extract a secret key for quantum conferencing

by a thermal-loss channel $\mathcal{E}$ modeled as a beam-splitter with transmissivity η and thermal noise $\bar{n}$, i.e., mixing the incoming signal with an environmental thermal state with $\bar{n}$ mean photons. As explained before, we assume the worst-case scenario, so that η is the minimum transmissivity of the links and $\bar{n}$ is the maximum thermal noise. After the action of the channel $\mathcal{E}$ on each link, the states are detected by a multipartite N-mode Bell detection.

This detection consists of a suitable cascade of beam-splitters followed by N homodyne detections. More precisely, we have a sequence of beam-splitters with increasing transmissivities $T_k = 1 - k^{-1}$ for $k = 2, \ldots, N$ as depicted in Fig. 2. Then, all the homodynes at the left measure the $\hat{q}$-quadrature while the final one at the bottom measures the $\hat{p}$-quadrature, with global outcome $\gamma := (q_2, \ldots, q_N, p)$ (see Supplementary Notes 1 and 2 for further description). One can check that this measurement ideally projects onto a displaced version of an asymptotic bosonic state Ψ that realizes the multipartite Einstein-Podolsky-Rosen (EPR) conditions $\sum_{k=1}^{N} \hat{p}_k = 0$ and $\hat{q}_k - \hat{q}_{k'} = 0$ for any $k, k' = 1, \ldots, N$.

After the classical outcome γ is broadcast to the users, their individual variables α_k will share correlations which can be post-processed into secret keys via error correction and privacy amplification. We may pick the shared trusted user as the one encoding the key, with all the others decoding it in direct reconciliation[7].

Entanglement-based representation. Let us write the network in entanglement-based representation. For each user, the coherent state $|\alpha\rangle$ can be generated by using a two-mode squeezed vacuum (TMSV) state Φ_{AB} where mode B is subject to heterodyne detection. The random outcome β of the detection is fully equivalent to prepare a coherent state on mode A whose amplitude α is one-to-one with β[41]. Recall that a TMSV state is a Gaussian state with covariance matrix (CM)[4]

$$\mathbf{V}_{AB} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \begin{cases} \mathbf{Z} := \mathrm{diag}(1,-1), \\ \mathbf{I} := \mathrm{diag}(1,1), \end{cases} \quad (2)$$

where parameter $\mu \geq 1$ quantifies the noise variance of each thermal mode. Up to factors[41], parameter μ also provides the variance of the Gaussian modulation of the coherent amplitude α on mode A after heterodyning B.

Assume that the users have N copies of the same TMSV state, whose A-part is sent to the relay through a communication channel $\mathcal{E}$. Also assume that the CM of the two-mode state after the channel has the form

$$\mathbf{V}'_{AB} = \begin{pmatrix} x\mathbf{I} & z\mathbf{Z} \\ z\mathbf{Z} & y\mathbf{I} \end{pmatrix}. \quad (3)$$

Because we consider a thermal-loss channel with transmissivity η and thermal noise $\bar{n}$, we have $x = \eta\mu + (1-\eta)(2\bar{n}+1)$, $y = \mu$, and $c = \sqrt{\eta}\sqrt{\mu^2-1}$. Then, after the Bell measurement and the communication of the outcome γ, the local modes $\mathbf{B} := B_1 \ldots B_N$ are projected onto a symmetric N-mode Gaussian state with CM

$$\mathbf{V}_{\mathbf{B}|\gamma} = \begin{pmatrix} \mathbf{\Delta} & \mathbf{\Gamma} & \cdots & \mathbf{\Gamma} \\ \mathbf{\Gamma} & \mathbf{\Delta} & \ddots & \mathbf{\Gamma} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{\Gamma} & \mathbf{\Gamma} & \cdots & \mathbf{\Delta} \end{pmatrix}, \quad (4)$$

where we have set $\mathbf{\Gamma} := (N^{-1}x^{-1}z^2)\mathbf{Z}$, and

$$\mathbf{\Delta} := \mathrm{diag}\left(y - \frac{N-1}{N}\frac{z^2}{x}, y - \frac{1}{N}\frac{z^2}{x}\right). \quad (5)$$

Details on the the derivation of Eq. (4) are given in the Supplementary Note 2.

Note that the conditional state $\rho_{B_iB_j|\gamma}$ between any pair of Bobs i and j is Gaussian with CM

$$\mathbf{V}_{B_iB_j|\gamma} = \begin{pmatrix} \mathbf{\Delta} & \mathbf{\Gamma} \\ \mathbf{\Gamma} & \mathbf{\Delta} \end{pmatrix}. \quad (6)$$

For $N = 2$ this state describes the shared state in a standard CV-MDI-QKD protocol[41]. Assuming no thermal noise ($\bar{n} = 0$), the state $\rho_{B_iB_j|\gamma}$ is always entangled and we may compute its relative entropy of entanglement (REE) $E_R(\rho_{B_1B_2|\gamma})$[48–50] using the formula for the relative entropy between Gaussian states[33,51]. This REE provides an upper bound to the rate achievable by any MDI-QKD protocol (DV or CV) based on a passive untrusted relay. For $N > 2$, one can check that the bipartite state $\rho_{B_iB_j|\gamma}$ may become separable when we decrease the transmissivity η, while it certainly remains discordant[52–54]. In the multi-user scenario, the security between two Bobs may still hold because the purification of their state is held partially by Eve and partially by the other Bobs, which play the role of trusted noise. In trusted noise QKD we know that security does not rely on the presence of bipartite entanglement while quantum discord provides a necessary condition[55].

Key rate of a star-network module. Once γ is received, the ith Bob heterodynes his local mode B_i with random outcome β_i, which is one-to-one with an encoded amplitude α_i in the prepare and measure description. In this way the local mode B_j of the jth Bob is mapped into a Gaussian state $\rho_{B_j|\gamma\beta_i}$ with CM $\mathbf{V}_{B_j|\gamma\beta_i}$ that can be computed using tools from refs. [4,56–58]. The subsequent heterodyne detection of mode B_j generates an outcome β_j which is one-to-one with an encoded α_j. It is clear that the Bell detection at

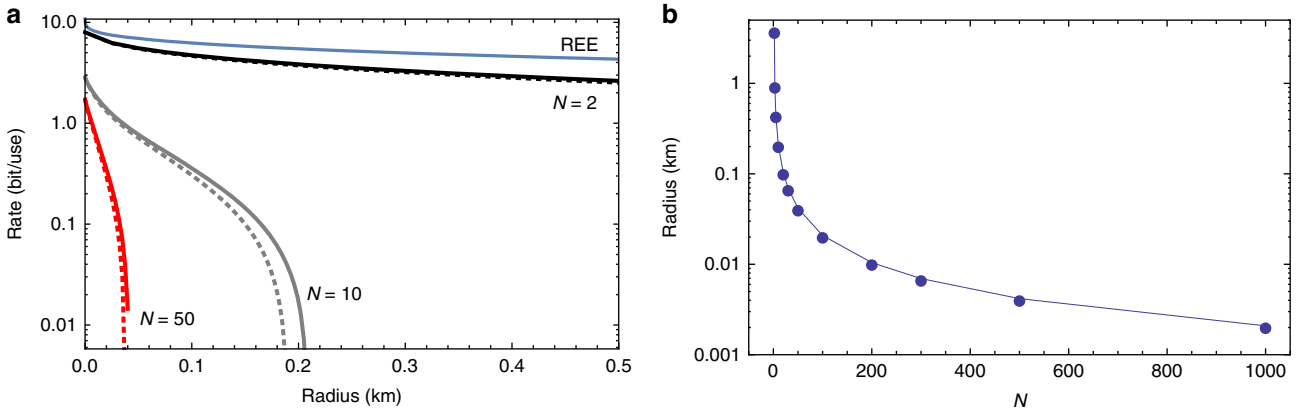

Fig. 3 Secret key rates and maximum distances for quantum conferencing. **a** We plot the conferencing key rate for a measurement-device-independent star network of $N = 2$ (black), 10 (gray), and 50 (red) users, as a function of the fiber distance d and assuming thermal noise $\bar{n} = 0$ (solid curves) and $\bar{n} = 0.05$ (dashed curves). The top blue curve is the relative entropy of entanglement (REE) of the reduced bipartite state specified by Eq. (6), which upper bounds the maximal key rate achievable with standard continuous-variable measurement-device-independent quantum-key-distribution CV-MDI-QKD ($N = 2$). **b** We plot the maximum fiber distance d versus the number of users N in a quantum conference

the relay and the local heterodyne meaurements of the various Bobs all commute, so that we may change their time order in the security analysis of the protocol. Thus, we can derive the mutual information $I(\beta_i : \beta_j)$ between the two Bobs. Similarly, we may compute the Holevo information $\chi(\beta_i : \mathbf{E})$ between the ith Bob and an eavesdropper (Eve) performing a collective Gaussian attack[59–61] associated with the thermal-loss channels[4].

The expression $K = I(\beta_i : \beta_j) - \chi(\beta_i : \mathbf{E})$, which is a function of all the parameters of the protocol, provides the asymptotic rate of secret key generation between any pair of users (see Supplementary Note 3). This is a conferencing key shared among all Bobs; it can be optimized over μ, and will depend on the number of Bobs N besides the channel parameters η and $\bar{n}$. Assuming a standard optical fiber with attenuation of 0.2 dB per km, we can map the transmissivity into a fiber distance d, using $\eta := 10^{-0.02d}$. Therefore, we have a rate of the form $K(\mu, N, d, \bar{n})$ which can be optimized over μ to give the maximal conferencing rate $K(N, d, \bar{n})$. The maximization over μ is required because for $N > 2$ the maximum rate is not obtained in the limit $\mu \gg 1$.

The conferencing rate is plotted in Fig. 3a for an MDI star network with an increasing number of users N. We compare the rates over the link-distance d for different values of thermal noise $\bar{n}$. As expected the rate decreases for increasing N. Despite this effect, our result shows that high-rate quantum conferencing is possible. For instance, in a star network with $N = 50$ users at $d \lesssim 40$ m from the central relay and thermal noise $\bar{n} = 0.05$, the key rate may be greater than $\simeq 0.1$ bits per use. In Fig. 3b, we set $\bar{n} = 0$ and plot the maximum distance for quantum conferencing versus the number of users, solving the equation $K(N, d, 0) = 0$. We see a trade-off between maximum distance and number of users. Despite this trade-off, we conclude that fiber-optic secure quantum conferencing between tens of users (belonging to a single star-network module) is indeed feasible within the typical perimeter of a large building.

Finite-size composable security. Within a module, consider a pair of Bobs, i and j, with local variables β_i and β_j after heterodyne detection. They aim at generating a secret key by reconciliating on β_i. The error correction routine is characterized by an error correction efficiency $\xi \in (0,1)$[62,63], a residual probability of error δ_{EC}, and an abort probability $1 - p > 0$. We also remark that β_i must be mapped into a discrete variable $\bar{\beta}_i$ taking 2^d values per quadrature.

Consider the mutual information $I(\beta_i : \beta_j)$ and Eve's Holevo bound $\chi(\beta_i : \mathbf{E})$ obtained from the reduced state of Eq. (6). Then, we have the following estimate for the δ-secret key rate after n uses of the module[46]

$$r_n^{\delta} \gtrsim \xi I(\beta_i : \beta_j) - \chi(\beta_i : \mathbf{E}) - \frac{1}{\sqrt{n}} \Delta_{\mathrm{AEP}}(2p\delta_{\mathrm{s}}/3, d), \qquad (7)$$

where $\delta = \delta_{\mathrm{s}} + \delta_{\mathrm{EC}} + \delta_{\mathrm{PE}}$, and $\Delta_{\mathrm{AEP}}(\xi, d) \leq 4(d+1)\sqrt{\log(2/\xi^2)}$. Here the error term δ_{s} is the smoothing parameter of the smooth conditional min-entropy[46]. For the Holevo bound $\chi(\beta_i : \mathbf{E})$ we assume the worst-case value compatible with the experimental data, up to a probability smaller than δ_{PE}. The rate r_n^{δ} is obtained conditioned that the protocol does not abort and yields a δ-secure key against collective Gaussian attacks.

The generalization to coherent attacks is obtained, as in ref. [46], by applying a Gaussian de Finetti reduction. We find that the asymptotic rates are approximately achieved for block sizes of 10^6–10^9 data points depending on the loss and noise in the channels. Examples for $N = 3$, 5, 10 are described in Fig. 4.

The composable security analysis starts from a parameter estimation procedure. As mentioned above, in estimating the channel parameters, we adopt the worst-case scenario where we choose the largest possible value of the thermal noise in each channel, and the lower available transmissivity, within the confidence intervals. This procedure may not be optimal at high loss, so that our estimates for the achievable communication distances are conservative estimates. Alternative (more performing) parameter estimation procedures, as those described in refs. [64,65,66], could be adapted to our network model and further improve its performance.

Discussion

We have introduced a network for quantum conferencing where modules can be linked together to achieve constant high-rate secure communication over arbitrarily long distances. The design of each module is based on a CV-MDI star network with many users. Our analysis shows how the secret key-rate of each star network decreases by increasing the distance from the central relay and/or the number of users. In ideal conditions, we find that 50 users may privately communicate at more than 0.1 bit per use within a radius of 40 m, distance typical of a large building. With a clock of 25 MHz[67], this is a key rate of the order of 2.5 Mbits per second for all the users. The secret keys established in the

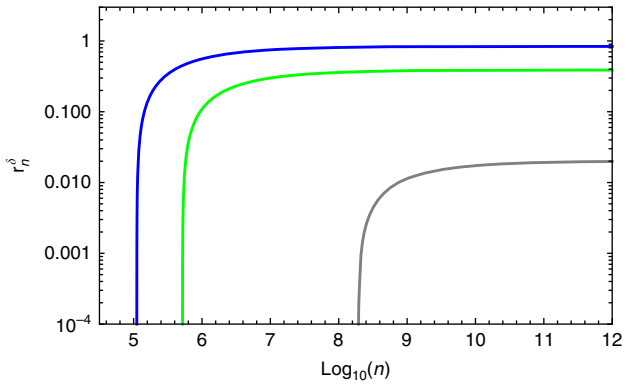

Fig. 4 Finite-size composable secret key rate r_n^δ of Eq. (7) (bits per use) versus sample size n, for error correction efficiency $\xi = 98\%$[62,63], success probability of the error correction routine $p = 0.9$, and security parameter $\delta < 10^{-20}$. The plot is obtained for a symmetric configuration with N users at a distance of 0.18 km from the relay (assuming 0.2 dB loss per km and thermal noise of $\bar{n} = 0.05$ photons). From top to bottom we consider $N = 3, 5, 10$

modules are then cascaded through the entire modular network: Adjacent modules are connected by trusted users generating a common key via one-time pad sessions.

We have studied the implementation of our protocol using coherent states, which are important for practical reasons. In Supplementary Note 4, we have also considered the case where the users use squeezed states. In such a case the performance improves, both in terms of achievable distance and the number of users. In any case, we remark that our network protocol provides a powerful application of CV-MDI-QKD that greatly outperforms its DV counterpart. In fact, while our protocol is deterministic, any linear optical implementation of a DV multipartite Bell detection is highly probabilistic, with a probability of success scaling as $\simeq 2^{-N}$ for N users. This means that a corresponding DV-MDI-QKD star network has an exponentially low rate no matter at what distance is implemented. See Supplementary Note 5 for details.

In Supplementary Note 6, we further analyze the performance of the protocol based on coherent states, assuming practical imperfections affecting the homodyne detectors and the beam splitters of the relay. Such undesirable features may arise from imperfect beam splitting operations, perturbing the multipartite Bell detection and degrading the performance of the scheme. Our results show that a proof-of-principle experiment is feasible with current technology, allowing to secure up to 9 users per module, over a radius of 12 m.

In conclusion, let us remark that our network is based on a generalization of CV MDI-QKD, where the multiuser keys are extracted within each single module. For this reason the final key is shorter than the private key extractable by just two remote end-users. In other words, the key rate of our protocol cannot reach the existing upper bounds for end-to-end network quantum communication[68,69] (see also refs. [70,71]). Finally, let us also note that additional studies may consider the multimode nature of sources and detectors, particularly for the optimized configuration of the protocol described in the Supplementary Note 4. In such a case, the security of the scheme can be recovered by applying the symmetrization of the multimode source described in ref. [72].

Methods

A detailed description of methods and techniques employed to obtain the results can be found in the Supplementary Notes accompanying this work.

Data availability

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

Received: 25 January 2019 Accepted: 29 July 2019
Published online: 30 September 2019

References

1. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information*. (University Press, Cambridge, 2000).
2. Watrous, J. *The Theory of Quantum Information*. (University Press, Cambridge, 2018).
3. Hayashi, M. *Quantum Information Theory: Mathematical Foundation* (Springer, 2017).
4. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
5. Braunstein, S. L. & van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).
6. Andersen, U. L., Neergaard-Nielsen, J. S., van Loock, P. & Furusawa, A. Hybrid discrete- and continuous-variable quantum information. *Nat. Phys.* **11**, 713–719 (2015).
7. Pirandola, S., et al. Advances in quantum cryptography. Preprint at https://arxiv.org/abs/1906.01645 (2019).
8. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
9. Weedbrook, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
10. Ottaviani, C., Mancini, S. & Pirandola, S. Gaussian two-mode attacks in one-way quantum cryptography. *Phys. Rev. A* **95**, 052310 (2017).
11. Filip, R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **77**, 022310 (2008).
12. Usenko, V. C. & Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **81**, 022318 (2010).
13. Weedbrook, C., Pirandola, S., Lloyd, S. & Ralph, T. C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **105**, 110501 (2010).
14. Weedbrook, C., Pirandola, S. & Ralph, T. C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86**, 022318 (2012).
15. Weedbrook, C., Ottaviani, C. & Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **89**, 012309 (2014).
16. Usenko, V. C. & Filip, R. Trusted noise in continuous-variable quantum key distribution: a threat and a defense. *Entropy* **18**, 20 (2016).
17. Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **4**, 726–730 (2008).
18. Ottaviani, C. & Pirandola, S. General immunity and superadditivity of two-way Gaussian quantum cryptography. *Sci. Rep.* **6**, 22225 (2016).
19. Ottaviani, C., Mancini, S. & Pirandola, S. Two-way Gaussian quantum cryptography against coherent attacks in direct reconciliation. *Phys. Rev. A* **92**, 062323 (2015).
20. Shapiro, J. H. Defeating passive eavesdropping with quantum illumination. *Phys. Rev. A* **80**, 022320 (2009).
21. Zhuang, Q., Zhang, Z., Dove, J., Wong, F. N. C. & Shapiro, J. H. Floodlight quantum key distribution: a practical route to gigabit-per-second secret-key rates. *Phys. Rev. A* **94**, 012322 (2016).
22. Gehring, T., Jacobsen, C. S. & Andersen, U. L. Single-quadrature continuous-variable quantum key distribution. *Quant. Inf. Comput.* **16**, 1081–1095 (2016).
23. Grosshans, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
24. Madsen, L. S. et al. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **3**, 1083 (2012).
25. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **7**, 378–381 (2013).
26. Zhang, Z. et al. Entanglement's benefit survives an entanglement-breaking channel. *Phys. Rev. Lett.* **111**, 010501 (2013).
27. Shapiro, J. H., Zhang, Z. & Wong, F. N. C. Secure communication via quantum illumination. *Quant. Inf. Proc.* **13**, 2171–2193 (2014).
28. Jacobsen, C. S., Gehring, T. & Andersen, U. L. Continuous variable quantum key distribution with a noisy laser. *Entropy* **17**, 4654–4663 (2015).
29. Huang, D., Huang, P., Lin, D. & Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201 (2016).
30. Zhang, Z., Zhuang, Q., Wong, F. N. C. & Shapiro, J. H. Floodlight quantum key distribution: demonstrating a framework for high-rate secure communication. *Phys. Rev. A* **95**, 012332 (2017).

31. Zhang, Z. et al. Experimental quantum key distribution at 1.3 Gbit/s secret-key rate over a 10-dB-loss channel. *Quantum Sci. Technol.* **3**, 025007 (2018).
32. Zhang, Y.-C. et al. Continuous-variable QKD over 50 km commercial fiber. Quantum. *Sci. Technol.* **4**, 035006 (2019).
33. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
34. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. Preprint at https://arxiv.org/abs/1510.08863 (2015).
35. Pirandola, S. et al. Theory of channel simulation and bounds for private communication. *Quant. Sci. Technol.* **3**, 035009 (2018).
36. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
37. Pirandola, S., Weedbrook, C., Eisert, J., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photon.* **9**, 641–652 (2015).
38. Pirandola, S. & Braunstein, S. L. Unite to build a quantum intenet. *Nature* **532**, 169–171 (2016).
39. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
40. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
41. Pirandola, S. et al. High-rate quantum cryptography in untrusted networks. *Nat. Photon.* **9**, 397–402 (2015).
42. Pirandola, S. et al. MDI-QKD: continuous- versus discrete-variables at metropolitan distances. *Nat. Photon.* **9**, 773–775 (2015).
43. Ottaviani, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: detailed security analysis of the symmetric configuration. *Phys. Rev. A* **91**, 022320 (2015).
44. Spedalieri, G. et al. Quantum cryptography with an ideal local relay. *Proc. SPIE* **9468**, 96480Z (2015).
45. Papanastasiou, P., Ottaviani, C. & Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **96**, 042332 (2017).
46. Lupo, C., Ottaviani, C., Papanastasiou, P. & Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: composable security against coherent attacks. *Phys. Rev. A* **97**, 052327 (2018).
47. Wu, Y. et al. Continuous-variable measurement-device-independent multipartite quantum communication. *Phys. Rev. A* **93**, 022325 (2016).
48. Vedral, V. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.* **74**, 197–234 (2002).
49. Vedral, V., Plenio, M. B., Rippin, M. A. & Knight, P. L. Quantifying entanglement. *Phys. Rev. Lett.* **78**, 2275–2279 (1997).
50. Vedral, V. & Plenio, M. B. Entanglement measures and purification procedures. *Phys. Rev. A* **57**, 1619–1633 (1998).
51. Banchi, L., Braunstein, S. L. & Pirandola, S. Quantum fidelity for arbitrary Gaussian states. *Phys. Rev. Lett.* **115**, 260501 (2015).
52. Giorda, P. & Paris, M. G. A. Gaussian quantum discord. *Phys. Rev. Lett.* **105**, 020503 (2010).
53. Adesso, G. & Datta, A. Quantum versus classical correlations in Gaussian states. *Phys. Rev. Lett.* **105**, 030501 (2010).
54. Pirandola, S., Spedalieri, G., Braunstein, S. L., Cerf, N. & Lloyd, S. Optimality of Gaussian discord. *Phys. Rev. Lett.* **113**, 140405 (2014).
55. Pirandola, S. Quantum discord as a resource for quantum cryptography. *Sci. Rep.* **4**, 6956 (2014).
56. Eisert, J., Scheel, S. & Plenio, M. B. Distilling Gaussian states with Gaussian operations is impossible. *Phys. Rev. Lett.* **89**, 137903 (2002).
57. Fiurášek, J. Gaussian transformations and distillation of entangled gaussian states. *Phys. Rev. Lett.* **89**, 137904 (2002).
58. Spedalieri, G., Ottaviani, C. & Pirandola, S. Covariance matrices under Bell-like detections. *Open Syst. Inf. Dyn.* **20**, 1350011 (2013).
59. Garcia-Patron, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
60. Navascues, M., Grosshans, F. & Acin, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).
61. Pirandola, S., Braunstein, S. L. & Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **101**, 200504 (2008).
62. Lin, D., Huang, D., Huang, P., Peng, J. & Zeng, G. High performance reconciliation for continuous variable quantum key distribution with LDPC code. *Int. J. Quant. Inf.* **13**, 1550010 (2015).
63. Milicevic, M., Feng, C., Zhang, Lei, M. & Gulak, P. G. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *npj Quantum Inf.* **4**, 21 (2017).
64. Lupo, C., Ottaviani, C., Papanastasiou, P. & Pirandola, S. Parameter estimation with almost no public communication for continuous-variable quantum key distribution. *Phys. Rev. Lett.* **120**, 220505 (2018).
65. Ruppert, L., Usenko, V. C. & Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **90**, 062310 (2014).
66. Thearle, O., Assad, S. M. & Symul, T. Estimation of output-channel noise for continuous-variable quantum key distribution. *Phys. Rev. A* **93**, 042343 (2016).
67. Wang, C. et al. 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel. *Sci. Rep.* **5**, 14607 (2015).
68. Pirandola, S. End-to-end capacities of a quantum communication network. *Comm. Phys.* **2**, 51 (2019).
69. Pirandola, S. Capacities of repeater-assisted quantum communications. Preprint at https://arxiv.org/abs/1601.00966 (2016).
70. Azuma, K., Mizutani, A. & Lo, H. K. Fundamental rate-loss trade-off for the quantum internet. *Nat. Comm.* **7**, 13523 (2016).
71. Rigovacca, L. et al. Versatile relative entropy bounds for quantum networks. *New J. Phys.* **20**, 013033 (2018).
72. Usenko, V. C., Ruppert, L. & Filip, R. Entanglement-based continuous-variable quantum key distribution with multimode states and detectors. *Phys. Rev. A* **90**, 062326 (2014).

Acknowledgements

This work was supported by the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1), the European Union's Horizon 2020 research and innovation program under grant agreement No 820466 (CiViQ), and the Innovation Fund Denmark via the Quantum Innovation Center Qubiz.

Author contributions

All authors contributed to the scientific discussions and the theoretical developments of the work. In particular, C.O. studied the asymptotic security of the protocols and obtained the analytical results, contributed to develop the modular structure, performed the analysis in the presence of practical imperfections, and wrote most of the paper. C.L. studied the finite-size and composable security of the scheme and edited the paper. R. L. performed numerical investigations and studied the REE upper bound. S.P. proposed the core idea of CV-MDI-QKD star network with arbitrary number of users, analyzed its performance compared to DV systems, edited the paper and supervised the entire project.

Additional information

Supplementary information accompanies this paper at https://doi.org/10.1038/s42005-019-0209-6.

Competing interests: S.P. is an Editorial Board Member of Communications Physics, but was not involved in the editorial review of, nor the decision to publish, this article. The remaining authors declare no competing interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

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