This is a repository copy of *General upper bound for distributing conferencing keys in arbitrary quantum networks*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/163404/

Version: Published Version

Article:

Pirandola, Stefano orcid.org/0000-0001-6165-5615 (2020) General upper bound for distributing conferencing keys in arbitrary quantum networks. IET Quantum Communication. pp. 22-25. ISSN 2632-8925

https://doi.org/10.1049/iet-qtc.2020.0006

Reuse
This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here: https://creativecommons.org/licenses/

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

IET Quantum Communication

Research Article

General upper bound for conferencing keys in arbitrary quantum networks

eISSN 2632-8925
Received on 27th January 2020
Revised 12th April 2020
Accepted on 29th May 2020
E-First on 10th July 2020
doi: 10.1049/iet-qtc.2020.0006
www.ietdl.org

Stefano Pirandola[1] ✉
[1]Department of Computer Science, University of York, York YO10 5GH, UK
✉ *E-mail: stefano.pirandola@york.ac.uk*

Abstract: Secure quantum conferencing refers to a protocol where a number of trusted users generate exactly the same secret key to confidentially broadcast private messages. By a modification of the techniques first introduced in (arXiv:1601.00966), the author derives a single-letter upper bound for the maximal rates of secure conferencing in a quantum network with arbitrary topology, where the users are allowed to perform the most powerful local operations assisted by two-way classical communications, and the quantum systems are routed according to the most efficient multipath flooding strategies. More precisely, the author bounds the ultimate rates that are achievable by single-message multiple-multicast protocols, where *N* senders distribute *N* independent secret keys, and each key is to be shared with an ensemble of *M* receivers.

1 I. Introduction

Quantum information science [1–5] is currently being developed at an unprecedented pace, with the field of quantum key distribution (QKD) [6–8] already extended to quantum-secured networks [9] and even satellite communications [10, 11]. Long-term plans to develop a fully-purpose quantum network, or ‘quantum internet’, are also contemplated from both a theoretical and experimental point of view [12–14]. Building quantum networks not only has the advantage of creating connectivity among many users, but also gives the possibility to overcome the intrinsic fundamental limitation imposed by the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [15], according to which the maximum number of quantum bits, entanglement bits (ebits) or private/secret bits, that can be transmitted or generated at the two ends of a lossy communication channel is limited to $-\log_2(1-\eta)$ bits per channel use, where η is the channel's transmissivity. This limit can be approached by point-to-point continuous variable protocols based on the reverse coherent information [16, 17] and can be beaten by using suitably relay-assisted QKD protocols, such as the recently-introduced twin-field QKD [18] (see also related experimental realisations [19, 20]), or by resorting to entanglement distillation repeaters based on quantum memories [21–23].

Using techniques from classical network theory [24–28] and tools more recently developed in quantum information theory [15, 29–34], the authors of [35, 36] established tight bounds (and capacities) for the repeater-assisted quantum communications over repeater chains and, more general, network scenarios. These results were first developed for the unicast case of a single sender and a single receiver in multi-hop quantum networks, and then extended [35, 37] to multiend configurations involving multiple senders and receivers, such as multiple unicasts, multicasts and multiple multicasts [26]. All these scenarios were considered in the setting of multiple independent messages, so that each sender–receiver pair was assigned a different key with respect to any other pair.

In this work, we extend the methodology of [35–37] to the case of single-message multicasts, i.e. a scenario where one or more senders aim to share exactly the same secret key with an ensemble of receivers in a multi-hop quantum network. When the sender is only one, this becomes a protocol of secure quantum conferencing in an arbitrary network topology. Using tools of network simulation and stretching [35], we can write a general upper bound to the sum of all the key rates that the senders can optimally achieve in distributing their secret keys to the destination set of the receivers. This bound has a single-letter form in terms of the relative entropy of enetanglement (REE) and includes a minimisation over suitable cuts of the network.

It is important to stress that this result not only applies to arbitrary network topologies but also arbitrary dimensions of the Hilbert space, finite or infinite. In other words, we consider quantum networks connected by discrete-variable quantum channels, but also bosonic channels. Following the methods in [15, 31, 32, 35–37], we can in fact introduce asymptotic notions of channel and network simulation that allows us to rigorously prove results in the infinite-energy limit.

The paper is organised as follows. In Section 2, we provide preliminary notions for understanding the basic theory behind the next derivation. In Section 3, we show our results for the distribution of conferencing keys in a quantum network, extending the notion of single-message multiple-multicast network to the quantum setting. Finally, Section 4 is for conclusions.

2 Preliminaries

2.1 Channel simulation

Given a quantum channel $\mathscr{E}$, we can simulate it by means of local operations (LOs) and classical communication (CC), briefly called LOCCs, applied to the input state ρ and a resource state σ. In other words, we may write $\mathscr{E}(\rho)=\mathscr{T}(\rho\otimes\sigma)$. In general, this simulation can be asymptotic, so that $\mathscr{E}(\rho)=\lim_\mu\mathscr{T}^\mu(\rho\otimes\sigma^\mu)$, for a sequence of LOCCs $\mathscr{T}^\mu$ and resource states σ^μ. Then, a channel is called teleportation-covariant if it is covariant with respect to the correction unitaries U_k of teleportation [38], i.e. finite-dimensional Pauli operators [39] or bosonic displacements [40, 41], depending on the dimension of the Hilbert space. Channel $\mathscr{E}$ is teleportation-covariant if, for any U_k, we have $\mathscr{E}(U_k\rho U_k^\dagger)=V_k\mathscr{E}(\rho)V_k^\dagger$ for unitary V_k. In particular, for $V_k=U_k$, $\mathscr{E}$ is called Weyl-covariant (or just Pauli covariant if the dimension is finite). In discrete variables, for a tele-covariant $\mathscr{E}$, we may write the simulation $\mathscr{E}(\rho)=\mathscr{T}_{\text{tele}}(\rho\otimes\sigma_{\mathscr{E}})$, where $\mathscr{T}_{\text{tele}}$ is teleportation and $\sigma_{\mathscr{E}}:=\mathscr{I}\otimes\mathscr{E}(\Phi)$ is the Choi matrix of the channel (here Φ denotes a finite-dimensional maximally-entangled state). In continuous variables, we write $\mathscr{E}(\rho)=\lim_\mu\mathscr{T}_{\text{tele}}^\mu(\rho\otimes\sigma_{\mathscr{E}}^\mu)$, where $\mathscr{T}_{\text{tele}}^\mu$ is the Braunstein-Kimble teleportation protocol based on a two-mode squeezed vacuum state Φ^μ with variance parameter μ, and $\sigma_{\mathscr{E}}^\mu:=\mathscr{I}\otimes\mathscr{E}(\Phi^\mu)$ is a sequence of quasi-Choi matrices.

2.2 *Entanglement measures*

Given a state ρ, its REE [42–44] is defined as $E_{\mathrm{R}}(\rho) = \inf_{\gamma \in \mathrm{SEP}} S(\rho || \gamma)$, where SEP is the set of separable states and $S(\rho || \gamma) := \mathrm{Tr}[\rho(\log_2 \rho - \log_2 \gamma)]$ is the quantum relative entropy. For an asymptotic state $\sigma := \lim_{\mu} \sigma^{\mu}$ defined from a sequence $\{\sigma^{\mu}\}$, we extend the definition considering $E_{\mathrm{R}}(\sigma) = \lim \inf_{\mu \to \infty} E_{\mathrm{R}}(\sigma^{\mu})$ (see [15, 31] for details). Typically, one identifies a suitable sequence of separable states γ^{μ} and write the upper bound $E_{\mathrm{R}}(\sigma) \leq \lim \inf_{\mu \to \infty} S(\sigma^{\mu} || \gamma^{\mu})$. The REE has important properties. First of all, it is monotonic under trace-preserving LOCCs Λ, i.e. we have the data processing inequality $E_{\mathrm{R}}[\Lambda(\sigma)] \leq E_{\mathrm{R}}(\sigma)$. Second, it is sub-additive over tensor products of states $\sigma^{\otimes n}$, i.e. we have $E_{\mathrm{R}}(\sigma^{\otimes n}) \leq n E_{\mathrm{R}}(\sigma)$. The REE is also asymptotically continuous: given two d-dimensional ε-close states $\| \rho - \sigma \| \leq \varepsilon$, we have $|E_{\mathrm{R}}(\rho) - E_{\mathrm{R}}(\sigma)| \leq 4\varepsilon \log_2 d + 2H_2(\varepsilon)$, where H_2 is the binary Shannon entropy.

2.3 *Quantum networks: formalism and simulation*

A quantum network $\mathcal{N}$ can be represented as an undirected finite graph [24] $\mathcal{N} = (P, E)$, where P represent the set of points (or nodes), while E is the set of undirected edges. We assume that every point P has a quantum register $\boldsymbol{p}$, i.e. an ensemble of quantum systems that are used for quantum communication and local quantum information processing. Between two points $\boldsymbol{x}$ and $\boldsymbol{y}$, there is an edge $(\boldsymbol{x}, \boldsymbol{y})$ if there is a corresponding quantum channel $\mathcal{E}_{\boldsymbol{xy}}$. In general, we assume that the channel is bidirectional, meaning that it can be used in forward direction $\boldsymbol{x} \to \boldsymbol{y}$ or backward $\boldsymbol{y} \to \boldsymbol{x}$. For two labelled points $\boldsymbol{p}_i$ and $\boldsymbol{p}_j$, we may also adopt the simpler notation $\mathcal{E}_{ij} := \mathcal{E}_{\boldsymbol{p}_i \boldsymbol{p}_j}$. Given two points $\boldsymbol{a}$ and $\boldsymbol{b}$, a cut $C: \boldsymbol{a} | \boldsymbol{b}$ with respect to these points is a bipartition $(\boldsymbol{A}, \boldsymbol{B})$ of P such that $\boldsymbol{a} \in \boldsymbol{A}$ and $\boldsymbol{b} \in \boldsymbol{B}$. Given a cut, its cut-set $\tilde{C}$ is defined by $\tilde{C} = \{(\boldsymbol{x}, \boldsymbol{y}) \in E : \boldsymbol{x} \in \boldsymbol{A}, \boldsymbol{y} \in \boldsymbol{B}\}$, i.e. represents the ensemble of edges across the bipartition. In general, a cut can be defined between multiple points, i.e. we may consider $C: \{\boldsymbol{a}_i\} | \{\boldsymbol{b}_j\}$ for $i = 1, N$ and $j = 1, M$. This means that the bipartition is such that $\boldsymbol{a}_i \in \boldsymbol{A}$ and $\boldsymbol{b}_j \in \boldsymbol{B}$ for any i and j.

Given a network $\mathcal{N}$, we may consider its simulation [35, 36]. This means that, for any edge $(\boldsymbol{x}, \boldsymbol{y})$, the quantum channel $\mathcal{E}_{\boldsymbol{xy}}$ can be replaced by a simulation $S_{\boldsymbol{xy}} = (\mathcal{T}_{\boldsymbol{xy}}, \sigma_{\boldsymbol{xy}})$ where an LOCC $\mathcal{T}_{\boldsymbol{xy}}$ is applied to a resource state $\sigma_{\boldsymbol{xy}}$, so that $\mathcal{E}_{\boldsymbol{xy}}(\rho) = \mathcal{T}_{\boldsymbol{xy}}(\rho \otimes \sigma_{\boldsymbol{xy}})$ for any input state. More generally, this may be an asymptotic simulation $\mathcal{E}_{\boldsymbol{xy}}(\rho) = \lim_{\mu} \mathcal{T}^{\mu}_{\boldsymbol{xy}}(\rho \otimes \sigma^{\mu}_{\boldsymbol{xy}})$ with sequences of LOCCs $\mathcal{T}^{\mu}_{\boldsymbol{xy}}$ and resource states $\sigma^{\mu}_{\boldsymbol{xy}}$. Therefore, we may define the LOCC simulation of the entire network $S(\mathcal{N}) = \{S_{\boldsymbol{xy}}\}_{(\boldsymbol{x}, \boldsymbol{y}) \in E}$ and a corresponding resource representation $\sigma(\mathcal{N}) = \{\sigma_{\boldsymbol{xy}}\}_{(\boldsymbol{x}, \boldsymbol{y}) \in E}$, where $\sigma_{\boldsymbol{xy}}$ may be asymptotic, i.e. defined by $\sigma_{\boldsymbol{xy}} = \lim_{\mu} \sigma^{\mu}_{\boldsymbol{xy}}$. In particular, for a network with teleportation-covariant channels, we may use teleportation LOCCs and the Choi representation $\sigma(\mathcal{N}) = \{\sigma_{\mathcal{E}_{\boldsymbol{xy}}}\}_{(\boldsymbol{x}, \boldsymbol{y}) \in E}$.

3 Multicasts of conferencing keys

We consider the model of single-message multiple-multicast network in the quantum setting. Here we have N senders $\{\boldsymbol{a}_i\}_{i=1}^{N} = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_N\}$ and M receivers $\{\boldsymbol{b}_j\}_{j=1}^{M} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_j, \ldots, \boldsymbol{b}_M\}$. Each sender $\boldsymbol{a}_i$ aims at generating the same conferencing secret key K_i with all the M receivers. Different senders distribute different keys to the ensemble of receivers, so that we have a total of N keys. In general, we assume that each point of the network can perform arbitrary LOs on their registers, assisted by two-way CCs with all the other points of the network. These adaptive LOCCs can be performed before and after each use of each channel in the network. We also assume that the global distribution of the N keys is performed assuming a multi-path flooding [45] protocol $\mathcal{P}$ where each channel of the network is actively exploited by the parties for each use of the network (see [35–37] for more details on these general protocols).

More precisely the aim of the ith sender is to share copies of a multipartite private state $\phi_{\boldsymbol{a}_i \{\boldsymbol{b}_j\}}$ with the destination set of the M receivers. This state is a direct generalisation of a GHZ state $(|0\rangle^{\otimes (M+1)} + |1\rangle^{\otimes (M+1)})/\sqrt{2}$ to include an additional shield system [46], and generates one private bit shared between the sender and all the receivers. After n uses of the network, the N senders and M receivers will share a global output state $\rho^{n}_{\{\boldsymbol{a}_i\}\{\boldsymbol{b}_j\}}$ which is ε-close to the target state

$$\phi := \bigotimes_{i=1}^{N} \phi_{\boldsymbol{a}_i \{\boldsymbol{b}_j\}}^{\otimes n R_i^{\varepsilon, n}}, \tag{1}$$

where $nR_i^{\varepsilon, n}$ is the number of copies distributed by the ith sender. By taking the limit of large n, small ε, and optimising over all protocols $\mathcal{P}$, one defines the capacity region for the achievable key rates $\{R_i\}$. We can then prove our main result.

Theorem 1: (Single-message multiple multicasts): Let us consider a quantum network $\mathcal{N} = (P, E)$ with resource representation $\sigma(\mathcal{N}) = \{\sigma_{\boldsymbol{xy}}\}_{(\boldsymbol{x}, \boldsymbol{y}) \in E}$, which may be a Choi-representation for a teleportation-covariant $\mathcal{N}$. Consider the most general multiple-multicast protocol where the i-th of N senders $\{\boldsymbol{a}_i\}$ distributes an independent key to a destination set of M receivers $\{\boldsymbol{b}_j\}$ at the rate R_i. Then, we have the following outer bound for the capacity region:

$$\sum_{i=1}^{N} R_i \leq \min_{C: \{\boldsymbol{a}_i\} | \{\boldsymbol{b}_j\}} E_{\mathrm{R}}^{\mathrm{m}}(C), \tag{2}$$

where $E_{\mathrm{R}}^{\mathrm{m}}(C)$ is the multi-edge flow of REE through cut C, defined by

$$E_{\mathrm{R}}^{m}(C) := \sum_{(\boldsymbol{x}, \boldsymbol{y}) \in \tilde{C}} E_{\mathrm{R}}(\sigma_{\boldsymbol{xy}}), \tag{3}$$

which is implicitly extended to asymptotic simulations.

Proof: Consider an arbitrary cut of the type $C: \{\boldsymbol{a}_i\} | \{\boldsymbol{b}_j\}$. With respect to this bipartition, we may write the distillable key K_{D} of the target state and write

$$\begin{aligned} K_{\mathrm{D}}(\{\boldsymbol{a}_i\} | \{\boldsymbol{b}_j\})_{\phi} &= n \sum_{i=1}^{N} R_i^{\varepsilon, n} \\ &\overset{\text{(i)}}{\leq} E_{\mathrm{R}}(\{\boldsymbol{a}_i\} | \{\boldsymbol{b}_j\})_{\phi} \\ &\overset{\text{(ii)}}{\leq} E_{\mathrm{R}}(\{\boldsymbol{a}_i\} | \{\boldsymbol{b}_j\})_{\rho^n} + \delta(\varepsilon, d), \end{aligned} \tag{4}$$

where we use (i) the fact that the distillable key of a state is upper bounded by its REE [46], and (ii) the continuity of the REE with respect to the states $\| \rho - \phi \| \leq \varepsilon$, where $\rho := \rho^{n}_{\{\boldsymbol{a}_i\}\{\boldsymbol{b}_j\}}$ is the output state and ϕ is the target state. In (4), the error term $\delta(\varepsilon, d)$ depends on the ε-closeness and the dimension d of the target private state ϕ. More in detail, this error term is $\delta(\varepsilon, d) = 4\varepsilon \log_2 d + 2H_2(\varepsilon)$, where $H_2(\varepsilon) := -\varepsilon \log_2(\varepsilon) - (1 - \varepsilon)\log_2(1 - \varepsilon)$ and the dimension of the private state grows at most exponentially in n, i.e. $d \leq 2^{\alpha_n n}$, where α_n tends to a finite constant. This is proven in [47, 48] for discrete-variable systems and [15] for both discrete- and continuous-variable systems (see also [31]). Therefore, we may write $\delta(\varepsilon, d)/n \leq 4\varepsilon \alpha_n + 2H_2(\varepsilon)/n$. By taking the limit for large n and small ε (weak converse limit), the right hand side goes to zero and we can neglect $\delta(\varepsilon, d)/n$. Therefore, by taking the weak converse limit in (4), we find

$$\lim_{\varepsilon,n}\sum_{i=1}^{N} R_i^{\varepsilon,n} \le \lim_{n\to\infty} n^{-1}E_{\mathrm{R}}(\{\boldsymbol{a}_i\}|\{\boldsymbol{b}_j\})_{\rho^n}. \tag{5}$$

The next ingredient is the simulation of the network. Given a simulation $S(\mathcal{N}) = \{S_{\boldsymbol{xy}}\}_{(\boldsymbol{x},\boldsymbol{y})\in E}$ with resource representation $\sigma(\mathcal{N}) = \{\sigma_{\boldsymbol{xy}}\}_{(\boldsymbol{x},\boldsymbol{y})\in E}$ (where we implicitly include asymptotic states), we may 'stretch' any adaptive protocol implemented over the network using the tools of [35, 36] and write the output state in the block form

$$\rho^n_{\{\boldsymbol{a}_i\}\{\boldsymbol{b}_j\}} = \bar{\Lambda}\left[\bigotimes_{(\boldsymbol{x},\boldsymbol{y})\in E}\sigma_{\boldsymbol{xy}}^{\otimes n}\right], \tag{6}$$

where $\bar{\Lambda}$ is a trace-preserving LOCC. By adopting an arbitrary cut of the type $C:\{\boldsymbol{a}_i\}|\{\boldsymbol{b}_j\}$, we can reduce this decomposition into the following:

$$\rho^n_{\{\boldsymbol{a}_i\}\{\boldsymbol{b}_j\}}(C) = \bar{\Lambda}_C\left[\bigotimes_{(\boldsymbol{x},\boldsymbol{y})\in \tilde{C}}\sigma_{\boldsymbol{xy}}^{\otimes n}\right], \tag{7}$$

where $\bar{\Lambda}_C$ is now local with respect to the bipartition introduced by the cut C. This decomposition is implicitly assumed to be asymptotic in the presence of asymptotic resource states, in which case it becomes of the following type:

$$\rho^n_{\{\boldsymbol{a}_i\}\{\boldsymbol{b}_j\}}(C) = \lim_{\mu}\bar{\Lambda}^{\mu}_C\left[\bigotimes_{(\boldsymbol{x},\boldsymbol{y})\in \tilde{C}}\sigma_{\boldsymbol{xy}}^{\mu\otimes n}\right], \tag{8}$$

for sequences of LOCCs $\bar{\Lambda}^{\mu}_C$ and resource states $\sigma^{\mu}_{\boldsymbol{xy}}$.

By replacing (7) in (5), we may exploit the monotonicity of the REE under trace preserving LOCCs and write

$$\lim_{\varepsilon,n}\sum_{i=1}^{N} R_i^{\varepsilon,n} \le E_{\mathrm{R}}^{\mathrm{m}}(C). \tag{9}$$

Then, if we minimise over all possible cuts of the type $C:\{\boldsymbol{a}_i\}|\{\boldsymbol{b}_j\}$, we may write the following bound for the asymptotic rates:

$$\sum_{i=1}^{N} R_i \le \min_{C:\{\boldsymbol{a}_i\}|\{\boldsymbol{b}_j\}} E_{\mathrm{R}}^{\mathrm{m}}(C), \tag{10}$$

which concludes the proof. □

Some considerations are in order. First of all, let us note that, for a distillable network, i.e. a network connected by distillable channels [15], such as pure-loss channels, quantum-limited amplifiers, dephasing and erasure channels, we have a simplification of the bound. A distillable channel $\mathcal{E}$ is a particular teleportation-covariant channel whose secret-key capacity $\mathcal{K}$ is equal to the REE of its Choi matrix, i.e. $\mathcal{K}(\mathcal{E}) = E_{\mathrm{R}}(\sigma_{\mathcal{E}})$. Therefore, for a distillable network with channels $\mathcal{E}_{\boldsymbol{xy}}$, for any cut C, we may write

$$E_{\mathrm{R}}^{\mathrm{m}}(C) = \sum_{(\boldsymbol{x},\boldsymbol{y})\in\tilde{C}} E_{\mathrm{R}}(\sigma_{\mathcal{E}_{\boldsymbol{xy}}}) \tag{11}$$

$$= \sum_{(\boldsymbol{x},\boldsymbol{y})\in\tilde{C}} \mathcal{K}(\mathcal{E}_{\boldsymbol{xy}}) := \mathcal{K}^{\mathrm{m}}(C), \tag{12}$$

where $\mathcal{K}^{\mathrm{m}}(C)$ is the multi-edge secret-key capacity of the cut C [35, 36].

Then, consider the case of a single sender ($N = 1$), that we denote by $\boldsymbol{a}$. This is the most basic scenario for quantum conferencing in a multi-hop quantum network. We can see that the bound in (2) simplifies to

$$R \le \min_{C:\boldsymbol{a}|\{\boldsymbol{b}_j\}} E_{\mathrm{R}}^{\mathrm{m}}(C), \tag{13}$$

where R is the maximum achievable rate. While this bound is generally large, there are network configurations where it is sufficiently tight. For instance, consider the case where the sender wants to generate a conferencing key with the destination set but it is limited to connect to an intermediate router node $\boldsymbol{r}$ via a quantum channel $\mathcal{E}_{\boldsymbol{ar}}$. Then, it is immediate to see that the conferencing key must satisfy $R \le E_{\mathrm{R}}(\sigma_{\boldsymbol{ar}})$, where $\sigma_{\boldsymbol{ar}}$ is the resource state associated with the simulation of $\mathcal{E}_{\boldsymbol{ar}}$. If the channel is distillable, we then have $R \le K(\mathcal{E}_{\boldsymbol{ar}})$. For instance, if it is a pure-loss channel with transmissivity η, we find $R \le -\log_2(1-\eta)$, i.e. the rate of the conferencing key cannot beat the PLOB bound [15].

4 Conclusions

In this work, we have studied the ultimate conferencing key rates that are achievable in a multi-hop quantum communication network. We have considered the general scenario of single-message multiple-multicast protocols, where N senders communicate with a destination set of M receivers, and each of the sender aims at generating the same secret key with the entire destination set. This general case can also be seen as a protocol for the simultaneous generation of N conferencing keys shared by the M receivers. For $N = 1$, this reduces to the basic configuration considered in the literature [49, 50].

Our results are heavily based on the tools and notions established in [35–37] for quantum networks, and [15] for point-to-point communications. In particular, we exploit the simulation and stretching techniques developed in these previous works to reduce the most general (adaptive) protocols into a block form, so that we can derive a single-letter upper bound for the capacity region in terms of the REE. Furthermore, our results do not depend on the dimension of the Hilbert space, in the sense that they apply to quantum conferencing schemes in quantum networks connected by DV or CV quantum channels.

5 Acknowledgments

This work has been supported by the European Union via the project 'Continuous Variable Quantum Communications' (CiViQ, grant no. 820466).

6 References

[1] Nielsen, M.A., Chuang, I.L.: *'Quantum computation and quantum information'* (Cambridge University Press, Cambridge, 2000)

[2] Braunstein, S.L., van Loock, P.: 'Quantum information with continuous variables', *Rev. Mod. Phys.*, 2005, **77**, p. 513

[3] Holevo, A.: *'Quantum systems, channels, information: a mathematical introduction'* (De Gruyter, Berlin-Boston, 2012)

[4] Weedbrook, C., Pirandola, S., García-Patrón, R., *et al.*: 'Gaussian quantum information', *Rev. Mod. Phys.*, 2012, **84**, p. 621

[5] Watrous, J.: *'The theory of quantum information'* (Cambridge University Press, Cambridge, 2018)

[6] Bennett, C.H., Brassard, G.: Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalaore, 1984, pp. 175–179

[7] Ekert, A.K.: 'Quantum cryptography based on Bell's theorem', *Phys. Rev. Lett.*, 1991, **67**, pp. 661–663

[8] Pirandola, S., Andersen, U.L., Banchi, L., *et al.*: 'Advances in quantum cryptography', preprint arXiv:1906.01645, 2019

[9] Fröhlich, B., Dynes, J.F., Lucamarini, M., *et al.*: 'A quantum access network', *Nature*, 2013, **501**, pp. 69–72

[10] Vallone, G., Bacco, D., Dequal, D., *et al.*: 'Experimental satellite quantum communications', *Phys. Rev. Lett.*, 2015, **115**, p. 040502

[11] Liao, S.-K., Cai, W.-Q., Handsteiner, J., *et al.*: 'Satellite-relayed intercontinental quantum network', *Phys. Rev. Lett.*, 2018, **120**, p. 030501

[12] Kimble, H.J.: 'The quantum internet', *Nature*, 2008, **453**, pp. 1023–1030

[13] Pirandola, S., Braunstein, S.L.: 'Physics: unite to build a quantum Internet', *Nature*, 2016, **532**, pp. 169–171

[14] Wehner, S., Elkouss, D., Hanson, R.: 'Quantum internet: a vision for the road ahead', *Science*, 2018, **362**, p. 303

[15] Pirandola, S., Laurenza, R., Ottaviani, C., *et al.*: 'Fundamental limits of repeaterless quantum communications', *Nat. Commun.*, 2017, **8**, p. 15043. See also arXiv:1510.08863 (2015)

[16] Pirandola, S., García-Patrón, R., Braunstein, S.L., *et al.*: 'Direct and reverse secret-key capacities of a quantum channel', *Phys. Rev. Lett.*, 2009, **102**, p. 050503

[17] García-Patrón, R., Pirandola, S., Lloyd, S., *et al.*: 'Reverse coherent information', *Phys. Rev. Lett.*, 2009, **102**, p. 210501

[18] Lucamarini, M., Yuan, Z.L., Dynes, J.F., *et al.*: 'Overcoming the rate–distance limit of quantum key distribution without quantum repeaters', *Nature (London)*, 2018, **557**, pp. 400–403

[19] Minder, M., Pittaluga, M., Roberts, G.L., *et al.*: 'Experimental quantum key distribution beyond the repeaterless secret key capacity', *Nat. Photon.*, 2019, **13**, pp. 334–338

[20] Liu, Y., Yu, Z.-W., Zhang, W., *et al.*: 'Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending', *Phys. Rev. Lett.*, 2019, **123**, p. 100505

[21] Briegel, H.-J., Dür, W., Cirac, J.I., *et al.*: 'Quantum repeaters: the role of imperfect local operations in quantum communication', *Phys. Rev. Lett.*, 1998, **81**, pp. 5932–5935

[22] Dür, W., Briegel, H.-J., Cirac, J.I., *et al.*: 'Quantum repeaters based on entanglement purification', *Phys. Rev. A*, 1999, **59**, p. 169

[23] Duan, L.M., Lukin, M.D., Cirac, J.I., *et al.*: 'Long-distance quantum communication with atomic ensembles and linear optics', *Nature (London)*, 2001, **414**, p. 413

[24] Slepian, P.: *'Mathematical foundations of network analysis* (Springer-Verlag, New York, 1968)

[25] Schrijver, A.: *'Combinatorial optimization'* (Springer-Verlag, Berlin, 2003)

[26] El Gamal, A., Kim, Y.-H.: *'Network information Theory'* (Cambridge University Press, United Kingdom, 2011)

[27] Cover, T.M., Thomas, J.A.: *'Elements of information Theory'* (Wiley, New Jersey, 2006)

[28] Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: *'Network flows: theory, algorithms and Applications'* (Prentice Hall, United States, 1993)

[29] Pirandola, S., Lupo, C.: 'Ultimate precision of adaptive noise estimation', *Phys. Rev. Lett.*, 2017, **118**, p. 100502

[30] Cope, T.P.W., Hetzel, L., Banchi, L., *et al.*: 'Simulation of non-Pauli channels', *Phys. Rev. A*, 2017, **96**, p. 022323

[31] Pirandola, S., Braunstein, S.L., Laurenza, R., *et al.*: 'Theory of channel simulation and bounds for private communication' *Quant. Sci. Technol.*, 2018, **3**, p. 035009

[32] Pirandola, S., Laurenza, R., Braunstein, S.L.: 'Teleportation simulation of bosonic Gaussian channels: strong and uniform convergence', *Eur. Phys. J.*, 2018, **D 72**, p. 162

[33] Laurenza, R., Lupo, C., Spedalieri, G., *et al.*: 'Channel simulation in quantum metrology', *Quantum Meas. Quantum Metrol.*, 2018, **5**, pp. 1–12

[34] Pirandola, S., Roy Bardhan, B., Gehring, T., *et al.*: 'Advances in photonic quantum sensing', *Nat. Photon.*, 2018, **12**, pp. 724–733

[35] Pirandola, S.: Capacities of repeater-assisted quantum communications, arXiv:1601.00966 (2016)

[36] Pirandola, S.: 'End-to-end capacities of a quantum communication network', *Commun. Phys.*, 2019, **2**, p. 51

[37] Pirandola, S.: 'Bounds for multi-end communication over quantum networks', *Quantum Sci. Technol.*, 2019, **4**, p. 045006

[38] Pirandola, S., Eisert, J., Weedbrook, C., *et al.*: 'Advances in quantum teleportation', *Nature Photon.*, 2015, **9**, pp. 641–652

[39] Bennett, C.H., Brassard, G., Crepeau, C., *et al.*: 'Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels', *Phys. Rev. Lett.*, 1993, **70**, pp. 1895–1899

[40] Braunstein, S.L., Kimble, H.J.: 'Teleportation of continuous quantum variables', *Phys. Rev. Lett.*, 1998, **80**, pp. 869–872

[41] Braunstein, S.L., D'Ariano, G.M., Milburn, G.J., *et al.*: 'Universal teleportation with a twist', *Phys. Rev. Lett.*, 2000, **84**, pp. 3486–3489

[42] Vedral, V.: 'The role of relative entropy in quantum information theory', *Rev. Mod. Phys.*, 2002, **74**, p. 197

[43] Vedral, V., Plenio, M.B., Rippin, M.A., *et al.*: 'Quantifying entanglement', *Phys. Rev. Lett.*, 1997, **78**, pp. 2275–2279

[44] Vedral, V., Plenio, M.B.: 'Entanglement measures and purification procedures', *Phys. Rev. A*, 1998, **57**, p. 1619

[45] Tanenbaum, A.S., Wetherall, D.J.: *'Computer Networks'* (Pearson, United States, 2010, 5th Edn.)

[46] Horodecki, K., Horodecki, M., Horodecki, P., *et al.*: 'Secure key from bound entanglement', *Phys. Rev. Lett.*, 2005, **94**, p. 160502

[47] Christiandl, M., Ekert, A., Horodecki, M., *et al.*: Lecture Notes in Computer Science 4392, 456–478 (2007). See also arXiv:quant-ph/0608199v3 for a more extended version

[48] Christiandl, M., Schuch, N., Winter, A.: 'Entanglement of the antisymmetric state', *Comm. Math. Phys.*, 2012, **311**, pp. 397–422

[49] Ottaviani, C., Lupo, C., Laurenza, R., *et al.*: 'Modular network for high-rate quantum conferencing', *Commun. Phys.*, 2019, **2**, p. 118

[50] Grasselli, F., Kampermann, H., Bruß, D.: 'Conference key agreement with single-photon interference', *New J. Phys.*, 2019, **21**, p. 123002