npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-024-00828-7

Optimal quantum key distribution networks: capacitance versus security

Lorenzo Cirigliano [1,2,3], Valentina Brosco [1,2,4] ✉, Claudio Castellano[4], Claudio Conti[1,2] & Laura Pilozzi[4]

The rate and security of quantum communications between users placed at arbitrary points of a quantum communication network depend on the structure of the network, on its extension and on the nature of the communication channels. In this work we propose a strategy for the optimization of trusted-relays based networks that intertwines classical network approaches and quantum information theory. Specifically, by suitably defining a quantum communication efficiency functional, we identify the optimal quantum communication connections through the network by balancing security and the quantum communication rate. The optimized network is then constructed as the network of the maximal quantum communication efficiency connections and its performance is evaluated by studying the scaling of average properties as functions of the number of nodes and of the network spatial extension.

Quantum communication networks[1] enable the realization of tasks beyond the reach of classical communication systems. Examples are unconditionally secure quantum key distribution[2,3] (QKD), quantum teleportation[4], clock-synchronization[5], distributed quantum computing[6], to mention just a few. Characterizing and optimizing quantum communication networks have a crucial relevance for the development of quantum cryptography applications[7] and hold the potential to advance our understanding of fundamental quantum phenomena[8], such as entanglement percolation[9] or the emergence of non-local quantum correlations[10–12].

The performance of quantum networks is determined by the nature of the quantum communication channels and protocols[13,14] and by the overall network topology. The optimization of quantum communication networks involves therefore the closing of security loopholes and the mitigation of the effect of losses through the development of quantum communication protocols, such as for example the measurement device independent QKD[15–17] and the twin-field QKD[18] protocols. But it is also pursued by optimizing the allocation of quantum resources for quantum sensing[19] and for distributed quantum computing[20] or by engineering optimal routing strategies[21–25], taking into account the peculiar features of the network elements and the network architecture.

In the ideal case the ultimate properties of network elements, such as the quantum communication links, are dictated by the laws of quantum mechanics, enforcing their security but also imposing intrinsic bounds[26,27] on the rate of quantum information transmission. Specifically, the fundamental limit of repeaterless quantum communication found by Pirandola, Laurenza, Ottaviani and Banchi[28], known as PLOB bound, prevents to achieve simultaneously high rates and long distances in transferring quantum states and distributing entanglement or secret quantum keys through a quantum link.

The global features of quantum communication networks are strongly dependent on the spatial distribution of the users. Recent theoretical works developed a random network approach to large-scale quantum communication networks based on optical fibers[29] or satellite links[30] and analyzed their connectivity, nodes distance and the presence of small world features[29,30].

In this work we employ the tools of classical network science to devise a strategy of optimization of quantum communication networks. PLOB bound can be indeed circumvented by means of intermediate repeaters[13], either of quantum[31] or classical nature (trusted nodes[32,33]), that help the communication between distant parties. With few notable exceptions[34], most field tests of metropolitan-scale quantum networks to date are based on point-to-point architecture and they involve trusted nodes, see refs. 35–39. Trusted nodes in general lower the security of the network[32,40,41]. Consequently, in designing a QKD network the question naturally arises on what is the optimal way to connect a given set of QKD users, to fulfill a given rate/security target, assuming that all trusted nodes have a certain probability p of being leaky. Here we address this optimization problem by introducing a quantum communication efficiency functional, that balances the quantum security and the quantum communication rate for each pair of users in the network. Note that in a classical network leakage can occur not only at nodes where the signal is amplified, but also along the connections between nodes: adding amplifiers therefore improves the capacitance

[1]Dipartimento di Fisica Università "Sapienza", P.le A. Moro, 2, I-00185 Rome, Italy. [2]Centro Ricerche Enrico Fermi, Piazza del Viminale, 1, I-00184 Rome, Italy. [3]Departamento de Física da Universidade de Aveiro & I3N, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal. [4]Istituto dei Sistemi Complessi (ISC-CNR), Via dei Taurini 19, I-00185 Rome, Italy. ✉e-mail: valentina.brosco@cnr.it

without necessarily reducing the security level. For this reason in classical networks there is no tradeoff between capacitance and security, which is instead inherent in QKD networks. We develop an algorithm that maximizes the quantum communication efficiency and constructs the optimal network, that we refer to as maximal quantum communication efficiency network. We then investigate, for a random distribution of users in the plane, the average properties of these optimal networks. Their performance is evaluated by studying the scaling of average properties as a function of the number of nodes and of the network extension. While the quantum communication rate is linked to geometrical properties, such as the average distance between users, the security depends on the topology. The optimization algorithm therefore goes beyond standard dynamic programming methods, such as the Dijkstra algorithm[42], that were previously employed in the context of quantum repeater network optimization[21].

Results

Communication efficiency of quantum networks

In its simplest realization a QKD network consists of a set of N users (nodes) that can send and receive quantum bits along a set of physical links. Here we assume that users are points located in a square of side L, as shown in Fig. 1. As physical connections we consider lossy bosonic links. In this case, following ref. 28, the QKD rate of a link, e, connecting two users located at the points $\mathbf{x}_a$ and $\mathbf{x}_b$ can be quantified by its quantum capacitance $q(e)$ fulfilling the PLOB relation

$$q(e) = -\log_2[(1 - e^{-d_{ab}/\lambda_0})]. \tag{1}$$

where $d_{ab} = |\mathbf{x}_a - \mathbf{x}_b|$ is the Euclidean distance between the users and λ_0 is a characteristic decay length. For optical fibers the attenuation in the C telecom band is of the order of 0.2 db/Km yielding $\lambda_0 \sim 22$ Km. Note that, since the link capacitance provides an estimate of the number of qubits sent per use of the channel, Eq. (1) sets to 15 km the distance at which a single qubit per use can be sent using a standard optical fiber connection. The quantum capacitance of a channel can be increased by means of repeaters. In particular, connecting the users a and b through a path featuring m trusted nodes, the capacitance of the channel[13] is given by

$$q(\{a \to b\}) = \min_{e \in \{a \to b\}} q(e). \tag{2}$$

As an example let us consider users a and b shown in Fig. 1a and let us assume that all other users can act as trusted nodes. We show two possible ways to connect a and b: a direct link or a path passing through three trusted nodes. In the first case the quantum capacitance is given by $q(e_{ab})$ while in the second case the capacitance is $q(e_{cd}) > q(e_{ab})$.

Such an increased capacitance is however associated to a potential vulnerability to attacks, since in most practical situations, an intermediate node can only be partially trusted, as discussed e.g. in ref. 41. All links are instead assumed to be unconditionally secure. To quantify this aspect we assume that every trusted node has a certain probability p of being malicious and we define the security of a path, $s(\{a \to b\})$ as the probability of finding only non-malicious trusted nodes along the path, i.e.

$$s(\{a \to b\}) \equiv (1 - p)^{\ell_{\{a \to b\}} - 1} \tag{3}$$

where $\ell_{\{a \to b\}}$ is the topological length of the path. This definition yields $s = 1$ for a path having topological length $\ell = 1$, i.e., no intermediate trusted nodes. Furthermore, it correctly gives $s = 0$ when $p = 1$ and $s = 1$ for $p = 0$.

Within the model defined by Eqs. (2) and (3), capacitance and security in general compete, i.e., longer paths may have larger capacitance but at the price of lower security. To describe this trade-off we define the communication efficiency $\epsilon_\alpha(\{a \to b\})$ of a path

$$\epsilon_\alpha(\{a \to b\}) = (1 - \alpha) q(\{a \to b\}) + \alpha \log s(\{a \to b\}) \tag{4}$$

where $\alpha \in [0, 1]$ is a user-tunable control parameter which gives more importance either to capacitance ($\alpha = 0$) or to security ($\alpha = 1$). For simplicity the communication efficiency is defined using the logarithm of the security that is proportional to the path length.

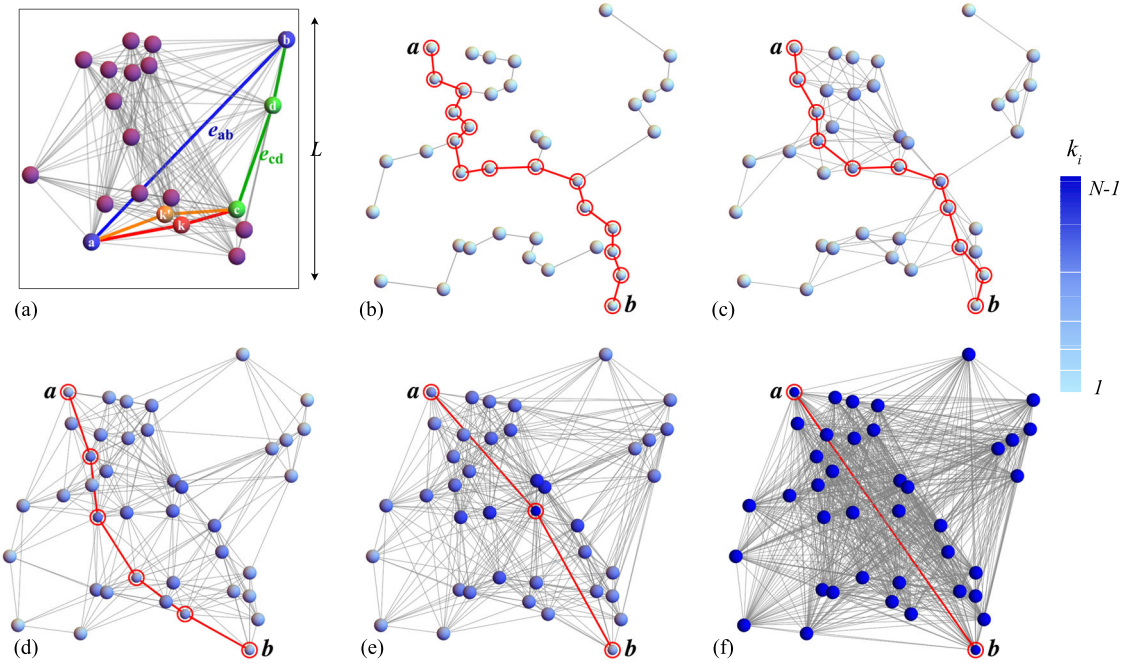


Fig. 1 | The optimal path between two nodes. a Distribution of $N = 20$ points in a square of size L representing the users of a QKD network. The colored lines represent possible paths between users a and b. **b** Maximum spanning tree for $N = 40$ nodes. Here and in the following panels the red edges represent the optimal path between user a and user b. Nodes are colored according to their degree. **c–f** Maximal Quantum Communication Efficiency networks $\mathcal{G}^*_\alpha$, obtained using our optimization algorithm, for $N = 40$, $L = \lambda_0$ and $\alpha = 0, 0.2, 0.3, 1$.

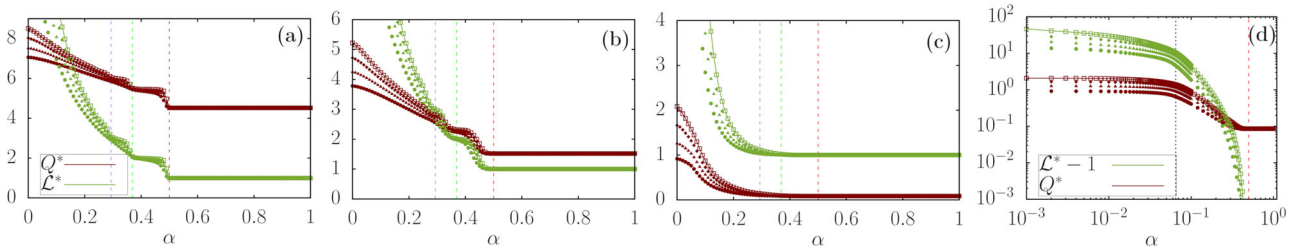


Fig. 2 | Average properties of optimal networks. Average capacitance and path length, Q^* and $\mathcal{L}^*$, of the MQCE networks as a function of α for $p = 1 - 1/e \simeq 0.63$. $N = 256$ (circles), $N = 512$ (triangles), $N = 1024$ (diamonds), $N = 2048$ (squares). **a** $L/\lambda_0 = 0.1$, **b** $L/\lambda_0 = 1$, **c** $L/\lambda_0 = 3$, **d** $L/\lambda_0 = 10$. Averages over 100 realizations for $N = 256$ and $N = 512$, and over 10 realizations for $N = 1024$ and $N = 2048$. Dashed lines correspond to the values of $\alpha_c^{0\to1}$ (red), $\alpha_c^{1\to2}$ (green) and $\alpha_c^{2\to3}$ (purple) evaluated using Eq. (12).

Given the positions of users in space and assuming that a direct link can be placed between any two of them, so that the network of all possible links $\mathcal{G}_0$ is a fully connected (FC) graph, there is an exponentially large number of possible paths between two nodes, a and b. For a given α, an optimal path $\{a\to b\}^*$ is defined as a path having maximal communication efficiency among all possible paths

$$\{a \to b\}^* = \arg\max\{\epsilon_\alpha(\{a \to b\})\}. \tag{5}$$

Clearly, in the limit $\alpha \to 0$, the optimal path maximizes the capacitance, by going through many, physically close, intermediate nodes. In the limit $\alpha \to 1$ the optimal path maximizes security and is thus the direct link between the two nodes. The global communication efficiency of a network $\mathcal{G}$ is defined as the average, over all node pairs, of the communication efficiency of the optimal paths defined over the network

$$E_\alpha[\mathcal{G}] = \frac{1}{N(N-1)} \sum_{a,b} \epsilon_\alpha(\{a \to b\}^*). \tag{6}$$

It is important to remark that in general there can be more than a single optimal path between two nodes. As an example in Fig. 1a we show two optimal paths between the nodes a and b passing through the node k and k', respectively. The two paths have the same communication efficiency since they have the same topological length, $\ell = 4$, and the same capacitance $Q = q(e_{cd})$, being e_{cd} the longest edge in both paths.

Network optimization

Given a set of N users, $\mathcal{N}$, distributed in a square of size L, and a tradeoff parameter α, our goal is to find a network connecting the N users having maximal communication efficiency and minimal number of links. To reach this goal we start by determining an optimal path for each pair of users. This is achieved by means of an algorithm described in detail in the Methods section. Once an optimal path is identified for each pair, we define the optimal network, $\mathcal{G}_\alpha^* \equiv (\mathcal{N}, \mathcal{E}_\alpha^*)$, as the graph union of the optimal paths, that is the network with node set $\mathcal{N}$ and edge set $\mathcal{E}_\alpha^*$ given by

$$\mathcal{E}_\alpha^* = \bigcup_{ab} \{a \to b\}^*. \tag{7}$$

This network has the maximum quantum communication efficiency, i.e. no other network $\mathcal{G}' \equiv (\mathcal{N}, \mathcal{E}')$ can have larger communication efficiency, i.e.,

$$E[\mathcal{G}'] \le E[\mathcal{G}_\alpha^*] \tag{8}$$

under the assumption of single-path[13,41] routing. For $\alpha = 0$ optimal networks maximize the capacitance. In this case, an efficient optimization algorithm was proposed by Pollack[43]. As discussed in ref. 44, beside maximizing network capacitance, Pollack's algorithm minimizes the number of links yielding as optimal network the maximum spanning tree (MST) connecting the N users (Fig. 1b).

The method developed in this work builds on Pollack's algorithm to construct the optimal network $\mathcal{G}_\alpha^*$ as prescribed by Eq. (7). Figure 1c–f shows instances of $\mathcal{G}_\alpha^*$ for different values of α. As one can see, it interpolates between the fully connected network, realized for $\alpha = 1$, and a much sparser network for $\alpha \to 0$. We note that for $\alpha \to 0$, $\mathcal{G}_\alpha^*$ does not necessarily reduce to the MST. This is related to the fact that, as we explained above, the optimal paths are non-unique. In principle, for generic α one could complement our algorithm with further optimization techniques to reduce the number of links of $\mathcal{G}_\alpha^*$ while preserving maximum communication efficiency. This further development is deferred to future work.

Maximal quantum communication efficiency networks

For concreteness, in this subsection we assume a completely random distribution of users in the square of size L. As highlighted above, optimal networks maximize the quantum communication efficiency functional defined by Eq. (6). Their structure and performance depend sensitively on the user-defined parameter α and on the distance-loss ratio, L/λ_0, that set the optimization regime. To show how these maximal quantum communication efficiency (MQCE) networks change across the different regimes, in Fig. 2 we plot their average capacitance,

$$Q^* = \frac{1}{N(N-1)} \sum_{ab} q(\{a \to b\}^*), \tag{9}$$

and average topological length,

$$\mathcal{L}^* = \frac{1}{N(N-1)} \sum_{ab} \ell_{\{a\to b\}^*} \tag{10}$$

as a function of α for different values of L/λ_0 ranging from the case of weak losses ($L/\lambda_0 = 0.1$) to the case of strong losses ($L/\lambda_0 = 10$).

Let us consider first the case of weak losses, $L/\lambda_0 \ll 1$, where the distance between any pair of users is, by construction, much smaller than the decay length λ_0; in this case we distinguish three regimes.

(i) For values of α larger than a threshold value α_c we observe $\mathcal{L}^* = 1$, corresponding to all optimal paths having $\ell_{\{a\to b\}^*} = 1$. In this regime $\mathcal{G}_\alpha^*$ coincides with the fully connected network. Moreover, since the structure of $\mathcal{G}_\alpha^*$ does not change with α, the average capacitance is constant, $Q^* = Q_{\rm FC}$ (see Methods for its evaluation). The critical value α_c is the lowest value of α such that, for every pair of users a, b in the system, it is more efficient to connect them through the direct link rather than using a trusted node c. This happens as long as the gain in communication efficiency due to increased capacitance, is smaller than the loss of communication efficiency associated to the introduction of an intermediate node, equal to $\alpha \log(1-p)$, yielding (see Methods for details)

$$\alpha_c = [1 - \log(1-p)]^{-1}. \tag{11}$$

(ii) On the left of this threshold value we observe the existence of a "step", i.e., an interval of α values over which $\mathcal{L}^*$ is practically constant and equal to 2. In this interval all optimal paths have 1 intermediate node. As α decreases other steps appear, corresponding to MQCE networks featuring all optimal paths having topological length $\mathcal{L}^* = 3$ (second step) and $\mathcal{L}^* = 4$ (third step).

The steps become sharper in the large N limit where a simple calculation (see Methods) shows that paths having m intermediate nodes become more efficient than those with $m-1$ intermediate ones for

$$\alpha_c^{m-1\to m} = [1-\Delta(m)\log(1-p)]^{-1}, \tag{12}$$

where

$$\Delta(m) = \frac{\log(2)}{\log(m+1)-\log(m)}. \tag{13}$$

Note that $\alpha_c^{0\to 1}$ coincides with the α_c defined above. The predictions $\alpha_c^{0\to 1}=0.5$, $\alpha_c^{1\to 2}\approx 0.369$ and $\alpha_c^{2\to 3}\approx 0.293$ are in very good agreement with the positions of the steps for $p=1-1/e$, appearing in Fig. 2a.

(iii) As α tends to 0, MQCE networks increasingly resemble the maximum spanning tree. In this limit the average topological length of optimal paths tends to increase as a power-law with N (see Methods).

Let us now consider the opposite case of strong losses, $L \gg \lambda_0$. In this limit the phenomenology is different and more difficult to interpret because, while most distances are much larger than λ_0, still some pairs of users are at a distance smaller than the decay length. These pairs are responsible for the observation that $\mathcal{L}^* > 1$ as soon as α gets smaller than the threshold value still given by Eq. (11) (see Fig. 2c, d). At variance with the previous case, for $\alpha < \alpha_c$ the average topological length of the optimal paths $\mathcal{L}^*$ grows rapidly as α is reduced, showing no steps at integer values. Moreover, there exist a value $\overline{\alpha}$ such that for $\alpha < \overline{\alpha}$, $\mathcal{L}^*$ and Q^* vary much less and assume values close to those of the MST network (see Methods).

A partially quantitative understanding of the nature of the different regimes can be achieved by considering how the properties of the optimal path linking a generic pair of users, a and b, change, as a function of their distance d_{ab} and of α, in the limit $N\to\infty$. In Fig. 3a we highlight with different colors the regions corresponding to different topological lengths of the optimal path between a and b. Boundaries shown in Fig. 3a are calculated analytically (see Methods). For large values of α security dominates and the optimal path is, for any d_{ab}/λ_0, the direct connection. When α is reduced the optimal path has a different behavior depending on the ratio d_{ab}/λ_0. For small d_{ab}/λ_0, when α is reduced it becomes more efficient to go through indirect paths going through $m=1, 2, 3, \ldots$, intermediate trusted nodes and so on, which are equally spaced along the line connecting a and b. For larger d_{ab}/λ_0, the gain in capacitance provided by a single intermediate trusted node is not sufficient to compensate the loss in security and, as α is reduced, the first transition occurs between the direct link and a path going through $\overline{m}>1$ trusted nodes. This first transition is followed, as in the previous case, by a one by one increase in the number of intermediate nodes as smaller α values are considered. For $d_{ab}/\lambda_0 \gg 1$, $\overline{m}$ grows linearly with d_{ab} and the position of the first transition scales as $1/d_{ab}$.

The phenomenology for the whole network shown in Fig. 2 results from the superposition of the behavior just depicted for all user pairs whose distances are distributed according to Eq. (18) (see Methods). Specifically, if $L \ll \lambda_0$ all pairs belong to the small distances regime of Fig. 3a. As a consequence they all undergo the same transitions for the same values of α, thus generating the steps observed in Fig. 2a. For $L \gg \lambda_0$ instead, most pairs are at distances larger than the decay length, but a few are still at distances much smaller than λ_0. Therefore, depending on the exact value of d_{ab}/λ_0, each user pair undergoes different transitions for different values of α. All these transitions get "mixed", thus explaining the lack of steps in this case and a smooth growth of the observables between α_c and $\overline{\alpha}$ (see Fig. 2d).

By balancing security and quantum capacitance, MQCE networks yield the optimal strategy to connect N users for quantum communications and, at the same time, they represent a customizable benchmarking tool for quantum communication networks. To illustrate the performance of MQCE networks we start by comparing their quantum capacitance to that of FC networks. As one can see in Fig. 3b, the outcome depends sensitively on the ratio L/λ_0. For $L/\lambda_0 \ll 1$ a limited increase of the average capacitance with respect to the FC network is observed. For values of L of the order of λ_0 the improved performance of the MQCE network becomes more significant. In this range of L/λ_0 values, the most important improvement concerns the minimum capacitance. While for FC networks some links have a strongly degraded capacitance, several orders of magnitude smaller than the average Q^*, in the optimized network min Q is only slightly smaller than the average, thus guaranteeing that communication is possible among any pairs of users. For very large values of L/λ_0 the MQCE network tends to coincide with the FC one, as the weight of capacitance in the quantum communication efficiency functional becomes extremely small. In this regime the average capacitance Q^* is essentially the same in the two networks and decays as $(L/\lambda_0)^{-2}$. In Fig. 3b we also note that in MQCE networks the minimum capacity reaches the threshold of one target bit per use of the channel, $Q_{\min}=1$, for values of L/λ_0 about one order of magnitude larger than in standard FC networks. For fixed values of λ_0, this implies that MQCE networks can provide the minimum quantum communication rate standard across much wider regions of space. Specifically, for the parameters in Fig. 3b, the maximum value of L to have at least 1 target bit transferred between any user of the network goes from $\approx 0.5\lambda_0$ (in the FC network) to $\approx 5\lambda_0$ in the MQCE network. A natural question arises concerning how the the security requirement affects the maximal achievable rate. To clarify this point in Fig. 3c we plot the average capacitance of MQCE networks, Q^* as a function of the average topological length $\mathcal{L}^*$, for different values of the ratio L/λ_0. It turns out that it is sufficient to allow $\mathcal{L}^*$ to grow from 1 (FC network) to 3 or 4 to ensure a considerable increase in the average capacitance, even one order of magnitude for large L/λ_0.

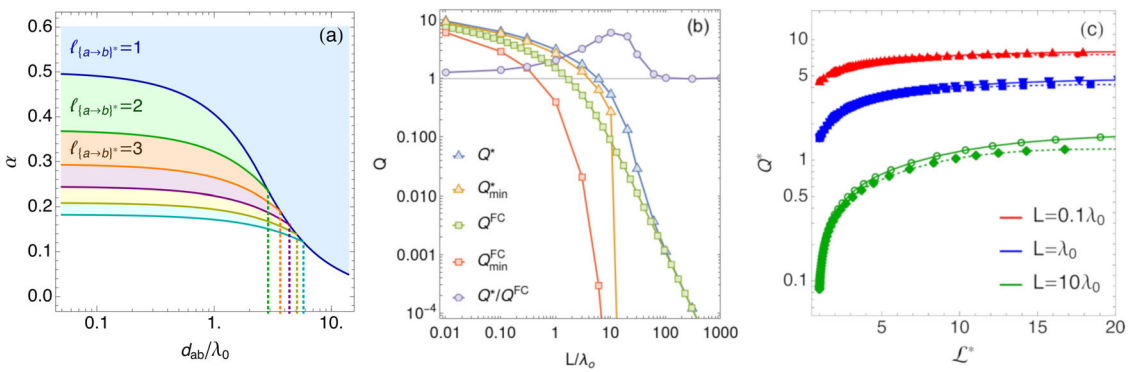


Fig. 3 | The phase diagram and the behavior of the average capacitance. **a** Transitions between the different regimes for $p=1-1/e$ and $N\to\infty$, representing the number of intermediate nodes in the optimal path for a pair of nodes at distance d_{ab} as a function of d_{ab} and α. Note that the curve separating the "direct link region" from the other regions has slope discontinuities corresponding to the dashed vertical lines. **b** Behavior of the average capacitance Q^*, and of the minimum capacitance $Q_{\min}$ as a function of L/λ_0 with $\alpha=0.1$, $p=0.1$, $N=100$ for the MQCE network, the FC network (computed analytically, see Methods). **c** Plot of the average capacitance of the MQCE network as a function of the average topological length for $p=1-1/e$, $N=512$ (dotted lines), $N=1024$ (solid lines) and various values of L/λ_0.

It is interesting also to analyze the structural features of the networks that the optimization algorithm generates. In Fig. 4 we report the dependence on α of the link density of the optimized network, $\rho = \langle k \rangle/(N-1)$, which is correlated with the cost to build the infrastructure. In all cases the density interpolates between a maximally dense network, the FC, (for $\alpha > \alpha_c$) and a much sparser network (for $\alpha \to 0$). As mentioned above, our algorithm does not exactly reproduce, in the limit $\alpha \to 0$, the MST (which has density $2/N$). The scaling of ρ vs N, which exhibits a decay $N^{-\omega}$, with an effective exponent to $\omega \approx 0.83$ implies that the optimized network has an average degree growing sublinearly with N. For large values of α the densities tend to converge to a finite limit, indicating that the networks are dense. For small but finite α values the initial decay with N appears analogous to the $\alpha = 0$ case, there is some evidence that for any $\alpha > 0$ the density tends to a constant.

Additional information on the optimized network is provided by Fig. 5, where the average length of optimal paths $\mathcal{L}^*$ is plotted as a function of the number of users. For small values of L/λ_0 and relatively large values of $\alpha < \alpha_c$ it is clear that $\mathcal{L}^*$ goes to a constant in the large-N limit (see Fig. 5a). This mirrors the presence of steps in Fig. 2. For smaller values of α and larger values of L/λ_0 the average optimal path length exhibits an initial power-law growth with N followed by a smooth crossover to a constant value.

The optimal network can be also characterized by measuring a quantity analogous to the betweenness usually considered in network analysis. The betweenness[45] of a node is the number of shortest paths among all pairs of nodes in the network that go through that node. For our purposes it is useful to define a modified betweenness where, instead of topological shortest paths, optimal paths are considered. Such a quantity provides a measure of the relevance of users, i.e., how crucial is their presence (and how damaging their removal). Nodes with high betweenness have, just because of their position in the topology, a high impact on the security of the network. In Fig. 6 we plot the histogram of the number of nodes having a given modified betweenness for various α. For $\alpha > \alpha_c$ the optimal network is fully connected and the values of the betweenness are all zero. When α becomes smaller than α_c a homogeneous distribution appears. As α is progressively reduced the distribution gets more heterogeneous, becoming extremely broad for $\alpha \to 0$. In such a case some nodes are particularly crucial and the network is overall highly vulnerable to external attacks.

Discussion

The realization of large-scale quantum communication networks is a task of crucial relevance for quantum cryptography and quantum computing applications. Existing quantum network implementations employ intermediate trusted nodes as a practical and efficient means to connect remote users, thereby overcoming the limitations imposed by rate/distance bounds. Relying on trusted nodes, however, carries the inherent risk associated with the probability of encountering malicious nodes. Given these constraints, in this work we addressed the problem of designing optimal quantum communication networks connecting a set of users randomly distributed in a square of size L. For each pair of users, we determined the optimal path connecting them by maximizing the quantum communication efficiency of the path and we constructed the optimal network, called maximal quantum communication efficiency network as the graph union of the optimal paths. MQCE networks therefore provide the optimal balance between security and quantum communication rate and they interpolate between Maximum Spanning Trees and Fully Connected networks, representing, respectively, the topologies having maximum quantum capacitance and maximum security. We carefully analyzed the performance of the MQCE networks showing that the optimization can largely increase the average capacitance while keeping high levels of security. We also analyzed structural properties of MQCE networks by means of numerical and analytical methods, showing how the tradeoff between capacitance and security affects their topological properties. Our work proposes a systematic and scalable approach for quantum communication network optimization that relies on the

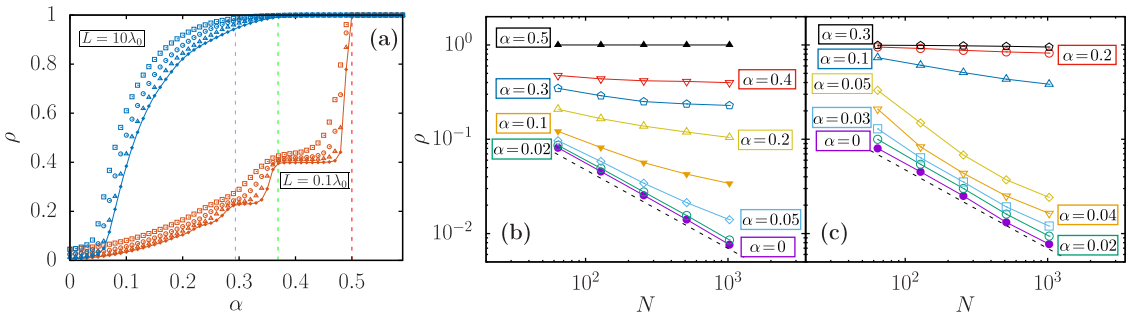
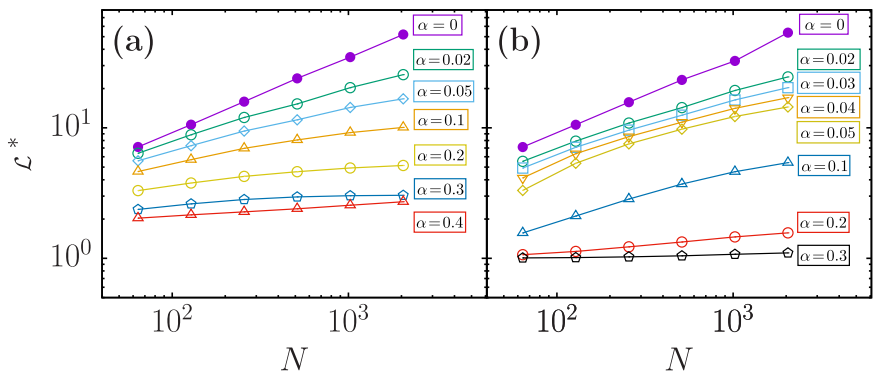


Fig. 4 | The link density of the optimal networks. a Density ρ as a function of α, for $p = 1 - 1/e$ and two values of L/λ_0 Averages over 100 realizations for $N = 128$(squares), $N = 256$(circles), and over 10 realizations for $N = 512$(triangles), $N = 1024$(diamonds). Dashed lines correspond to the values of $\alpha_c^{0\to1}$ (red), $\alpha_c^{1\to2}$ (green) and $\alpha_c^{2\to3}$ (purple) evaluated using Eq. (12). **b** Dependence of the density on N for $L/\lambda_0 = 0.1$. The dashed line shows the scaling $1/N$. **c** Dependence of the density on N for $L/\lambda_0 = 10$.

Fig. 5 | Size dependence of the average length of optimal paths. Plot of $\mathcal{L}^*$ vs N for several values of α, $p = 1 - 1/e$, **a** $L/\lambda_0 = 0.1$, **b** $L/\lambda_0 = 10$.



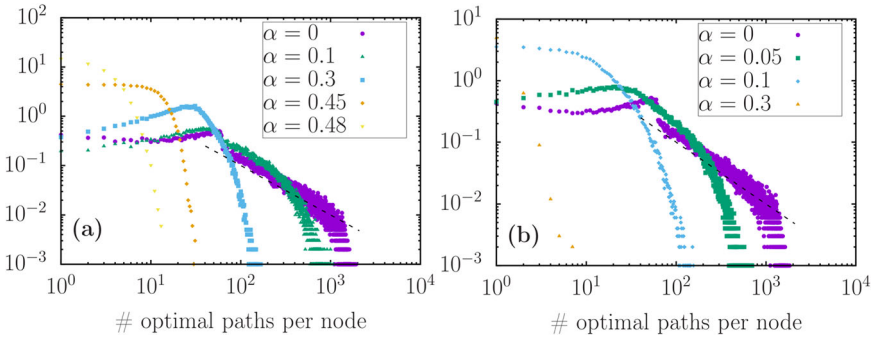


Fig. 6 | The impact of individual nodes on security is heterogeneous. Distribution of the number of nodes having a given modified betweenness for $N = 64$, $p = 1 - 1/e$, $L/\lambda_0 = 0.1$ (**a**), $L/\lambda_0 = 10$ (**b**), and several values of α.

construction of a network model and the corresponding quantum communication efficiency functional. So far we considered simple networks featuring only trusted nodes and lossy bosonic links but our work lays the basis for the study of general quantum communication networks.

We expect the performance of MQCE networks to be significantly affected by the spatial distribution of points; for simplicity we assumed a uniform distribution but it would be interesting to consider other possibilities. A further crucial assumption underpinning our work is that of single-path routing; more powerful routing strategies, where systems are transmitted in parallel through different quantum communication channels have been proposed to improve the capacitance[13,46] or the security[41]. In these situations, an extension of our algorithm may provide a way to combine the two approaches to fullfill simultaneously well-defined capacitance and security requirements. The degeneracy of the optimal path could then acquire further practical relevance. Eventually, our method could be extended to different quantum key distribution schemes such as entanglement-based quantum key distribution[47–49]. In conclusion, we stress that our freely available code (https://github.com/lorenzocirigliano/quantum-networks-optimization) can be straightforwardly used to design optimal quantum communication networks for given location of users.

Methods

Optimization algorithm

The task of constructing MQCE networks cannot be addressed using dynamic programming methods such as Dijkstra's[42], Prim's[50] or Pollack's[43] algorithms. Specifically, because of the inherently nonlocal nature of the problem arising from the interplay of topological and geometric terms in the communication efficiency functional, if the optimal path between a and b goes through node c nothing guarantees that the subpath between a and c, belonging to $\{a \to b\}^*$, yields also the optimal path between a and c. Consequently, we have to resort to alternative approaches to tackle this problem. In ref. 43 Pollack presents, among others, a matrix-based algorithm for solving the maximum capacity route problem, which is equivalent for us to finding the maximum capacitance between any pair of users. Starting from a matrix whose element $Q_{jk}^{(0)}$ is the capacitance of the link between node j and k given by Eq. (1) and $Q_{jj}^{(0)} = \infty$, an iterative procedure is defined. The elements of $Q^{(m)}$ at step m are defined by

$$Q_{jk}^{(m)} = \max_{\ell}\left[\min\left(Q_{j\ell}^{(0)}, Q_{\ell k}^{(m-1)}\right)\right] \tag{14}$$

where $\ell = 1, \ldots, N$. In this way the element $Q_{jk}^{(m)}$ is the maximum capacitance of paths between j and k going through at most m intermediate nodes. Iterating, the process, convergence is reached at most when $m + 1 = N - 1$. Individual elements of $Q^{(m)}$ provide at convergence the maximum capacitance between all node pairs. We modify Pollack's original algorithm as follows. Given α, at each iteration m we evaluate the quantity

$$\epsilon_{jk} = (1-\alpha)Q_{jk}^{(m)} + \alpha m \log(1-p). \tag{15}$$

This is the maximal communication efficiency of paths between j and k of length at most $m + 1$. As m is increased, the first term in Eq. (15) grows and tends to a constant, while the second is negative and is linear in m. Hence, for each pair (j, k), ϵ_{jk} reaches a maximum as a function of m for a value m_{jk}^*. Note that m^* needs not to be the same for all pairs. The communication efficiency of the optimal path between j and k is thus

$$\epsilon(\{j \to k\}^*) = (1-\alpha)Q_{jk}^{(m_{jk}^*)} + \alpha \log(1-p) m_{jk}^*. \tag{16}$$

This procedure gives the communication efficiency of the optimal paths between any two users. In order to construct one of these (in principle many) paths we proceed as follows. The capacitance $Q_{jk}^{(m_{jk}^*)}$ associated to the optimal path between j and k necessarily appears in the initial matrix $Q^{(0)}$, as element $Q_{ln}^{(0)}$. All entries of Q are assumed to be different. This indicates that the optimal path between j and k necessarily goes through the link between l and n, which, indeed, determines the capacitance of the optimal path. Starting from the matrix $Q^{(0)}$ we construct the unweighted graph A containing an edge between all node pairs such that the corresponding element in $Q^{(0)}$ is larger than $Q_{ln}^{(0)}$. In this graph A we find the optimal path as the topological shortest path going from j to k with the constraint that it goes through the link (l, n). Clearly, although the link between l and n is uniquely determined there are often many alternative shortest paths going through it; this gives rise to a large number of degenerate optimal paths.

The efficiency of the fully connected network

To calculate the efficiency of a fully connected network, which coincides with its capacitance, we need the probability distribution for the distance between any pair of points in a square of size L. This quantity coincides with the distribution of distances between two points randomly distributed in the square, which is a special case of the distribution for a generic rectangular substrate derived in ref. 51. Note that the quantity N does not play any role. Considering nodes distributed in a square of side L, the distance distribution is

$$g(d) = \frac{1}{L} f\left(\frac{d}{L}\right) \tag{17}$$

where

$$f(z) = 2z \begin{cases} \pi - 4z + z^2 & 0 \le z \le 1 \\ 4\arcsin\left(1/z\right) - (2+\pi) + 4\sqrt{z^2-1} - z^2 & 1 \le z \le \sqrt{2}. \end{cases} \tag{18}$$

Given this distribution, the value of the capacitance averaged over all node pairs is then:

$$Q_{FC} = -\frac{1}{\ln 2}\int_0^\infty dz\, f(z)\ln(1-e^{-z/\tilde{\lambda}}), \tag{19}$$

where $\tilde{\lambda} = \lambda_0/L$. In the limit $L \ll \lambda_0$ one can safely approximate $e^{-z/\tilde{\lambda}} \approx 1 - z/\tilde{\lambda}$, hence

$$Q_{FC} = -\frac{\langle \ln(z/\tilde{\lambda})\rangle}{\ln 2}. \tag{20}$$

In the limit $L \gg \lambda_0$ instead, taking

$$\ln(1-e^{-d/\lambda_0}) \approx -e^{-z/\tilde{\lambda}}, \tag{21}$$

we can write

$$Q_{FC} \approx \frac{1}{\ln 2}\int_0^\infty dz f(z) e^{-z/\tilde{\lambda}}. \tag{22}$$

Since for small z we have $f(z) \approx 2\pi z$, then

$$Q_{FC} \approx \frac{2\pi}{\ln 2}\left(\frac{\lambda_0}{L}\right)^2. \tag{23}$$

In this regime, the value of Q_{FC} is determined by the contribution of the few links shorter than λ_0, which have a large capacitance.

Optimization regimes for a single pair

We consider $N \to \infty$. In this limit we can always assume that for any pair of users at distance d_{ab}, there are m ($\forall m$) equally spaced intermediate users along the line joining a and b, so that the distance between nearest neighboring nodes is $d_{ab}/(m+1)$. The efficiency of the path going through m intermediate nodes (including the direct link, which is the case $m = 0$) is therefore:

$$E(m) = -(1-\alpha)\log_2(1-e^{-d_{ab}/[(m+1)\lambda_0]}) + \alpha \log(1-p)m. \tag{24}$$

For sufficiently large α it is more efficient to use the direct link, $m = 0$. As α is reduced it becomes more efficient to use indirect paths, with $m > 0$.

For $d_{ab} < \lambda_0$, if one plots $E(m)$ vs α for $m = 0, 1, 2, 3, \ldots$ one observes that the intersections of the lines for $m > 0$ with the line for the direct link ($m = 0$) occur for decreasing α as m is increased. As a consequence, starting from $\alpha = 1$, at a given $\alpha_c^{0\to 1} \equiv \alpha_c$ it becomes more efficient to follow the path of length 2 (i.e., with $m = 1$ intermediate nodes) rather than the direct link (with $m = 0$). Analogously, for a smaller $\alpha_c^{1\to 2}$ the path of length 3 becomes more efficient than the path of length 2 and so on. Hence we observe a series of transitions, where it becomes more efficient to use paths with m intermediate nodes with respect to paths with $m-1$ nodes, with increasing $m = 1, 2, 3, \ldots$ The location $\alpha_c^{m-1\to m}$ of the m-th transition is given by the condition

$$E(m) = E(m-1), \tag{25}$$

which, in the limit $d_{ab} \to 0$, yields Eq. (12). These transitions are indicated by the solid lines in Fig. 3a. For $d_{ab} \gg \lambda_0$ instead, the intersection of $E(m)$ with $E(0)$ (efficiency of the direct link) occurs at a value of α that grows initially with m, up to a value $\overline{m}$. After this value the position of the intersection decreases with m. This means that, instead of having a transition from the direct link to a path with one trusted node, for $\alpha = \alpha^{0\to\overline{m}}$ there is a transition from the direct link to a path going through $\overline{m} > 1$ intermediate nodes. This first transition is followed by other transitions of the same kind as before, in which the number of intermediate nodes is increased by 1, $\alpha_c^{m-1\to m}$ for $m > \overline{m} + 1$. The value of $\overline{m}$ is found by determining $\alpha_c^{0\to m}$ using the condition

$$E(m) = E(0), \tag{26}$$

and checking, for a given d_{ab}/λ_0, which of the $\alpha_c^{0\to m}$ is the largest. In the limit of large d_{ab}/λ_0, $\overline{m}$ gets large as well; in other words, starting from $\alpha = 1$ one jumps from the direct link to a path of larger and larger topological length, but this happens for smaller and smaller values of $\alpha_c^{0\to\overline{m}}$, vanishing as $1/d_{ab}$. Figure 3a represents the scenario just described.

Optimization regimes for the whole network

The previous discussion (and Fig. 3a) consider a single pair, with given distance d_{ab}, and is exact in the limit $N \to \infty$. The phenomenology of the whole system of size L is the superposition of what happens for each pair in the system where distances, spanning the range $0 < d_{ab} < \sqrt{2}L$ are distributed according to Eq. (18). For $L/\lambda_0 \to 0$ all distances d_{ab} are necessarily much smaller than λ_0. In the expression for $E(m)$ one can expand the exponential to first order and the values $\alpha_c^{m-1\to m}$ obtained by solving the equation $E(m) = E(m-1)$ do not depend on d_{ab}. Hence the transitions for all pairs occur exactly for the same values of α, given by Eq. (12). Thus the average optimal path length $\mathcal{L}$ exhibits, as a function of α, steps which are, in the limit $L/\lambda_0 \to 0$, perfectly sharp (Fig. 2a).

For generic L/λ_0, distances d_{ab} are distributed over the range between 0 and $\sqrt{2}L$. For the smallest of them the scenario just depicted applies and transitions occur for the values written in Eq. (12). But for any finite $L \ll \lambda_0$ there are corrections to the values of Eq. (12), shown by the decreasing behavior of the curves in Fig. 3a). This explains why, for $0 < L \ll \lambda_0$, steps are not perfectly sharp but broadened (even for $N \to \infty$): the transitions from $m-1 \to m$ intermediate nodes occur, for the various pairs, at slightly different values of α. As m grows the transitions are closer (see the denser lines in Fig. 3a); the broadening becomes stronger so that steps of high order m cannot be clearly identified.

For L/λ_0 not infinitesimally small but still smaller than 1, an estimate of the average position of the steps is obtained by using the condition (25), after setting $d_{ab} = \langle d_{ab}\rangle \approx 0.52L$[51]. The values obtained, which are a decreasing function of L, explain why the positions of the observable steps in Fig. 2b, c, which for $L/\lambda_0 \to 0$ are given by Eq. (12), decrease as L grows. At the same time the increase of L leads to an increased "mixing" of the transitions. As a consequence, the steps get less sharp and the concept of step progressively loses meaning.

For large L/λ_0, the connection between the regimes for a single pair and the overall behavior of the system is more involved. Indeed, if $L/\lambda_0 \gg 1$ despite the fact that for the overwhelming majority of pairs $d_{ab}/\lambda_0 \gg 1$ there are always some pairs of users whose distance is $d_{ab} \ll \lambda_0$. For them, the optimal path involves a number m of intermediate nodes growing one at a time for the values of α given by Eq. (12). This explains why, for any L, one observes $\mathcal{L} > 0$ as soon as $\alpha < \alpha_c = [1 - \log(1-p)]^{-1}$ (see Fig. 2d). However, for $L \gg \lambda_0$ the overwhelming majority of distances are much larger than λ_0 and the length of the optimal path is described by the right part of Fig. 3a. For a given $\alpha < \alpha_c$ the optimal path for these pairs involves m intermediate nodes, with m assuming a range of values depending on the precise value of d_{ab}/λ_0. For this reason the average length of optimal paths $\mathcal{L}$ does not assume integer values but instead it changes continuously with α, thus explaining the lack of steps in this case. This "mixing" involves all distances up to the largest one in the system, $d_{max} = \sqrt{2}L$, for which the transition to optimal paths longer than 1 occurs for the smallest α value. We can therefore estimate that for $\alpha < \alpha_c^{0\to\overline{m}}(d_{max})$ all pairs are connected by topologically long paths and the network is essentially a MST. This leads to the identification of the threshold $\overline{\alpha}$ observed in Fig. 2d as

$$\overline{\alpha} \approx \alpha_c^{0\to\overline{m}}(d = \sqrt{2}L) \sim 1/L. \tag{27}$$

Capacitance of the Maximum Spanning Tree

The length of the longest link (i.e. the link with lowest capacitance) in an Euclidean MST is given by[52]

$$\max d_e \simeq L\sqrt{\frac{\log N}{\pi N}}, \quad N \gg 1.$$

Assuming that the majority of the optimal paths pass through the link with minimum capacitance, we can estimate Q_{MST} as the capacitance of such a link. Hence we have

$$Q_{\mathrm{MST}} \simeq -\log_2\left[1-\exp\left(\frac{L}{\lambda_0}\sqrt{\frac{\log N}{\pi N}}\right)\right], \tag{28}$$

which is in good agreement with the results in Fig. 2 for $L \ll \lambda_0$ and is increasingly accurate as N grows also in the other cases.

Data availability

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

Code availability

The code used for this study is available in GitHub (https://github.com/lorenzocirigliano/quantum-networks-optimization). At the same link is available the code for designing the optimal network for arbitrary spatial location of users.

Received: 2 October 2023; Accepted: 12 March 2024;
Published online: 29 April 2024

References

1. Azuma, K., Bäuml, S., Coopmans, T., Elkouss, D. & Li, B. Tools for quantum network design. *AVS Quantum Sci.* **3**, 014101 (2021).
2. Bennett, C. H. & Brassard, G. Quantum cryptography:public key and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp.175–179 (IEEE, 1984).
3. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
4. Hermans, S. L. N. et al. Qubit teleportation between non-neighbouring nodes in a quantum network. *Nature* **605**, 663 (2022).
5. Kómár, P. et al. A quantum network of clocks. *Nat. Phys.* **10**, 582 (2014).
6. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet:A vision for the road ahead. *Science* **362**, 303 (2018).
7. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Optics Photonics* **12**, 1012 (2020).
8. Nokkala, J., Piilo, J. & Bianconi, G. Complex quantum networks: a topical review. Preprint at https://arxiv.org/abs/2311.16265 (2023).
9. Acín, A., Cirac, J. I. & Lewenstein, M. Entanglement percolation in quantum networks. *Nat. Phys.* **3**, 256 (2007).
10. Gisin, N. Entanglement 25 years after quantum teleportation: Testing joint measurements in quantum networks. *Entropy* **21**, 325 (2019).
11. Poderini, D. et al. Experimental violation of n-locality in a star quantum network. *Nat. Commun.* **11**, 2467 (2020).
12. Carvacho, G. et al. Quantum violation of local causality in an urban network using hybrid photonic technologies. *Optica* **9**, 572 (2022).
13. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019).
14. Coutinho, B. C., Munro, W. J., Nemoto, K. & Omar, Y. Robustness of noisy quantum networks. *Commun. Phys.* **5**, 105 (2022).
15. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
16. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **9**, 397 (2015).
17. Erkilic, Ö. et al. Surpassing the repeaterless bound with a photon-number encoded measurement-device-independent quantum key distribution protocol. *npj Quantum Inf.* **9**, 29 (2023).
18. 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 (2018).
19. Krisnanda, T., Paterek, T., Paternostro, M. & Liew, T. C. Quantum neuromorphic approach to efficient sensing of gravity-induced entanglement. *Phys. Rev. D* **107**, 086014 (2023).
20. Meter, R. V., Nemoto, K. & Munro, W. Communication links for distributed quantum computation. *IEEE Trans. Comput.* **56**, 1643 (2007).
21. Meter, R. V., Satoh, T., Ladd, T. D., Munro, W. J. & Nemoto, K. Path selection for quantum repeater networks. *Network. Sci.* **3**, 82 (2013).
22. Harney, C. & Pirandola, S. End-to-end capacities of imperfect-repeater quantum networks. *Quantum Sci. Technol.* **7**, 045009 (2022).
23. Hahn, F., Pappa, A. & Eisert, J. Quantum network routing, and local complementation. *npj Quantum Inf.* **5**, 76 (2019).
24. Schoute, E., Mancinska, L., Islam, T., Kerenidis, I. & Wehner, S. Shortcuts to quantum network routing. Preprint at https://arxiv.org/abs/1610.05238 (2016).
25. Pant, M. et al. Routing entanglement in the quantum internet. *npj Quantum Inf.* **5**, 25 (2019).
26. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct, and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
27. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
28. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
29. Brito, S., Canabarro, A., Chaves, R. & Cavalcanti, D. Statistical properties of the quantum internet. *Phys. Rev. Lett.* **124**, 210501 (2020).
30. Brito, S., Canabarro, A., Cavalcanti, D. & Chaves, R. Satellite-based photonic quantum networks are smallworld. *PRX Quantum* **2**, 010304 (2021).
31. Azuma, K. et al. Quantum repeaters: From quantum networks to the quantum internet. *Rev. Modern Phys.* **95**, 1539–0756 (2023).
32. Salvail, L. et al. Security of trusted repeater quantum key distribution networks. *J. Comput. Secur.* **18**, 61 (2010).
33. Mehic, M. et al. Quantum key distribution. *ACM Comput. Surv.* **53**, 1 (2020).
34. Joshi, S. K. et al. A trusted node-free eight-user metropolitan quantum communication network. *Sci. Adv.* **6**, eaba0959 (2020).
35. Elliott, C. et al. Current status of the darpa quantum network. In *SPIE Proceedings* (eds. Donkor, E. J., Pirich, A. R. & Brandt, H. E.) (SPIE, ADDRESS, 2005).
36. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *N. J. Phys.* **11**, 075001 (2009).
37. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. *Optics Express* **19**, 10387 (2011).
38. Wang, S. et al. Field, and long-term demonstration of a wide area quantum key distribution network. *Optics Express* **22**, 21739 (2014).
39. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4600 kilometres. *Nature* **589**, 214 (2021).
40. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Modern Phys.* **81**, 1301 (2009).
41. Solomons, N. R. et al. Scalable authentication, and optimal flooding in a quantum network. *PRX Quantum* **3**, 020311 (2022).
42. Dijkstra, E. A note on two problems in connexion with graphs. *Numer. Math.* **1**, 269 (1959).

43. Pollack, M. Letter to the editor - the maximum capacity through a network. *Oper. Res.* **8**, 733 (1960).
44. Hu, T. C. The maximum capacity route problem. *Oper. Res.* **9**, 898 (1961).
45. Newman, M. *Networks: An Introduction*. (Oxford University Press, Inc., New York, NY, USA, 2010).
46. Das, S., Bäuml, S., Winczewski, M. & Horodecki, K. Universal limitations on quantum key distribution over a network. *Phys. Rev. X* **11**, 041016 (2021).
47. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical, and einstein-podolsky-rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).
48. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
49. Zhang, W. et al. Quantum secure direct communication with quantum memory. *Phys. Rev. Lett.* **118**, 220501 (2017).
50. Prim, R. C. Shortest connection networks, and some generalizations. *Bell Syst. Tech. J.* **36**, 1389 (1957).
51. Philip, J. The probability distribution of the distance between two random points in a box, Technical Report Number TRITA MAT 07 MA 10, http://www.math.kth.se/~johanph/habc.pdf (1991).
52. Penrose, M. D. The longest edge of the random minimal spanning tree. *Ann. Appl. Probab.* **7**, 340 (1997).

Acknowledgements

This work was funded by the HEISINGBERG "Spatial Quantum Optical Annealer for Spin Hamiltonians" EU Research and Innovation Project under Grant Agreement No. 101114978. V.B. acknowledge support from Project PNRR MUR PE_0000023-NQSTI financed by the European Union Next Generation EU. V.B. and L.P. acknowledge support from PON Ricerca e Innovazione 2014-2020 FESR /FSC - Project ARS01_00734 QUANCOM, Ministero dell'Università e Ricerca and PNRR MUR project CN_00000013-ICSC financed by the European Union Next Generation EU. The funders played no role in study design, data collection, analysis and interpretation of data, or the writing of this manuscript.

Author contributions

C.Co., L.P. and V.B. conceived the initial idea. C.Ca. and L.C. expanded the concept and developed the code. L.P., V.B., C.Ca. and L.C. developed the theoretical part. L.C. carried out the numerical analysis. All the authors contributed to data analysis, figure preparation, and to manuscript writing.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Valentina Brosco.