

RESEARCH

Open Access



40-user fully connected entanglement-based quantum key distribution network without trusted node

Xu Liu^{1†}, Jingyuan Liu^{1†}, Rong Xue¹, Heqing Wang², Hao Li², Xue Feng^{1,3}, Fang Liu^{1,3}, Kaiyu Cui^{1,3}, Zhen Wang², Lixing You², Yidong Huang^{1,3,4} and Wei Zhang^{1,3,4*}

*Correspondence:
zwei@tsinghua.edu.cn

[†]Xu Liu and Jingyuan Liu contributed equally to this work.

¹ Beijing National Research Center for Information Science and Technology (BNRist), Beijing Innovation Center for Future Chips, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China

Full list of author information is available at the end of the article

Abstract

Quantum key distribution (QKD) would play an important role in future information technologies due to its theoretically proven security based on the laws of quantum mechanics. How to realize QKDs among multiple users in an effective and simple way is crucial for its real applications in communication networks. In this work, we propose and demonstrate a fully connected QKD network without trusted node for a large number of users. Using flexible wavelength division multiplexing/demultiplexing and space division multiplexing, entanglement resources generated by a broadband energy-time entangled quantum light source are distributed to 40 users. Any two users share a part of entanglement resources, by which QKD is established between them. As a result, it realizes a fully connected network with 40 users and 780 QKD links. The performance of this network architecture is also discussed theoretically, showing its potential on developing quantum communication networks with large user numbers owing to its simplicity, scalability, and high efficiency.

Keywords: Quantum entanglement distribution, Quantum key distribution, Quantum network, Quantum communication

Introduction

Quantum key distribution (QKD) has been regarded as a mature technique in security applications of quantum communication [1, 2]. Since the first QKD protocol BB84 [3] was proposed, QKD has been actively developed both in security proofing [4, 5] and in practical implementation [6, 7]. The decoy state QKD [8–10] was proposed to solve the impurity of a single-photon source and avoid photon number splitting. Subsequently, measurement-device-independent QKD [11–14] was proposed, which is robust against attacks from the measurement devices. In the last few years, twin-field QKD (TF-QKD) [15–18] has been investigated, which is based on single-photon interference and can provide high key rates over long distances to surpass the rate-distance limit of repeaterless QKD. Based on TF-QKD, the secure distance of QKD in field test was extended to 511 km through sending-or-not-sending (SNS) protocol [19].

However, an optimal method to build quantum communication networks based on QKD has yet to be developed. Quantum repeater-based networks [20–22] can be the ultimate blue print for constructing the global quantum Internet. However, quantum memory [23, 24] and entanglement swapping [25, 26] technologies still remain to be improved for practical applications. Meanwhile, trusted node networks [27–30] have been widely developed and implemented. Trusted node networks are suitable for constructing long-distance backbone core networks, however, they are inefficient for constructing multiple-user group networks. On the other hand, their security is compromised because every connected node in the network must be trusted, which is difficult to guarantee. Another type of QKD network is based on active switches [31–33], in which only some of the pairing users are connected at a time. The network efficiency is limited to some duty cycles of switches. Moreover, additional time is required to reinitialize the new communication channel when the topology is changed [34]. In addition, a type of point-to-multipoint network based on passive beam splitter and single-photon point-to-point QKD [35, 36] has been investigated, in which single photons from a central node are distributed to multiple users by a passive beam splitter. Every user must exchange keys with the central node, implying that the central node must be trusted.

The last type of QKD network is the fully connected network without trusted node. Every user can be connected directly to each other. A type of fully connected quantum network with four users based on wavelength multiplexing has been reported in a pioneering study [37]. To fully connect the four users, 12 wavelength channels are required. Namely, a minimum of $N \times (N - 1)$ wavelength channels are required to fully connect N users, which limits the scalability of the scheme. Furthermore, an improved scheme was proposed by introducing a 1×2 beam splitter [38]. The scheme supported an eight-user fully connected QKD network with 16 wavelength channels. Recently, another type of fully connected QKD network was proposed [39]. In this scheme, resources of entangled photon pairs occupied with two correlated wavelength channels were directly distributed to eight users by a passive beam splitter to construct a fully connected subnet. To expand the user scale of the network, 16 such subnets were constructed using resources with different wavelength channel pairs. However, the connections between subnets relied on a trusted central node, which is an obvious weakness on its security.

In this work, we propose a two-layer QKD network architecture without trusted node, which could support a fully connected quantum communication network with stronger scalability. We specifically realize a 40-user fully connected QKD network supported by a broadband energy-time entangled photon pair source, in which each user can simultaneously generate secure keys with every other user via a QKD link. Five subnets are constructed using space multiplexing technology based on passive beam splitters. In each subnet, the entanglement resource of photon pairs with a correlated wavelength channel pair are randomly distributed to eight users, realizing a fully connected subnet. On the other hand, 10 additional entanglement resources with different correlated wavelength channel pairs are demultiplexed. The photons in these channels are flexibly multiplexed and distributed to different subnets, establishing connections between the subnets. Hence, the 40 users in the QKD network are fully connected without the assistance of trusted nodes. To the best of our knowledge, this is the largest experimentally demonstrated fully connected QKD network supported by a single quantum light source.

Methods

Network architecture

Based on space multiplexing and wavelength multiplexing of entangled photon pairs, we propose a two-layer fully connected QKD network architecture. The signal and idler photons of the energy-time entangled state from a broadband quantum light source are distributed to all users in the network. Entanglement resources of 15 correlated wavelength channel pairs from the broadband quantum light source are required to fully connect the 40 users. An illustration of the network architecture is shown in Fig. 1. The two wavelength channels with opposite subscripts belong to a specific correlated wavelength channel pair i.e., $(\lambda_1, \lambda_{-1})$, $(\lambda_2, \lambda_{-2})$, etc. The network architecture is segmented into two layers, the intra-subnet layer and inter-subnet layer. A sketch of the intra-subnet layer is shown in Fig. 1(a). In this layer, photons with a specific pair of correlated wavelengths are distributed to N users by a passive beam splitter. The signal and idler photons of this entanglement resource are randomly distributed to any user. Hence, each user will have coincidence events with any other user, thereby forming a subnet with a fully connected topology. If the user number of this subnet is appropriate, most photon pairs will be randomly distributed to two different users, which is a simple yet efficient approach to realize a fully connected network.

A sketch of the inter-subnet layer is shown in Fig. 1(b). Two subnets are illustrated as two fully connected mesh graphs, which are supported by two independent entanglement resources with different correlated wavelength channel pairs (λ_1 / λ_{-1} and λ_2 / λ_{-2}). An additional entanglement resource with the correlated wavelength channel pair of $(\lambda_6 / \lambda_{-6})$ is introduced to connect the two subnets. The signal and idler photons with the entanglement resource of $(\lambda_6 / \lambda_{-6})$ are separated by wavelength division multiplexing components and distributed to the two corresponding subnets. The photons are randomly distributed to the users by the same passive beam splitter along with photons of wavelengths $(\lambda_1 / \lambda_{-1})$ or $(\lambda_2 / \lambda_{-2})$ in each subnet. Therefore, each user in one subnet will have coincidence events with any user in the other subnet due to entangled photon pairs with correlated wavelengths $(\lambda_6 / \lambda_{-6})$. Hence, based on this two-layer network architecture, any two users in the network have a connection of coincidence events, realizing a fully connected entanglement distribution network. In this work, we realize a large-scale entanglement distribution network with 40 users based on this architecture, as shown in Fig. 1(c). Five fully connected subnets (A, B, C, D, and E) are supported by five entanglement resources (from λ_1 / λ_{-1} to λ_5 / λ_{-5}). Ten additional entanglement resources (from λ_6 / λ_{-6} to $\lambda_{15} / \lambda_{-15}$) are introduced to realize the full connections among the five subnets. Hence, each user in the five subnets have coincidence events with any other user in the network, namely, every pair of users can share an entangled resource. Based on the shared entanglement resource, any two users in the network could establish QKD between them, realizing a fully connected QKD network without trust node. The detailed wavelength allocation of users is given in Supplementary Materials (See Supplementary Table 2). Each user in the network connects with the entanglement resource provider by one optical fiber, in which photons of six specific wavelength channels are sent to the user. Two of them are the correlated wavelength channels supporting the connections in the subnet. The other four wavelength channels are used to connect the users between different subnets.

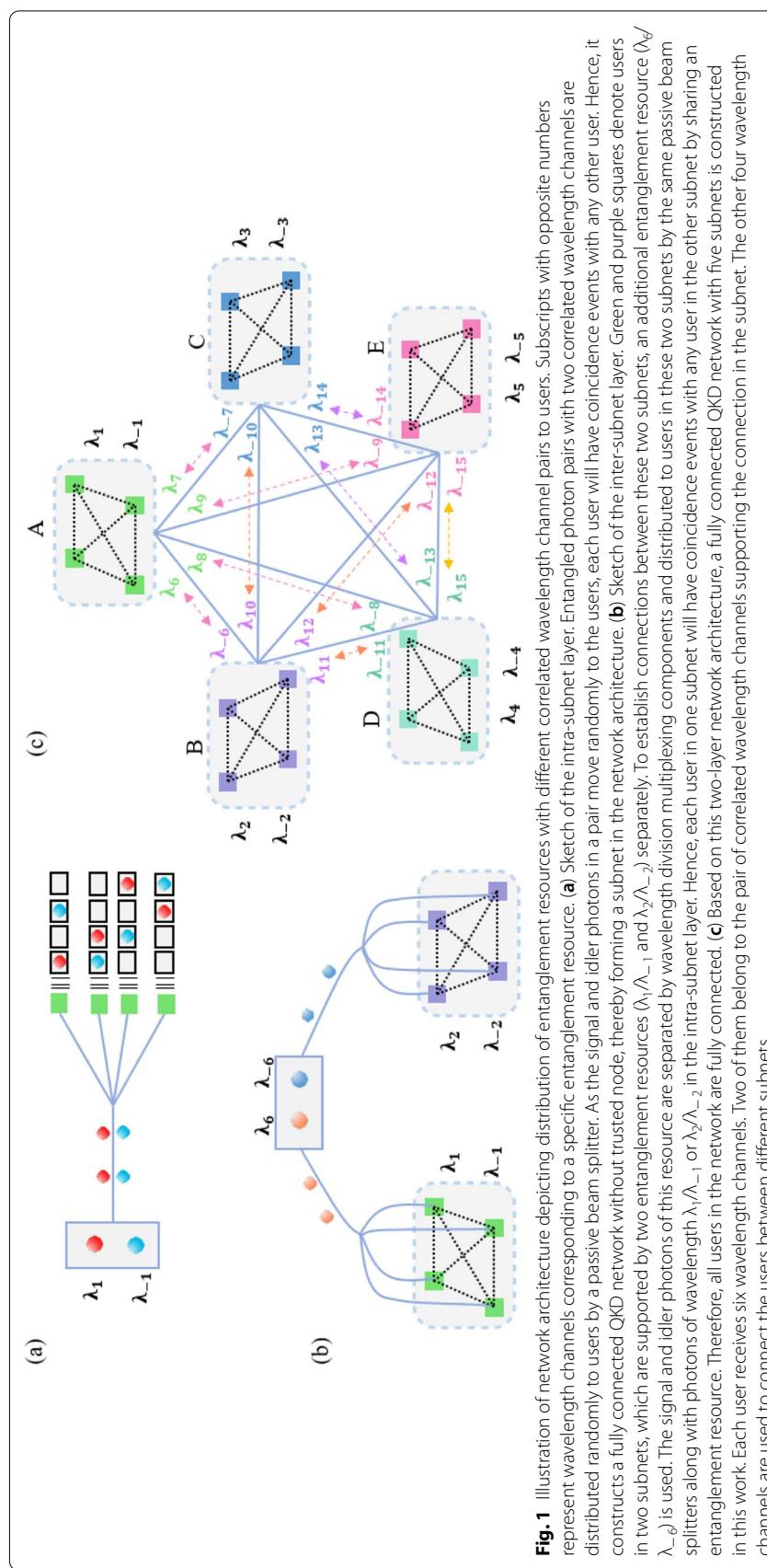


Fig. 1 Illustration of network architecture depicting distribution of entanglement resources with different correlated wavelength channel pairs to users. Subscripts with opposite numbers represent wavelength channels corresponding to a specific entanglement resource. **(a)** Sketch of the intra-subnet layer. Entangled photon pairs with two correlated wavelength channels are distributed randomly to users by a passive beam splitter. As the signal and idler photons in a pair move randomly to the users, each user will have coincidence events with any other user. Hence, it constructs a fully connected QKD network without trusted node, thereby forming a subnet in the network architecture. **(b)** Sketch of the inter-subnet layer. Green and purple squares denote users in two subnets, which are supported by two entanglement resources (λ_1/λ_{-1} and λ_2/λ_{-2}) separately. To establish connections between these two subnets, an additional entanglement resource (λ_1/λ_{-2}) is used. The signal and idler photons of this resource are separated by wavelength division multiplexing components and distributed to users in these two subnets by the same passive beam splitters along with photons of wavelength λ_1/λ_{-1} or λ_2/λ_{-2} in the intra-subnet layer. Hence, each user in one subnet will have coincidence events with any user in the other subnet by sharing an entanglement resource. Therefore, all users in the network are fully connected. **(c)** Based on this two-layer network architecture, a fully connected QKD network with five subnets is constructed in this work. Each user receives six wavelength channels. Two of them belong to the pair of correlated wavelength channels supporting the connection in the subnet. The other four wavelength channels are used to connect the users between different subnets

Results

Experimental setup

The experimental system of the 40-user fully connected QKD network without trusted node is shown in Fig. 2. In the experiments, broadband energy-time entangled photon pairs are generated by spontaneous four-wave mixing (SFWM) under continuous wave pumping in a silicon waveguide of length 3 mm. The central wavelength of the pump light is 1545.32 nm, corresponding to the International Telecommunication Union (ITU) channel of C40. Owing to the energy conservation of the SFWM process, the signal and idler photons are distributed symmetrically around the pump light wavelength. They are separated by an arrayed waveguide grating system based on their wavelengths with 100 GHz spacing (See Supplementary Fig. 4(a) in Supplementary Materials). Fifteen entanglement resources are extracted from the quantum light source, which corresponded to correlated wavelength channel pairs of C35/C45, C34/C46, ..., C21/C59, as shown in Fig. 2(b). The corresponding coincidences of entangled photon pairs with correlated wavelength channels can be seen in Supplementary Materials, Supplementary Fig. 4(b). The first five entanglement resources (represented in green) are used to support the connection of users in the five subnets. The remaining 10 entanglement resources (represented in orange) are used to connect users between the subnets. Subsequently, these wavelength channels are multiplexed by commercial dense wavelength division multiplexing components, as illustrated in Fig. 1(c), and then sent to the passive beam splitters. In each subnet, the passive beam splitter distributes the input photons to all users randomly. The quantum light source, wavelength demultiplex/multiplex components, and passive beam splitters can be treated as a provider of entanglement resources for the network. Two specific users in subnet A received the photons from the provider through optical fibers of 1 km and 2 km, separately. Other users connected to the provider by short fiber patch cords.

In each user, a normal dispersion component, an anomalous dispersion component, and two NbN superconducting nanowire single-photon detectors (SNSPDs) are equipped for performing symmetric dispersive optics QKD (DO-QKD) [39]. The symmetric DO-QKD is modified from the conventional DO-QKD scheme [40–42] to fully adapt to the entanglement distribution network based on passive beam splitters. High-dimensional encoding based on the time of recorded single-photon detection events can be used in symmetric DO-QKD to improve the utilization of coincidence events by multi-bit key generation per coincidence.

Experimental results

First, the properties of the entanglement distribution were measured to verify the feasibility of the network architecture and to evaluate the quality of coincidences between the users. For each user, the photons were directly detected by the SNSPD. The results are shown in Fig. 3. Figure 3(a) shows the typical results for two specific users in the same subnet. The five peaks show the results of coincidence counts in the five subnets (A, B, C, D, and E), which were supported by the resources of correlated wavelength channel pairs of (C35, C45), (C34, C46), (C33, C47), (C32, C48), and (C31, C49), respectively. For clarity, the coincidence peaks of the five subnets are plotted in the same figure

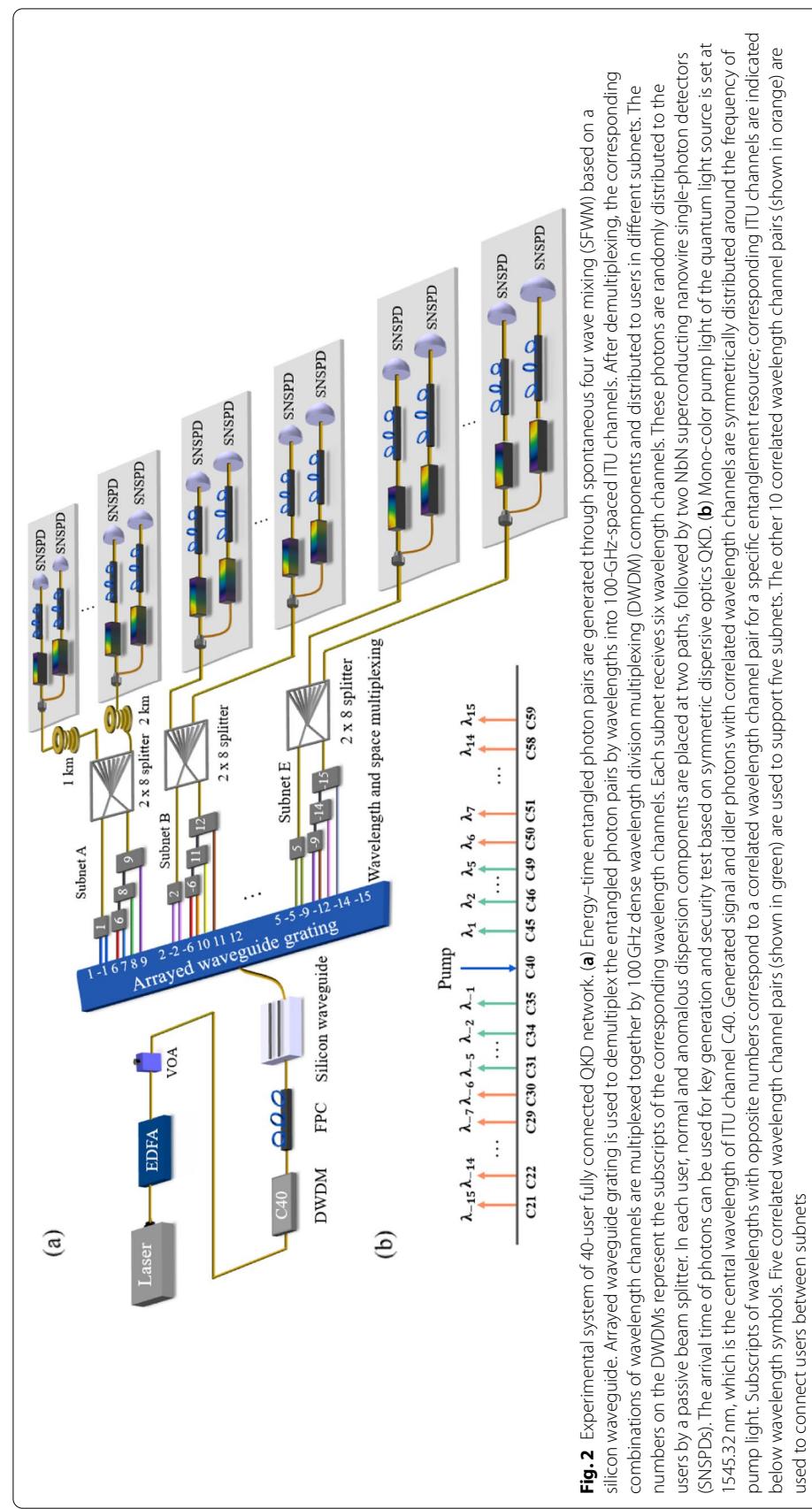


Fig. 2 Experimental system of 40-user fully connected QKD network. **(a)** Energy-time entangled photon pairs are generated through spontaneous four wave mixing (SFWM) based on a silicon waveguide. Arrayed waveguide grating is used to demultiplex the entangled photon pairs by wavelengths into 100-GHz-spaced ITU channels. After demultiplexing, the corresponding combinations of wavelength channels are multiplexed together by 100-GHz dense wavelength division multiplexing (DWDM) components and distributed to users in different subnets. The numbers on the DWDMs represent the subscripts of the corresponding wavelength channels. Each subnet receives six wavelength channels. These photons are randomly distributed to the users by a passive beam splitter. In each user, normal and anomalous dispersion components are placed at two paths, followed by two NbN superconducting nanowire single-photon detectors (SNSPDs). The arrival time of photons can be used for key generation and security test based on symmetric dispersive optics QKD. **(b)** Mono-color pump light of the quantum light source is set at 1545.32 nm, which is the central wavelength of ITU channel C40. Generated signal and idler photons with correlated wavelength channels are symmetrically distributed around the frequency of pump light. Subscripts of wavelengths with opposite numbers correspond to a correlated wavelength channel pair for a specific entanglement resource; corresponding ITU channels are indicated below wavelength symbols. Five correlated wavelength channel pairs (shown in green) are used to support five subnets. The other 10 correlated wavelength channel pairs (shown in orange) are used to connect users between subnets.

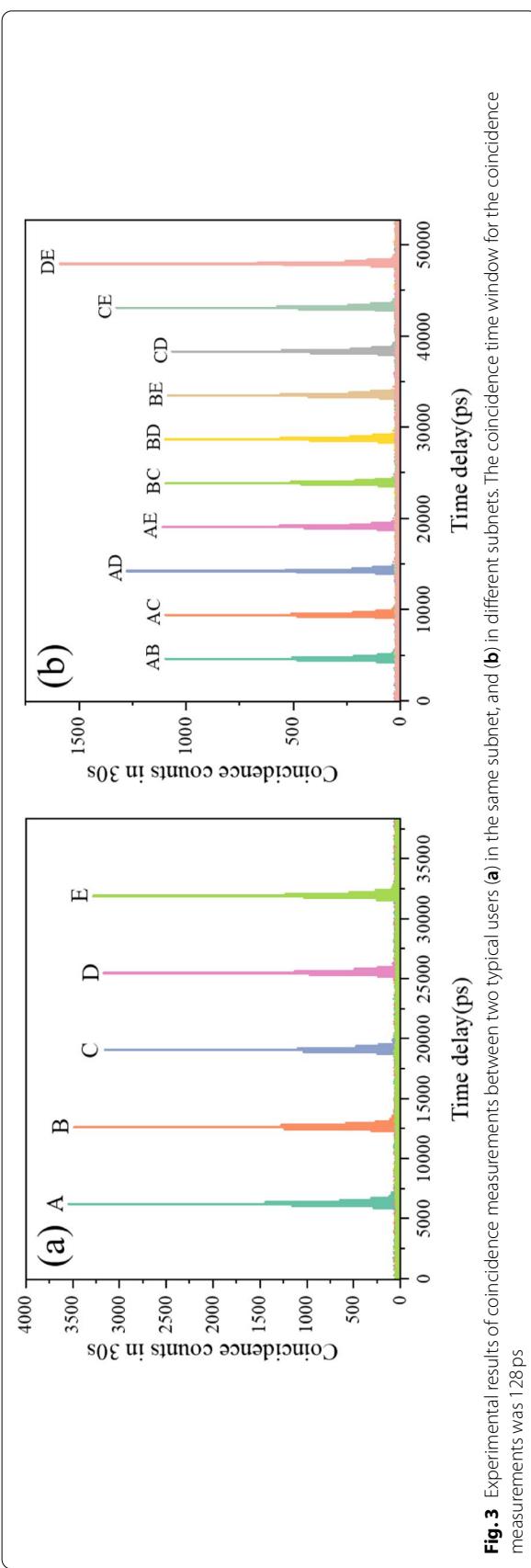


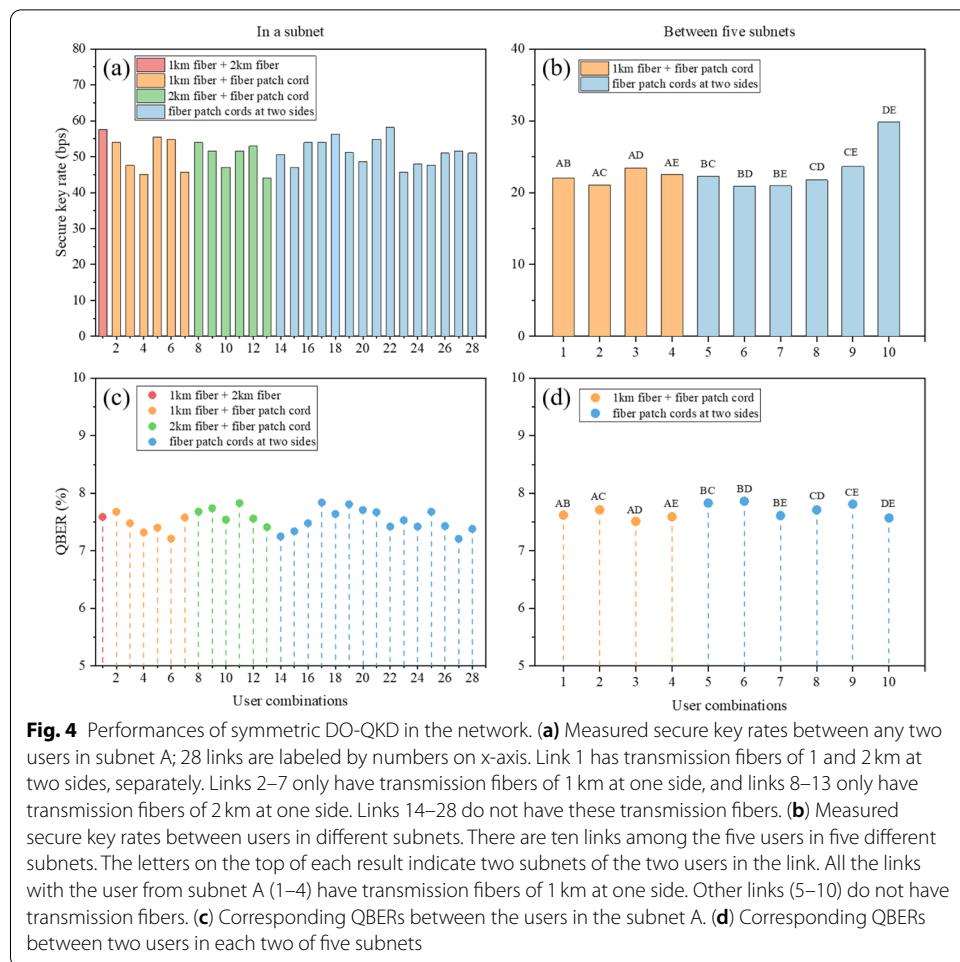
Fig. 3 Experimental results of coincidence measurements between two typical users (a) in the same subnet, and (b) in different subnets. The coincidence time window for the coincidence measurements was 128 ps

with different offsets in the time delays. The time window for the coincidence measurement was 128 ps. It can be seen that the coincidence to accidental coincidence ratios (CARs) of all the peaks are higher than 70. Figure 3(b) shows the typical coincidence results between users of different subnets. In each subnet, one specific user was selected to perform the coincidence measurement. Hence, 10 connections existed among the five users in different subnets. The 10 peaks in the figure show the coincidence results of the 10 connections with different time offsets for clarity. The time window for the coincidence measurement was 128 ps. The first coincidence peak is marked as AB, which indicates the result for the users from subnets A and B. It was supported by the entanglement resource with correlated wavelength channel pair (λ_6, λ_{-6}), and so on for the other coincidence peaks. All the peaks show CARs exceeding 60. The results in Fig. 3 show that the photon pairs distributed to any two users can be well discriminated under a narrow coincidence window by the coincidences, regardless of whether they are in the same or different subnets.

It is noteworthy that the average coincidence counts between two users in different subnets are smaller than those between two users in the same subnet. It is due to the difference of photon pair distributions in these two cases. For two users in different subnets, the signal and idler photons in a pair are distributed to the two users by two different beam splitters respectively. If the two beam splitters both have n output ports, the possibility that the two users could receive this photon pair is proportional to $1/n^2$. On the other hand, for two users in the same subnet, the signal and idler photons in a pair are distributed to the two users by the same beam splitter. There are two situations, i.e., the signal photon is guided to one user and the idler photon is guided to the other user, and vice versa. If the beam splitter also has n output ports, the possibility that the two users could receive this photon pair is proportional to $2/n^2$, considering the contributions of both situations. Thereby it will result in an almost two-fold coincidence counts for two users in the same subnet, compared to two users in different subnets. The differences in coincidence counts shown in Fig. 3(b) are primarily due to the differences in insertion loss induced by the wavelength division multiplexers for the photon pairs of different entanglement resources.

Subsequently, the performance of the QKD in this network was measured using the setup shown in Fig. 2(a). A symmetric DO-QKD was applied to realize secure key generation in all the links in the network. In this QKD scheme, the arrival time of photons was recorded and used for key generation and security tests. A high-dimensional time encoding process with three levels was optimized to attain the maximum secure key generation rates. For example, for typical two users in subnet A and B, after the optimization process, the raw key generation rate between the two users is 35.2 bits per second (bps) under a QBER of 7.6%. Through security test, secure key rate of 22 bps is obtained. More details of the symmetric DO-QKD, key generation and security test are introduced in the [Supplementary Materials](#).

Figure 4 shows the measurement results of QKD performance. First, we randomly selected a subnet, which is subnet A in our experiment, and the secure key rates between any two users in subnet A were measured, as shown in Fig. 4 (a). There are 28 links in the subnet, which are labeled by numbers along the x-axis. Since two specific users receive photons from the provider through transmission fibers of 1 and 2 km respectively, the



links including these two users have different transmission conditions. Link 1 has transmission fibers of 1 and 2 km on two sides, separately. Links 2–7 only have transmission fibers of 1 km on one side, whereas links 8–13 only have transmission fibers of 2 km on one side. Links 14–28 do not have these transmission fibers. It can be seen that all the links exhibited similar performances since the lengths of transmission fibers introduced in the experiment are quite short. The average secure key rate is ~ 51 bps. To demonstrate the secure key generation between two users in different subnets, we randomly selected one user in each of the five subnets. There were ten links among the five users. The performances of the symmetric DO-QKD of these links were measured, and the results are shown in Fig. 4(b). The letters on the top of each result indicate the two subnets of the two users of the corresponding link. All the links with the user from subnet A (1–4) have transmission fibers of 1 km on one side. Other links (5–10) do not contain transmission fibers. It can be seen that all these links show similar performances. The average secure key rate is ~ 22 bps, which is lower than that shown in Fig. 4(a). It is consistent with the coincidence results of entanglement distribution. The corresponding results of quantum bit error rate (QBER) between the users in the subnet A and in each two of the five subnets are shown in Fig. 4(c) and Fig. 4(d). The QBERs are all bounding at less than 8% by the bin sifting process.

Discussion

In this work, we proposed a QKD network architecture with two layers, based on quantum entanglement distribution by both wavelength division multiplexing (WDM) and space division multiplexing (SDM). A natural question is how to fully utilize its capacity. A simple comparison can be used to explain the best application form of this architecture. Let's consider three cases. In all of them, m^2 entanglement resources (m is a positive integer) are provided by a broadband quantum light source. They locate at different wavelength channel pairs and could be divided by WDM. Each entanglement resource has a photon pair generation rate of δ . Moreover, the losses of optical components and optical fibers for entanglement distribution are neglected for simplicity.

The first case is a single layer network with only SDM, in which all the entanglement resources are sent to all the users by a passive beam splitter. The user number is set as $m \times n$ (n is also a positive integer). Since photons are sent to all the users randomly by the beam splitter, the received single-photon rate of a specific user is

$$R_{s,1} = \frac{2m^2}{m \times n} \delta = \frac{2m}{n} \delta$$

Also, the received photon pair rate of any two specific users is $R_{c,1} = 2 \frac{m^2}{(m \times n)^2} \delta = \frac{2}{n^2} \delta$.

A parameter R_c/R_s is introduced to characterize the ratio of noise photons received by a specific user when establishing QKD with another user. The smaller the R_c/R_s , the greater the ratio of noise photons received by a specific user. In this case, it can be seen that $R_c/R_s = 1/(m \times n)$, showing that the ratio of noise photons received by a specific user is totally determined by the user number of the network.

The second case is the proposed two-layer network with both WDM and SDM. Assuming that the network has m subnets and each subnet has n users, the total user number is also $m \times n$. In the network, m entanglement resources support m subnet as shown in Fig. 1(a), while $m(m-1)$ entanglement resources are used to realize connections between different subnets as shown in Fig. 1(b). This setting means that any two subnets are connected by 2 entanglement resources, which ensures that the received photon pair rate between any two users is the same, no matter they are in the same subnet or not. It is easy to calculate the received single-photon rate of a specific user and the received photon pair rate of any two specific users in this network

$$R_{s,2} = \frac{2}{n} \delta + \frac{2(m-1)}{n} \delta = \frac{2m}{n} \delta$$

$$R_{c,2} = \frac{2}{n^2} \delta$$

It can be seen that they are the same with those of the first case. It seems that the two-layer network architecture has no advantage comparing with the single-layer one.

However, it is worth noting that in the two-layer network architecture, each entanglement resource only contributes to a part of connections in the network. For a specific connection in a subnet, only one entanglement resource supports it. While, for a specific connection between different subnets, only two entanglement resources support it. If the connection is used to realize QKD, the photons of corresponding

entanglement resources could be selected by optical filters at the users. It is the third case, the two-layer network with entanglement resource selection at user ends. It can be expected that the entanglement resource selection would not impact the received photon pair rate of the two users, but the received single-photon rate of a specific user would be reduced to

$$R_{s,2} = \frac{2}{n}\delta$$

Hence, $R_c/R_s = 1/n$, it is only determined by the user number in a subnet. If $n=1$, it is the case of fully-connected network only based on WDM [34]. As a conclusion, above comparisons show that the proposed two-layer network architecture has better coincidence performance than the single-layer one if entanglement resource selection is applied at user ends. Moreover, the single-layer network and the fully-connected WDM quantum network [34] in the previous works could be looked as two special cases of the two-layer network architecture in this work.

To analyze the performance of QKD realized in this network architecture, more factors should be considered, such as the number and performance of the quantum resources provided by the quantum light source, the losses introduced by transmission fibers and components for entanglement distribution, and the performance of the single-photon detectors. Beside their efficiency and dark count rate, the counting rate of the single-photon detectors is also important in this network architecture, since it determine how many entanglement resources could be introduced in this network. To explore the potential of this network architecture on realizing fully-connected QKD network with large user number, we established a theoretical model of DO-QKD and calculated the performance of QKD links in the networks of above three cases (The method and main parameters are introduced in the [supplementary materials](#)). The results are shown in Fig. 5.

Figure 5 (a) is a contour map showing the secure key rate between any two users in the single-layer network. The x-label is the user number in the network. The y-label is the entanglement resources introduced into the network, which is indicated by the total photon pair rate provided by the quantum light source. It can be seen that the secure key rate decreases with increasing user number under a given photon pair rate, since the optical loss of the QKD link between two users rises if output port number of the passive beam splitter increases. On the other hand, for a specific user number, the secure key rate rises with increasing photon pair rate firstly, then decreases after it reaches a maximum. There are two reasons that account for the performance degradation under high photon pair rate. On one hand, for the single-photon events recorded by a user, if more than one single-photon events are recorded in one frame, they should be discarded in the frame-sifting process of the DO-QKD protocol. It would lead to the decreased coincidence count between two users, reducing the raw key rate. On the other hand, the correlation between photons of two users will decrease when a large number of useful single-photon events are discarded, which would lead to a decreased security, reducing the secure key capacity. The dash line in the figure is the upper limit of the entanglement resources introduced into the network, which is determined by the counting rate of the single-photon detectors.

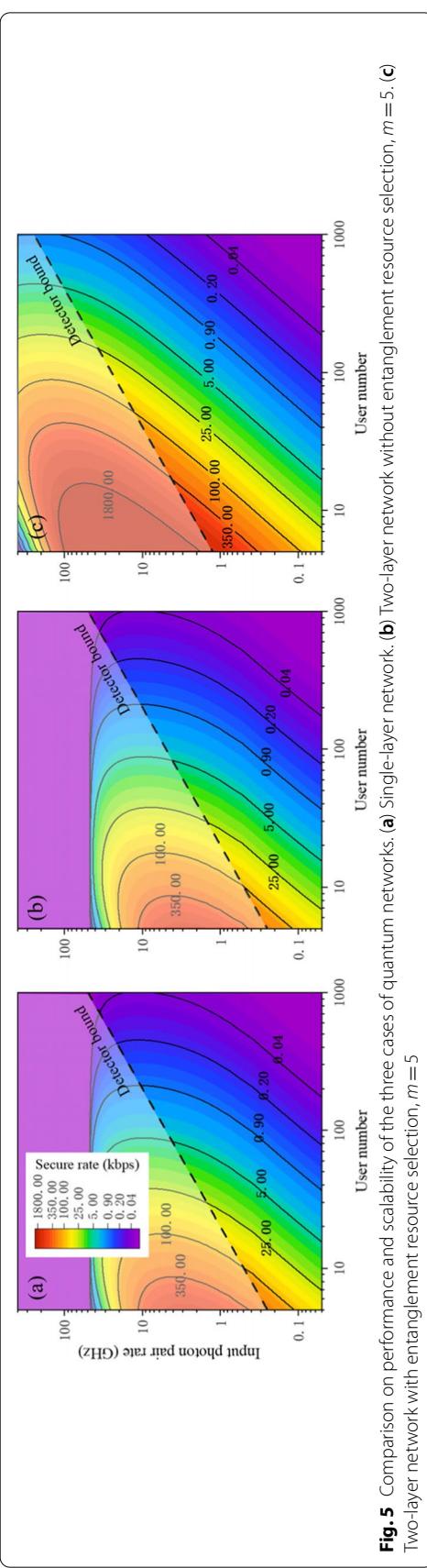


Fig. 5 Comparison on performance and scalability of the three cases of quantum networks. **(a)** Single-layer network. **(b)** Two-layer network without entanglement resource selection, $m=5$. **(c)** Two-layer network with entanglement resource selection, $m=5$

Hence, only the performance under the dash line is available, indicating that the performance of single-photon detectors is crucial for scaling the quantum network.

The calculation results of two-layer network without entanglement resource selection is shown in Fig. 5(b). In the calculation, it is assumed that the network has 5 subnets ($m=5$), hence the user number should be a multiple of 5 and the contour is plotted by interpolation. The number of the entanglement resources should be $m^2=25$. The y-label shows the total contributions of all the 25 entanglement resources when changing δ . It can be seen that the QKD performances of this network is almost the same with those of the single-layer network. The performance of two-layer network with entanglement resource selection are calculated under the same parameter setting as Fig. 5(b), which is shown in Fig. 5(c). It is clear that the QKD performance is highly improved comparing with those of the single-layer network, showing the benefits of entanglement resource selection. The comparison among the QKD performance in Fig. 5 agrees with the above qualitative analysis. Since photons of different wavelengths are not distinguished in the single-layer network, the entanglement resource selection by optical filter at user side is a prominent advantage of the two-layer network.

In the experiment of this work, the entanglement resources introduced into the network is quite small (total photon pair rate is about 0.06 GHz), which is far from the limitations introduced by the frame-sifting process of the DO-QKD protocol and the counting rate of the single-photon detectors. The calculation results in Fig. 5 show that the network performances are almost the same in all the cases when total photon pair rate is lower than 0.1 GHz. On the other hand, to realize large-scale quantum network, massive entanglement resources should be introduced into the network through an ultra-broadband quantum light source, or multiple quantum light sources. In this condition, entanglement resource selection is crucial for the network performance and scalability.

In this work, we focused on the application scenarios with short transmission distance and large user number, such as local area networks, campus networks and community access networks. It can be expected that a network with smaller user number could support longer transmission distance by reducing the additional loss introduced by the multi-port beam splitters. An extreme case is that the entanglement distribution is only realized by WDM and no multi-port beam splitter is applied in the network. In this case, each link is supported by one entanglement resource to realize point-to-point QKD. Our previous work has shown that in this network the entanglement-based DO-QKD protocol could support fiber transmission links of several tens kilometers with reasonable secure key rate [42].

Conclusions

In this work, we propose a fully connected QKD network architecture without trusted node for a large number of users. It has two layers, by which the entanglement resources provided by a broadband quantum light source are distributed to users by WDM and SDM. Any two users in the network share a part of entanglement resources, by which QKD is established between them. The experiment demonstration realizes a fully connected network with 40 users and 780 QKD links. The average secure key rate between users in the same subnet is ~ 51 bps and that between users in different subnets is

~22 bps. The performance of this network architecture is also discussed theoretically. It shows that the proposed two-layer network architecture has better performance than the single-layer network with passive beam splitter, if entanglement resource selection at user ends is applied. It provides an effective and simple way to realize quantum communication networks with large user numbers.

Abbreviations

QKD: Quantum key distribution; BB84: Bennett-Brassard-84; TF-QKD: twin-field quantum key distribution; SWFM: Spontaneous four-wave mixing; ITU: International Telecommunication Union; DWDM: Dense wavelength division multiplexing; SNSPD: Superconducting nanowire single-photon detector; DO-QKD: Dispersive optics quantum key distribution; CAR : Coincidence to accidental coincidence ratio; QBER: Quantum bit error rate; WDM: Wavelength division multiplexing; SDM: Space division multiplexing.

Supplementary Information

The online version contains supplementary material available at <https://doi.org/10.1186/s43074-022-00048-2>.

Additional file 1.. See the supplementary material for experimental details, description of symmetric DO-QKD, bin shifting process for key generation and security testing of the system.

Acknowledgements

Not applicable.

Authors' contributions

Wei Zhang and Xu Liu proposed the scheme. Xu Liu, Rong Xue and Wei Zhang performed experiments and analyzed data. Jingyuan Liu took the theoretical analysis. Xu Liu, Jingyuan Liu and Wei Zhang wrote the manuscript. Yidong Huang revised the manuscript and supervised the project. Xue Feng, Fang Liu, Kaiyu Cui contributed to discussion of this study and the revision of the manuscript. Heping Wang, Hao Li, Zhen Wang and Lixing You provided superconducting nanowire single-photon detectors and revised the manuscript. All authors read and approved the final manuscript.

Funding

National Key R&D Program of China (2017YFA0303704), Beijing Natural Science Foundation (BNSF) (Z180012), National Natural Science Foundation of China (NSFC) (61875101, 91750206, 61575102), Beijing Academy of Quantum Information Sciences and the Tsinghua University Initiative Scientific Research Program.

Availability of data and materials

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

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

¹Beijing National Research Center for Information Science and Technology (BNRist), Beijing Innovation Center for Future Chips, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China. ²State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China. ³Frontier Science Center for Quantum Information, Beijing 100084, China. ⁴Beijing Academy of Quantum Information Sciences, Beijing 100193, China.

Received: 16 October 2021 Accepted: 8 January 2022

Published online: 24 January 2022

References

1. Scarani V, et al. The security of practical quantum key distribution. *Rev Mod Phys*. 2009;81:1301–50.
2. Pirandola S. Advances in quantum cryptography. *Adv Opt Photon*. 2020. <https://doi.org/10.1364/AOP361502>.
3. Brassard CB, a. G. Quantum cryptography: public key distribution and coin tossing. *Proc IEEE Int Conf on Comp Sys Signal Process (ICASSP)*. 1984:175–9.
4. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett*. 2000;85:441–4.
5. Cerf NJ, Bourennane M, Karlsson A, Gisin N. Security of quantum key distribution using d-level systems. *Phys Rev Lett*. 2002;88:127902. <https://doi.org/10.1103/PhysRevLett.88.127902>.

6. Korzh B, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat Photonics*. 2015;9:163.
7. Diamanti E, Lo H-K, Qi B, Yuan Z. Practical challenges in quantum key distribution. *Npj quantum. Inform.* 2016;2:16025.
8. Hwang WY. Quantum key distribution with high loss: toward global secure communication. *Phys Rev Lett.* 2003;91:057901. <https://doi.org/10.1103/PhysRevLett.91.057901>.
9. Wang X-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys Rev Lett.* 2005;94:230503.
10. Zhao Y, Qi B, Ma X, Lo HK, Qian L. Experimental quantum key distribution with decoy states. *Phys Rev Lett.* 2006;96:070502. <https://doi.org/10.1103/PhysRevLett.96.070502>.
11. Braunstein SL, Pirandola S. Side-channel-free quantum key distribution. *Phys Rev Lett.* 2012;108:130502.
12. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Phys Rev Lett.* 2012;108:130503.
13. Zhou Y-H, Yu Z-W, Wang X-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys Rev A*. 2016;93:042324. <https://doi.org/10.1103/PhysRevA.93.042324>.
14. Yin HL, et al. Measurement-device-independent quantum key distribution over a 404 km optical Fiber. *Phys Rev Lett.* 2016;117:190501. <https://doi.org/10.1103/PhysRevLett.117.190501>.
15. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature*. 2018;557:400–3. <https://doi.org/10.1038/s41586-018-0066-6>.
16. Ma X, Zeng P, Zhou H. Phase-matching quantum key distribution. *Phys Rev X*. 2018;8:031043. <https://doi.org/10.1103/PhysRevX.8.031043>.
17. Wang X-B, Yu Z-W, Hu X-L. Twin-field quantum key distribution with large misalignment error. *Phys Rev A*. 2018;98. <https://doi.org/10.1103/PhysRevA.98.062323>.
18. Chen JP, et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. *Phys Rev Lett.* 2020;124:070501. <https://doi.org/10.1103/PhysRevLett.124.070501>.
19. Chen J-P, et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat Photonics*. 2021;15:570–5. <https://doi.org/10.1038/s41566-021-00828-5>.
20. Briegel HJ, Dür W, Cirac JI, Zoller P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys Rev Lett.* 1998;81:5932–5.
21. Kimble HJ. The quantum internet. *Nature*. 2008;453:1023–30. <https://doi.org/10.1038/nature07127>.
22. Pirandola S. End-to-end capacities of a quantum communication network. *Communications Physics*. 2019;2:51.
23. Specht HP, et al. A single-atom quantum memory. *Nature*. 2011;473:190–3.
24. Pang X-L. A hybrid quantum memory-enabled network at room temperature. *Sci Adv.* 2020.
25. de Riedmatten H, et al. Long-distance entanglement swapping with photons from separated sources. *Phys Rev A*. 2005;71.
26. Sun Q-C, et al. Entanglement swapping over 100 km optical fiber with independent entangled photon-pair sources. *Optica*. 2017;4:1214.
27. Chen T-Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt Express*. 2009;17:6540–9.
28. Peev M, et al. The SECOQC quantum key distribution network in Vienna. *New J Phys*. 2009;11:075001.
29. Sasaki M, et al. Field test of quantum key distribution in the Tokyo QKD network. *Opt Express*. 2011;19:10387–409.
30. Stucki D, et al. Long-term performance of the Swiss quantum quantum key distribution network in a field environment. *New J Phys*. 2011;13:123001.
31. Chen T-Y, et al. Metropolitan all-pass and inter-city quantum communication network. *Opt Express*. 2010;18:27217–25.
32. Herbaus I, Blauensteiner B, Poppe A, Jennewein T, Hübel H. Demonstration of active routing of entanglement in a multi-user network. *Opt Express*. 2013;21:29013–24.
33. Chang XY, et al. Experimental realization of an entanglement access network and secure multi-party computation. *Sci Rep*. 2016;6:29453.
34. Price A. Pragmatic quantum cryptography in next-generation photonic networks Ph. D thesis: University of Bristol; 2019.
35. Townsend PD. Quantum cryptography on multiuser optical fibre networks. *Nature*. 1997;385:47–9.
36. Iris C, Robert JY, Paul DT. Quantum information to the home. *New J Phys*. 2011;13:063039.
37. Wengerowsky S, Joshi SK, Steinlechner F, Hübel H, Ursin R. An entanglement-based wavelength-multiplexed quantum communication network. *Nature*. 2018;564:225–8.
38. Joshi, S. K. A trusted node-free eight-user metropolitan quantum communication network. *science advances* 6, eaba0959, doi: <https://doi.org/10.1126/sciadv.aba0959> (2020).
39. Liu X, et al. An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution. *APL Photonics*. 2020;5:076104.
40. Mower J, et al. High-dimensional quantum key distribution using dispersive optics. *Phys Rev A*. 2013;87:062322.
41. Lee C, et al. Entanglement-based quantum communication secured by nonlocal dispersion cancellation. *Phys Rev A*. 2014;90:062331.
42. Liu X, et al. Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km. *Appl Phys Lett*. 2019;114:141104. <https://doi.org/10.1063/1.5089784>.

Publisher's Note

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