




An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution

Cite as: APL Photonics 5, 076104 (2020); <https://doi.org/10.1063/5.0002595>

Submitted: 27 January 2020 . Accepted: 22 June 2020 . Published Online: 08 July 2020

Xu Liu , Xin Yao, Rong Xue, Heqing Wang, Hao Li, Zhen Wang, Lixing You , Xue Feng, Fang Liu, Kaiyu Cui, Yidong Huang, and Wei Zhang 



View Online



Export Citation



CrossMark

ARTICLES YOU MAY BE INTERESTED IN

[Amorphous superconducting nanowire single-photon detectors integrated with nanophotonic waveguides](#)


APL Photonics 5, 076106 (2020); <https://doi.org/10.1063/5.0004677>

[Integrated vortex beam emitter in the THz frequency range: Design and simulation](#)

APL Photonics 5, 076102 (2020); <https://doi.org/10.1063/5.0010546>

[Enhancing the modal purity of orbital angular momentum photons](#)

APL Photonics 5, 070802 (2020); <https://doi.org/10.1063/5.0005597>



AMERICAN ELEMENTS

THE ADVANCED MATERIALS MANUFACTURER®

additive manufacturing epitaxial crystal growth cerium oxide polishing powder silver nanoparticles sputtering targets III-IV semiconductors CVD precursors europium phosphors

Li Be gallium lump glassy carbon nanodispersions He
 Na Mg surface functionalized nanoparticle: Al Si P S Cl Ar
 K Ca Sc Ti V Cr Mn Fe Co Ni Cu Zn Ga Ge As Se Br Kr
 Rb Sr Y Zr Nb Mo Tc Ru Rh Pd Ag Cd In Sn Sb Te I Xe
 Cs Ba La Hf Ta W Re Os Ir Pt Au Hg Tl Pb Bi Po At Rn
 Fr Ra Ac Rf Db Sg Bh Hs Mt Ds Rg Cn Fl Uu Lv Uu

deposition slugs OLED Lighting spintronics solar energy
 osmium nanoribbons thin films chalcogenides AuNPs
 GDC Li-ion battery electrolytes 99.999% ruthenium spheres

endoheedral fullerenes copper nanoparticles diamond micropowder
 CIGS MBE grade materials palladium catalysts flexible electronics
 beta-barium borate borosilicate glass dysprosium pellets YBCO
 pyrolytic graphite 3d graphene foam indium tin oxide mesoporous silica
 raman substrates sapphire windows tungsten carbide InGaAs
 barium fluoride carbon nanotubes lithium niobate scandium powder

perovskite crystals yttrium iron garnet alternative energy h-BN
 gold nanocubes graphene oxide macromolecules photonics
 rhodium sponge fiber optics beamsplitters infrared dyes zeolites
 fused quartz metallocenes platinum ink buckyballs Ti-6Al-4V

Now Invent.™
 The Next Generation of Material Science Catalogs

American Elements opens up a world of possibilities so you can **Now Invent!**
 Over 15,000 certified high purity laboratory chemicals, metals, & advanced materials and a state-of-the-art Research Center. Printable GHS-compliant Safety Data Sheets. Thousands of new products. And much more. All on a secure multi-language "Mobile Responsive" platform.

www.americanelements.com



An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution

Cite as: APL Photon. 5, 076104 (2020); doi: 10.1063/5.0002595

Submitted: 27 January 2020 • Accepted: 22 June 2020 •

Published Online: 8 July 2020



View Online



Export Citation



CrossMark

Xu Liu,¹  Xin Yao,¹ Rong Xue,¹ Heqing Wang,² Hao Li,² Zhen Wang,² Lixing You,²  Xue Feng,^{1,3} Fang Liu,^{1,3} Kaiyu Cui,^{1,3} Yidong Huang,^{1,3,4} and Wei Zhang^{1,3,4,a)} 

AFFILIATIONS

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

^{a)}Author to whom correspondence should be addressed: zwei@tsinghua.edu.cn

ABSTRACT

Quantum key distribution (QKD) is a crucial technology for information security in the future. Developing simple and efficient ways to establish QKD among multiple users is important to extend the applications of QKD in communication networks. Herein, we proposed a scheme of symmetric dispersive optics QKD and demonstrated an entanglement-based quantum network based on it. In the experiment, a broadband entangled photon pair source was shared by end users via wavelength and space division multiplexing. The wide spectrum of generated entangled photon pairs was divided into 16 combinations of frequency-conjugate channels. Photon pairs in each channel combination supported a fully connected subnet with eight users by a passive beam splitter. Eventually, it showed that an entanglement-based QKD network over 100 users could be supported by one entangled photon pair source in this architecture. It has great potential on applications of local quantum networks with large user number.

© 2020 Author(s). All article content, except where otherwise noted, is licensed under a Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>). <https://doi.org/10.1063/5.0002595>

I. INTRODUCTION

Information security is of significant importance in many applications. Nowadays, the security of these applications is mainly based on public-key cryptography,^{1,2} which assumes that the computation power is limited. Quantum key distribution (QKD) can provide cryptographic keys with information-theoretic security by the nature of quantum physics,^{3–6} which may revolutionize the protection way of information exchange in the future. Since the first protocol⁷ (BB84) was proposed, QKD has been developed significantly.^{8–14} Many field tests of QKD have been implemented, proving it to be a reliable technology.^{15–17}

In recent years, how to build quantum networks conveniently and efficiently becomes the focus of research on QKD. The quantum repeater-assisted network¹⁸ has the great potential to construct a global quantum network. The end-to-end tight ultimate capacities for repeater-assisted quantum network have been explored recently.¹⁹ However, the quantum memories and entanglement swapping are normally used to extend and route quantum states to construct arbitrary network, where the technologies in quantum memories remain to be improved for practical applications. The quantum nodal network has achieved great developments,^{20–22} which connects multiple point-to-point QKD links by trusted nodes. In the future, it may be also fulfilled by the quantum relayed

satellite.^{23–25} Although it is promising on realizing long-distance backbone QKD networks, it is not efficient to provide QKD services in local networks with many users and complicated connections, such as networks in companies, campuses, and communities. To improve the efficiency of QKD networks, the concept of quantum access network is proposed, which allows multiple users to share the receivers or sources.^{26,27} The first quantum access network was proposed by Townsend,²⁸ in which single photons from a central node are distributed to multiple end users by a passive beam splitter. However, it realizes point-to-multipoint network by point-to-point QKD between the central node and each end user. Except for the low efficiency, the secure connection between these end users depends on the relay of the central node. Hence, the security of the whole network extremely relies on the fidelity of the central node.

Quantum entanglement is the crucial resource for certified generation of shared randomness,^{29,30} quantum communication,^{31,32} and so on. The flexibility on entanglement distribution among multiple users may provide new ways to realize QKD networks.³³ In a previous study, the signal and idler photons from entangled photon pairs were divided and distributed to two sets of users.³⁴ On each side, an optical switch was used to distribute photons to a specific user. In this way, entanglement-based QKD can be established between the two specific users at the two sides, achieving a quantum network with active routing function. However, the users on the same side cannot establish QKD in this architecture. What is more, the network efficiency would be limited to some duty cycles of optical switches, which is a common problem for the point-to-multipoint architectures based on optical switches.³⁵ Besides, it has been reported that the switch-based networks need

additional time to re-initialize the new communication channel when they change their topology.³⁶ Recently, a fully connected QKD network was proposed and demonstrated experimentally based on a broadband polarization-entangled quantum light source.³⁷ Every two users in the network were allocated with photon pairs in two correlated wavelength channels by wavelength division multiplexing technology. It can be expected that a minimum of $N \times (N - 1)$ wavelength channels are required to fully connect N users in this architecture. Hence, it rapidly depletes the bandwidth resource of quantum light source as the user number increases. In a recent study, the utilization of the entanglement resources is improved by introducing beam splitting in the wavelength division multiplexing entanglement-based QKD network.³⁸

In this paper, we develop a quantum network based on another way of quantum entanglement distribution, in which the entangled photon pairs generated by a quantum light source are sent to N end users by a $1 \times N$ beam splitter directly. In this way, the two photons in each pair may be distributed to any user randomly. Hence, any two end users will have coincidence events, which can be used to establish a QKD network with full connection conveniently. However, it can be expected that the rates of coincidence events between users will be decreased rapidly if the user number supported by the quantum light source increases. To utilize the coincidence events efficiently, we use the dispersive optics QKD (DO-QKD) based on energy-time entanglement to achieve the QKD network. An attractive property of the entanglement-based DO-QKD is that high-dimensional time encoding can be utilized in this scheme, which supports multi-bit key generation per coincidence,³⁹ improving the utilization of coincidence events.

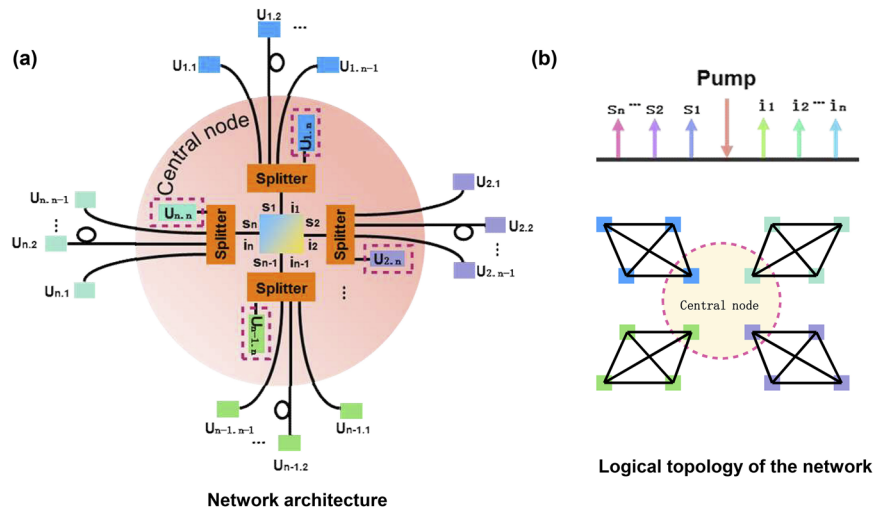


FIG. 1. Illustration of the proposed QKD network. (a) The sketch of the network architecture. The energy-time entangled photon pairs are divided into different wavelength channels by wavelength division multiplexing. The signal and idler photons in two frequency-conjugate wavelength channels are multiplexed together and further distributed by a $1 \times N$ beam splitter to N users, supporting a subnet of QKD. In the scenario of local networks, the quantum light source and the $1 \times N$ beam splitters are set in the central node. Each subnet also provides a user to the center node, which is shown by the dashed square in the figure. Two users in different subnets can eventually establish cryptographic keys through the central node. (b) The logical topology of the network. The illustration on the top shows that the generated photon pairs of the quantum light source are over a wide wavelength region and each pair of correlated wavelength channels supports a subnet. Each subnet is a fully connected QKD network and provides a user to the central node, which connects all the subnets.

To further improve the utilization of the entanglement resource provided by the quantum light source, we also introduce wavelength multiplexing in this entanglement-based QKD network, exploring how many users can be supported by one quantum light source in this way. Figure 1(a) shows the sketch of the network architecture. The quantum light source located in the central node generates energy-time entangled photon pairs over a wide wavelength region, which are divided into different channels by wavelength division multiplexing. The signal and idler photons in two frequency-conjugate wavelength channels are entangled and contribute to coincidence events. They are selected and multiplexed into one optical fiber and then distributed to N users randomly by a $1 \times N$ beam splitter. In this way, any two users in a subnet would receive photons entangled with each other, which can be indicated by the coincidence measurement between them. Then, the QKD can be established between any two of these N users based on the coincidence events, realizing a fully connected QKD subnet. The beam splitter also can be placed in the central node in the scenario of local networks. If the quantum light source could support M frequency-conjugate wavelength channel combinations, it can support M QKD subnets. To connect these subnets, the simplest way is that each subnet provides a user to the central node, as shown in Fig. 1(a). In this architecture, the central node acts as a trusted relay node. Any two users in different subnets can eventually establish cryptographic keys through the central node. The logical topology structure of this architecture is shown in Fig. 1(b). The illustration on the top shows that the generated photon pairs of the quantum light source are over a wide wavelength region and each pair of correlated wavelength channels supports a subnet. Each subnet has a fully connected mesh topology, while all the subnets are connected by the central node.

It can be seen that this QKD network architecture utilizes the entanglement resource with high efficiency and robustness. First, the entanglement-based DO-QKD with high-dimensional time encoding is applied to enhance the utilization of the coincidence events. Second, the broadband characteristics of quantum light source are utilized sufficiently by wavelength division multiplexing to support many subnets. Finally, if the user number of each subnet is not too small, most photon pairs would be distributed to two different users randomly, which is a simple but efficient way to realize a fully connected subnet. On the other hand, only the trust on the central node is required. The insecurity of an end user will not impact the QKD between other users in a subnet. If the central node is insecure, the cryptographic keys between users in different subnets will be insecure. However, it will not impact the QKDs between users in the same subnet.

II. SYMMETRIC DO-QKD

In the scheme of entanglement-based DO-QKD, the signal and idler photons are sent to two users. Normal and anomalous dispersion components are introduced at the two sides to carry out the security test, which is guaranteed by the nonlocal dispersion cancellation effect⁴⁰ of energy-time entangled photon pairs. It has been proven to be secure against collective attacks.^{41,42} However, the two users have different configurations in the conventional

entanglement-based DO-QKD scheme, one user has normal dispersion component and the other has anomalous dispersion component. It cannot be used to establish the QKD network based on a $1 \times N$ beam splitter. Therefore, we propose a modified scheme named as “symmetric DO-QKD” to support the proposed QKD network architecture, which is shown in Fig. 2.

Figure 2(a) shows the sketch of the conventional DO-QKD scheme. A beam splitter separates photons to two paths at Alice’s side. An anomalous dispersion ($AD_{Alice.1}$) component is introduced in one path (path A1). Let us assume that it has a dispersion parameter of $+2D$. Bob’s configuration is similar to that of Alice. He also has a dispersion component ($ND_{Bob.1}$) in one path (path B1), but it has normal dispersion with a dispersion parameter of $-2D$. Then, we can take a transformation on the configuration of conventional DO-QKD scheme, as shown in Fig. 2(b). At Alice’s side of this configuration, an anomalous dispersion ($AD_{Alice.2}$) component is introduced before the beam splitter with a dispersion parameter of D . While the dispersion parameter of $AD_{Alice.1}$ in path A1 reduces to D , a new dispersion component of normal dispersion ($ND_{Alice.1}$) is introduced in the other path (path A2), which has a dispersion parameter of $-D$. Similar transformation is made at Bob’s side. A dispersion component denoted by $ND_{Bob.2}$ is introduced before the beam splitter with a dispersion parameter of $-D$. Another dispersion component denoted by $AD_{Bob.2}$ is introduced in path B2 with a dispersion parameter of D . And the dispersion parameter of $ND_{Bob.1}$ reduces to $-D$. It can be seen that in this transformed scheme, the photons sent to paths A1, A2, B1, and B2 experience the same dispersion with those in the conventional scheme as shown in Fig. 2(a). Hence, the two schemes are equivalent. Since the dispersion parameters of $AD_{Alice.2}$ and $ND_{Bob.2}$ are D and $-D$, the energy-time entangled photon pairs would experience nonlocal dispersion cancellation⁴⁰ after the signal and idler photons pass through the two dispersion components. Narrow coincidence peak would be maintained if the photon pairs are measured after the nonlocal dispersion cancellation, which is desired for DO-QKD. $AD_{Alice.2}$ and $ND_{Bob.2}$ marked in dotted gray boxes can be considered as a part of fiber transmission with

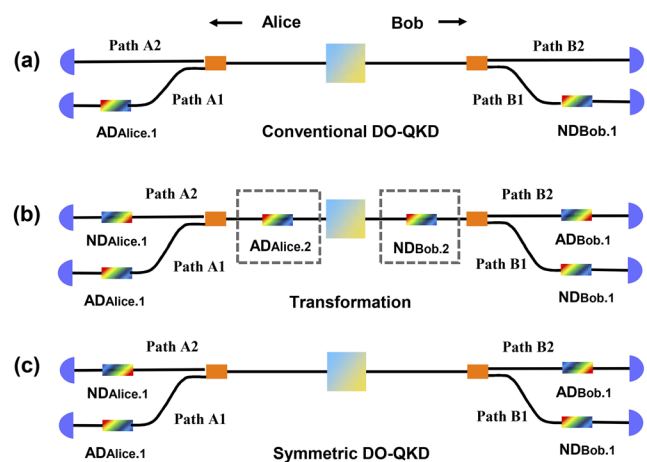


FIG. 2. Transformation from conventional DO-QKD to symmetric DO-QKD.

good dispersion compensation, which leads to the symmetric DO-QKD scheme as shown in Fig. 2(c). In the symmetric DO-QKD, two dispersive components with anomalous and normal dispersions are introduced in the two paths at both Alice and Bob's sides. And the dispersions experienced by the energy-time entangled photon pairs in the fiber transmission should be properly compensated. It is named "symmetric" since the users have the same configurations, which solves the problem of the conventional one. Hence, the symmetric DO-QKD scheme can be used in the network based on a $1 \times N$ beam splitter. It can be seen that a symmetric DO-QKD system is equivalent to a conventional DO-QKD system, while the dispersion parameters of $AD_{Alice,1}$ and $ND_{Bob,1}$ ($\pm 2D$) in the assumed conventional DO-QKD system should be two times over those of $AD_{Alice,1}$, $ND_{Alice,1}$, $ND_{Bob,1}$, and $AD_{Bob,1}$ ($\pm D$). The symmetric DO-QKD scheme also can establish two measurement bases by matching the paths with dispersive components with different dispersions. As shown in Fig. 2(c), one includes path A1 and path B1, and the other includes path A2 and path B2. It should be predefined before QKD operation that which one is the "time" basis and which one is the "frequency" basis.

III. EXPERIMENTAL SYSTEM

To demonstrate the proposed QKD network architecture based on symmetric DO-QKD, we establish the experimental system as shown in Fig. 3.

The energy-time entangled photon pairs are generated in a broad telecom band through the spontaneous four-wave mixing (SFWM) effect in a piece of silicon waveguide under continuous-wave (CW) pumping. The silicon waveguide was 3 mm in length on a silicon-on-insulator (SOI) photonic chip. An arrayed waveguide grating (AWG) is used to filter the output photons. In the experimental system, the wide spectrum of the signal and idler photons is divided into 32 wavelength channels. Each combination of correlated wavelength channels that satisfy the energy conservation condition of SFWM is further multiplexed together by a dense wavelength division multiplexing (DWDM) component and then distributed randomly to eight users by a 1×8 planar lightwave circuit splitter (PLCS). Hence, the source supports 16 subnets. At each

end user, the photons are split into two paths by a fiber coupler and detected by superconducting nanowire single-photon detectors (SNSPDs). The fiber polarization controllers (FPCs) before the SNSPDs are used to maximize the detection efficiencies. A normal dispersion component and an anomalous dispersion component are introduced in the two paths. Hence, all the end users have the same configurations and any two users in a subnet can establish the symmetric DO-QKD and generate cryptographic keys between them. The cryptographic keys between users in different subnets are relied on the central node, which includes the quantum light source and the PLCs. In each subnet, one specific user is placed in the central node for the connections between different subnets. Considering the scenario of local networks, the fiber lengths between the central node and end users are tens of meters in the experimental system. Hence, the impact of fiber dispersion can be neglected in the experiments. See the experimental details in [supplementary material 1](#).

IV. ENTANGLEMENT DISTRIBUTION

High-quality entanglement distribution was first tested in the experimental system as shown in Fig. 4. First of all, we tested the broadband characteristics of the quantum light source. The AWG used in the experiment covers the International Telecommunication Union (ITU) channels of C21–C60. To fully utilize the filtering channels of the AWG, the mono-color pump light of the quantum light source is set at 1545.32 nm, which is the central wavelength of the channel of C40. The correlated wavelength channels for the signal and idler photons are distributed symmetrically around this channel of AWG. We selected channels of C44 ~ C59 as the signal channels and channels of C21 ~ C36 as the idler channels. In the measurement, the SNSPDs (with FPCs) were connected to the output fiber of the AWG for specific ITU channels. The performances of the wavelength division in the system and corresponding coincidence results are shown in Fig. 4.

The single-photon count rates of these channels were measured under a specific pumping level which was fixed in the following experiments, which are shown in Fig. 4(a). It can be seen that the photon count rates of all the channels are close due to the broadband characteristics of the photon pair generation by SFWM in

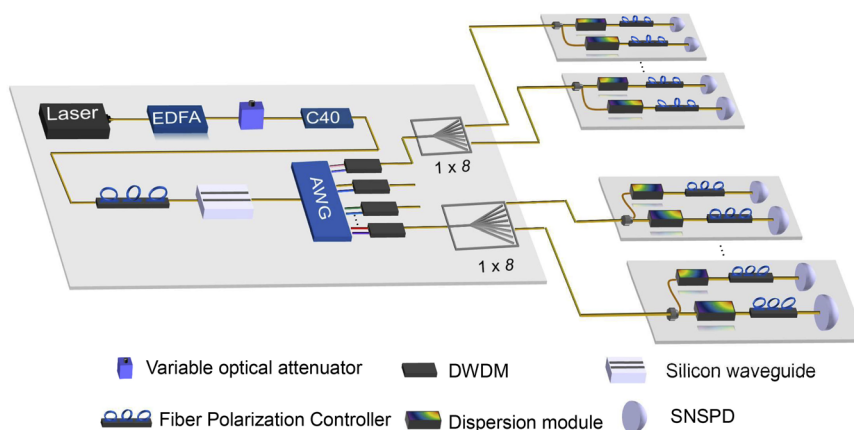


FIG. 3. Experimental system of the QKD network based on symmetric DO-QKD. In each user, the normal and anomalous dispersion modules are introduced for the nonlocal dispersion cancellations. The photons are detected by superconducting nanowire single-photon detectors (SNSPDs). This experimental system supports 16 subnets, and each subnet has 8 end users. DWDM: dense wavelength division multiplexing component; ND (AD): normal dispersion (anomalous dispersion) components; FPC: fiber polarization controller.

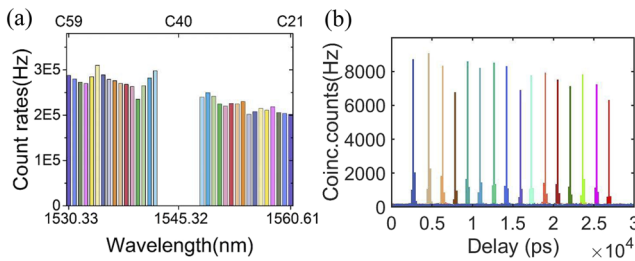


FIG. 4. Performances of the wavelength division in the system and corresponding coincidence results. (a) Single-photon count rates of different wavelength channels. (b) Experimental results of coincidence counts of 16 correlated wavelength channel combinations under a time bin width of 192 ps.

the silicon waveguide. The coincidence counts of each combination of correlated signal and idler channels are shown in Fig. 4(b). For clarity, the coincidence peak positions of different channel combinations were shifted with a fixed time delay of 1600 ps. It can be seen that the signal and idler photons in all the correlated channel combinations have good coincidences. Each channel combination can be used to constitute a subnet. In the following experiments, we demonstrated the performances of subnet supported by channels of C31 and C49.

In the experimental system, the signal and idler photons with channels of C31 and C49 are multiplexed and distributed to eight end users of a subnet by a 1×8 PLCS. In this way, every two users in the subnet have coincidence events of entangled photon pairs, which is the base to realize the symmetric DO-QKD network. To show the performance of the entanglement distribution between the end users, all the coincidence events of 28 user combinations in this typical subnet are measured by the SNSPDs. The results are shown in Fig. 5, in which the two figures show the measured coincidence count rates and the corresponding CARs between any two users, respectively. It can be seen that any two users in the subnet have coincidence events out of the entangled photon pairs. They support the fully connected subnet, even though the distribution by the 1×8 PLCS reduces the coincidence rates to several tens of counts per second. On the other hand, all the CARs are higher than 100 indicating the preservation of the high-quality entanglement after its distribution, which could support the high-performance QKD.

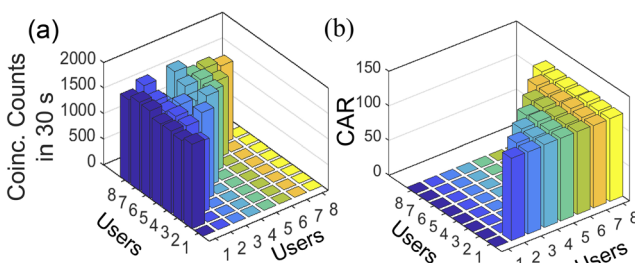


FIG. 5. Results of entanglement distribution of all the user combinations in a typical subnet acquired in 30 s under a time bin width of 192 ps. (a) The coincidence counts. (b) The CARs.

V. KEY GENERATION IN THE NETWORK

In the experimental system, the entanglement-based symmetric DO-QKD protocol was used to generate cryptographic keys between the end users in the network. The high-dimensional time encoding was utilized in the symmetric DO-QKD scheme, which supported multi-bit key generation per coincidence (see details in the [supplementary material](#)), improving the utilization of the entanglement resource in this network. As shown in Fig. 3, both normal and anomalous dispersion components are introduced in each user in this scheme. Thus, all the end users in the network have the same configurations. For any two users, there are two bases between them and both of them experience the effect of nonlocal dispersion cancellation using the matched dispersion components. The coincidences under the two bases are used for the security test and key generation, which are named as “S base” and “K base,” respectively. If one user uses the path with the normal dispersion component as the S base, the other user should select the path with anomalous dispersion component as the S base, and vice versa. Then, the remaining measurement base is used as the K base. The base selection between the users in the subnet should be predefined before QKD operation.

We measured the performances of entanglement-based symmetric DO-QKDs in the experimental system. Typical results of coincidence counts under four possible measurement base combinations between two end users in a subnet (supported by photons with channels of C31 and C49) are shown in Fig. 6. In these figures, K1, K2, S1, and S2 indicate the measurement bases predefined between two end users. It can be seen that the coincidence peak is narrow due to the nonlocal dispersion cancellations if it is measured under K bases at both sides, which are shown in Fig. 6(a). It is also narrow if it is measured under S bases at both sides, which are shown in Fig. 6(d). However, the coincidence peaks are broadened if they are measured under different bases, which are shown in Figs. 6(b) and 6(c). These results show that the symmetric configurations in these users are able to realize DO-QKD. According to

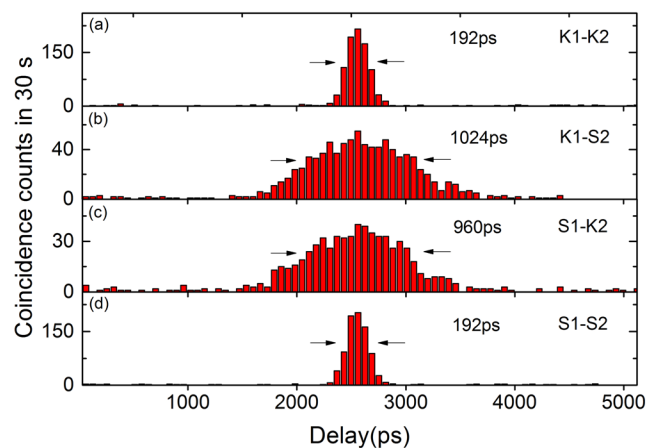


FIG. 6. A typical result of coincidence counts between two end users under four possible measurement basis combinations acquired in 30 s. (a) Coincidence counts under K1 and K2. (b) Coincidence counts under K1 and S2. (c) Coincidence counts under S1 and K2. (d) Coincidence counts under S1 and S2.

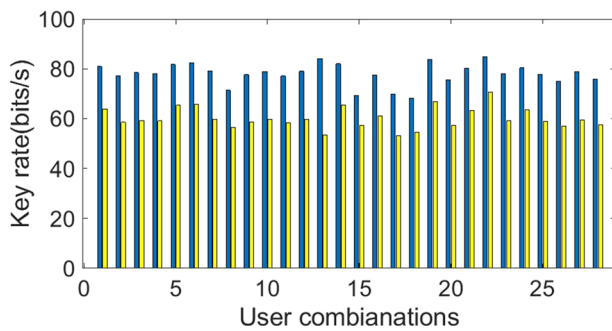


FIG. 7. Performances of symmetric DO-QKDs of all the user combinations in the subnet. The blue and yellow columns indicate the generation rates of raw keys and secure keys between any two users, respectively.

the single-photon detection events measured under K1–K2 base, the performance of raw key generation between these two users can be optimized by adjusting the parameters of the high-dimensional time encoding (please see details in [supplementary material](#)). Eventually, a raw key rate of 80.9 bits per second (bps) can be achieved with a quantum bit error rate (QBER) lower than 5% under an optimized time encoding format, which generates 4 bits of raw keys per coincidence event. On the other hand, the secure information that two users could extract per coincidence can also be calculated according to the experimental results as shown in [Fig. 6](#), by which the secure key rate between the two users after privacy amplification can be estimated to 63.7 bps (see the [supplementary material](#) for details of the analysis).

Furthermore, we measured the performances of symmetric DO-QKDs of all the user combinations in this subnet. The results are shown in [Fig. 7](#), in which the blue and yellow columns indicate the generation rates of raw keys and secure keys, respectively. Their difference is due to the costs of error correction and privacy amplification. It can be seen that any two users in the subnet can generate cryptographic keys by the symmetric DO-QKD with an average secure key rate of ~60 bps.

In the network architecture shown in [Fig. 1\(a\)](#), cryptographic key generation between users in different subnets is relied on the specific users in the central node. The two users in different subnets first generated keys with the corresponding users of their subnets in the central node by symmetric DO-QKD. Then, the central node performed a bitwise exclusive OR operation between the two keys and sent the new key via a classical channel to one of the users. Eventually, the user can decode the other one's original key by another bitwise exclusive OR operation, by which the two users share the same cryptographic keys. Finally, according to the broadband performances as shown in [Fig. 4](#), a network with 112 users (16 subnets with 7 end users per subnet) can be realized in the experimental system based on symmetric DO-QKD and the architecture shown in [Fig. 1](#).

VI. DISCUSSION

The proposed symmetric DO-QKD has two effects in this network. First, the users have the same configurations in this scheme, which make it feasible to introduce the DO-QKD into the network

based on entanglement distribution through a $1 \times N$ beam splitter. Second, the high-dimensional time encoding used in the symmetric DO-QKD is beneficial to improve the utilization of the coincidence events that are precious resources for QKD in such a network architecture with a large number of users.

The limit of this QKD network is the loss induced by the $1 \times N$ splitters and the filtering system. As the user number N increases, the photon count rates that the users receive are reduced. The count rates of the experimental system could be enhanced in some ways. First, the photon pair generation rate of the quantum light source could be improved by a higher pump level and better silicon waveguide sample with a smaller coupling loss. Second, the losses of the optical components for entanglement distribution could be reduced by optimizing the optical circuit design and realizing it by silicon photonic integration. Finally, it is clear that higher count rates require more entanglement resources, which can be achieved by distributing more correlated wavelength channels to one subnet. It requires quantum light sources with broader bandwidth. Once the count rates are increased significantly, the subnet can support more users accordingly. Besides, quantum light sources with broader bandwidth are also helpful to support more subnets, which also provide an effective way to expand the user number.

In this experiment, the fiber lengths between the central node and the end users are short under the consideration of the scenario of local networks. It can be expected that the geographical scale of this network architecture could be extended by introducing long-distance fiber transmissions with proper compensations for the fiber dispersions and fine clock distribution for time synchronization. It is also worth noting that wavelength multiplexing technology of entanglement resources provided by a broadband quantum light source is quite flexible in constituting quantum networks.^{33,43} For example, if we use part of the entanglement resources to establish the subnets and other parts of the entanglement resources to connect these subnets by entanglement distribution, a fully connected QKD network without the central trusted node would be constructed, which is preferred for the application scenarios requiring more rigorous security. On the other hand, the entanglement-based QKD networks realized in this way could also be constructed by other QKD schemes beside symmetric DO-QKD, if the users in these schemes have the same configuration, such as the E91 protocol³ based on polarization entanglement.

SUPPLEMENTARY MATERIAL

See the [supplementary material](#) for the experimental details, bin shifting process for key generation, and security testing of the system.

ACKNOWLEDGMENTS

This work was supported by the National Key R&D Program of China (Grant Nos. 2017YFA0303704, 2018YFB2200400, and 2017YFA0304000), the National Natural Science Foundation of China (NSFC) (Grant Nos. 61875101, 91750206, and 61575102), the Beijing National Science Foundation (BNSF) (Grant No. Z180012), the Beijing Academy of Quantum Information Sciences (Grant No.

Y18G26), and the Tsinghua University Initiative Scientific Research Program.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

- ¹R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM* **21**, 120–126 (1978).
- ²S. Halevi and H. Krawczyk, "Public-key cryptography and password protocols," *ACM Trans. Inf. Syst. Secur.* **2**, 230–268 (1999).
- ³A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, 661–663 (1991).
- ⁴C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.* **68**, 557–559 (1992).
- ⁵P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.* **85**, 441–444 (2000).
- ⁶S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," [arXiv:1906.01645](https://arxiv.org/abs/1906.01645) (2019).
- ⁷C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing int," in *Proceedings of IEEE International on Computers, Systems and Signal Processing*, 9–12 December 1984, Bangalore, India (IEEE, 1984), pp. 175–179.
- ⁸B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plevs, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica* **4**, 163–167 (2017).
- ⁹X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.* **94**, 230503 (2005).
- ¹⁰S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.* **108**, 130502 (2012).
- ¹¹H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.* **108**, 130503 (2012).
- ¹²V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
- ¹³P. Sibson, J. E. Kennard, S. Stanisis, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," *Optica* **4**, 172–177 (2017).
- ¹⁴S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.* **8**, 15043 (2017).
- ¹⁵Y. Tang, H. Yin, S. Chen, Y. Liu, W. Zhang, X. Jiang, L. Zhang, J. Wang, L. You, J. Guan, D. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T. Chen, Q. Zhang, and J. Pan, "Field test of measurement-device-independent quantum key distribution," *IEEE J. Sel. Top. Quantum Electron.* **21**, 116–122 (2015).
- ¹⁶C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. Ben Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, "Large-alphabet encoding for higher-rate quantum key distribution," *Opt. Express* **27**, 17539–17549 (2019).
- ¹⁷M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo qkd network," *Opt. Express* **19**, 10387–10409 (2011).
- ¹⁸H. J. Kimble, "The quantum internet," *Nature* **453**, 1023–1030 (2008).
- ¹⁹S. Pirandola, "End-to-end capacities of a quantum communication network," *Commun. Phys.* **2**, 1–10 (2019).
- ²⁰M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.* **11**, 075001 (2009).
- ²¹T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Opt. Express* **17**, 6540–6549 (2009).
- ²²T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and intercity quantum communication network," *Opt. Express* **18**, 27217–27225 (2010).
- ²³S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.* **120**, 030501 (2018).
- ²⁴S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, "Satellite-to-ground quantum key distribution," *Nature* **549**, 43 (2017).
- ²⁵J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," *Science* **356**, 1140–1144 (2017).
- ²⁶B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature* **501**, 69–72 (2013).
- ²⁷I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.* **13**, 063039 (2011).
- ²⁸P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," *Nature* **385**, 47–49 (1997).
- ²⁹S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, "Random numbers certified by Bell's theorem," *Nature* **464**, 1021–1024 (2010).
- ³⁰F. Xu, J. H. Shapiro, and F. N. C. Wong, "Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring," *Optica* **3**, 1266–1269 (2016).
- ³¹X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A* **76**, 012307 (2007).
- ³²L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," *Nat. Commun.* **3**, 1083 (2012).
- ³³A. Ciurana, V. Martin, J. Martinez-Mateo, B. Schrenk, M. Peev, and A. Poppe, "Entanglement distribution in optical networks," *IEEE J. Sel. Top. Quantum Electron.* **21**, 37–48 (2015).
- ³⁴X.-Y. Chang, D.-L. Deng, X.-X. Yuan, P.-Y. Hou, Y.-Y. Huang, and L.-M. Duan, "Experimental realization of an entanglement access network and secure multi-party computation," *Sci. Rep.* **6**, 29453 (2016).
- ³⁵I. Herbauts, B. Blauensteiner, A. Poppe, T. Jennewein, and H. Hübel, "Demonstration of active routing of entanglement in a multi-user network," *Opt. Express* **21**, 29013–29024 (2013).
- ³⁶A. Price, "Pragmatic quantum cryptography in next-generation photonic networks," Ph.D. thesis, University of Bristol, 2019.

- ³⁷S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, “An entanglement-based wavelength-multiplexed quantum communication network,” *Nature* **564**, 225–228 (2018).
- ³⁸S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, Ž. Samec, L. Kling, A. Qiu *et al.*, “A trusted-node-free eight-user metropolitan quantum communication network,” [arXiv:1907.08229](https://arxiv.org/abs/1907.08229) (2019).
- ³⁹X. Liu, X. Yao, H. Wang, H. Li, Z. Wang, L. You, Y. Huang, and W. Zhang, “Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km,” *Appl. Phys. Lett.* **114**, 141104 (2019).
- ⁴⁰J. D. Franson, “Nonlocal cancellation of dispersion,” *Phys. Rev. A* **45**, 3126–3132 (1992).
- ⁴¹J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, “High-dimensional quantum key distribution using dispersive optics,” *Phys. Rev. A* **87**, 062322 (2013).
- ⁴²C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, “Entanglement-based quantum communication secured by nonlocal dispersion cancellation,” *Phys. Rev. A* **90**, 062331 (2014).
- ⁴³Y. Li, Y. Huang, T. Xiang, Y. Nie, M. Sang, L. Yuan, and X. Chen, “Multiuser time-energy entanglement swapping based on dense wavelength division multiplexed and sum-frequency generation,” *Phys. Rev. Lett.* **123**, 250505 (2019).