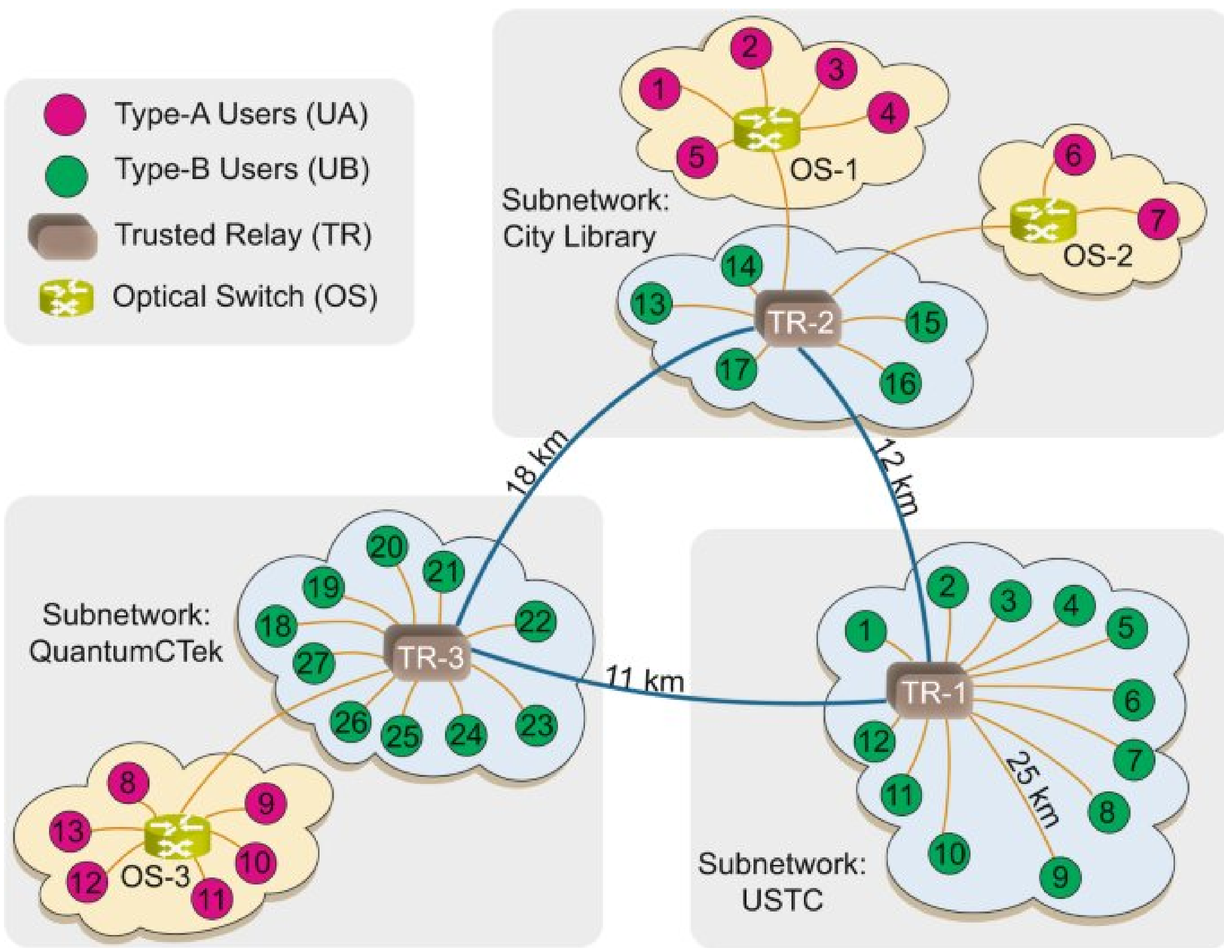
Implementing a 46-node quantum metropolitan area network

September 30 2021, by Thamarasee Jeewandara



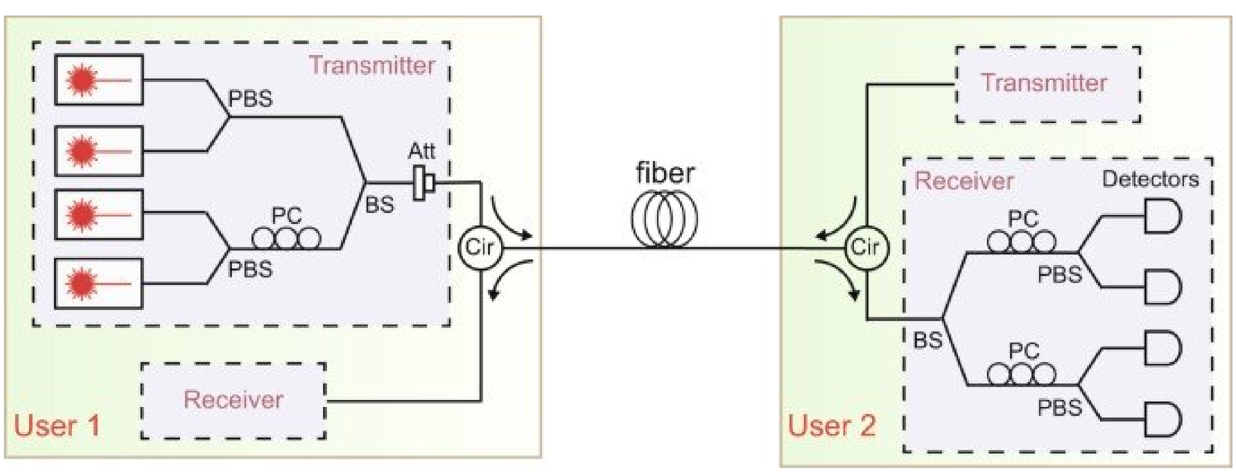
The topological structure of our quantum network. The network mainly comprises three subnetworks that are directly connected to each other. In each subnetwork, there are multiple users connected to intermediate nodes in different ways, either by an all-pass optical switch (OS) or by a trusted relay (TR). Users connected by a switch are denoted as red dots (Type-A Users, UA), holding both a quantum transmitter and a receiver. Users connected to a trusted relay are denoted as green dots (Type-B Users, UB), only holding a quantum transmitter. Specifically, UA-1 to UA-5 are connected to OS-1, UA-6 and UA-7 are connected to OS-2, UA-8 to UA-13 are connected to OS-3, UB-1 to UB-12 are connected to TR-1, UB-13 to UB-17 are connected to TR-2, and UB-18 to UB-27 are connected to TR-3. Credit: Nature Quantum Information, 10.1038/s41534-021-00474-3

Quantum key distribution (QKD) is a method used for secure or secret key exchanges between two remote users. Using secure communication, cyberscientists ultimately aim to establish a global quantum network. Existing field tests suggest that such quantum networks are feasible. To achieve a practical quantum network, several challenges must be overcome including the realization of varied topologies at large scales, simple network maintenance and robustness to node failures. In a new report now published on *Science Advances*, Teng-Yun Chen and a research team in quantum physics, quantum information and interdisciplinary information sciences in China, presented a field operation of a quantum metropolitan area network with 46 nodes. They realized diverse topological structures and ran the network for 31 months via standard equipment. They then realized QKD pairing and key management for secure communications including real-time voice telephone, text messaging and file transmission with one-time pad encryption to support 11 pairs of users to make simultaneous audio calls. The technique can be combined with an intercity quantum backbone and via ground-satellite links to form a global quantum network.

Global quantum network

In this work, Chen et al. constructed a 46-node quantum metropolitan-area network throughout the city of Hefei. Quantum key distribution

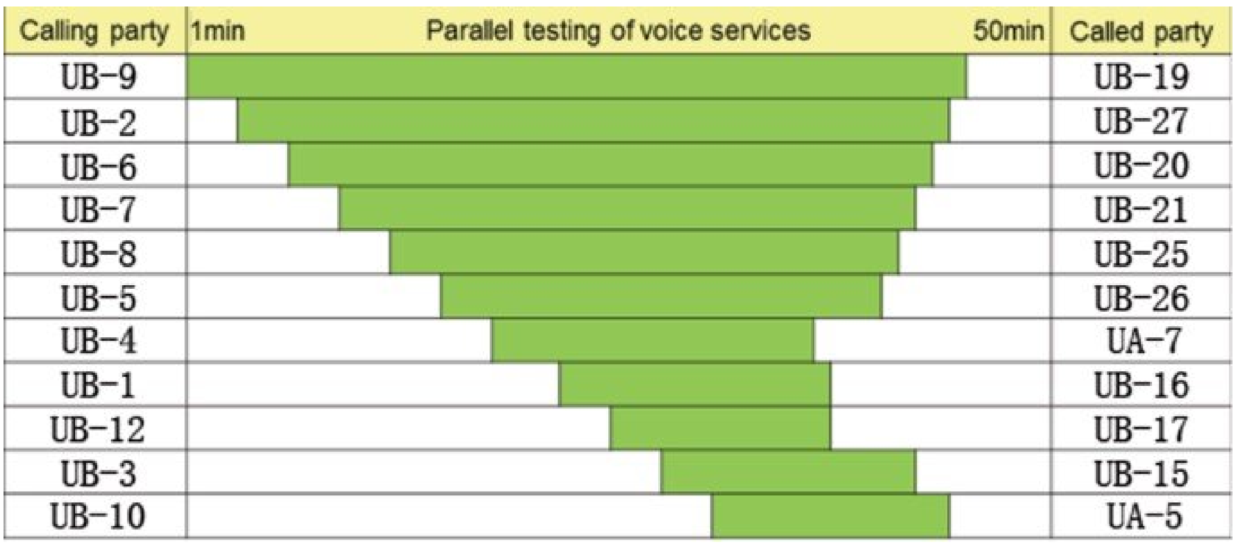
(QKD) ultimately aims to construct a global quantum network where communication traffics have information-theoretic security guarantees. A global QKD network can maintain two types of links including the ground network and satellite network, where the ground network can be further divided into a backbone, metropolitan and access networks to cover intercity distance and fiber-to-home distances. Researchers have studied the feasibility of the QKD between two users through long-distance free space, telecom fibers and simulated ground-satellite links. Examples of the field tests of QKD networks that are already realized include a three-user network by DARPA, a six-node network in Europe, the SwissQuantum network as well as a mesh-type six-node network in Tokyo. The satellite network provided a promising method to realize intercontinental, secure communication as a result of low transmission attenuation in space while serving as a trusted relay to connect remote user nodes or subnetworks. Scientists had recently implemented a large-scale satellite network containing four metropolitan-area networks, a backbone network and two satellite-ground links. However, these QKD experiments and networks are still preliminary, the team therefore addressed the challenges surrounding the realization of a large-scale practical QKD network.



A schematic for the QKD set-up. There are four laser sources in the transmitter emitting four corresponding polarization states in the BB84 protocol. The polarization is modulated via the PBS and the PC, and the average light intensity is modulated via the attenuator. Each laser produces three light pulses with different intensities including signal, decoy and vacuum states. The signal and decoy states contain mean photon numbers of 0.6 and 0.2 per pulse, respectively, and the ratio between the signal, decoy, and vacuum states is 6:1:1. The optical misalignment is less than 0.5%. In the detection side, a four-channel InGaAs single-photon detector is integrated with the following parameters. The detection efficiency is 10%, the dark count is 10−6, the dead time is 2 μs, the afterpulse probability is less than 0.5% and the effective gate width is 500 ps. The receiver detects the light signal with the PC as a polarization feedback. The Cir is used to realize transmission and reception of light signals simultaneously. BS: beam splitter; PBS: polarizing beam splitter; PC: polarization controller; Att: attenuator; Cir: circulator. Credit: Nature Quantum Information, 10.1038/s41534-021-00474-3

Building a 46-node quantum metropolitan-area network

Chen et al. built a 46-node quantum metropolitan-area network to connect 40 user nodes, three trusted relays and three optical switches, throughout Hefei. The network covered the entire urban area and connected several organizations within the city districts including governments, banks, hospitals, and research universities. They first reviewed the basic topological structures in a network where the most robust method used a fully connected topology where each user was directly connected to every other user in the network. The type of network did not require the users to trust one another. User nodes can also be connected via a central switch in a star-like network, where two users can build secure keys with a sufficient number of trusted relays. For instance, the Shanghai-Beijing backbone used this technique; however, the disadvantage is that the users must trust the relay. Chen et al. constructed three subnetworks in USTC, QuantumCTek and the City Library that are distributed 15 km apart.



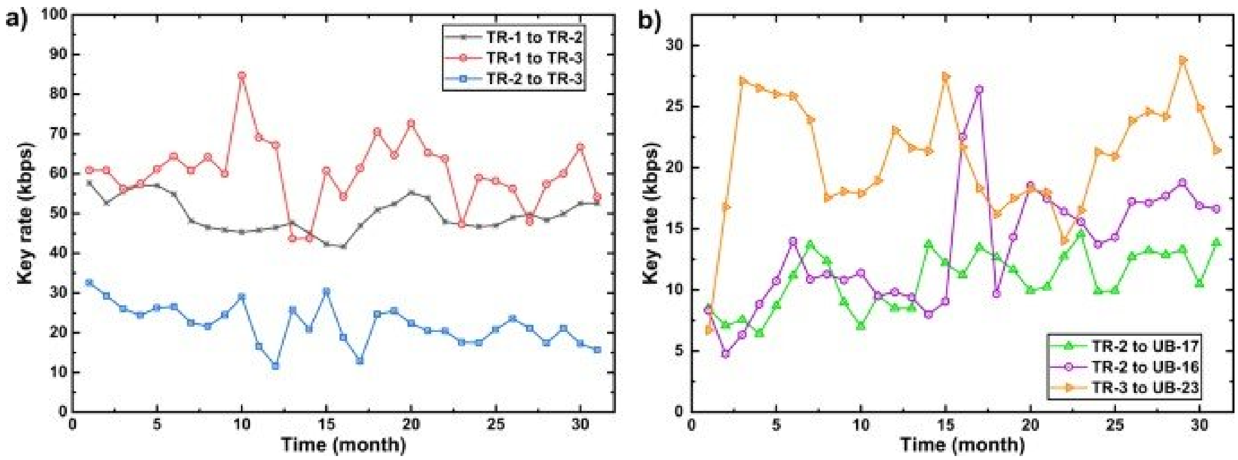
Twenty-two users simultaneously make calls with QKD protocols. The green areas represent the duration over which users make calls. Credit: Nature Quantum Information, 10.1038/s41534-021-00474-3

Network topology and standard QKD equipment

The researchers realized two basic types of topological connection structures including the full connection between three subnetworks and star-like connections for local access networks. During the experiments, the team used an optical switch known as a trusted node at the center of the star-like subnetwork. Using the trusted node, they assigned classical keys between users to function as a classical router, while the all-pass optical switches acted as quantum routers to redistribute quantum signals. Based on the setup, any two users could communicate directly without interfering with other users. Chen et al. further developed a type of switch module comprising four input and eight output ports, the other contained a 16-port switch that enabled eight pairs of users to communicate simultaneously. The team used a protocol to generate secret keys between directly connected users and trusted relays. If one user had a quantum transmitter and the other had a quantum receiver, they could generate keys. The platform therefore contained two types of users; those directly connected to a switch containing both a transmitter and receiver, and users directly connected to a trusted relay with only a quantum transmitter. As a result, the scientists used two types of equipment; one to transmit signals and another to transmit and receive signals at the same time. After basis reconciliation and error correction, they standardized the QKD equipment to greatly reduce the number of devices used.

Designing a switching strategy: Applications and robustness of the network

Chen et al. developed a key management process to allow users to generate keys in high priority. To accomplish this, they designed a switching strategy based on the number of keys stored in the local memories for the users. They then connected a 16-port optical switch to 16 users to obtain a total of 120 possible key-pairing schemes by which two users could be connected for the QKD process for a switching time ranging from 10 to 60 minutes. To join the network, a new user first had to send a heartbeat frame from their QKD device to the key management server for authentication to then que the device to generate keys. For security, the team followed the standard decoy-state BB84 security analysis and generated the secret key rate of the BB84 quantum key distribution protocol. Based on the application of the network, the users made use of the generated secure keys to transfer information confidently. Using the network, Chen et al. transmitted encrypted information, including real-time voice telephone, instant messaging, and digital files with the one-time pad encryption method. The total delay in the encryption process was less than 50 μs. When the researchers tested the capacity of the network for 50 minutes, all 22 users could simultaneously make calls for six minutes, within the quantum network. To test the stability and robustness of the system, they continuously ran the network for 31 months.



The key rates versus time for some representative links. (a) The key rates between the three trusted relays. (b) The key rates between trusted relay and user. In the robustness test, 11 user nodes have continuously run for 31 months. The key rates are recorded every 30 s and taken average over a month. The detailed key rates are given in Supplementary Tables V and VI. Credit: Nature Quantum Information, 10.1038/s41534-021-00474-3

Outlook

In this way, Teng-Yun Chen and colleagues developed a practical and large-scale metropolitan quantum key distribution (QKD) network with commercial QKD products for practical use in Hefei, China. The team could scale the quantum network by adding more users and relays to connect to the Shanghai-Beijing backbone as a national network. The network can also be combined with other QKD protocols to overcome imperfections of measurement devices for efficient and secure communication.

More information: Teng-Yun Chen et al, Implementation of a 46-node quantum metropolitan area network, *npj Quantum Information* (2021). DOI: 10.1038/s41534-021-00474-3

Sebastian Nauerth et al, Air-to-ground quantum communication, *Nature Photonics* (2013). DOI: 10.1038/nphoton.2013.46