PHOTONICS Research

Round-trip multi-band quantum access network

Yuehan Xu,[1] Tao Wang,[1,2,3,4] Huanxi Zhao,[1] Peng Huang,[1,2,3] and Guihua Zeng[1,2,3,5]

[1]State Key Laboratory of Advanced Optical Communication Systems and Networks, Center of Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China
[2]Shanghai Research Center for Quantum Sciences, Shanghai 201315, China
[3]Hefei National Laboratory, CAS Center for Excellence in Quantum Information and Quantum Physics, Hefei 230026, China
[4]e-mail: tonystar@sjtu.edu.cn
[5]e-mail: ghzeng@sjtu.edu.cn

Received 4 April 2023; revised 12 June 2023; accepted 20 June 2023; posted 21 June 2023 (Doc. ID 492448); published 1 August 2023

The quantum network makes use of quantum states to transmit data, which will revolutionize classical communication and allow for some breakthrough applications. Quantum key distribution (QKD) is one prominent application of quantum networks, and can protect data transmission through quantum mechanics. In this work, we propose an expandable and cost-effective quantum access network, in which the round-trip structure makes quantum states travel in a circle to carry information, and the multi-band technique is proposed to support multi-user access. Based on the round-trip multi-band quantum access network, we realize multi-user secure key sharing through the continuous-variable QKD (CV-QKD) protocol. Due to the encoding characteristics of CV-QKD, the quadrature components in different frequency bands can be used to transmit key information for different users. The feasibility of this scheme is confirmed by comprehensive noise analysis, and is verified by a proof-of-principle experiment. The results show that each user can achieve excess noise suppression and 600 bit/s level secure key generation under 30 km standard fiber transmission. Such networks have the ability of multi-user access theoretically and could be expanded by plugging in simple modules. Therefore, it paves the way for near-term large-scale quantum secure networks.

https://doi.org/10.1364/PRJ.492448

1. INTRODUCTION

A quantum network is an interconnected network that makes use of the properties of quanta to transmit data, and could revolutionize ways of information exchange in the future [1]. The quantum network [2] has many breakthrough applications, such as a quantum secure network through quantum key distribution (QKD) [3–10] or quantum secure direct communication [11,12]. In addition, it can also perform tasks impossible in classical physics, such as distributed quantum computing [13] and accurate global timing [14], whcih will bring accurate navigation and Earth sensing. Moreover, the quantum network could even lead to accurate telescopes [15] and new fundamental tests of quantum nonlocality, quantum teleportation [16], and quantum gravity [17].

QKD is one prominent application of quantum networks, and is the core technology of quantum secure communication [18]. It can provide secure keys for legal parties even in the presence of eavesdroppers, and its theoretical security is guaranteed by the basic principles of quantum mechanics [19]. The QKD protocol can be divided into discrete-variable QKD (DV-QKD) [20] and continuous-variable QKD (CV-QKD) [21–42] according to the physical quantity that carries key information. According to the quantum technology roadmap released by OIDA [43], point-to-point QKD has been matured to build networks and gradually commercialized [44–64]. A representative quantum secure network is the Beijing–Shanghai trunk line [65], which achieves quite long distance transmission. In addition, the Cambridge quantum metropolitan area network is constructed with high bandwidth data transmission [66]. Furthermore, quantum networks in the United Kingdom have been operating for several years with three nodes separated by 5–10 km optical fiber [67]. The 46-node quantum metropolitan area network in Hefei realizes real-time voice telephone, text messaging, and file transmission [68]. For multi-user access, the quantum access network (QAN) proposed by Fröhlich *et al.* [69] is the first scheme to realize the upstream QAN between users and a common node.

The physical implementation of a quantum network for QKD is an important issue. On one hand, constructors need to consider the coverage of the quantum network, which can be divided into backbone networks, metropolitan area networks, and access networks. On the other hand, builders should also be concerned with quantum network topologies, such as star, tree, and mesh. For different coverages and topologies, the physical structure of the quantum network is a vital issue. Considering the preparation and measurement of quantum states by multi-users, the quantum states generated from

different sources require a large number of detectors, while those generated from the same source will interfere with each other and be difficult to separate. An alternative scheme is to build large-scale networks based on the mature point-to-point QKD system. However, limited by its complexity, this scheme cannot support access services for such a large number of users. Therefore, a new type of quantum network architecture needs to be proposed to simplify the original complex network with multi-user access.

Therefore, we propose an expandable and cost-effective quantum network physical structure, called round-trip multi-band QAN (RM-QAN), to improve network performance and support multi-user access. The RM network structure utilizes quantum states traveling in a circle to transmit data, and uses the frequency division multiplexing (FDM) technique to isolate different users. In RM-QAN, each user requires only one modulator and one circulator when plugging into the network. In addition, only one laser and one detector are needed to build the entire network, which is flexible and cost effective. Such networks could theoretically support multi-user access without performance penalty, and network users can achieve 600 bit/s level quantum secure key generation under 30 km network range. Moreover, network scalability and noise suppression are excellent, which is a promising solution for building near-term multi-user quantum secure networks.

In this paper, our RM-QAN scheme is introduced in detail. First, we describe the physical structure of RM-QAN and expound upon its advantages. In addition, we use RM-QAN to realize CV-QKD and evaluate the performance of QKD through a complete noise analysis. Based on this physical structure, we construct a proof-of-principle experimental platform and verify the feasibility of multi-user secure key sharing. Finally, we provide a conclusion.

2. RESULT

A. Physical Structure of RM-QAN

Our RM-QAN physical structure is described as follows. In the QAN, the quantum network unit (QNU) is the device held by the user, which corresponds to the optical network unit (ONU) [70–72] in the optical access network. The QNU does not need to be responsible for receiving light in our scheme, nor does it need to be responsible for generating light sources. Instead, QNU needs only to modulate the key information. It reduces the overall system cost of the QAN. The work of generating and receiving light is all done by the quantum line terminal (QLT). QLT is the terminal equipment used to connect quantum trunks, which corresponds to the optical line terminal (OLT) [70–72] in the optical access network. Notably, QLT serves as a terminal in the QAN, distinct from its function as a relay. In this scheme, multiple QNUs share their respective keys with the same QLT. The round-trip structure is divided into two stages. First, the optical carrier is transmitted from the QLT side to the QNU side. There is a loss of $1/N$ in this part, but it is not involved in the transmittance of QKD. Second, the optical carrier is transmitted from the QNU side to the QLT side. Light transmitted to the QLT side is brought together from signals of all users. There is also a loss of $1/N$ in this part, which is involved in the transmittance of QKD. Therefore, the multi-user quantum network can be completed with one laser and one detector, which is more efficient than other schemes. In our scheme, according to the upstream transmission direction, it can be understood that QNU is Alice and QLT is Bob in the classical scheme.

For a single user, this QKD scheme is actually a plug-and-play QKD architecture. The plug-and-play scheme was proposed in Ref. [73] and experimentally verified in DV-QKD [74–76] and CV-QKD [77]. In addition, the plug-and-play scheme has corresponding commercial QKD systems [78]. For security, QNU can further randomize the global phase of each pulse, measure the incoming intensity, and introduce sufficient attenuation, and the standard security proofs of a one-way system can be used [79], which has been used in the CV case [77].

FDM is a multiplexing technology that modulates multiple baseband signals to different frequency carriers and then superimposes them to form a composite signal. The FDM method is like a "frequency modulation (FM) radio system," which can be tuned to different frequencies to receive information from different sources. In the implementation, since the quadrature components can be modulated on different frequency bands, they can be used to transmit the quantum key [52,53], and therefore the FDM method can be adopted for multi-user key distribution. Time division multiplexing (TDM) is an alternative scheme, but it has a high requirement of time slot control. The principle of our scheme is described in detail below.

As can be seen from the schematic diagram of RM-QAN in Fig. 1, there are multiple QNUs corresponding to one QLT. First, a continuous wave is generated and transmitted by QLT in the optical layer. Then, it is divided into N pieces through an N:1 splitter, which does not carry any data. After receiving light, QNU will conduct secure key modulation through a radio frequency (RF) signal, which carries the information on different frequency bands, and can be distinguished clearly on the spectrum. QNU selects the number $k \in \{0,1,2,3\}$ to form a random sequence of length n with equal probability. Then QNU prepares n coherent states according to the random sequence. The ith coherent state can be expressed as

$$|\alpha_k\rangle = |\alpha e^{i(2k+1)\pi/4}\rangle, \quad i \in \{0,1,\cdots,n\}, \tag{1}$$

where $\alpha^2 = V_{\mathrm{QNU}}/2 = V_{\mathrm{A}}/2$. V_{QNU} is the modulation variance of QNU in our scheme. Since QNU is equivalent to Alice, all V_{QNU} below are replaced by the more familiar expression V_{A}. Assuming that the carrier frequency registered for the first QNU is A MHz and the carrier frequency interval of adjacent QNUs is B MHz, the carrier frequency modulated by the second QNU can be expressed as $A + B$ MHz. Similarly, the carrier frequency modulated by the Nth QNU is $A + N \cdot B$ MHz. In the modulation process, the original signal k is separated into two groups of information a and b in binary, where a represents the first binary number, and b represents the second binary number. Then, the baseband signal is modulated according to the corresponding carrier frequency of each QNU. Therefore, the transmitted signal can be represented by

$$f(t) = a\,\sin(\omega t) + b\,\cos(\omega t), \tag{2}$$

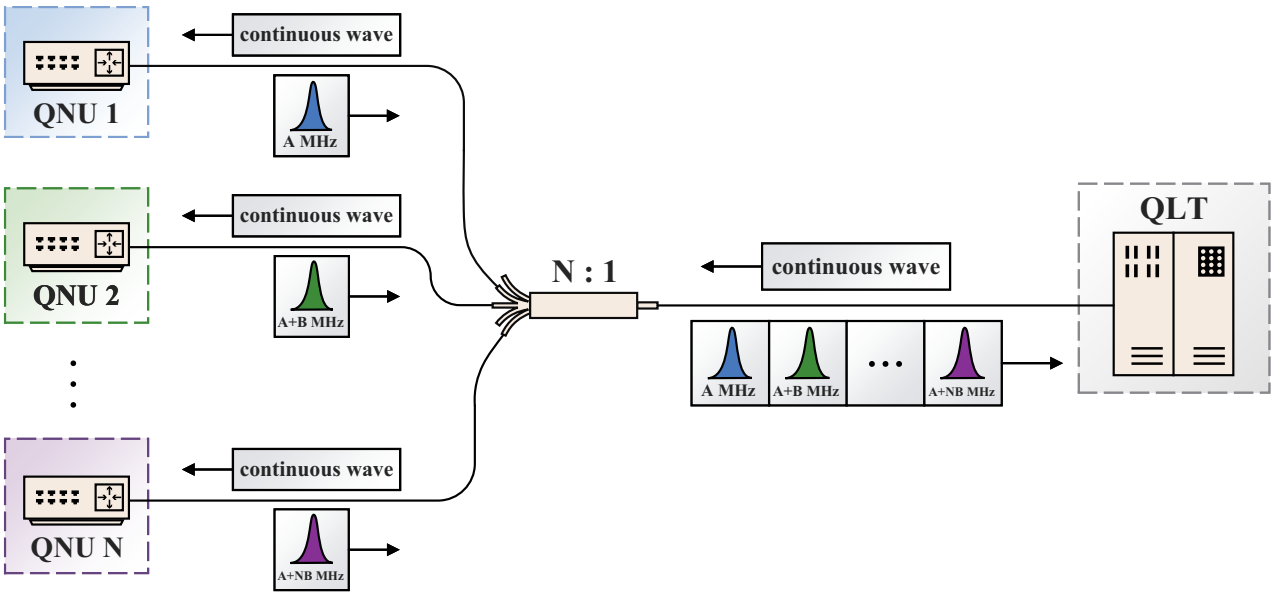


Fig. 1. Schematic diagram of the round-trip multi-band quantum access network (RM-QAN). First, a continuous wave is generated and transmitted by the quantum line terminal (QLT). Then, the continuous wave is divided into N pieces through an N:1 splitter. The quantum network unit (QNU) modulates the key information on different carrier frequencies to be distinguished clearly on the spectrum. Then the key is transmitted back through the round-trip structure, and the modulated signal light is returned to the splitter. Finally, the signal light is passed back to the QLT, which demodulates the received signal.

where ω is the carrier frequency, and t is the time series. The advantage of this modulation method is that the signal can keep a four-state orthogonal form. Then the key is transmitted back through the round-trip structure, and the modulated signal light is returned to the splitter. The signal light modulated by each QNU is gathered together by the splitter to form a signal light containing N frequency bands. Finally, the signal light is passed back to the QLT through the round-trip structure.

After receiving through a coherent receiver, QLT will get a mixed multi-band spectrum, in which the information is indistinguishable in the time domain but can be clearly distinguished in the frequency domain. QLT first checks all bands that QNU has registered. When accessing the network, each QNU needs to register its frequency band, i.e., carrier frequency. QLT checks the registered bands to see which QNU is currently communicating. This registration method can effectively prevent Eve from using illegal frequency bands to obtain information. For these bands, QLT uses bandpass filtering to separate them. Then, QLT performs the first phase shift recovery for the information, which addresses the optical phase drift during signal transmission. After that, since the key obtained at this time still carries out spectrum shifting, QLT needs to remove its carrier by coherent demodulation for each QNU. Coherent demodulation can obtain baseband signals $g_a(t)$ and $g_b(t)$. The formula of coherent demodulation is

$$g_a(t) = f(t)\sin(\omega t) = \frac{b}{2}\sin(2\omega t) - \frac{a}{2}\cos(2\omega t) + \frac{a}{2},$$
$$g_b(t) = f(t)\cos(\omega t) = \frac{a}{2}\sin(2\omega t) + \frac{b}{2}\cos(2\omega t) + \frac{b}{2}, \quad (3)$$

where ω is the carrier frequency, and t is the time series. Then $g_a(t)$ and $g_b(t)$ are low pass filtered to obtain the baseband signal for each QNU. After that, QLT downsamples the obtained data according to the symbol rate. QLT then performs a second phase shift recovery to complete the original data restoration. The second recovery is because the data may have rotation as a whole due to the phase of the RF signal, and the original data need to be obtained by the inverse operation as a whole. Finally, QLT does the frame synchronization for data alignment.

To prove that the interference between each user's signal does not exist, assume that

$$E_{SN}(t) = A_{SN}\cos(\omega_{SN}t + \phi_{SN}),$$
$$E_{\mathrm{L}}(t) = A_{\mathrm{L}}\cos(\omega_{\mathrm{L}}t + \phi_{\mathrm{L}}), \quad (4)$$

where E_{SN} represents the signal of the Nth user, E_{L} represents the local oscillator (LO), A_{SN} and A_{L} denote power, $\omega_{SN} = \omega_{\mathrm{O}} + \omega_N$ and $\omega_{\mathrm{L}} = \omega_{\mathrm{O}}$ are the frequency, ω_{O} represents the frequency of light, ω_N represents the carrier frequency of the Nth user, ϕ_{SN} and ϕ_{L} represent the phase, and t denotes the time series. The output optical power after coherent detection is

$$\begin{aligned} P &= K(|E_{\mathrm{S1}} + \cdots + E_{SN} + E_{\mathrm{L}}|^2 - |E_{\mathrm{S1}} + \cdots + E_{SN} - E_{\mathrm{L}}|^2) \\ &= 4K\sum_{i=1}^{N}[A_{\mathrm{S}i}A_{\mathrm{L}}\cos(\omega_{\mathrm{S}i}t + \phi_{\mathrm{S}i})\cos(\omega_{\mathrm{L}}t + \phi_{\mathrm{L}})] \\ &= 2K\sum_{i=1}^{N}\sqrt{P_{\mathrm{L}}P_{\mathrm{S}i}}\{\cos(\omega_i t + \phi_{\mathrm{S}i} - \phi_{\mathrm{L}}) \\ &\quad + \cos[(2\omega_{\mathrm{O}} + \omega_i)t + \phi_{\mathrm{S}i} + \phi_{\mathrm{L}}]\}, \end{aligned} \quad (5)$$

where K is the coefficient of photoelectric conversion. Therefore, the beat frequencies between different users' signals

are eliminated after coherent detection. The frequency of the latter term $\sum_{i=1}^{N}\cos[(2\omega_O+\omega_i)t+\phi_{Si}+\phi_L]$ is far beyond the bandwidth of the detector and cannot be detected. Only the former term $\sum_{i=1}^{N}\cos(\omega_i t+\phi_{Si}-\phi_L)$ still exists. In conclusion, interference between different users does not exist after coherent detection.

This round-trip structure is mainly vulnerable to Eve's practical security attacks, including the phase remapping attack [80,81] and the Trojan-horse attack [79]. For the phase remapping attack, the effective solutions are that QNU checks the arrival time of the reference pulse and the signal pulse by monitoring, verifying that she is applying the correct modulations to her states [80]. For the Trojan-horse attack, since we cannot use the isolator in the two-way structure, the filter can be used to exclude the eavesdropper's input light [79]. In addition, there are three technical countermeasures: (1) installing a watchdog detector with a switch at the entrance of QLT that randomly routes a small fraction of incoming signals to this detector; (2) opening the door for Eve for a smaller time duration; (3) reducing the width of phase modulation voltage pulse [82]. Certainly, from a theoretical perspective, a higher amount of privacy amplification can help QNU and QLT to destroy the partial information of Eve. We need to estimate the maximum leakage due to Trojan-horse attacks, and incorporate these elements in the security proof [79,83,84].

The RM physical structure has many advantages compared with downstream and upstream QANs. In the downstream QAN, the transmitters are located at QLT, while the receivers are located at QNU [85]. This downstream scheme has two major disadvantages. First, each QNU in the network requires a detector, which is normally expensive and difficult to operate. Second, it is impossible to locate the data of each user certainly. Therefore, all detectors must run at the same speed as the transmitter to avoid missing the key, which means that most of the detector's bandwidth is unused. In the upstream QAN, QNU is responsible for transmitting the key, and QLT is responsible for receiving the key [69]. The upstream scheme still requires multiple laser sources to prepare a quantum signal, which is difficult for ordinary users to afford. In addition, the network capacity has to be determined before building the upstream QAN.

RM-QAN solves the above issues well. In our scheme, each QNU needs only one modulator and one circulator to plug into the network, and the entire network requires only one laser and one detector, which is efficient. Moreover, the bandwidth of the detector is fully used due to FDM. In addition, network scalability and noise suppression are wonderful, which means a large number of users can easily access it at any time.

B. CV-QKD Based on RM-QAN

1. Secret Key Rate

In the following, we evaluate the reachable secret key rate under the RM-QAN for discrete modulation coherent state (DMCS) CV-QKD [34]. The formula of the secret key rate for unit system repetition frequency is in Appendix A. For the practical CV-QKD system, the secret key rate K_s can be calculated as

$$K_s = RK_p, \tag{6}$$

where R is the repetition frequency of the CV-QKD system. The excess noise is the untrusted noise in the system. Through the physical noise analysis in Section 3, the excess noise of the RM-QAN can be described as

$$\varepsilon = \varepsilon_{RB}+\varepsilon_{FC}+\varepsilon_{OC}+\varepsilon_{MO}+\varepsilon_{AM}+\varepsilon_{PH}. \tag{7}$$

In Eq. (7), ε_{RB} represents the noise introduced by Rayleigh backscattering. ε_{FC} denotes the noise introduced by the frequency cross talk, which is caused by photons leaking from other frequency bands. In addition, ε_{OC} represents the noise introduced by the imperfection of the optical circulator, especially concerning the isolation and directionality. ε_{MO} is the modulation noise caused by the uncertainty of modulation voltage. The change in the number of photons caused by spontaneous radiation will be reflected in the amplitude of the laser, forming amplitude noise ε_{AM}. The spontaneous radiation of the laser causes not only a change of intensity but also a random change in the frequency of the laser pulse signal, forming phase noise ε_{PH}. Specific theoretical derivation values of each noise component can be found in Section 3.A.

Other parameters are quantum efficiency $\eta = 0.42$, electrical noise $v_{el} = 0.18$, reconciliation efficiency $\beta = 0.97$, modulation variance $V_A = 0.5$ SNU, and repetition frequency $R = 1$ MHz. The N:1 splitter on the return path can introduce $1/N$ loss on each arm, thereby reducing the secret key rate of all users, and transmittance will change to $T = 10^{-\alpha L/10}/N_S$, where N_S is the branch number of the N:1 splitter. In the next step, we can introduce high speed optical switches to eliminate the loss caused by the splitter. The comparison diagram of the secret key rate between this scheme of different network capacities N and other classical schemes is shown as Fig. 2.

In Fig. 2, the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound has the farthest transmission distance when

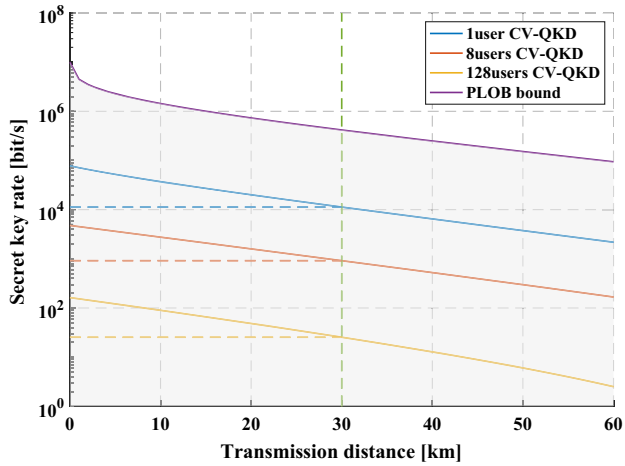


Fig. 2. Comparison diagram of secret key rate between this scheme of different network capacities and other classical schemes. Parameters are set as $\eta = 0.42$, $v_{el} = 0.18$, $\beta = 0.97$, $V_A = 0.5$ SNU (shot noise unit), $R = 1$ MHz. It describes the change of secret key rate at different transmission distances in the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound and round-trip multi-band continuous-variable quantum key distribution (CV-QKD) with different users, where the ordinate value corresponding to the dotted line is the secret key rate under the condition of 30 km achieved in theory.

the secret key rate is determined without a repeater and the highest secret key rate when the transmission distance is determined [86]. The curve of CV-QKD in different users is the relationship between the secret key rate and the distance corresponding to the different network capacities of RM-QAN. As can be seen from the figure, the secret key rate of all schemes decreases with the increase of transmission distance. Our scheme does not exceed the limit of PLOB under the same transmission distance. In addition, when the network capacity increases, the secret key rate decreases due to the gradual increase of optical circulator noise and frequency cross talk noise. The secret key rate will decrease obviously with the increase of network capacity, since the assumed eavesdropper Eve can obtain $(N-1)/N$ signal, resulting in the increase of maximum information that Eve can get. However, RM-QAN can still support the encoding of 128 users. It conforms to the concept of "the last kilometer" multi-access network.

2. Network Capacity

Network capacity is defined as how many users the network system can support and is mainly affected by the branch number of the N:1 splitter. The network capacity of RM-QAN is also affected by noise. The physical noise analysis in Section 3 shows that only optical circulator noise and frequency cross talk noise are related to network capacity N. When network capacity is small, frequency cross talk noise is the main component of excess noise. However, when network capacity is large, frequency cross talk noise tends to be constant, and optical circulator noise is the main part of the noise. According to previously calibrated parameters, the relationship among network capacity, transmission distance, and secret key rate is shown in Fig. 3.

In Fig. 3, the abscissa represents the transmission distance, the ordinate represents network capacity, and the color legend on the right of the graph represents the value of the secret key rate of each user, which decreases gradually from red to blue. Different network capacity scenarios are distinguished in Fig. 3 due to the varying transmittance attenuation caused by different splitting ratios, resulting in a direct effect on the secret key rate of users. As can be seen from Fig. 3, when network capacity is determined, the secret key rate decreases gradually with the increase of transmission distance. When the transmission distance is determined, the secret key rate decreases with the increase of network capacity. When users are added, the change of excess noise is small, and the secret key rate of each user remains almost constant. Certainly, if the detector bandwidth is not high enough, the number of users will be mainly limited by the detector bandwidth under the FDM scheme. If the number of users is larger, QLT requires higher output optical power to ensure that QNU achieves a certain output modulation variance, and we can use a high output power laser. It reflects that the RM quantum network scheme can accept a high network capacity without a performance penalty. In practical implementation, to achieve more accurate modulation variance adjustment, the light entering QNU and the total optical power will be larger, so network capacity will decrease. If network capacity is determined, the secret key rate of each user will be stable and not affected when more users access this network. In addition, our scheme needs only an optical circulator and a phase modulator (PM) to plug in a user, which has a low cost requirement for new users to access and a small impact on the secret key rate of each existing user. In conclusion, this scheme has high practicability.

C. Experiment Verification

1. Experimental Setup

The optical structure of RM-QAN used in the experiment is shown in Fig. 4. First, the light generated by the laser of QLT is divided into two parts by a beam splitter (BS) with a 2:1 ratio. The laser we use in the experiment has a very narrow linewidth, typically 100 Hz. Therefore, the interval between light before transmission and after transmission is less than the coherent length of the laser. On this basis, we realize homodyne detection, which means the beat frequency is zero. Light of higher power acts as the LO of the system. Light of lower power passes through a variable optical attenuator (VOA) to the optical circulator. The function of QLT's VOA is to weaken light into appropriate optical power. Light is transmitted from port1 to port2 of the optical circulator and to the 30 km optical fiber spool. Afterward, the continuous wave laser is transmitted to a BS through the optical fiber spool. Then the light is evenly divided into eight QNUs by BS with a ratio of 8:1. Due to the limitation of modulated RF signal ports, we connected three QNUs in one experiment and verified the experimental

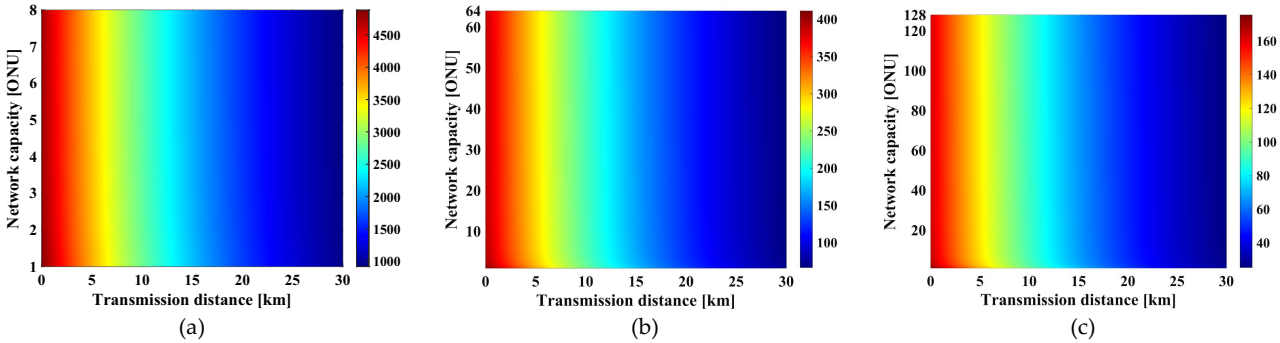


Fig. 3. Relationship among network capacity, transmission distance, and secret key rate. Parameters are set as $\eta = 0.42$, $v_{el} = 0.18$, $\beta = 0.97$, $V_A = 0.5$ SNU, $R = 1$ MHz. It describes the change of secret key rate at different transmission distances and different network capacities. The legend on the right shows the value of the secret key rate of each user. (a) Network capacity is eight. (b) Network capacity is 64. (c) Network capacity is 128.

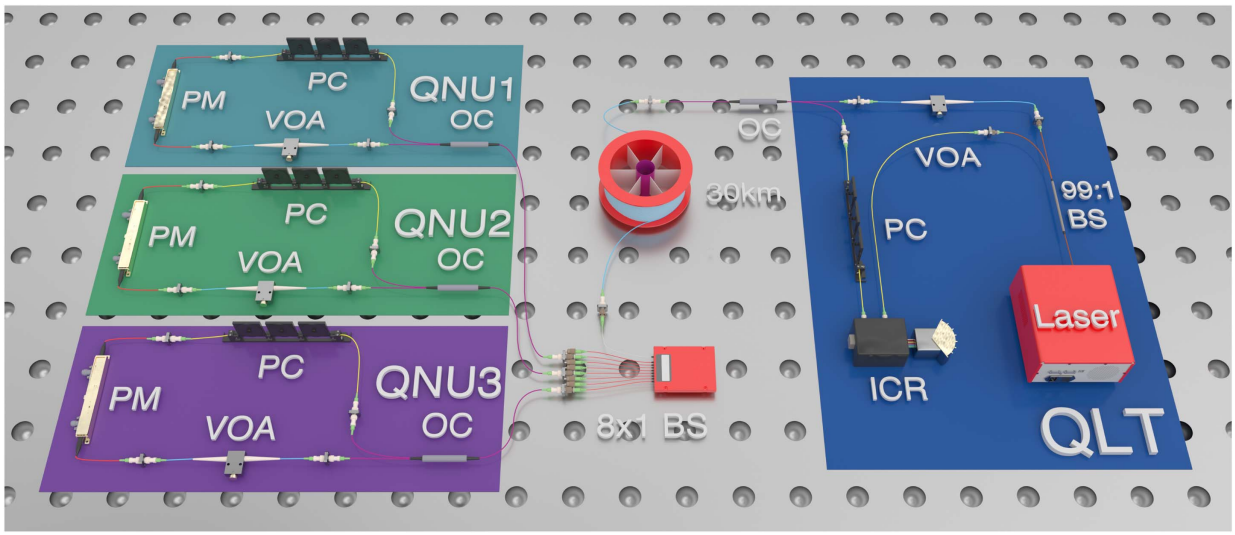


Fig. 4. Optical configuration of the round-trip multi-band scheme. First, the light transmitted by the laser of QLT is divided into two parts by a beam splitter (BS) with a 2:1 ratio. The light of higher power acts as the local oscillator (LO) of the system. The light of lower power passes through a variable optical attenuator (VOA) to the optical circulator. Light is transmitted from port1 to port2 of the optical circulator and to the 30 km optical fiber spool. Afterward, a continuous wave is transmitted to a BS through the optical fiber spool. After arriving at the QNU, light is transmitted to a VOA through port2 to port3 of the optical circulator, and then enters a phase modulator (PM) for signal modulation. Afterward, the signal light enters the polarization controller (PC). After passing through the PC, it enters through port1 of the optical circulator, exits through port2, and returns to BS. After passing through the optical fiber spool again, the signal light enters from port2 of the optical circulator at the QLT and comes out from port3. Then the signal light reaches the PC of QLT. Finally, the signal light and LO light enter the integrated coherent receiver (ICR).

possibility of eight users through multiple experiments. After arriving at the QNU, light is transmitted to a VOA through port2 to port3 of the optical circulator. The function of QNU's VOA is to balance the optical power of each user. However, due to the manual adjustment of VOA, the optical power of each user cannot be completely identical, so there are differences in the signal-to-noise ratio (SNR) of each user in the experimental results. In practical implementation, the electronically controlled VOA can accurately control the output optical power of the QNU side. Light then enters a PM for QKD modulation, which is achieved using an arbitrary waveform generator (AWG). Different QNUs modulate information on different carrier frequencies, which can be distinguished on the spectrum diagram. QNU1, QNU2, and QNU3 in Fig. 4 select 10 MHz, 20 MHz, and 30 MHz bands, respectively. Afterward, the signal light enters the polarization controller (PC). The function of QNU's PC is to adjust the polarization of each user, which can be eliminated after we use all polarization-maintaining fiber in practical implementation. After passing through the PC, it enters through port1 of the optical circulator, exits through port2, and returns to BS with an optical ratio of 8:1. At BS, the signal lights of the QNUs are converged into an optical fiber. After passing through the optical fiber spool again, the signal light enters from port2 of the optical circulator at the QLT and comes out from port3. Then the signal light reaches the PC of QLT for overall polarization adjustment. Finally, the signal light and LO light enter the integrated coherent receiver (ICR). After detection, the signal is collected in an oscilloscope. According to the Nyquist sampling theorem, the sampling frequency must be higher than two times the highest signal frequency. In this case, there is no signal spectrum aliasing, and the signal can be completely recovered. We adopt the no-switching scheme [26] and the reverse reconciliation scheme [24], which means that we use data obtained by QLT as a basis for reconciliation. In the case of reverse reconciliation, we can judge the maximum amount of information that Eve can obtain through the parameter estimation process, and then remove this part in privacy amplification to ensure the security of the final secret key. In this scenario, it can resist Eve's splitting attack.

2. Signal Processing

To separate the data of different users, FDM is adopted in the experiment. In the modulation of QNU, the modulated signal is the waveform generated by the baseband signal and corresponding carrier frequency. The signal can be represented by Eq. (2). Then the AWG loads the signal $f(t)$ to the PM for phase modulation. There are two advantages to operating like this. First, the signal formed in this way has an extremely strong ability to resist phase shift and noise. Second, the signal must be an orthogonal four-state CV-QKD signal after coherent demodulation. Their relative positions will not be changed, but only by the overall rotation, which is convenient for signal recovery. After coherent demodulation, the signal must be an orthogonal four-state CV-QKD signal. Their relative positions will not be changed, but will be rotated only as a whole.

In the demodulation of QLT, bandpass filtering is first employed for different frequency bands. Afterward, QLT determines whether there is a signal on each registered frequency band. After that, the first phase shift recovery is carried out to recover the optical phase. Since the obtained signal is adopted spectrum shifting, QLT uses coherent demodulation to restore the original signal of the baseband. It should be noted

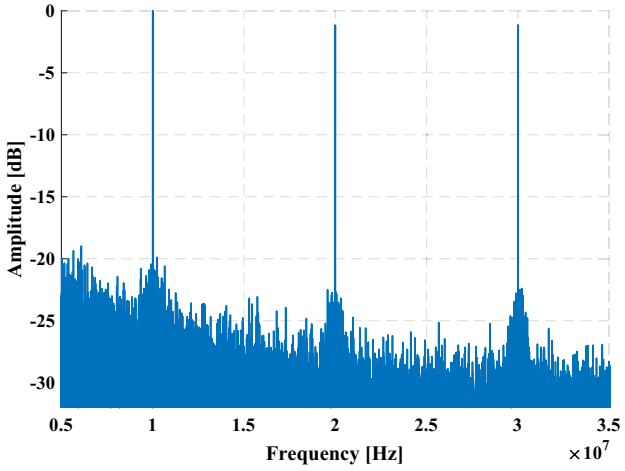


Fig. 5. Spectrum diagram of the signal obtained by QLT through the coherent receiver. It describes the change of amplitude at different frequencies.

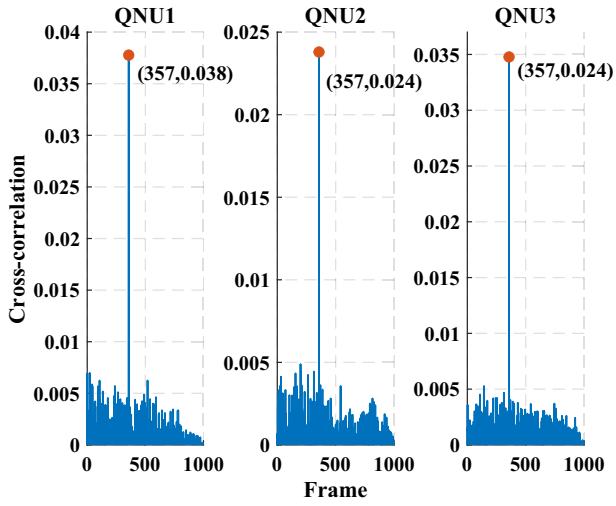


Fig. 7. Cross-correlation of the signal modulated by three QNUs and the signal received by QLT. It describes the change of the cross-correlation of three QNUs at different frames, where the red points represent the successful result.

that the coherent demodulation of QLT needs to be used for $g_a(t)$ and $g_b(t)$. The formula of coherent demodulation can be expressed as Eq. (3). QLT uses low pass filtering of the baseband frequency to get the baseband signal. After downsampling, the second phase shift recovery is carried out to rotate the signal as a whole. Then, the signal is determined by cross-correlation to complete frame synchronization. In frame synchronization, it is necessary to pay attention to the effect of mean value on cross-correlation. After that, QLT will do the parameter estimation to evaluate excess noise and further the information Eve can acquire, excluding this part in the post-processing. We also monitor the input optical power at both QNU and QLT to close the potential practical security loophole.

3. Experimental Results

The experimental results of RM-QAN are presented in the following. As can be seen from Fig. 5, the 10 MHz, 20 MHz, and 30 MHz frequency bands modulated by three QNUs can be clearly seen in the mixed spectrum obtained by QLT. There is no spectrum aliasing in these bands. Since the modulation scheme is DMCS, the signal constellation presents four states, which correspond to the different values of k in Eq. (1). Different values of k correspond to different colors. As shown in constellation diagrams of three QNUs in Fig. 6, the signal variance gradually decreases to the variance of shot noise with the reduction of SNR. It can also be seen from the constellation diagrams that the four states become more and more indistinguishable with the decrease in SNR. However, the result of cross-correlation is still clear in Fig. 7, which can easily complete frame synchronization. Since AWG is a clock synchronized with the oscilloscope, each red point in Fig. 7 should have the same horizontal coordinate, which means the frame synchronization position should be with the same value. It was well verified in our experiments with excellent frame synchronization results. In addition, the excess noise of 100 frames of each QNU fluctuates around zero, as shown in Fig. 8. Excess noise mainly comes from frequency cross talk noise, and the fluctuation comes from the deviation of data statistics. Their

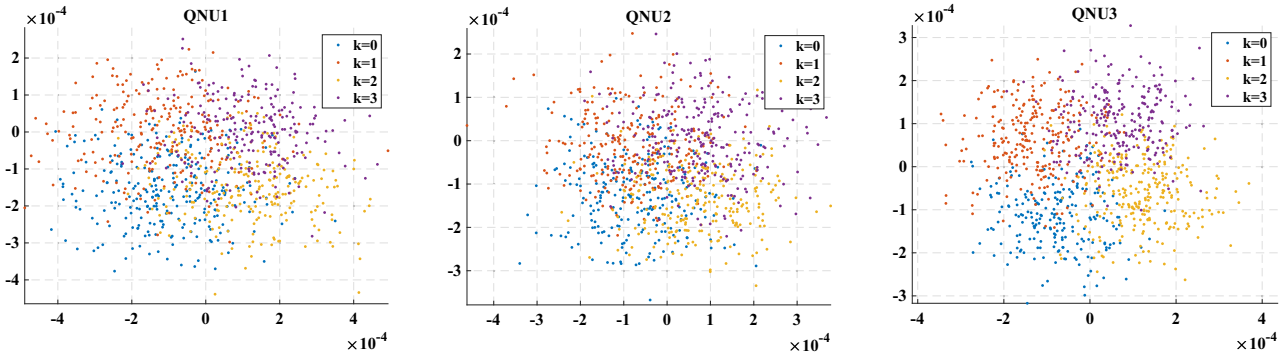


Fig. 6. (a) Signal constellation of QNU1, with $V_A = 0.5587$ SNU. (b) Signal constellation of QNU2, with $V_A = 0.5170$ SNU. (c) Signal constellation of QNU3, with $V_A = 0.5641$ SNU. The data in the figure were obtained through several experiments, where k represents different states in discrete modulation coherent state (DMCS) CV-QKD. Different values of k correspond to different colors.

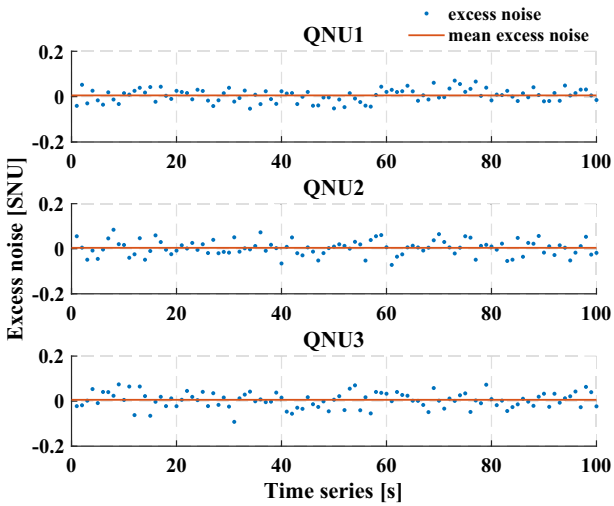


Fig. 8. Excess noise scatter diagram of three QNUs. It describes the change of the excess noise of three QNUs at different times, where the red line represents the mean value of excess noise of three QNUs. The mean excess noise of QNU1, QNU2, and QNU3 is 0.0054 SNU, 0.0040 SNU, and 0.0059 SNU, respectively.

average is slightly more than zero. Inconsistent noise from different users results from statistical deviation in finite samples. Since we filter out noise from other users, the noise from different users will tend to be same when the amount of data is large. In Fig. 9, the ordinate value corresponding to the dotted line is the achievable secret key rate under the condition of 30 km in our experiment, where the secret key rate of QNU1 is 825.82 bit/s, the secret key rate of QNU2 is 674.46 bit/s, and the secret key rate of QNU3 is 635.95 bit/s. At present, due to the limitation of modulated RF signal ports, we have carried out experimental verification with eight users in multiple experiments. The feasibility of realizing more users can be fully inferred from the results, which can be realized by a BS with multiple interfaces.

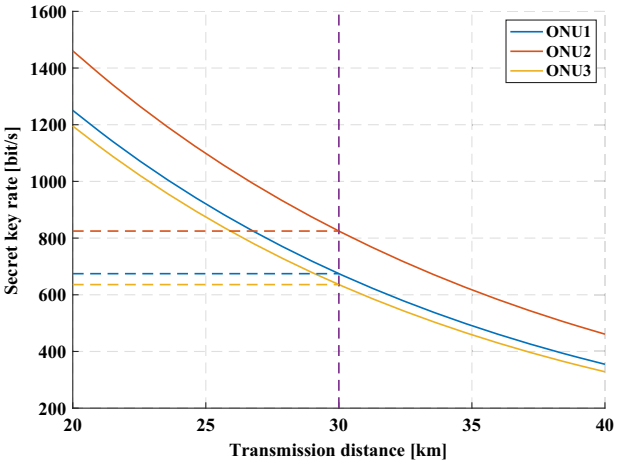


Fig. 9. Secret key rate curves of the three QNUs in the experiment. It describes the change of the secret key rate of three QNUs at different transmission distances, where the ordinate value corresponding to the dotted line is the secret key rate under the condition of 30 km achieved in our experiment. The secret key rate of QNU1 is 825.82 bit/s, the secret key rate of QNU2 is 674.46 bit/s, and the secret key rate of QNU3 is 635.95 bit/s.

3. DISCUSSION

A. Physical Noise Analysis

In RM-QAN, the total noise can be classified into trusted noises and untrusted noises according to the traditional QKD noise model. Trusted noises are those that can be calibrated by the receiver QLT, which cannot be controlled by Eve, and they constitute electronic noise v_{el} in the secret key rate bound calculation model. Untrusted noises, however, are caused by channel non-idealities or device non-idealities. These noises cannot be calibrated accurately and are controllable by Eve. Therefore, these noises constitute excess noise ε in the secret key rate bound calculation model and indicate the extent of eavesdropping. To ensure the security of the QKD access network, we performed an analysis of actual physical noise. The untrusted noises introduced by our special scheme are Rayleigh backscattering noise ε_{RB}, frequency cross talk noise ε_{FD}, and optical circulator noise ε_{OC}. These are all untrusted noises. At the same time, we also briefly analyze the classical untrusted noise and classical trusted noise in general CV-QKD. In this way, the system performance can be analyzed by this updated physical noise model.

1. Rayleigh Backscattering Noise

In our scheme, light is transmitted from QLT by a round-trip structure, modulated by QNU, and received by QLT. This round-trip structure has a scattering effect, resulting in noise. Scattering noise is mainly divided into Rayleigh backscattering noise and Raman scattering noise. Raman scattering noise mainly affects the wavelength division multiplexing (WDM) system [87]. However, our FDM access network uses a single laser, which makes the wavelength unique. Moreover, theoretical analysis shows that the influence of Raman scattering on CV-QKD can be ignored because the LO light acts as a filter. In conclusion, only Rayleigh backscattering noise needs to be considered [88].

Rayleigh backscattering noise ε_{RB} is caused by the interference of noise photons in the same spectral segment in the coherent detection of QLT, which can neither be filtered out nor attenuated. Rayleigh backscattering can occur anywhere in the fiber, and it cannot be monitored by a timing detector. Therefore, Rayleigh backscattering noise is something that needs to be considered in our scheme. The number of scattered photons produced by the Rayleigh backscattering effect is [88]

$$\langle \hat{N}_{RB} \rangle = (1 - T)10^{\beta/10} \langle \hat{N}_{QNU} \rangle R, \tag{8}$$

where R is the repetition frequency of the system, and $\eta = 10^{-L_{QNU}/10}$. Since all QNUs are in parallel, L_{QNU} is the loss inside one QNU round-trip. The transmittance is $T = 10^{-\alpha L/10}$, where L represents the length of the optical fiber, and α denotes the attenuation coefficient. β represents the Rayleigh backscattering coefficient. $\langle \hat{N}_{QNU} \rangle = 0.5V_A$ is the number of photons returning from QNU, where V_A is the modulation variance. τ is the electric integration time of the heterodyne detector, namely, the gate pulse time; then, Rayleigh backscattering noise is

$$\varepsilon_{\mathrm{RB}} = \frac{2\langle \hat{N}_{\mathrm{RB}} \rangle \tau}{\eta T} = \frac{2(1-10^{-\alpha L/10})10^{\beta/10}\langle \hat{N}_{\mathrm{QNU}} \rangle R\tau}{\eta 10^{-\alpha L/10}} = \frac{(1-10^{-\alpha L/10})10^{\beta/10} V_{\mathrm{A}} R\tau}{10^{-L_{\mathrm{QNU}}/10}10^{-\alpha L/10}}. \quad (9)$$

As shown in Fig. 10, this image describes the relationship between Rayleigh backscattering noise $\varepsilon_{\mathrm{RB}}$ and transmission distance L. As can be seen from the figure, Rayleigh backscattering noise increases gradually with the increase of transmission distance, but its order of magnitude is always within an acceptable range.

2. Frequency Cross Talk Noise

Because our access network scheme uses FDM to distinguish users, it inevitably produces photon cross talk between different frequency bands. When filtering the frequency band of a single user, the photons from other frequency bands leak in and produce noise. This noise is called frequency cross talk noise $\varepsilon_{\mathrm{FC}}$.

Before considering the frequency cross talk noise of all other users to a single user, we can simply consider the noise between any two bands ε_{F}. First, frequency interval Δf is an important parameter to describe noise between frequency bands ε_{F}. In addition, the intensity of signal light also affects interband noise ε_{F}, which can be described by modulation variance V_{A}. As the FDM scheme needs to use a bandpass filter to separate signals in different bands, the parameters of the filter also affect the noise between bands ε_{F}. The influence of interband noise ε_{F} is also different for different filter types. The classical Butterworth filter, which is used in our experiment, will be analyzed in the following. The Butterworth filter is mainly affected by the passband range and stopband range of the bandpass filter. It should be noted that other parameters of the filter, such as sampling rate, maximum passband attenuation, and maximum stopband attenuation, can be taken as reasonable values. Within reasonable limits, these parameters have little influence on filtering results. In conclusion, interband noise ε_{F} is mainly affected by frequency interval Δf, modulation variance V_{A}, passband range, and stopband range.

Before establishing the QKD link, we calibrated the appropriate stopband and passband for the bandwidth filters of individual users through experimental test data in advance. By searching for the optimal SNR, the optimal passband and stopband are found. Naturally, it is also possible to determine a better adaptive dynamic filter through machine learning and other algorithms to achieve a better filtering effect, but this is not within the scope of this paper. After hundreds of experiments, we got a reasonable passband and stopband range. Since signals mainly exist in the first main lobe, we take the passband boundary as the first main lobe of the signal and the stopband boundary as the second main lobe of the signal. This filtering result may not be the best, but it has met our experimental requirements.

Since the filtering process is solving linear differential equations with constant coefficients, we use the Monte Carlo method to obtain the noise between frequency bands ε_{F}. After several simulations, we obtained the relation between frequency interval Δf and frequency division noise ε_{F} under different modulation variances V_{A}, as shown in Fig. 11.

The dots in the figure represent values obtained by the Monte Carlo method, and the curves are obtained by the nonlinear fitting method. It can be seen from the figure that the noise between frequency bands ε_{F} is proportional to the modulation variance V_{A} and decreases with the increase of frequency interval Δf. It is worth mentioning that V_{A} is rounded to better represent it in Fig. 11. The value of V_{A} does not affect the generality of the resulting formula. Thus, interband noise ε_{F} can be expressed as

$$\varepsilon_{\mathrm{F}} = V_{\mathrm{A}}(e^{a} + \Delta f^{b}), \quad (10)$$

where $a = 27.27$ and $b = -2.066$. Given the noise between any two frequency bands ε_{F}, we can calculate the frequency

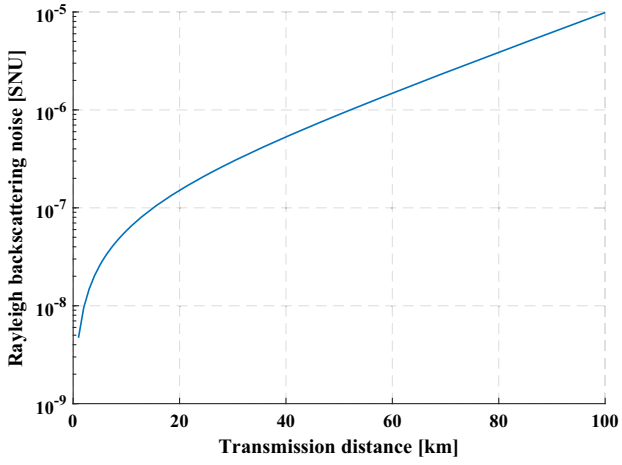


Fig. 10. Relationship between Rayleigh backscattering noise and transmission distance. Parameters are set as $\beta = -40$ dB, $\alpha = 0.2$ dB/km, $V_{\mathrm{A}} = 0.5$ SNU, $R = 1$ MHz, $\tau = 1$ ns, $L_{\mathrm{QNU}} = 3$ dB. It describes the change of Rayleigh backscattering noise at different transmission distances.

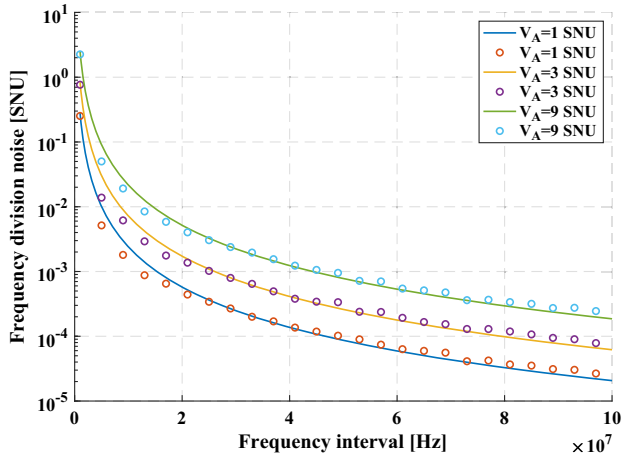


Fig. 11. Relation between frequency interval and frequency division noise under different modulation variances. Parameters are set as $a = 27.27$, $b = -2.066$. Hollow points are obtained by the Monte Carlo method, and curves are obtained by nonlinear fitting. It describes the change of frequency division noise at different frequency intervals and different modulation variances (V_{A}).

cross talk noise ε_{FC} of a single user, which is affected by all other users. In our experiment, we found that noise ε_F when there are users on both sides at the same distance is the same as noise ε_F when there are users on only one side. So frequency cross talk noise ε_{FC} is relevant only to the presence or absence of the user at a certain distance. Thus, we get the influence of the number of users, namely, network capacity N, on noise ε_{FC} when $V_A = 1$ SNU, as shown in Fig. 12.

The dots in the figure represent discrete values of noise ε_{FC} under different network capacities, and the curves represent continuous values derived from the nonlinear fitting method. As can be seen from the figure, the frequency cross talk noise ε_{FC} influenced by all other users increases gradually with the increase of network capacity, but the increase rate decreases gradually. It can be described as

$$\varepsilon_{FC} = V_A c e^{d/N}, \tag{11}$$

where $c = 3.815 \times 10^{-3}$ and $d = -0.4576$. Thus, we can get that noise ε_{FC} will gradually approach the value of c with the increase of network capacity N, as shown in the inset of Fig. 12. When network capacity is $N = 10,000$, ε_{FC} is extremely close to 3.815×10^{-3}. When network capacity tends to be infinite, $\varepsilon_{FC} = 3.815 \times 10^{-3}$.

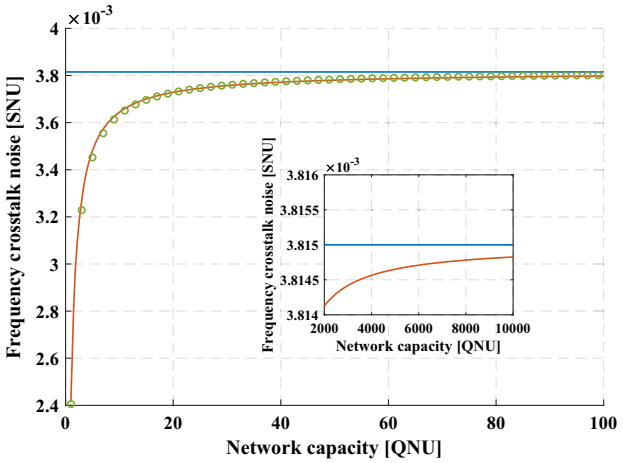


Fig. 12. Relation between network capacity and frequency cross talk noise. Parameters are set as $c = 3.815 \times 10^{-3}$, $d = -0.4576$. Hollow points are obtained by the Monte Carlo method, and curves are obtained by nonlinear fitting. The inset shows what happens when the network capacity is large. It describes the change of frequency cross talk noise at different network capacities.

3. Optical Circulator Noise

The round-trip QAN introduces an optical circulator to complete the optical round-trip scheme. However, the optical circulator is not found in the classical CV-QKD system. Moreover, the noise introduced by the optical circulator is non-ignorable when there are a large number of users. Therefore, we analyze the noise effect of the optical circulator on the system.

An optical circulator is a multiport nonreciprocal optical device. Its function is to make the optical signal be transmitted only along the specified port order. The three-port optical circulator we use is transmitted from port1 to port2 and from port2 to port3. The unique parameters in the optical circulator are isolation and directionality. Directionality is also called the cross talk of the optical circulator. The isolation is due to the imperfection of the optical circulator. When light is reversed, some light will still pass through. Directionality is caused by the structure of the optical circulator and other reasons, so that part of the light passing through port1 is directly output from port3. The isolation of the optical circulator is defined as the ratio of input optical power to output optical power in reverse light transmission [89]. The directionality of the optical circulator is the ratio of the input optical power of port1 to the output optical power of port3 when port2 is terminated and there is no reflection [89]. Therefore, the isolation and directionality of the optical circulator can be expressed as

$$\begin{aligned} I_{21} &= 10\lg(P_{21}/P_{12}), \\ I_{32} &= 10\lg(P_{32}/P_{23}), \\ D &= 10\lg(P_{1in}/P_{3out}), \end{aligned} \tag{12}$$

where I_{21} is the optical isolation from port2 to port1, and I_{32} is the optical isolation from port3 to port2. In the case of port2 to port1, P_{21} is the optical power transmitted by port2, and P_{12} is the optical power received by port1. In the case of port3 to port2, P_{32} is the optical power transmitted by port3, and P_{23} is the optical power received by port2. D is the directionality of the optical circulator, where P_{1in} is the optical power input of port1, and P_{3out} is the optical power output of port3.

For different optical structures, the noise introduced by the optical circulator is different. For our scheme, as shown in Fig. 13, the following analysis can be carried out.

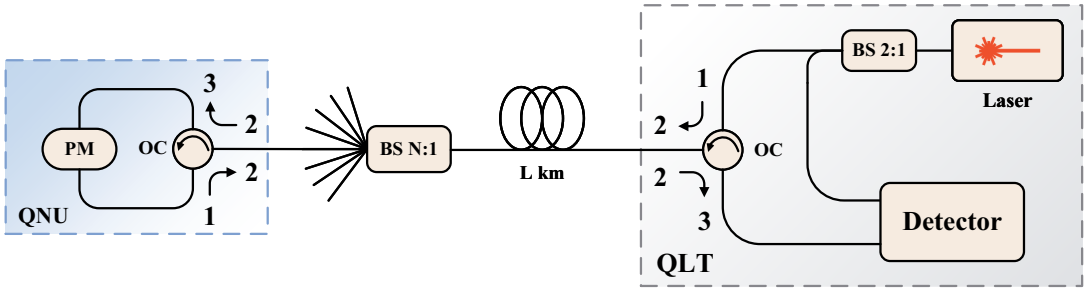


Fig. 13. Schematic diagram of optical circulator noise. The optical circulator of QLT receives light from the laser at port1 and transmits it to QNU at port2. The signal light returned by QNU is then received at port2 and output to the detector at port3. The optical circulator of QNU receives light from the QLT at port2, and then transmits it to the PM at port3.

First, we analyze the optical circulator of QLT. It receives light from the laser at port1 and transmits it to QNU at port2. The signal light returned by QNU is then received at port2 and outputs to the detector at port3. As the signal light is returned to the optical circulator, some light will enter port1 from port2 and return to the laser. Therefore, we added an optical isolator behind the laser to avoid damaging the laser and generating noise. Lasers usually need optical isolators to protect them, so the optical isolator in our scheme is not shown in Fig. 13. For the light received by port1, some will be directly output to the detector from port3, which will become noise photons and generate noise. The noise can be described as

$$\varepsilon_{\mathrm{OC}}^{\mathrm{QLT}} = \frac{10^{D/10} V_{\mathrm{A}}}{10^{-\alpha L/10} 10^{-L_{\mathrm{QNU}}/10}}, \tag{13}$$

where L is the length of the optical fiber, α is the attenuation coefficient, and the transmittance is $T = 10^{-\alpha L/10}$. Since all QNUs are in parallel, L_{QNU} is the loss inside one QNU for a round trip. V_{A} is the modulation variance.

Second, we analyze the optical circulator of QNU. The optical circulator in the QNU receives light from the QLT at port2, and then transmits it to the PM at port3. Afterward, it receives the modulated signal light at port1 and outputs it to the QLT at port2. As light from the QLT enters the optical circulator, some enters port1 from port2, which finally enters the PM. However, light will be screened out by PM due to the unipolarity of PM and will not produce noise. For the signal light received by port1, some light will directly output to the PM from port3, becoming noise photons and generating noise. The noise can be described as

$$\varepsilon_{\mathrm{OC}}^{\mathrm{QNU}} = 10^{D/10} N V_{\mathrm{A}}, \tag{14}$$

where N is network capacity and also the number of QNUs.

In summary, the total noise $\varepsilon_{\mathrm{OC}}$ introduced by the optical circulator is

$$\begin{aligned} \varepsilon_{\mathrm{OC}} &= \frac{10^{D/10} V_{\mathrm{A}}}{10^{-\alpha L/10} 10^{-L_{\mathrm{QNU}}/10}} + 10^{D/10} N V_{\mathrm{A}} \\ &= 10^{D/10} V_{\mathrm{A}} (N + 10^{\alpha L/10} 10^{L_{\mathrm{QNU}}/10}). \end{aligned} \tag{15}$$

Based on the above analysis, assuming that $D = 60$ dB, $\alpha = 0.2$ dB/km, $V_{\mathrm{A}} = 0.5$ SNU, and $L_{\mathrm{QNU}} = 3$ dB, we can get the relation between optical circulator noise and transmission distance, and the relation between optical circulator noise and network capacity, as shown in Fig. 14.

As seen from the figure, the noise of the optical circulator increases gradually with the increase of transmission distance and network capacity, but it is within the acceptable range.

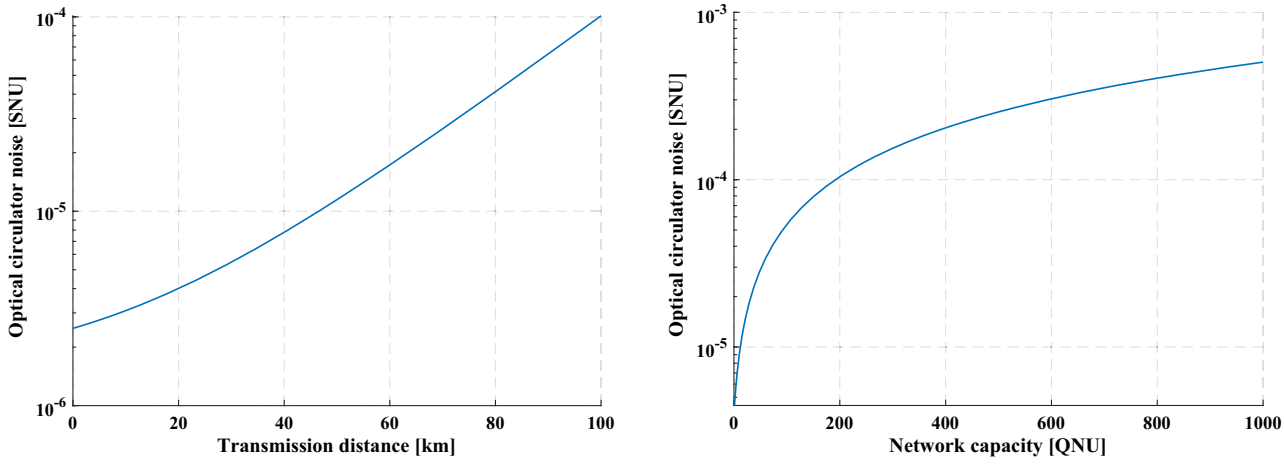
4. Other Untrusted Noise

In addition to the above mentioned Rayleigh backscattering noise $\varepsilon_{\mathrm{RB}}$, frequency cross talk noise $\varepsilon_{\mathrm{FC}}$, and optical circulator noise $\varepsilon_{\mathrm{OC}}$, which are the characteristics of the scheme, untrusted noise also includes modulation noise $\varepsilon_{\mathrm{MO}}$ [90], amplitude noise $\varepsilon_{\mathrm{AM}}$ [90], and phase noise $\varepsilon_{\mathrm{PH}}$ [90].

The first is modulation noise. Because of the uncertainty of modulation voltage, noise will be introduced in the modulation process, and we need to find the relationship between the macro uncertainty of voltage and the optical quadrature components. In Ref. [90], the relationship between modulation voltage and optical quadrature components has been derived, which can be expressed as

$$\varepsilon_{\mathrm{MO}} = V_{\mathrm{A}} \left[\pi \frac{\Delta U_{\mathrm{DAC}}}{U_{\mathrm{DAC}}} + \frac{1}{2} \left(\pi \frac{\Delta U_{\mathrm{DAC}}}{U_{\mathrm{DAC}}} \right)^2 \right]^2, \tag{16}$$

in which U_{DAC} represents the voltage of the digital-to-analog converter (DAC) in AWG, ΔU_{DAC} denotes the specific deviation of U_{DAC}, and V_{A} is the modulation variance. In our experiment, $\Delta U_{\mathrm{DAC}} = 0.01 U_{\mathrm{DAC}}$, which is decided by the resolution of the voltage of AWG; $V_{\mathrm{A}} = 0.5$ SNU, which corresponds to our experimental setup. In this case, $\varepsilon_{\mathrm{MO}} = 5.09 \times 10^{-4}$, indicating that the contribution of modulation noise is small in the total noise.



(a) (b)

Fig. 14. (a) Relation between optical circulator noise and transmission distance. The image describes the change of optical circulator noise at different transmission distances. (b) Relation between optical circulator noise and network capacity. It describes the change of optical circulator noise at different network capacities. Parameters are set as $D = 60$ dB, $\alpha = 0.2$ dB/km, $V_{\mathrm{A}} = 0.5$ SNU, $L_{\mathrm{QNU}} = 3$ dB.

Because the LO used in coherent detection is physically realized by a laser, the laser has intensity noise and phase noise. The physical cause of the relative intensity noise of the laser is that the laser source uses the principle of excited radiation to produce more photons. In addition, the change in the number of photons caused by spontaneous radiation is reflected in the amplitude of the laser, forming amplitude noise. Therefore, amplitude noise can be calculated as

$$\begin{aligned}\varepsilon_{\mathrm{AM}} &= \varepsilon_{\mathrm{RIN}}^{\mathrm{sig}} + \varepsilon_{\mathrm{RIN}}^{\mathrm{LO}} \\ &= V_{\mathrm{A}}\left(\sqrt{\mathrm{RIN}_{\mathrm{sig}}\Delta v_{\mathrm{A}}} + 0.25\mathrm{RIN}_{\mathrm{LO}}\Delta v_{\mathrm{B}}\right). \end{aligned} \tag{17}$$

Consider that the typical parameters of the laser are $\mathrm{RIN}_{\mathrm{sig}} = \mathrm{RIN}_{\mathrm{LO}} = 8 \times 10^{-11}$ Hz^{-1}, $\Delta v_{\mathrm{A}} = \Delta v_{\mathrm{B}} = 10$ kHz, $V_{\mathrm{A}} = 0.5$ SNU, and amplitude noise $\varepsilon_{\mathrm{AM}} = 4.47 \times 10^{-4}$.

The spontaneous radiation of the laser causes not only the change of intensity but also the random change in the frequency of the laser pulse signal, forming phase noise. Due to the spontaneous radiation phenomenon inside the semiconductor laser, the photon generated by it is random in polarization and phase, which will directly affect the amplitude and phase of the light field formed by the excited radiation. For amplitudes, the magnitude is restored to the mean by glazing the radiation field with the inversion of the particle number in the laser medium, but the phase has no such resilience. Therefore, phase noise can be described as

$$\varepsilon_{\mathrm{PH}} = 2\pi\tau V_{\mathrm{A}}(\Delta v_{\mathrm{A}} + \Delta v_{\mathrm{B}}). \tag{18}$$

According to the conventional parameter of coherence detection to weak coherent light, assume that $\tau = 1$ ns, $\Delta v_{\mathrm{A}} = \Delta v_{\mathrm{B}} = 10$ kHz, $V_{\mathrm{A}} = 0.5$ SNU, and phase noise $\varepsilon_{\mathrm{PH}} = 6.28 \times 10^{-5}$.

5. Trusted Noise

In addition to the untrusted noise mentioned above, there is also trusted noise that can be calibrated or controlled by QLT. Here we briefly describe three kinds of common trusted noise: detector thermal noise $\varepsilon_{\mathrm{DET}}$, analog-to-digital converter (ADC) quantization noise $\varepsilon_{\mathrm{ADC}}$, and common-mode rejection ratio (CMRR) noise $\varepsilon_{\mathrm{CMRR}}$ [90].

Detector thermal noise is a kind of white Gaussian noise. Its amplitude distribution is Gaussian, the mathematical expectation is zero, and its power spectral density is constant. Thermal noise is a kind of noise produced by electronic components in the system, mainly by resistors and metal–oxide–semiconductor (MOS) tubes. The generation of resistance thermal noise is related to the thermal motion of electrons. Therefore, the thermal noise of the detector can be expressed as

$$\varepsilon_{\mathrm{DET}} = 2\frac{\mathrm{NEP}^2 B\tau}{hfP_{\mathrm{LO}}}, \tag{19}$$

where NEP (in $\mathrm{W}/\sqrt{\mathrm{Hz}}$) is the equivalent noise power. NEP represents the optical signal power required to be input when SNR = 1. If we take the general parameters NEP = 4.5 $\mathrm{pW}/\sqrt{\mathrm{Hz}}$, $B = 250$ MHz, $\tau = 1$ ns, $hf = 1.28 \times 10^{-19}$ J, and $P_{\mathrm{LO}} = 8$ mW, then $\varepsilon_{\mathrm{DET}} = 9.99 \times 10^{-3}$.

The weak coherent state is detected and amplified by a balanced detector such that the final output voltage signal is proportional to the measured canonical component. However, if the output voltage is quantized by an ADC, the ADC introduces additional noise to the weak coherent state, making the excess noise larger. The same as detector noise, we convert a macroscopic physical quantity such as ADC noise into noise on the canonical component of the quantum state. Therefore, ADC quantization noise can be expressed as

$$\varepsilon_{\mathrm{ADC}} = \frac{2\tau}{hf(g\rho)^2 P_{\mathrm{LO}}}\left(\frac{1}{12}\frac{R_{\mathrm{U}}^2}{2^{2n}} + V_{\mathrm{ADC}}\right). \tag{20}$$

We can estimate ADC noise by common parameters $n = 10$ bit, $\tau = 1$ ns, $hf = 1.28 \times 10^{-19}$ J, $g = 20$ kΩ, $\rho = 0.85$ A/W, $P_{\mathrm{LO}} = 8$ mW, $R_{\mathrm{U}} = 1$ V, and $V_{\mathrm{ADC}} = 10^{-8}$ V^2; then $\varepsilon_{\mathrm{ADC}} = 6.05 \times 10^{-4}$.

A practical differential amplifier in a balanced detector amplifies not only the differential currents, but also their average currents. If a heterodyne detector consisting of two homodyne detectors is used for detection, the final noise introduced by CMRR is

$$\varepsilon_{\mathrm{CMRR}} = \frac{hfV_{\mathrm{A}}^2\mathrm{RIN}_{\mathrm{sig}}\Delta v_{\mathrm{A}}}{8\tau P_{\mathrm{LO}}(10^{\mathrm{CMRR}/10})^2} + \frac{\tau P_{\mathrm{LO}}\mathrm{RIN}_{\mathrm{LO}}\Delta v_{\mathrm{B}}}{2hf(10^{\mathrm{CMRR}/10})^2}. \tag{21}$$

Assuming that CMRR = 30 dB, $P_{\mathrm{LO}} = 8$ mW, $\tau = 1$ ns, $V_{\mathrm{A}} = 0.5$ SNU, $\mathrm{RIN}_{\mathrm{sig}} = \mathrm{RIN}_{\mathrm{LO}} = 8 \times 10^{-11}$ Hz^{-1}, $\Delta v_{\mathrm{A}} = \Delta v_{\mathrm{B}} = 10$ kHz, and $hf = 1.28 \times 10^{-19}$ J, in this case, $\varepsilon_{\mathrm{CMRR}} = 2.50 \times 10^{-4}$. This noise depends largely on the size of the relative intensity noise of the LO, so the relative intensity noise of the LO is required to be extremely low.

4. CONCLUSION

In conclusion, we propose a flexible and efficient quantum network physical structure, namely, RM-QAN. In detail, this QAN can make quantum states travel in a circle to transmit data due to the round-trip structure. It can also support multi-user access through multi-band quantum state transmission and separation. Based on this proposed network, we realize multi-user secure key sharing through CV-QKD. The theoretical noise model of the multi-user CV-QKD has been established, the user capacity and theoretical key rate of the scheme have been discussed, and the proof-of-principle experimental verification has been carried out. The proof-of-principle experiment shows that each QNU can share a practical secret key rate of about 600 bit/s at a transmission distance of 30 km with QLT.

Certainly, there are three main challenges in the practical implementation of this scheme. (1) At this stage, we analyze the secret key rate bounds in the asymptotic regime, and the finite-size effects and composable security are not considered, which are critical to the final practical implementation. In such a security framework, we need longer data blocks to overcome the finite-size effect, which requires a higher communication rate and larger data storage, and therefore has requirements for hardware and algorithms. (2) The practical access of more users also needs a classical communication protocol related to the data link layer and network layer to realize information synchronization, such as the handshake protocol between QNU and QLT. After accessing more QNUs, QLT needs to exchange more classical data in the post-processing stage, requiring the high bandwidth of the classical channel.

(3) For practical security, the effective countermeasures of the phase remapping attack [80,81] and the Trojan-horse attack [79] have been proposed and can be added in further implementation.

The advantage of our scheme is the simple optical structure in the physical layer. Specifically, the round-trip structure requires only one laser and one detector in the entire network, and only one modulator and one circulator need to be plugged in when a new user accesses. Performance evaluation shows such networks have low physical excess noise for each user theoretically and can support multi-user access and quantum secure key generation. Moreover, this scheme can coexist with classical communication, since classical communication can adopt different frequency bands in FDM. Combined with the comprehensive protocols of the data link layer and network layer and practical security countermeasures, this scheme can be an effective solution for QKD access network establishment. This work lays the foundation for the subsequent establishment and application of a large-scale and multi-user QAN.

APPENDIX A

In the following, we derive the secret key rate of DMCS CV-QKD under collective attack. Specifically, in the case of reverse negotiation, the secret key rate for unit system repetition rate can be written as

$$K_{\mathrm{p}} = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{A1}$$

where $\beta \in (0,1)$ is reverse negotiation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the maximum information that Eve can extract from Bob's secret key. According to Bob's measurement variance $V_{\mathrm{B}} = \eta T(V + \chi_{\mathrm{tot}})$ and conditional variance $V_{\mathrm{B|A}} = \eta T(1 + \chi_{\mathrm{tot}})$, where T is the transmittance of the channel, I_{AB} can be calculated as

$$\begin{aligned} I_{\mathrm{AB}}^{\mathrm{hom}} &= \frac{1}{2}\log_2 \frac{V_{\mathrm{B}}}{V_{\mathrm{B|A}}} = \frac{1}{2}\log_2 \frac{V + \chi_{\mathrm{tot}}}{1 + \chi_{\mathrm{tot}}}, \\ I_{\mathrm{AB}}^{\mathrm{het}} &= 2 \times \frac{1}{2}\log_2 \frac{V_{\mathrm{B}}}{V_{\mathrm{B|A}}} = \log_2 \frac{V + \chi_{\mathrm{tot}}}{1 + \chi_{\mathrm{tot}}}, \end{aligned} \tag{A2}$$

where $V = V_{\mathrm{A}} + 1$ is the equivalent variance of pure two-mode entangled states. $V_{\mathrm{A}} = 2\alpha^2$ is the modulation variance in the preparation–measure model. Because heterodyne detection measures two quadrature components at the same time, mutual information is multiplied by the coefficient 2. The total noise χ_{tot} can be described as

$$\begin{aligned} \chi_{\mathrm{tot}} &= \chi_{\mathrm{line}} + \chi_{\mathrm{det}}/T, \\ \chi_{\mathrm{line}} &= 1/T - 1 + \varepsilon, \end{aligned} \tag{A3}$$

where χ_{line} denotes channel noise, χ_{det} represents detection noise, and ε is excess noise. For homodyne detection, $\chi_{\mathrm{det}} = \chi_{\mathrm{hom}} = [(1-\eta) + v_{\mathrm{el}}]/\eta$, and for heterodyne detection, $\chi_{\mathrm{det}} = \chi_{\mathrm{het}} = [1 + (1-\eta) + 2v_{\mathrm{el}}]/\eta$. η denotes quantum efficiency, and v_{el} represents electrical noise.

The core of secret key rate calculation is to evaluate the upper bound of the information Eve steals. Under collective attack, the Holevo bound is used to limit the maximum information Eve can extract from Bob, so χ_{BE} is

$$\chi_{\mathrm{BE}} = S(\rho_{\mathrm{E}}) - \int \mathrm{d}m_{\mathrm{B}} p(m_{\mathrm{B}}) S(\rho_{\mathrm{E}}^{m_{\mathrm{B}}}), \tag{A4}$$

where m_{B} represents the measurements of Bob, $p(m_{\mathrm{B}})$ represents the probability density of the measurements, $\rho_{\mathrm{E}}^{m_{\mathrm{B}}}$ is Eve's conditional quantum state under Bob's measurements, and S denotes the von Neumann entropy of quantum state ρ. Eve's system can purify the system AB_1, Bob's measurement can purify system AEFG, and $S(\rho_{\mathrm{AFG}}^{m_{\mathrm{B}}})$ and m_{B} are independent of each other in the protocol, so χ_{BE} can be simplified as

$$\chi_{\mathrm{BE}} = S(\rho_{\mathrm{AB}_1}) - S(\rho_{\mathrm{AFG}}^{m_{\mathrm{B}}}). \tag{A5}$$

Theoretical security analysis of the CV-QKD protocol under collective attack shows that under the condition of known covariance matrix γ_{AB_1} of state ρ_{AB_1}, if Eve's eavesdropping operation is a Gaussian operation, it can get the most information, which is called "Gaussian attack optimality theorem." The theorem states that if the final quantum state ρ_{AB_1} shared by Alice and Bob is regarded as a Gaussian state, the calculated stolen information by Eve is an upper bound of the real stolen information. The information entropy calculation of the Gaussian state is relatively simple, which means the above equation can be simplified as

$$\chi_{\mathrm{BE}} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{A6}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. λ_i is the symplectic eigenvalue of the covariance matrix, where $\lambda_{1,2}$ correspond to the covariance matrix γ_{AB_1} of representational state ρ_{AB_1}, and $\lambda_{3,4,5}$ correspond to the covariance matrix $\gamma_{\mathrm{AFG}}^{m_{\mathrm{B}}}$ of representational state $\rho_{\mathrm{AFG}}^{m_{\mathrm{B}}}$. On the one hand, the covariance matrix γ_{AB_1} depends only on Alice and the channel, which is independent of the specific detection mode. It can be expressed as

$$\gamma_{\mathrm{AB}_1} = \begin{bmatrix} V \cdot I_2 & \sqrt{T} Z_4 \cdot \sigma_z \\ \sqrt{T} Z_4 \cdot \sigma_z & T(V + \chi_{\mathrm{line}}) \cdot I_2 \end{bmatrix}, \tag{A7}$$

where $I_2 = \mathrm{diag}(1,1)$, $\sigma_z = \mathrm{diag}(1,-1)$, and Z_4 reflects the correlation between patterns AB_1. It can be described as

$$Z_4 = 2\alpha^2 (l_0^{3/2} l_1^{-1/2} + l_1^{3/2} l_2^{-1/2} + l_2^{3/2} l_3^{-1/2} + l_3^{3/2} l_0^{1/2}), \tag{A8}$$

where

$$\begin{aligned} l_{0,2} &= \frac{1}{2} e^{-\alpha^2} (\cosh \alpha^2 \pm \cos \alpha^2), \\ l_{1,3} &= \frac{1}{2} e^{-\alpha^2} (\sinh \alpha^2 \pm \sin \alpha^2). \end{aligned} \tag{A9}$$

It can be found that this matrix is similar to the covariance matrix in the Gaussian modulation coherent state (GMCS) CV-QKD protocol, except that the Einstein–Podolsky–Rosen (EPR) correlation in the GMCS CV-QKD protocol is $Z_{\mathrm{G}} = \sqrt{V^2 - 1}$. When $V_{\mathrm{A}} < 0.5$, Z_4 is extremely close to Z_{G}. Under this condition, it can be considered that the information χ_{BE} Eve steals from Bob is equal in both protocols. Based on this conclusion, the secret key rate can be deduced according to the GMCS CV-QKD protocol, and corresponding parameters A and B are

$$A = V^2 + T^2(V + \chi_{\text{line}})^2 - 2TZ_4^2,$$
$$B = (TV^2 + TV\chi_{\text{line}} - TZ_4^2)^2. \quad \text{(A10)}$$

On the other hand, matrix $\gamma_{\text{AFG}}^{m_{\text{B}}}$ can be calculated as

$$\gamma_{\text{AFG}}^{m_{\text{B}}} = \gamma_{\text{AFG}} - \sigma_{\text{AFGB}_3}^T H \sigma_{\text{AFGB}_3}, \quad \text{(A11)}$$

where the symplectic matrix H represents the measurement method in the pattern B_3. For homodyne detection, $H_{\text{hom}} = (X\gamma_{B_3}X)^{\text{MP}}$, where $X = \text{diag}(1, 0)$. MP stands for the Moore–Penrose inverse of the matrix. For heterodyne detection, $H_{\text{het}} = (\gamma_{B_3} + I_2)^{-1}$. Matrices γ_{B_3}, γ_{AFG}, and σ_{AFGB_3} can be obtained by decomposing the following covariance matrix:

$$\gamma_{\text{AFGB}_3} = \begin{bmatrix} \gamma_{\text{AFG}} & \sigma_{\text{AFGB}_3}^T \\ \sigma_{\text{AFGB}_3} & \gamma_{B_3} \end{bmatrix}, \quad \text{(A12)}$$

which can be obtained by the transformation of the matrix describing system AB_3FG. The matrix of system AB_3FG is

$$\gamma_{\text{AB}_3\text{FG}} = (Y^{\text{BS}})^T[\gamma_{\text{AB}_1} \oplus \gamma_{\text{F}_0\text{G}}]Y^{\text{BS}}, \quad \text{(A13)}$$

where γ_{AB_1} is given in Eq. (A7). $\gamma_{\text{F}_0\text{G}}$ describes the EPR state of variance v, which is used for equivalent electrical noise of the detector. So $\gamma_{\text{F}_0\text{G}}$ is

$$\gamma_{\text{F}_0\text{G}} = \begin{bmatrix} v \cdot I_2 & \sqrt{v^2 - 1} \cdot \sigma_z \\ \sqrt{v^2 - 1} \cdot \sigma_z & v \cdot I_2 \end{bmatrix}, \quad \text{(A14)}$$

where v depends on the detection method. For homodyne detection, $v = \eta\chi_{\text{hom}}/(1 - \eta) = 1 + v_{\text{el}}/(1 - \eta)$, and for heterodyne detection, $v = (\eta\chi_{\text{het}} - 1)/(1 - \eta) = 1 + 2v_{\text{el}}/(1 - \eta)$. Finally, matrix Y^{BS} describes the function of the BS on pattern B_2 and pattern F_0, which is used for the equivalent quantum efficiency of the detector. Therefore, matrix Y^{BS} can be denoted as

$$Y_{\text{B}_2\text{F}_0}^{\text{BS}} = \begin{bmatrix} \sqrt{\eta} \cdot I_2 & \sqrt{1 - \eta} \cdot I_2 \\ -\sqrt{1 - \eta} \cdot I_2 & \sqrt{\eta} \cdot I_2 \end{bmatrix},$$
$$Y^{\text{BS}} = I_{\text{A}} \oplus Y_{\text{B}_2\text{F}_0}^{\text{BS}} \oplus I_{\text{G}}. \quad \text{(A15)}$$

After obtaining the above matrix, we can find the symplectic eigenvalues of matrix $\gamma_{\text{AFG}}^{m_{\text{B}}}$. In the following, we directly give their calculation formula:

$$\lambda_{3,4}^2 = \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right), \quad \text{(A16)}$$

where C and D are determined by the specific detection method. For homodyne detection,

$$C_{\text{hom}} = \frac{V\sqrt{B} + T(V + \chi_{\text{line}}) + A\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})},$$
$$D_{\text{hom}} = \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}, \quad \text{(A17)}$$

and for heterodyne detection,

$$C_{\text{het}} = \frac{1}{[T(V + \chi_{\text{tot}})]^2}\{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}} \times [V\sqrt{B} + T(V + \chi_{\text{line}})] + 2T(V^2 - 1)\},$$
$$D_{\text{het}} = \left[\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right]^2. \quad \text{(A18)}$$

The last symplectic eigenvalue is

$$\lambda_5 = 1. \quad \text{(A19)}$$

Funding. Key R&D Program of Guangdong Province (2020B030304002); Shanghai Municipal Science and Technology Major Project (2019SHZDZX01); National Natural Science Foundation of China (61671287, 61971276, 62101320); National Key Research and Development Program of China (2016YFA0302600).

Author Contributions. G. Z. conceived the research. Y. X. and T. W. carried out the experiment. Y. X., T. W., and H. Z analyzed the data and wrote the manuscript. P. H. provided the technical guide for secret key rate analysis and post processing. All authors contributed to the data collection, discussed the results, and reviewed the manuscript.

Disclosures. The authors declare no conflicts of interest.

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

REFERENCES

1. S. Khatri, "Towards a general framework for practical quantum network protocols," Ph.D. thesis (Louisiana State University and Agricultural & Mechanical College, 2021).
2. H. J. Kimble, "The quantum internet," Nature **453**, 1023–1030 (2008).
3. M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future European quantum key distribution network," Security Commun. Netw. **1**, 57–74 (2008).
4. D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the Swiss quantum quantum key distribution network in a field environment," New J. Phys. **13**, 123001 (2011).
5. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**, 21739–21756 (2014).
6. R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," npj Quantum Inf. **3**, 30 (2017).
7. A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami, and M. Sasaki, "Quantum key distribution network for multiple applications," Quantum Sci. Technol. **2**, 034003 (2017).
8. E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, A. A. Kanapin, A. S. Sokolov, S. S. Vorobey, A. V. Miller, V. E. Ustimchik, M. N. Anufriev, A. Trushechkin, R. R. Yunusov, V. L. Kurochkin, Y. V. Kurochkin, and A. K. Fedorov, "Demonstration of a quantum key distribution network in urban fibre-optic communication lines," Quantum Electron. **47**, 798 (2017).
9. Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: challenges and solutions," Opt. Express **26**, 24260–24273 (2018).
10. E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, T. Walther, F. Wissel, and M. Gunkel, "Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding," PRX Quantum **3**, 020341 (2022).

11. S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," Nature **564**, 225–228 (2018).
12. Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," Light Sci. Appl. **10**, 183 (2021).
13. C. Simon, "Towards a global quantum network," Nat. Photonics **11**, 678–680 (2017).
14. P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," Nat. Phys. **10**, 582–587 (2014).
15. D. Gottesman, T. Jennewein, and S. Croke, "Longer-baseline telescopes using quantum repeaters," Phys. Rev. Lett. **109**, 070503 (2012).
16. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," Nature **390**, 575–579 (1997).
17. D. Rideout, T. Jennewein, G. Amelino-Camelia, T. F. Demarie, B. L. Higgins, A. Kempf, A. Kent, R. Laflamme, X. Ma, R. B. Mann, E. Martin-Martinez, N. C. Menicucci, J. Moffat, C. Simon, R. Sorkin, L. Smolin, and D. R. Terno, "Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities," Classical Quantum Gravity **29**, 224011 (2012).
18. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
19. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
20. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," arXiv, arXiv:2003.06557 (2020).
21. R. Polkinghorne and T. Ralph, "Continuous variable entanglement swapping," Phys. Rev. Lett. **83**, 2095 (1999).
22. T. C. Ralph, "Security of continuous-variable quantum cryptography," Phys. Rev. A **62**, 062306 (2000).
23. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
24. F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," arXiv, arXiv quant-ph/0204127 (2002).
25. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
26. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," Phys. Rev. Lett. **93**, 170504 (2004).
27. F. Grosshans and N. J. Cerf, "Continuous-variable quantum cryptography is secure against non-Gaussian attacks," Phys. Rev. Lett. **92**, 047905 (2004).
28. M. Navascués, F. Grosshans, and A. Acin, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," Phys. Rev. Lett. **97**, 190502 (2006).
29. R. Garca-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**, 190503 (2006).
30. J. Lodewyck and P. Grangier, "Tight bound on the coherent-state quantum key distribution with heterodyne detection," Phys. Rev. A **76**, 022332 (2007).
31. J. Sudjana, L. Magnin, R. Garca-Patrón, and N. J. Cerf, "Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching," Phys. Rev. A **76**, 052301 (2007).
32. R. Renner and J. I. Cirac, "de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," Phys. Rev. Lett. **102**, 110504 (2009).
33. M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," Phys. Rev. Lett. **102**, 020504 (2009).
34. A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," Phys. Rev. Lett. **102**, 180504 (2009).
35. Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," Phys. Rev. A **79**, 012307 (2009).
36. A. Leverrier and P. Grangier, "Simple proof that gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **81**, 062314 (2010).
37. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
38. A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation," Phys. Rev. A **83**, 042312 (2011).
39. A. Leverrier, R. Garca-Patrón, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," Phys. Rev. Lett. **110**, 030502 (2013).
40. A. Leverrier, "Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction," Phys. Rev. Lett. **118**, 200501 (2017).
41. K. Brádler and C. Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," Phys. Rev. A **97**, 022310 (2018).
42. S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," Phys. Rev. X **9**, 021059 (2019).
43. OSA Industry Development Associates, *OIDA Quantum Photonics Roadmap* (2020).
44. A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-switching quantum key distribution using broadband modulated coherent light," Phys. Rev. Lett. **95**, 180503 (2005).
45. B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," Phys. Rev. A **76**, 052323 (2007).
46. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378–381 (2013).
47. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**, 041009 (2015).
48. D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," Phys. Rev. X **5**, 041010 (2015).
49. Z. Qu, I. B. Djordjevic, and M. A. Neifeld, "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection," Opt. Lett. **41**, 5507–5510 (2016).
50. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**, 19201 (2016).
51. D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," Opt. Lett. **41**, 3511–3514 (2016).
52. S. Kleis, M. Rueckmann, and C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," Opt. Lett. **42**, 1588–1591 (2017).
53. F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," Quantum **3**, 193 (2019).
54. G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nat. Photonics **13**, 839–842 (2019).
55. Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, "Continuous-variable QKD over 50 km commercial fiber," Quantum Sci. Technol. **4**, 035006 (2019).

56. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
57. H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, "High-speed Gaussian-modulated continuous-variable quantum key distribution with a local oscillator based on pilot-tone-assisted phase compensation," Opt. Express **28**, 32882–32893 (2020).
58. S. Ren, S. Yang, A. Wonfor, I. White, and R. Penty, "Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator," Sci. Rep. **11**, 9454 (2021).
59. W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, "Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance," PRX Quantum **2**, 040334 (2021).
60. G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, J. Teng, W. Chen, G.-C. Guo, and Z.-F. Han, "Measurement-device-independent quantum key distribution for nonstandalone networks," Photon. Res. **9**, 1881–1891 (2021).
61. F.-Y. Lu, X. Lin, S. Wang, G.-J. Fan-Yuan, P. Ye, R. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, G.-C. Guo, and Z.-F. Han, "Intensity modulator for secure, stable, and high-performance decoy-state quantum key distribution," npj Quantum Inf. **7**, 75 (2021).
62. S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," Nat. Photonics **16**, 154–161 (2022).
63. G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, and Z.-F. Han, "Robust and adaptable quantum key distribution network without trusted nodes," Optica **9**, 812–823 (2022).
64. F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, "Hacking measurement-device-independent quantum key distribution," Optica **10**, 520–527 (2023).
65. Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature **589**, 214–219 (2021).
66. J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," npj Quantum Inf. **5**, 101 (2019).
67. A. Wonfor, C. White, A. Lord, R. Nejabati, T. P. Spiller, J. F. Dynes, A. J. Shields, and R. V. Penty, "Quantum networks in the UK," Proc. SPIE **11712**, 1171207 (2021).
68. T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, H.-F. Zhang, K. Cui, H. Liang, X.-G. Li, Y. Mao, L.-J. Wang, S.-B. Feng, Q. Chen, Q. Zhang, L. Li, N.-L. Liu, C.-Z. Peng, X. Ma, Y. Zhao, and J.-W. Pan, "Implementation of a 46-node quantum metropolitan area network," npj Quantum Inf. **7**, 134 (2021).
69. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69–72 (2013).
70. C.-H. Yeh, C.-W. Chow, and C.-H. Hsu, "40-Gb/s time-division-multiplexed passive optical networks using downstream OOK and upstream OFDM modulations," IEEE Photon. Technol. Lett. **22**, 118–120 (2009).
71. C. Xia, N. Chand, A. Velázquez-Bentez, Z. Yang, X. Liu, J. E. Antonio-Lopez, H. Wen, B. Zhu, N. Zhao, F. Effenberger, R. Amezcua-Correa, and G. Li, "Time-division-multiplexed few-mode passive optical network," Opt. Express **23**, 1151–1158 (2015).
72. A. Wang, L. Zhu, J. Liu, C. Du, Q. Mo, and J. Wang, "Demonstration of hybrid orbital angular momentum multiplexing and time-division multiplexing passive optical network," Opt. Express **23**, 29457–29466 (2015).
73. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," Appl. Phys. Lett. **70**, 793–795 (1997).
74. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New J. Phys. **4**, 41 (2002).
75. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," Phys. Rev. Lett. **96**, 070502 (2006).
76. P. Zhang, K. Aungskunsiri, E. Martn-López, J. Wabnig, M. Lobino, R. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, "Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client," Phys. Rev. Lett. **112**, 130501 (2014).
77. D. Huang, P. Huang, T. Wang, H. Li, Y. Zhou, and G. Zeng, "Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol," Phys. Rev. A **94**, 032305 (2016).
78. https://www.idquantique.com.
79. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A **73**, 022320 (2006).
80. F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," New J. Phys. **12**, 113026 (2010).
81. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
82. N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," New J. Phys. **16**, 123030 (2014).
83. N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk analysis of trojan-horse attacks on practical quantum key distribution systems," IEEE J. Sel. Top. Quantum Electron. **21**, 168–177 (2014).
84. M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. Yuan, and A. J. Shields, "Practical security bounds against the trojan-horse attack in quantum key distribution," Phys. Rev. X **5**, 031030 (2015).
85. Y. Huang, T. Shen, X. Wang, Z. Chen, B. Xu, S. Yu, and H. Guo, "Realizing a downstream-access network using continuous-variable quantum key distribution," Phys. Rev. Appl. **16**, 064051 (2021).
86. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nat. Commun. **8**, 15043 (2017).
87. M. Fujiwara, J.-I. Kani, H. Suzuki, and K. Iwatsuki, "Impact of back-reflection on upstream transmission in WDM single-fiber loopback access networks," J. Lightwave Technol. **24**, 740–746 (2006).
88. D. Subacius, A. Zavriyev, and A. Trifonov, "Backscattering limitation for fiber-optic quantum key distribution systems," Appl. Phys. Lett. **86**, 011103 (2005).
89. R. Hui, *Introduction to Fiber-Optic Communications* (Academic, 2019).
90. F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations," Adv. Quantum Technol. **1**, 1800011 (2018).