Fully connected twin-field quantum key distribution network

Chunfeng Huang[1], Rui Guan[1], Xin Liu[1], Wenjie He[1], Shizhuo Li[1], Hao Liang[1], Ziyang Luo[1], Zhenrong Zhang[2], Wei Li[3,4], and Kejin Wei[1]
[1] *Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning 530004, China*
[2] *Guangxi Key Laboratory of Multimedia Communications and Network Technology, School of Computer Electronics and Information, Guangxi University, Nanning 530004, China*
[3] *School of Artificial Intelligence Science and Technology, University of Shanghai for Science and Technology, Shanghai 200093, China*
[4] *Institute of Photonic Chips, University of Shanghai for Science and Technology, Shanghai 200093, China*

Quantum key distribution (QKD) is a key application in quantum communication, enabling secure key exchange between parties using quantum states. Twin-field (TF) QKD offers a promising solution that surpasses the repeaterless limits, and its measurement-device-independent nature makes it suitable for star-type network architectures. In this work, we propose and demonstrate a fully connected TF-QKD network architecture, where users prepare quantum signals and send them to network nodes. These nodes use splitters to route the signals to measurement units, enabling secure key distribution among arbitrary users. A proof-of-principle demonstration with three users successfully achieved secure key sharing over simulated link losses of up to 30 dB, with an average rate of 5.01×10^{-7} bit per pulse. Additionally, simulations show that the architecture can support up to 32 users with a secure key rate of 280.90 bits/s under typical fiber loss conditions. This approach represents a significant advancement in the topology of untrusted-node QKD networks and holds promise for practical, large-scale applications in secure communication.

I. INTRODUCTION

Quantum key distribution (QKD) is one of the most mature applications of quantum information processing [1]. It uses quantum states to securely distribute symmetric keys between communication parties. Since the first QKD protocol was proposed [2], significant efforts have steadily advanced QKD technology [3–8]. Recently, a record-breaking achievement was made, with secure key rates exceeding tens of megahertz [5, 6]. Trusted-node QKD networks [9–14], including integrated space-ground quantum communication networks [14], have been rapidly advancing. However, challenges persist, particularly in long-distance transmission and network expansion, both of which are crucial for the wider deployment of QKD.

In previous protocols and systems [15, 16], the key generation rate decreases exponentially as the transmission distance increases. Without quantum repeaters, QKD is unable to overcome the fundamental rate-distance limits [17, 18]. Fortunately, twin-field (TF) QKD [19] provides a practical long-distance solution that exceeds the repeaterless limit. Several protocol variants have been proposed to improve practicality [20–23], such as sending-or-not-sending (SNS) [21] and no-phase-post selection (NPP) [22, 23], which partially eliminate the need for phase-slice post-selection. Significant experimental advances have confirmed TF-QKD's superior rate-loss scaling [24–28], with recent demonstrations extending beyond 1000 km [28].

Similar to measurement-device-independent QKD [29], participants in TF-QKD send quantum signals to an intermediate measurement node, enabling immunity to all potential side-channel attacks on measurement devices. This configuration is well-suited for star-type network expansion. However, the stringent requirements of twin-field phase tracking, typically involving additional service fibers and optical frequency-locking hardware, present challenges to building the scalability of TF-QKD networks. Recently, TF-QKD networks based on various TF-QKD network architechture including a simple ring architechture [30] and a $2 \times N$ plug-and-play architechture [31] have been proposed to bypass using phase and frequency locking techonolgy. However, these network architectures require additional components to prevent security vulnerabilities associated with bidirectional optical paths [32–35]. Furthermore, to enable multi-user key distribution, time-division multiplexing of a single detection unit is required. This presents a significant challenge to the detector's bandwidth as the number of users increases, thereby reducing the achievable secure key rate per user.

In this study, we propose and demonstrate a fully connected TF-QKD network architecture. Our architecture is inspired by recent advancements in protocols [36–38] and open-architecture TF-QKD schemes [39–43], eliminating the need for additional channels and de-

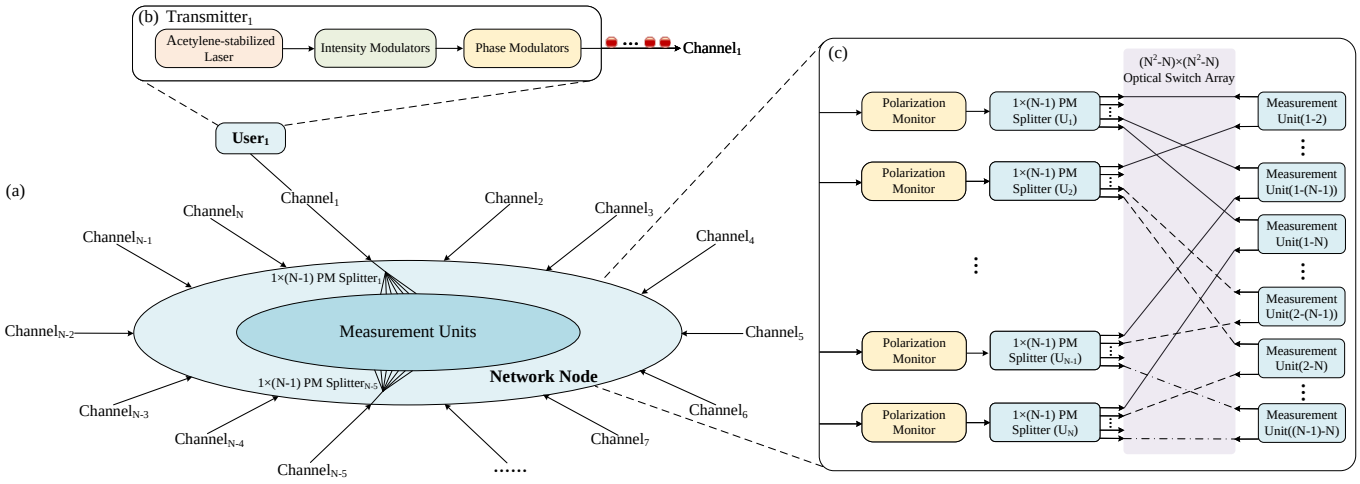

FIG. 1. (a) Schematic of the physical layer of the fully connected TF QKD network architecture for N users. (b) Schematic of the user transmitter device, which includes frequency-stabilized coherent light based on a local frequency references, intensity modulations, and phase modulations. (c) Schematic of the network node configuration, which includes the same number of polarization alignment modules and $1 \times (N-1)$ polarization-maintaining splitters, along with an optical switch array and measurement units satisfying a fully connected setup.

vices to synchronize the frequencies of independent light sources, thereby offering greater flexibility and scalability. Furthermore, each user prepares quantum signals and sends them to a network node in single-path transmission, which inherently provides immunity to bidirectional transmission security vulnerabilities. Furthermore, the node employs beam splitters to route the received quantum signals to different single-photon interference measurement units, enabling secure key distribution among arbitrary users. We conduct a proof-of-principle demonstration of a three-user fully connected TF-QKD network, where secure key sharing is successfully achieved between any pair of users over a simulated link loss of up to 30 dB, with an average rate of 5.01×10^{-7} bit per pulse. Additionally, we perform simulations based on the parameters of the experimental system. The results show that our network architecture can support up to 32 users in a symmetric scenario, with a secure key rate of 280.90 bits/s between user pairs under a fiber channel loss of 20 dB. This network architecture enhances the topology of untrusted-node QKD networks and promotes their practical applications.

II. NETWORK ARCHITECTURE

The fully connected TF QKD network architecture is depicted in Figure 1. The physical layer adopts a star topology consisting of end users, fiber channels, and untrusted network node, as shown in Figure 1(a). Each user is equipped with a transmitter, located at the terminal of channel extending from the central node, as shown in Figure 1(b). The network node includes polarization monitors, polarization-maintaining splitters, an optical switch array, and single-photon interference measurement units. Full connectivity among multiple users is achieved through the designed of nodal components, as exemplified in Figure 1(c).

An N-user network instance is considered here to further elucidate our network. Each user's transmitter comprises a laser source, intensity modulators, and phase modulators. The user prepares frequency-stabilized light signal based on a local frequency reference, then modulate the light signal's intensity and phase according to the specific TF-QKD protocol. The modulated signal is transmitted to network nodes via fiber channel.

The polarization monitor at the network node tracks and compensates for polarization drift in the user signal. The signal is then aligned and coupled into a $1 \times (N-1)$ polarization-maintaining splitter, where it is randomly directed to one of its branches. The $N-1$ branches of the splitter enable connections between the user and the remaining $N-1$ users. The $(N^2-N) \times (N^2-N)$ optical switch array allocates input ports to the branches of all splitters. For example, any user who intends to communicate with User-1 can establish a complete quantum channel by accessing the measurement unit through the optical switch. For an N-user network, up to $N \times (N-1)/2$ measurement units are required to achieve full connectivity. Figure 1(c) shows an N-user fully connected configuration. Considering some dedicated line communication scenarios, network node can also form a static configuration by directly wiring splitters and measurement units, as demonstrated in the three-user network in Section III.

In this network, key distribution between any pair of users is implemented based on the TF-QKD protocol, which requires coherent control of the light fields from remote users. The frequency difference between independent user lasers or phase shifts induced by channel fluctuations affect the coherence of these light fields. Building

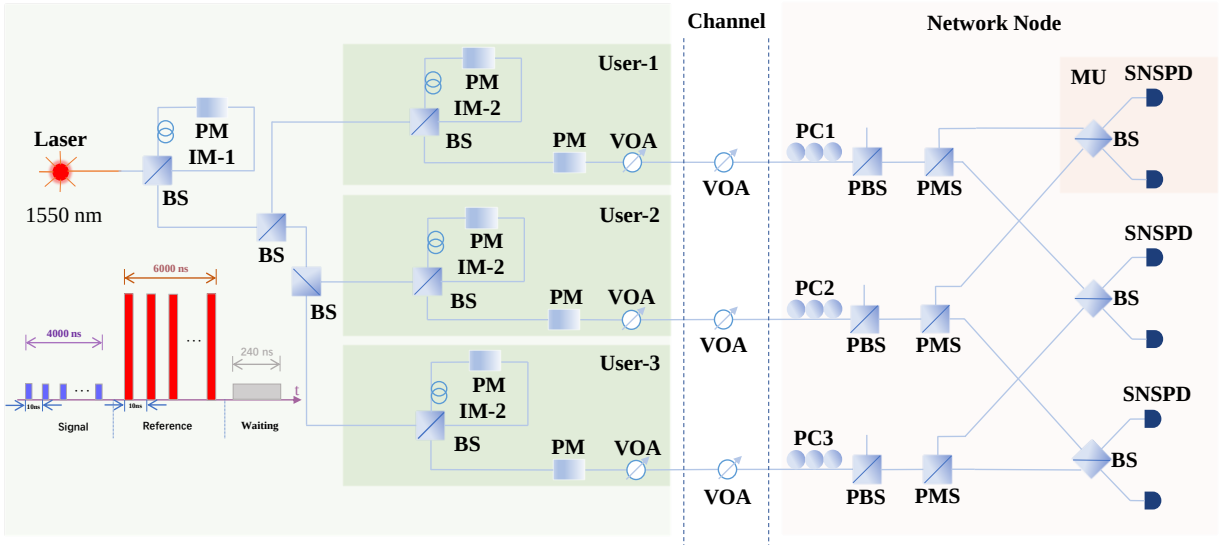

FIG. 2. Schematic of our experimental setup. A commercial laser serves as the light source for all users. Each frame of light pulse is modulated by the first intensity modulation module (IM-1) into 400 signal pulses, 600 reference pulses, and 24 vacuum pulses. The intensity modulation module includes beam splitter (BS) and a phase modulator (PM). Subsequently, each user employs a second intensity modulation module (IM-2) and a phase modulator (PM) to implement encoding, decoy intensity modulation, and discrete random phase modulation on the optical pulses. The pulses are then attenuated via a variable optical attenuator (VOA), followed by a simulated channel using VOA. At the network node, quantum signals from user pass through polarization controller (PC) and polarization beam splitter (PBS), then couple into a polarization-maintaining splitter (PMS). The signals from the user pairs interfere at a BS within the measurement unit (MU). Finally, the quantum signals are detected by superconducting nanowire single-photon detectors (SNSPDs).

on recent advancements [43], users can employ acetylene-stabilized laser, eliminating the need for a shared optical frequency reference. This makes it possible for the independent lasers of users in the network to maintain frequency alignment using a local frequency reference. Furthermore, there are mature solutions to effectively compensate for the phase shifts caused by fiber fluctuations over several hundred kilometers, either through real-time feedback [26, 27, 39] or post-processing techniques [28, 43].

III. EXPERIMENT

To validate the proposed architecture, we build a proof-of-principle experimental setup, which includes three fully connected users in a TF-QKD network. Figure 2 shows the schematic of experimental setup. A laser source operating at 1550 nm generates optical pulses at a 100 MHz clock rate, with a pulse width of approximately 500 ps. These pulses enter the first intensity modulation module (IM-1), which is a Sagnac-based interferometer. The optical pulses are modulated into sequential frame-based signals. Specifically, each frame consists of 1024 optical pulses, comprising 400 signal pulses, 600 reference pulses and 24 vacuum pulses. These pulses are then sent to the three users.

Each user encodes the signal pulses according to the three-intensity sending-or-not-sending (SNS) TF QKD protocol [44, 45] by employing the second intensity modulation module (IM-2), thereby producing a signal window for key extraction and a decoy window to estimate information leakage. Subsequently, a phase modulator (PM) is employed to perform 16-level random phase modulation over a range of 2π to the signal pulses. Finally, the signal pulses are attenuated to the single-photon level using a variable optical attenuator (VOA) before entering the channel.

Signals from different users reach the network node through a channel simulated by a VOA. The arriving quantum signals are first processed by a polarization controller (PC) to align their polarization to the one of orthogonal modes of the followed polarization beam splitter (PBS). The signals are then efficiently coupled into a 1×2 fast-axis block polarization-maintaining splitter (PMS), and randomly routed to different branches with the same polarization. The signals from the user pairs interfere with the same polarization at the beam splitter (BS) within the measurement unit (MU). The interference outputs between user pairs are detected by two superconducting nanowire single-photon detectors (SNSPDs), with detection efficiency around 45% and a dark count rate of about 8×10^{-8}. The detected photon events are recorded by the TDC and then processed by a computer. The detection events of the reference pulse are used in post-processing to estimate the phase fluctuation between users. Within the effective arrival time t, the detection events in the decoy window are further

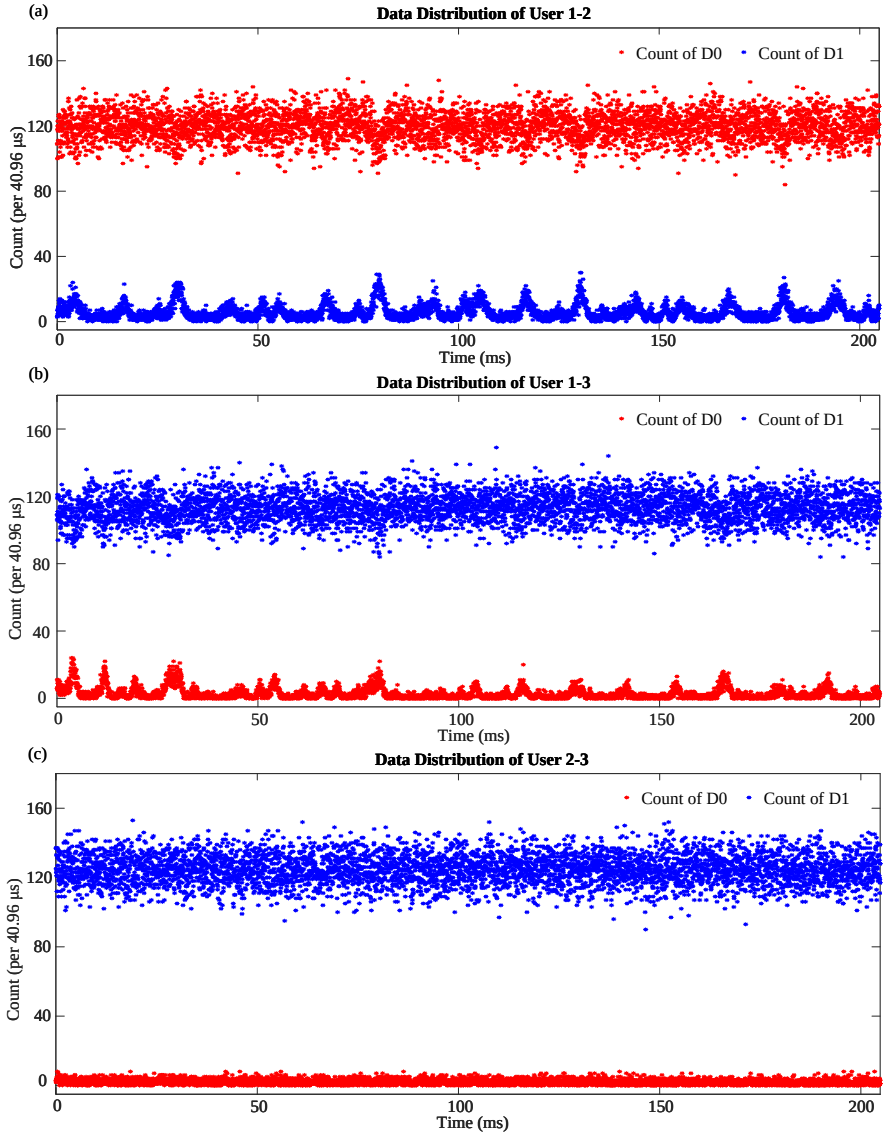

FIG. 3. Interference results between users in a three-user fully connected network within 200 ms. The interference results are captured by recording the counts of the detectors D0 and D1. The average interference visibilities for user pairs 1-2, 1-3, and 2-3 are 90.87%, 95.82%, and 96.72%, respectively.

filtered according to the following condition:

$$|\cos(\theta_i - \theta_j - \varphi_{ij})| \geq \cos(\pi/16), \tag{1}$$

where θ_i (θ_i) is the encoded phase of user-i (j) to be announced in post-processing, and φ_{ij} is the phase fluctuation between users. We also apply the actively odd-parity pairing (AOPP) method [45] to suppress bit-flip errors and improve the secure key rate.

IV. RESULTS

Using the described network system, we first measure the interference between users to preliminarily assess system performance. The measurement is conducted with the phase modulator installed but not actively modulating. The interference results are obtained by monitoring the counts from detectors in the MU, as shown in Figure 3. We observe that the average interference visibilities for user pairs 1-2, 1-3, and 2-3 are 90.87%, 95.82%, and 96.72%, respectively, over a period of approximately 200 ms. Due to the single laser scheme adopted, phase fluctuations affecting interference visibility in the experiment primarily originate from optical components.

We then perform a three-user TF-QKD network experiment. The transmittance for the users is simulated using optical attenuators, which model the transmittance of fiber links with lengths of 100 km and 150 km, assuming a loss coefficient of 0.2 dB/km. Based on the similar

transmittance of all users, we select the same implementation parameters for simplicity. Considering the finite-key effect, the secure key rate of after AOPP is calculated using [45]

$$R = \frac{1}{N}\{n_1'(1-h(e_1^{'ph})) - f n_t' h(E') - 2\log_2\frac{2}{\varepsilon_{cor}} - 4\log_2\frac{1}{\sqrt{2}\varepsilon_{PA}\hat{\varepsilon}}\}, \tag{2}$$

where N is the total number of send pulse pairs, $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy function. f is the error correction efficiency equal to 1.1. n_t' is the number of remaining bits after AOPP. E' is the bit-flip error rate of the remaining bits after AOPP. ε_{cor} is the failure probability of error correction, ε_{PA} is the failure probability of privacy amplification, $\hat{\varepsilon}$ is the coefficient obtained using the chain rules of smooth min- and max-entropy, with all three parameters being set to 10^{-10}. Detailed parameter estimation for the three-intensity SNS-TF QKD with AOPP protocol can be found in Appendix A.

For each transmittance level, a total of 10^{10} signal pulses are emitted by each user. The detection events of the reference pulses are extracted within a time window of 200 ms, and only the data with stable interference are retained. We estimate phase fluctuation from the reference data during this time interval and apply these values to compensate for the phase fluctuation of signal pulses for secure key generation. As shown in Figure 4(a), the secure key rate for user pairs 1-2, 1-3, and 2-3 is respectively 2.38×10^{-8} (6.87×10^{-6}), 1.88×10^{-7} (9.35×10^{-6}), and 1.29×10^{-6} (2.02×10^{-5}) bits/pulse under a simulated channel loss of 30 (20) dB. Detailed implementation parameters and measurement results are summarized in Appendix B.

To evaluate the network's performance with an increasing number of users, we consider our system parameters along with the splitter loss and clock rate parameters from reference [46]. The network performance in a symmetric scenario is shown in Figure 4(b). The results indicate that this network architecture can support a 32-user fully connected network, achieving secure key rates of 490.63 bits/s per user pair for a simulated fiber loss of 10 dB and 208.90 bits/s per user pair for a simulated fiber loss of 20 dB.

V. CONCLUSION

In summary, we propose a fully connected TF-QKD network architecture, designed to efficiently support secure key distribution among multiple users without relying on trusted nodes. Each user is connected to a central node equipped with splitters, which randomly route quantum signals to measurement units, enabling secure key sessions between arbitrary user pairs. A three-user experimental demonstrate the feasibility of this network expansion strategy, achieving stable secure key distribution across all pairwise connections. Furthermore, simulations show that this network can support up to 32 users with a secure key rate of 280.90 bits/s for user pairs under a simulated channel loss of 20 dB.

This work advances the practical deployment of untrusted-node QKD networks, offering a scalable and efficient solution for future quantum-secured communication infrastructures. Furthermore, this architecture, combined with compact integrated chip-based systems [47] and cost-effective hybrid quantum-classical system [48], is expected to further drive the practical application of QKD network. Beyond QKD, this architecture could be adapted into other quantum protocols, such as quantum digital signature [49] and quantum blockchain [50].

ACKNOWLEDGMENT

This study was supported by the National Natural Science Foundation of China (Nos. 62171144 and 62031024), Guangxi Science Foundation (Nos. 2025GXNSFAA069137 and GXR-1BGQ2424005), and Innovation Project of Guangxi Graduate Education (No. YCSW2022040).

Appendix A: Three-intensity SNS-TF QKD with active odd parity pairing (AOPP) protocol

Here, we describe the three-intensity SNS-TF QKD protocol [21, 44] adopted in our network demonstration, where the AOPP method is employed to extract the final secret key. Given that user-i and user-j in the network request key distribution session. User-$i(j)$ possesses three sources with different intensities, denoted as $\mu_{o_i}, \mu_{x_i}, \mu_{y_i}(\mu_{o_j}, \mu_{x_j}, \mu_{y_j})$, where $\mu_{o_i}(\mu_{o_j})$ represents vacuum source. In each time window, user-$i(j)$ randomly determines whether the optical pulse originates from the vacuum source $\mu_{o_i}(\mu_{o_j})$ with probability p_o, the decoy source $\mu_{x_i}(\mu_{x_j})$ with probability p_x, or a signal window with probability $p_y = 1 - p_o - p_x$. If a signal window is determined, user-$i(j)$ then randomly chooses between the source $\mu_{o_i}(\mu_{o_j})$ with probability $1-\epsilon$ and the source $\mu_{y_i}(\mu_{y_j})$ with probability ϵ. For vacuum source in the signal window, user-$i(j)$ encodes bit 0(1), whereas for source $\mu_{y_i}(\mu_{y_j})$ in the signal window, user-$i(j)$ encodes bit 1(0).

Considering a key distribution session, the total number of pulses sent by user-$i(j)$ is N. The number of source pairings $lr(l \in \{\mu_{o_i}, \mu_{x_i}, \mu_{y_i}\}, r \in \{\mu_{o_j}, \mu_{x_j}, \mu_{y_j}\})$ can be represented as N_{lr}, and the total number of corresponding single detector response events is represented as n_{lr}. The yield of source lr can be defined as $S_{lr} = n_{lr}/N_{lr}$, and the expected value is represented as $\langle S_{lr}\rangle$. Based on the above definitions, we have:

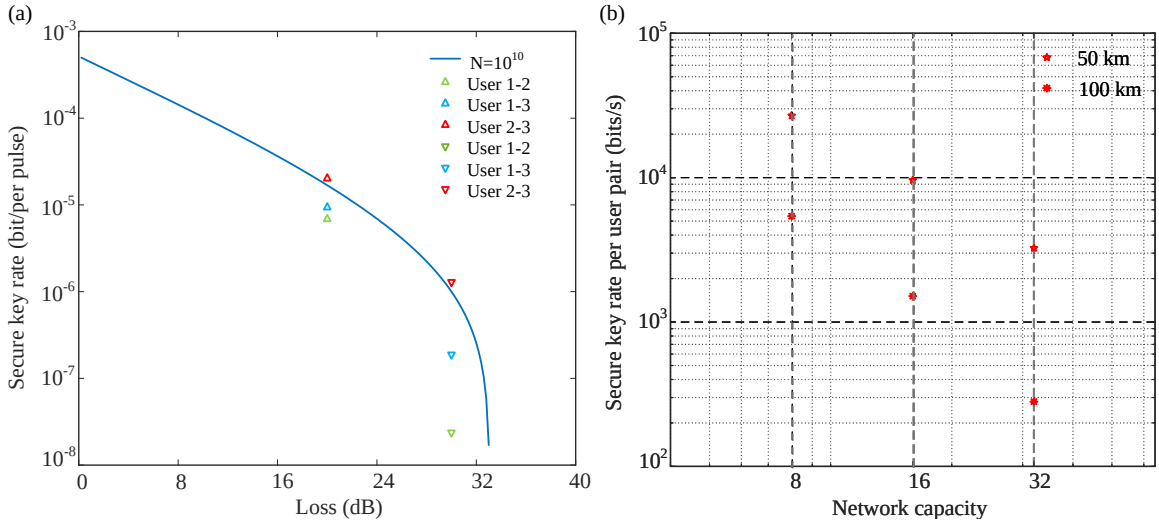

FIG. 4. (a) Experimental results in a three-user fully connected network. (b) The secure key rate per user pair in a 32-user fully connected network.

TABLE I. The three-intensity parameters under different simulated losses, including intensities and probabilities. $\{\mu_o, \mu_x, \mu_y\}$ represent three sources with different intensities. p_x is the probability of sending decoy intensity μ_x. p_y is the probability of sending the signal window. ε is the probability of sending during the signal window. μ_{ref} is the intensity of reference pulse.

Loss (dB)	μ_y	μ_x	μ_o	p_x	p_y	ε	μ_{ref}
20	0.44	0.01	0.0016	0.23	0.72	0.25	1.5
30	0.43	0.01	0.0016	0.36	0.53	0.25	1.5

$$\begin{aligned} N_{\mu_{o_i}\mu_{o_j}} &= \left[p_o^2 + 2p_o p_y(1-\varepsilon)\right] N, \\ N_{\mu_{o_i}\mu_{x_j}} = N_{\mu_{x_i}\mu_{o_j}} &= \left[p_o + p_y(1-\varepsilon)\right] p_x N, \\ N_{\mu_{o_i}\mu_{y_j}} = N_{\mu_{y_i}\mu_{o_j}} &= p_o p_y \varepsilon N. \end{aligned} \tag{A1}$$

For the time window in which user-i and user-j select source μ_{x_i} and μ_{x_j}, the users will announce the phases encoded and perform post-selection on the single detector response events based on the following conditions:

$$1 - \left|\cos\left(\theta_i - \theta_j - \varphi_{ij}\right)\right| \le \lambda, \tag{A2}$$

where θ_i and θ_j are the encoding phase of the pulses for user-i and user-j respectively, φ_{ij} the phase fluctuation between user-i and user-j, and λ is a small positive value. Let the number of source pairings satisfying the above condition be denoted as N_x, and the number of error events as m_x. Then, the error rate for the window $\mu_{x_i}\mu_{x_j}$ us given by $T_x = m_x/N_x$.

To obtain the secure key rate, the users need to estimate the lower bound of the number of untagged bits and the upper bound of the phase error rate of the untagged bits. After performing decoy state analysis, the lower bound of the expected counting rate for the states $|01\rangle\langle 01|$ and $|10\rangle\langle 10|$ can be expressed as follows:

$$\begin{aligned} \underline{\langle s_{01}\rangle} &= \frac{\mu_y^2 e^{\mu_x}\underline{\left\langle S_{\mu_{o_i}\mu_{x_j}}\right\rangle} - \mu_x^2 e^{\mu_y}\overline{\left\langle S_{\mu_{o_i}\mu_{y_j}}\right\rangle} - \left(\mu_y^2 - \mu_x^2\right)\overline{\left\langle S_{\mu_{o_i}\mu_{o_j}}\right\rangle}}{\mu_y\mu_x\left(\mu_y - \mu_x\right)}, \\ \underline{\langle s_{10}\rangle} &= \frac{\mu_y^2 e^{\mu_x}\underline{\left\langle S_{\mu_{x_i}\mu_{o_j}}\right\rangle} - \mu_x^2 e^{\mu_y}\overline{\left\langle S_{\mu_{y_i}\mu_{o_j}}\right\rangle} - \left(\mu_y^2 - \mu_x^2\right)\overline{\left\langle S_{\mu_{o_i}\mu_{o_j}}\right\rangle}}{\mu_y\mu_x\left(\mu_y - \mu_x\right)}, \end{aligned} \tag{A3}$$

then the lower bound of the counting rate for the untagged bits can be expressed as follows:

$$\underline{\langle s_1\rangle} = \frac{1}{2}(\underline{\langle s_{01}\rangle} + \underline{\langle s_{10}\rangle}). \tag{A4}$$

The lower bound of the expected values for the number of untagged bit 1 and untagged bit 0 are given by:

$$\begin{aligned} \underline{\langle n_{10}\rangle} &= N p_y^2 \epsilon(1-\epsilon)\mu_y e^{-\mu_y}\underline{\langle s_{10}\rangle}, \\ \underline{\langle n_{01}\rangle} &= N p_y^2 \epsilon(1-\epsilon)\mu_y e^{-\mu_y}\underline{\langle s_{01}\rangle}. \end{aligned} \tag{A5}$$

The upper bound of the expected values for the phase error rate 1 is given by:

$$\overline{\left\langle e_1^{ph}\right\rangle} = \frac{\langle T_x\rangle - e^{-2\mu_x}\left\langle S_{\mu_{o_i}\mu_{o_j}}\right\rangle/2}{2\mu_x e^{-2\mu_x}\underline{\langle s_1\rangle}}. \tag{A6}$$

TABLE II. Detailed experimental results under different simulated losses, including the secure key rate considering finite-key effect and AOPP. The detection events are labeled as "Detected-$ijab$", where '$i(j)$' and '$a(b)$' represent the signal Z or decoy X time windows and intensities determined by user-$i(j)$.

	User1-2	User1-3	User2-3	User1-2	User1-3	User2-3
Loss (dB)	20			30		
N	10^{10}			10^{10}		
R (bits/pulse)	6.8×10^{-6}	9.35×10^{-6}	2.02×10^{-5}	$2.38\times10-8$	1.88×10^{-7}	1.29×10^{-6}
Detected $ZZyy$	3984035	4077966	3645054	854517	601800	648818
Detected $ZZoy$	6088650	5973265	5217181	1022963	954205	912414
Detected $ZZyo$	5160981	4848325	6250619	912024	751293	1024881
Detected $ZZoo$	147816	85275	105192	12931	11578	16709
Detected $ZXyx$	2348664	2261991	2816486	791683	1046887	1003973
Detected $ZXox$	166084	182167	213010	95600	32038	71703
Detected $ZXyo$	445273	594330	552265	179775	359825	206623
Detected $ZXoo$	14484	6656	12434	5705	3344	6423
Detected $XZxy$	2421535	1853833	2490897	992859	983220	784572
Detected $XZoy$	587264	501135	407128	349189	202943	228031
Detected $XZxo$	211380	192685	140001	34267	97368	70640
Detected $XZoo$	15243	7888	12356	7475	2976	4317
Detected $XXxx$	130416	180341	127632	103282	104274	145071
Detected $XXox$	16158	13966	24151	23824	12949	22445
Detected $XXxo$	18007	14983	12346	13302	25180	21872
Detected $XXoo$	350	788	475	702	1518	651
Detected $XXxx$-accepted	19109	26176	20232	17799	19131	23062
Correct $XXxx$-accepted	17381	24176	18694	16538	17859	21208
QBER ZZ before AOPP	26.86%	27.78%	24.64%	30.95%	26.45%	25.57%
QBER ZZ after AOPP	1.84%	1.19%	1.16%	1.16%	0.95%	1.13%

We further calculate the lower bounds on the number of untagged bit n_1' and the phase error rate $e_1'^{ph}$ after AOPP according to the methods in reference [45]. The related formulas of n_1' are as follows:

$$
\begin{aligned}
u &= \frac{n_g}{2n_{odd}},\\
\underline{n_{10}} &= \varphi^L(\underline{\langle n_{10}\rangle}),\\
\underline{n_{01}} &= \varphi^L(\underline{\langle n_{01}\rangle}),\\
\underline{n_1} &= \underline{n_{01}} + \underline{n_{01}},\\
n_1^r &= \varphi^L\left(\frac{\underline{n_1}}{n_t}\frac{\underline{n_1}}{n_t}\frac{un_t}{2}\right),\\
n_{10}' &= 2n_1^r\left(\frac{\underline{n_{10}}}{\underline{n_1}} - \sqrt{\frac{-\ln\epsilon}{2n_1^r}}\right),\\
n_{01}' &= 2n_1^r\left(\frac{\underline{n_{01}}}{\underline{n_1}} - \sqrt{\frac{-\ln\epsilon}{2n_1^r}}\right),\\
n_{min} &= \min(n_{01}', n_{10}'),\\
n_1' &= 2\varphi^L\left(n_{min}\left(1-\frac{n_{min}}{2n_1^r}\right)\right),
\end{aligned}
\tag{A7}
$$

where n_t is the raw key generated by users-i and user-j, n_g is the number of pair if users-i and user-j perform AOPP to their raw keys. n_{odd} is the number of pair with odd-parity when user-j randomly groups their raw keys two by two. ϵ is the failure probability of parameter estimation. $\varphi^U(x)$ and $\varphi^L(x)$ are the upper and lower bounds after using Chernoff bound [51] to estimate the real values based on the expected values.

The related formulas of $e_1'^{ph}$ are as follows:

$$
\begin{aligned}
r &= \frac{\underline{n_1}}{\underline{n_1}-2n_1^r}\ln\frac{3(\underline{n_1}-2n_1^r)^2}{\epsilon},\\
e_\tau &= \frac{\varphi^U(2n_1^r\overline{\langle e_1^{ph}\rangle})}{2n_1^r - r},\\
\overline{M_s} &= \varphi^U((n_1^r - r)e_\tau(1-e_\tau)) + r,\\
e_1'^{ph} &= \frac{2\overline{M_s}}{n_1'}.
\end{aligned}
\tag{A8}
$$

Finally, the secure key rate can expressed by:

$$R = \frac{1}{N}\{n_1'(1-h(e_1^{'ph})) - f n_t' h(E') - 2\log_2\frac{2}{\varepsilon_{cor}} - 4\log_2\frac{1}{\sqrt{2}\varepsilon_{PA}\hat{\varepsilon}}\}. \tag{A9}$$

Appendix B: Detailed experimental results

Here, we summarize the parameters of the three-intensity SNS protocol used in our experiment, as shown in Table I. Table II presents detailed experimental results under different simulated losses, including the single-detector response events used to calculate the secure key rate and the AOPP results.

[1] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, 10.1126/science.aam9288 (2018).

[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, Bangalore, India, 1984) pp. 175–179.

[3] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 10.1103/PhysRevLett.117.190501 (2016).

[4] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, Phys. Rev. Lett. **121**, 10.1103/PhysRevLett.121.190502 (2018).

[5] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussières, and Z. Hugo, Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, Nat. Photon. **17**, 422 (2023).

[6] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, High-rate quantum key distribution exceeding 110 mb s-1, Nat. Photon. **17**, 416 (2023).

[7] Y.-H. Li, S.-L. Li, X.-L. Hu, C. Jiang, Z.-W. Yu, W. Li, W.-Y. Liu, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, F. Xu, Q. Zhang, X.-B. Wang, Y. Cao, C.-Z. Peng, and J.-W. Pan, Free-space and fiber-integrated measurement-device-independent quantum key distribution under high background noise, Phys. Rev. Lett. **131**, 10.1103/PhysRevLett.131.100802 (2023).

[8] Y. Li, W.-Q. Cai, J.-G. Ren, C.-Z. Wang, M. Yang, L. Zhang, H.-Y. Wu, L. Chang, J.-C. Wu, B. Jin, H.-J. Xue, X.-J. Li, H. Liu, G.-W. Yu, X.-Y. Tao, T. Chen, C.-F. Liu, W.-B. Luo, J. Zhou, H.-L. Yong, Y.-H. Li, F.-Z. Li, C. Jiang, H.-Z. Chen, C. Wu, X.-H. Tong, S.-J. Xie, F. Zhou, W.-Y. Liu, Y. Ismail, F. Petruccione, N.-L. Liu, L. Li, F. Xu, Y. Cao, J. Yin, R. Shu, X.-B. Wang, Q. Zhang, J.-Y. Wang, S.-K. Liao, C.-Z. Peng, and J.-W. Pan, Microsatellite-based real-time quantum key distribution, Nature 10.1038/s41586-025-08739-z (2025).

[9] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J. D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J. B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, The secoqc quantum key distribution network in vienna, New J. Phys. **11**, 10.1088/1367-2630/11/7/075001 (2009).

[10] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Field test of quantum key distribution in the tokyo qkd network, Opt. Express **19**, 10387 (2011).

[11] 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**, 10.1364/oe.22.021739 (2014).

[12] J. F. Dynes, A. Wonfor, W. W. S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. 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**, 10.1038/s41534-019-0221-4 (2019).

[13] 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).
[14] 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 (2021).
[15] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photon. **8**, 595 (2014).
[16] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. **2**, 16025 (2016).
[17] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).
[18] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).
[19] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).
[20] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 10.1103/PhysRevX.8.031043 (2018).
[21] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 10.1103/PhysRevA.98.062323 (2018).
[22] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 10.1103/PhysRevApplied.11.034053 (2019).
[23] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 10.1038/s41534-019-0175-6 (2019).
[24] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photon. **13**, 334 (2019).
[25] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km, Phys. Rev. Lett. **124**, 10.1103/PhysRevLett.124.070501 (2020).
[26] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nature Photonics **15**, 530 (2021).
[27] 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, Nature Photonics **16**, 154 (2022).
[28] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution over 1000 km fiber distance, Phys. Rev. Lett. **130**, 210801 (2023).
[29] H. K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[30] X. Zhong, W. Wang, R. Mandil, H.-K. Lo, and L. Qian, Simple multiuser twin-field quantum key distribution network, Phys. Rev. Appl. **17**, 014025 (2022).
[31] C. H. Park, M. K. Woo, B. K. Park, Y.-S. Kim, H. Baek, S.-W. Lee, H.-T. Lim, S.-W. Jeon, H. Jung, S. Kim, and S.-W. Han, 2 × n twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing, npj Quantum Inf. **8**, 48 (2022).
[32] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 10.1103/PhysRevA.73.022320 (2006).
[33] Y. Zhao, B. Qi, and H.-K. Lo, Quantum key distribution with an unknown and untrusted source, Phys. Rev. A **77**, 052327 (2008).
[34] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, Security analysis of an untrusted source for quantum key distribution: passive approach, New Journal of Physics **12**, 023024 (2010).
[35] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, New Journal of Physics **16**, 10.1088/1367-2630/16/12/123030 (2014).
[36] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).
[37] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 10.1103/PRXQuantum.3.020315 (2022).
[38] X. Liu, D. Luo, Z. Zhang, and K. Wei, Mode-pairing quantum key distribution with advantage distillation, Phys. Rev. A **107**, 062613 (2023).
[39] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, Nat. Commun. **14**, 928 (2023).
[40] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, and J.-W. Pan, Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking, Phys. Rev. Lett. **130**, 10.1103/PhysRevLett.130.030801 (2023).
[41] W. Li, L. Zhang, Y. Lu, Z. P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X. B. Wang, Q. Zhang, L. You, F. Xu, and J. W. Pan, Twin-field quantum key distribution without phase locking, Phys Rev Lett **130**, 250802 (2023).
[42] L. Zhou, J. Lin, C. Ge, Y. Fan, Z. Yuan, H. Dong, Y. Liu, D. Ma, J.-P. Chen, C. Jiang, X.-B. Wang, L.-X. You, Q. Zhang, and J.-W. Pan, Independent-optical-frequency-comb-powered 546-km field test of twin-field quantum key distribution, Phys. Rev. Appl. **22**, 10.1103/PhysRevApplied.22.064057 (2024).
[43] J.-P. Chen, F. Zhou, C. Zhang, C. Jiang, F.-X. Chen, J. Huang, H. Li, L.-X. You, X.-B. Wang, Y. Liu, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution with local frequency reference, Phys. Rev. Lett. **132**, 10.1103/PhysRevLett.132.260802 (2024).

[44] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution in practice, Sci. Rep. **9**, 10.1038/s41598-019-39225-y (2019).

[45] C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, Composable security for practical quantum key distribution with two way classical communication, New J. Phys. **23**, 10.1088/1367-2630/ac0285 (2021).

[46] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, A quantum access network, Nature **501**, 69 (2013).

[47] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-speed measurement-device-independent quantum key distribution with integrated silicon photonics, Phys. Rev. X **10**, 10.1103/PhysRevX.10.031030 (2020).

[48] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, S. Juarez, P. Rydlichowski, D. Vicinanza, G. Roberts, and A. J. Shields, Coherent quantum communications across national scale telecommunication infrastructure (2024), arXiv:2405.11990 [quant-ph].

[49] Y. Du, B.-H. Li, X. Hua, X.-Y. Cao, Z. Zhao, F. Xie, Z. Zhang, H.-L. Yin, X. Xiao, and K. Wei, Chip-integrated quantum signature network over 200 km, Light Sci. Appl. **14**, 108 (2025).

[50] C.-X. Weng, R.-Q. Gao, Y. Bao, B.-H. Li, W.-B. Liu, Y.-M. Xie, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, Beating the fault-tolerance bound and security loopholes for byzantine agreement with a quantum solution, Research **6**, 0272 (2023).

[51] H. Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, The Annals of Mathematical Statistics **23**, 493 (1952).