Research
A SCIENCE PARTNER JOURNAL

RESEARCH ARTICLE

Experimental Efficient Source-Independent Quantum Conference Key Agreement

Wen-Ji Hua[1,2†], Yi-Ran Xiao[1,2†], Yu Bao[1,2], Hua-Lei Yin[2,1,3,4*], and Zeng-Bing Chen[1*]

[1]National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China. [2]School of Physics and Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, Beijing 100872, China. [3]Beijing Academy of Quantum Information Sciences, Beijing 100193, China. [4]Yunnan Key Laboratory for Quantum Information, Yunnan University, Kunming 650091, China.

*Address correspondence to: hlyin@ruc.edu.cn (H.-L.Y.); zbchen@nju.edu.cn (Z.-B.C.)
†These authors contributed equally to this work.

Citation: Hua W-J, Xiao Y-R, Bao Y, Yin H-L, Chen Z-B. Experimental Efficient Source-Independent Quantum Conference Key Agreement. *Research* 2025;8:Article 1034. https://doi.org/10.34133/research.1034

Submitted 16 September 2025
Revised 12 November 2025
Accepted 24 November 2025
Published 22 December 2025

Copyright © 2025 Wen-Ji Hua et al. Exclusive licensee Science and Technology Review Publishing House. No claim to original U.S. Government Works. Distributed under a Creative Commons Attribution License (CC BY 4.0).

Multipartite entanglement enables secure group key distribution among multiple users while providing immunity against hacking attacks targeting source devices, thereby realizing source-independent quantum conference key agreement (SI-QCKA). However, previous experimental demonstrations of SI-QCKA have encountered substantial technical challenges, primarily due to the low efficiency and scalability limitations inherent in the generation and distribution of multipartite entanglement. Here, we experimentally demonstrate a scalable and efficient SI-QCKA protocol using polarization-entangled photon pairs in a 3-user star network, where Greenberger–Horne–Zeilinger correlations are realized via a post-matching method. We achieve a secure group key rate of 2.11×10^{4} bits/s under the single-user channel transmission of 1.64×10^{-1} in a symmetric channel loss network. Additionally, we conduct 6 sets of experiments to investigate the impact of varying channel transmission and random basis selection probabilities on secure key rates. Our work establishes an efficient pathway for SI-QCKA and demonstrates potential scalability for future large-scale multiuser quantum networks.

Introduction

Quantum networks are envisioned to facilitate global-scale secure quantum communication between any users through state-of-the-art quantum technologies. To date, several categories of quantum network configurations have been developed [1–3], supporting various applications including distributed quantum sensing and metrology [4–7], distributed quantum computing [8–10], and quantum communication [11–16], which are fundamentally unattainable through classical networks. Quantum cryptography is essential for enabling secure communication in quantum networks [17–19]. As a representative application of quantum cryptography, quantum key distribution (QKD) has attracted extensive attention due to its information-theoretic security [20,21]. Remarkable progress has been achieved in both theoretical frameworks and experimental implementations of QKD [22–26], establishing a robust foundation for its practical applications [27–35]. To extend practical applications of QKD, point-to-point protocols must evolve into multiuser configurations. Quantum conference key agreement (QCKA) is a notable application [36–39], enabling the distribution of secure keys among multiple users. Additionally, more efficient protocols leveraging multipartite entanglement have been developed to reduce resource requirements [40–46].

Despite extensive theoretical proposals of QCKA protocols [36,38,41,47–54], technical difficulties have constrained experimental implementations to primarily focus on multipartite entanglement distribution schemes [37,55–57]. A representative experimental demonstration based on the N-BB84 protocol [50], employing 4-photon Greenberger–Horne–Zeilinger (GHZ) entangled states, has effectively demonstrated secure key distribution through a 50-km fiber [57]. However, the experimental requirements for high-intensity entanglement sources and long-distance communication channels hinder its practical implementation [37,58–63].

To circumvent the obstacles, measurement-device-independent quantum conference key agreement (MDI-QCKA) protocols have been developed [36]. MDI-QCKA establishes quantum correlations among users by postselecting GHZ entangled states through a multiphoton interferometer [64], thereby permitting measurement devices to be controlled by an untrusted party. The MDI-QCKA experiment has been successfully implemented [65,66]. However, the high demands for time synchronization and pulse indistinguishability introduce considerable practical difficulties. Moreover, the complexity of the GHZ analyzer grows rapidly as the number of users increases. Therefore, the realization of QCKA in practical quantum networks remains a major challenge.

Here, we experimentally demonstrate an efficient multiuser source-independent QCKA protocol [67] based on Bell state distribution. We note that entanglement-based protocols are naturally source-independent, which guarantees the system is secure against all security loopholes related to source imperfections or active hacking attacks targeting the source device [68,69]. The protocol establishes multipartite quantum correlations via the post-matching method [70], thus avoiding the need for multipartite entangled state generation. By employing polarization-entangled photon pair sources, we have successfully implemented a tripartite QCKA system, where fidelity and visibility of the bipartite entanglement between each pair of users reach up to 97% and 96%, respectively. We conduct 6 sets of tests under varying channel transmission and basis selection probabilities, attaining a high key rate of 2.11×10^{4} bit/s at the channel transmission of 1.64×10^{-1} and a Z-basis selection probability of 0.9. Furthermore, the implementation can be integrated into quantum networks, such as the fully connected QKD network architecture [71], by leveraging dense wavelength division multiplexing technology. As user numbers scale, the system requires only additional detection devices, ensuring flexibility for user adjustments. Therefore, this approach offers a resource-efficient, technically feasible, and scalable scheme for future large-scale quantum multiparty networks.

Results

Protocol description

In Fig. 1, we present a schematic overview of the source-independent QCKA protocol's workflow, emphasizing the distribution of Bell pairs and the establishment of GHZ correlation. Unlike many previous protocols utilizing GHZ states, the source-independent QCKA protocol [67] enables multiple users to acquire secure keys using entangled photon pair sources. The required maximally entangled Bell states are expressed as $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ in the Z basis and $|\Phi^+\rangle = (|++\rangle + |--\rangle)/\sqrt{2}$ in the X basis. We note that the experimentally generated $|\Psi^-\rangle$ state, used for its higher visibility, can be transformed into the required $|\Phi^+\rangle$ state. This transformation, which corresponds to Alice applying an $X_A Z_A$ local operation, is accounted for computationally in classical post-processing, as will be detailed in the "Experimental results" section. Here, $|0\rangle$ and $|1\rangle$ represent the eigenstates of the Z basis, while $|+\rangle$ and $|-\rangle$ denote the eigenstates of the X basis, with $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. For n users, denoted as Alice, Bob_1, Bob_2,..., $\mathrm{Bob}_{(n-1)}$, the key steps of the protocol are outlined as follows:

1. Entanglement distribution. In each round, an untrusted central node (Eve) generates $n-1$ polarization-entangled photon pairs in the state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ These pairs are distributed with one photon sent to Alice and the other to each user Bob_i $(i = 1, 2, \ldots, n-1)$.
2. Basis selection and measurement. Each user independently measures the photons in either the Z basis with probability p_z or the X basis with probability $1 - p_z$. Measurement results are recorded as valid events only when Alice and Bob_i select the same measurement basis and simultaneously detect photons.
3. Post-matching and key correlation. Users publicly announce their basis choices. Valid events are grouped according to the chosen basis and sorted by measurement time. The measurement results are ordered and labeled as a_j^{iz} (a_j^{ix}) for Alice and b_j^{iz} (b_j^{ix}) for Bob_i, where i corresponds to Bob_i and j denotes the time sequence.

For Z-basis measurement results: Alice computes the parity bits $c_j^{iz} = a_j^{1z} \oplus a_j^{iz}$ and broadcasts them. Each Bob_i derives the correlated keys via $b_j^{iz'} = c_j^{iz} \oplus b_j^{iz}$, thereby obtaining bit strings with GHZ correlation $a_j^{1z} = b_j^{1z'} = \ldots = b_j^{(n-1)z'}$.

For X-basis measurement results: Alice computes $a_j^{1x'} = \oplus_i a_j^{ix}$. The expected outcome is $a_j^{1x'} = \oplus_i b_j^{ix}$, which can be verified to establish bounds on potential eavesdropping.

4. Error correction. The error rate in the X basis is evaluated to quantify the potential information leakage to eavesdroppers. Subsequently, error correction is performed on the raw keys obtained from Z-basis measurements to ensure identical bit strings between the communicating users.
5. Privacy amplification. To reduce the residual information potentially acquired by an adversary, privacy amplification is applied to the keys. This process compresses the key length according to the estimated information leakage and generates the final secure keys.

Experimental setup

The experimental setup is illustrated in Fig. 2, involving 3 users: Alice, Bob_1, and Bob_2. A picosecond pulse laser at 780 nm with a repetition frequency of 96.7 MHz is first split by a 50:50 beam splitter (BS) and subsequently injected into 2 Sagnac loops, generating 2 polarization-entangled photon pairs simultaneously at a wavelength of 1,560 nm. The Sagnac interferometer splits the 780-nm pump pulse into 2 counter-propagating beams that traverse the same PPKTP crystal. Because these 2 paths are inherently phase-stable and perfectly overlapped spatially, the photon pairs generated from both directions are fundamentally indistinguishable. This indistinguishability results in a coherent superposition of the 2 processes, which is the key mechanism for creating the high-fidelity polarization-entangled state. The state of the entangled photon pairs is prepared as $|\Psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$to achieve higher visibility. Here, $|H\rangle$ and $|V\rangle$ denote horizontally and vertically polarized photons, respectively.

Subsequently, the photon pairs are split and delivered to Alice, Bob_1, and Bob_2, respectively, where projection measurements are performed. Within the 2 separate photon pairs, Alice receives one photon from each entangled pair, while the remaining 2 photons are allocated to 2 distinct users, thereby establishing unique polarization-entangled correlations between Alice and each individual user. Alice has twice the devices of other users to measure 2 photons simultaneously. Notably, all users employ BSs with identical splitting ratios, and the probability of basis selection is determined by the ratio of the BS. Photons traveling along the 2 arms of the BS are measured in the Z basis and the X basis, respectively. The variable optical attenuators (VOAs) are utilized to evaluate the system's performance under varying channel

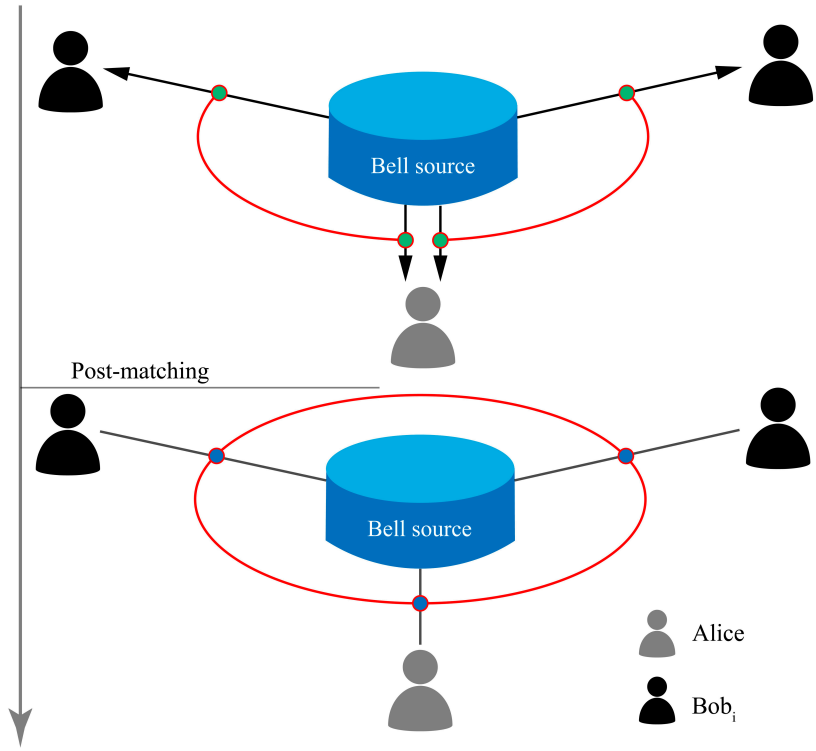


Fig. 1. Schematic of the 3-party source-independent QCKA protocol (Alice, Bob_1, and Bob_2). The central node functions as a Bell source, generating entangled Bell pairs that are distributed to Alice–Bob_1 and Alice–Bob_2. Subsequently, the users perform random measurements on the received photons, choosing either the *Z* basis or the *X* basis. The event in which a pair is measured by Alice and Bob_1 (or Bob_2) in the same basis will be recorded as a valid event. After processing the measurement results of the valid events using the post-matching method, we can establish GHZ correlation, from which raw key strings can be generated.

transmission. After passing through the VOAs, the photons are detected by a superconducting nanowire single-photon detector (SNSPD). All the SNSPDs are connected to a time-to-digital converter to record the arrival times of the detected photons. The average dark count rates of the SNSPDs in our experiment are below 20 Hz, with an average detection efficiency of 83%. An event in which Alice and Bob_1 (or Bob_2) simultaneously detect a photon under the same basis within a time window of 5.16 ns is recorded as a correlation count, corresponding to a valid event in the protocol.

To maximize the recording of valid events, the photons within the same entangled pair must arrive at the SNSPDs with minimal time difference. Consequently, the optical paths traveled by the photons are carefully adjusted to be as equal as possible. Additionally, appropriate time delays are applied to the signals from different SNSPDs to compensate for subtle differences in the optical path lengths. The introduced time delays are kept minimal, with their values optimized to maximize the coincidence count rates. The coincidence counts are then utilized to extract the secure keys and estimate information leakage following the protocol.

Performance

It is vital to ensure that high-quality entanglement is generated and distributed to all users. Therefore, we perform a series of experiments to evaluate the performance of the experimental system. During these experiments, all the VOAs are set to 0 dB, while the total channel transmission excluding the detector efficiency in the system between the entanglement source (Eve) and each user (Alice, Bob_1, and Bob_2) is maintained at approximately 1.64×10^{-1}. Additionally, the BSs employed for random basis selection are not plugged in the setup during the experiments and the HWPs in the measurement sites are set at the required angles based on the experimental demands. To minimize the influence of the extinction ratio difference between the transmission and reflection paths of the PBS before VOAs, only the transmitted photons are detected and recorded. The average down-converted mean photon number μ of the 2 entangled photon pairs is about 0.023 per pulse, remaining consistent throughout the demonstration experiment. In the characterization experiments, the coincidence count rates of both pairs of users exceed 10^4 per second, with the coincidence count to accidental coincidence count ratios surpassing 50, which indicates that each pair of users successfully shares a pair of entangled photons with high fidelity.

Furthermore, the quality of the polarization entanglement shared by the users can be quantitatively assessed through the visibility and fidelity of the entangled photon pairs. To measure the visibility of the photon pairs, we perform a 2-photon interference experiment. Figure 3A illustrates the photon interference fringes between Alice and Bob_1, while Fig. 3D depicts those between Alice and Bob_2. θ_A denotes the polarization angle of Alice, and θ_{B_i} denotes the polarization angle of Bob_i. We fix θ_A at 0° and 45° while sweeping θ_{B_i} from 0° to 180° to measure the coincidence counts *N*. The average visibility is calculated by $V = \left(N_{\max} - N_{\min}\right) / \left(N_{\max} + N_{\min}\right)$ For Alice and Bob_1, the average visibility is $V_{AB_1} = 96.43\% \pm 0.26\%$, and for Alice and Bob_2, it is $V_{AB_2} = 96.12\% \pm 0.76\%$. Both of them surpass the $1/\sqrt{2}$ visibility threshold required for the violation of the Clauser–Horne–Shimony–Holt (CHSH) inequality [72].

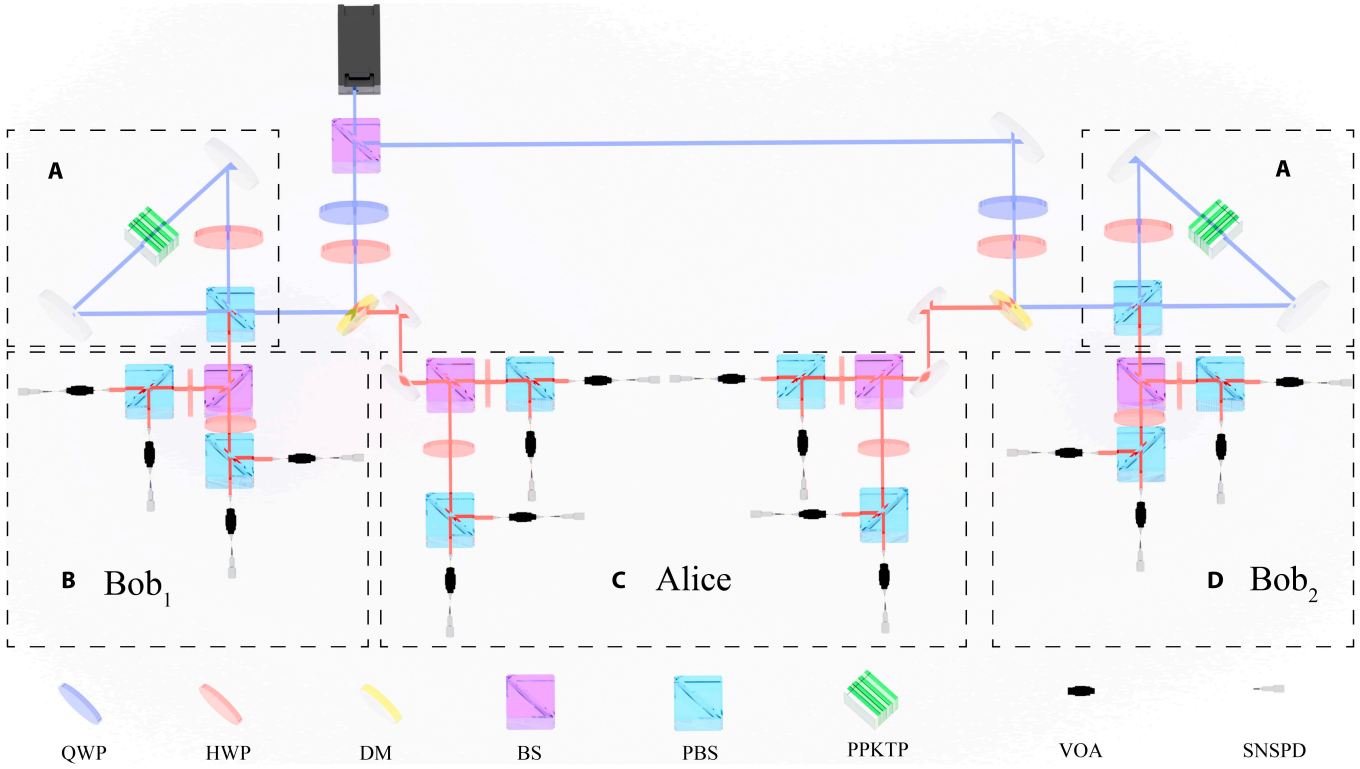


Fig. 2. Schematic of the QCKA experimental setup. (A) Sagnac loops. Laser pulses centered at a wavelength of 780 nm are injected into Sagnac loops, where polarization-entangled photon pairs at a wavelength of 1,560 nm are generated via type II spontaneous parametric down-conversion in a periodically poled potassium titanyl phosphate (PPKTP) crystal. The half-wave plates (HWPs) in the Sagnac loops are operational at both 780- and 1,560-nm wavelengths. Entangled photon pairs are sequentially allocated to Alice, Bob_1, and Bob_2 for polarization projection measurements. (B to D) The single-photon polarization measurements of the users. In the measurement sites, beam splitters (BSs) are utilized for random basis selection. The HWPs following the BS cooperate with the polarizing beam splitter (PBS) to perform projection measurements. The HWPs are set at 0°/45° and 22.5°/67.5° for measurements in the horizontal/vertical (H/V) and diagonal/anti-diagonal (D/A) bases, respectively. Photons are then measured in different bases and detected by distinct SNSPDs. QWP, quarter-wave plate; DM, dichroic mirror.

Then, we plug in an additional QWP before each HWP at all the measurement sites of the users to perform quantum state tomography and calculate the fidelity of the entangled photons with the maximum likelihood estimation of the density matrix [73]. The reconstruction of the density matrix is detailed in the "Density matrix reconstruction via maximum likelihood estimation" section. The density matrix of the photon pairs, estimated based on the experimental data, is shown in Fig. 3. For Alice and Bob_1, the average fidelity with respect to the Bell state $|\Psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$is $F_{AB_1} = 97.08\,\% \pm 0.03\,\%$, and for Alice and Bob_2, it is $F_{AB_2} = 96.98\,\% \pm 0.06\,\%$, revealing the high quality of the entanglement shared by the users.

Finally, we calculate the 4 expectation values required for computing the CHSH inequality parameter S by measuring the coincidence counts under 4 distinct combinations of wave plate angles [72], i.e., $S = E(0°, -22.5°) + E(0°, 22.5°) + E(-45°, -22.5°) - E(-45°, 22.5°)$. For Alice and Bob_1, $S_{AB_1} = 2.714 \pm 0.006$, and for Alice and Bob_2, $S_{AB_2} = 2.720 \pm 0.005$, both of which are close to the theoretical upper bound of $2\sqrt{2}$. The detailed values are illustrated in Fig. 3.

Experimental results

We experimentally demonstrate the tripartite source-independent QCKA protocol utilizing the established polarization-entangled photon pair source. Through applying the post-matching method to the measurement results, users can generate the raw keys and estimate the information leakage based on the coincidence counts. The length of the secure key is given by [50,54,74]:

$$L_{\text{QCKA}} = n_Z\left\{1 - H(\phi^Z) - f\max_i\left[H\left(E^Z_{AB_i}\right)\right]\right\} - \log_2\frac{2(n-1)}{\epsilon_{\text{cor}}} - 2\log_2\frac{1}{2\epsilon_{\text{sec}}} \quad (1)$$

where n_Z is the number of entangled photon pairs detected in the Z basis, $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ represents the binary Shannon entropy, and ϕ^Z is the upper limit of the phase error rate in the Z basis accounting for statistical fluctuations. f is the error correction efficiency, $E^Z_{AB_i}$ is the marginal error rates between Alice and the corresponding Bob_i, n is the number of users, ϵ_{cor} is the failure probability of error verification, and ϵ_{sec} is the failure probability of privacy amplification. In the experiment, $n = 3$, and n_Z, ϕ^Z, and $E^Z_{AB_i}$ are calculated from the experiment data [67]. The remaining parameters used are provided in the "Supplementary data" section.

Given that the quantum bit error rates (QBERs) vary under different measurement bases in the experiment, we perform the following operations to improve the calculated secure key rate according to Eq. 1. First, we define the transformations: $|H\equiv+\rangle$, $|V\equiv-\rangle$, $|D\equiv0\rangle$, and $|A\equiv1\rangle$, where $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ represent

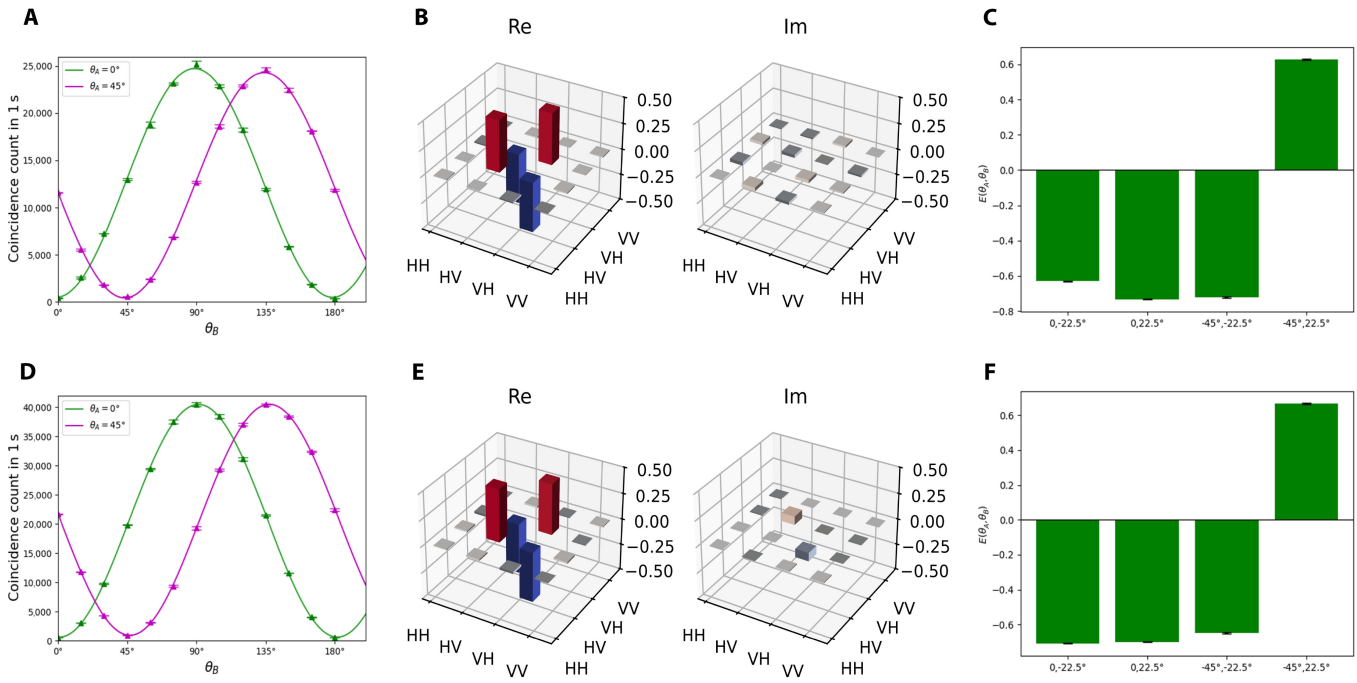


Fig. 3. The characterization parameters of the 2 entangled photon pairs. (A) to (C) correspond to Alice and Bob_1, and (D) to (F) correspond to Alice and Bob_2. (A and D) Two-photon interference fringes as functions of the polarizer angles of Alice and Bob_1 (or Bob_2) under 2 different phase bases. Alice sets θ_A to 0° (green points, fitted with green line) and 45° (magenta points, fitted with magenta line), while Bob_i sweeps θ_{B_i} from 0° to 180°. (B and E) Quantum state tomography results. The real and imaginary parts of the density matrix are depicted with respect to $|\Psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$. (C and F) The 4 expectation values used to calculate the S parameter of the CHSH inequality. (C) $E_{AB_1}(0°, -22.5°) = -0.631 \pm 0.004$, $E_{AB_1}(0°,22.5°) = -0.733 \pm 0.003$, $E_{AB_1}(-45°, -22.5°) = -0.723 \pm 0.003$, and $E_{AB_1}(-45°,22.5°) = 0.627 \pm 0.004$. (F) $E_{AB_2}(0°, -22.5°) = -0.708 \pm 0.003$, $E_{AB_2}(0°,22.5°) = -0.700 \pm 0.003$, $E_{AB_2}(-45°, -22.5°) = -0.647 \pm 0.003$, and $E_{AB_2}(-45°,22.5°) = 0.666 \pm 0.003$.

the diagonal and anti-diagonal polarization states, respectively. Then, after recording the experimental measurement results using the encoding scheme, we perform a classical post-processing operation equivalent to the quantum operation $X_A Z_A \otimes I_{B_i}$ on the acquired data. Here, X and Z denote the Pauli operators, I represents the identity operator, and the subscripts indicate their respective target (A for Alice and B_i for Bob_i). After these operations, the quantum states of the qubits can be equivalently expressed as $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ in the Z basis and $|\Phi^+\rangle = (|++\rangle + |--\rangle)/\sqrt{2}$ in the X basis. This conversion improves the secure key rate and ensures the consistency between the experimental system and the theoretical protocol. To simplify the subsequent descriptions, we treat the measured quantum states as $|\Phi^+\rangle$ in the following discussions.

To investigate the influence of the Z-basis selection probability p_z and the channel transmission on the secure key rate, we select probabilities of 0.9 and 0.5, and conduct the experiment under 3 different channel transmission values, thereby calculating the secure key rates for a total of 6 scenarios with Eq. 1. The initial channel transmission values between each user and the central node Eve are all measured to be about 1.64×10^{-1}. In experiments, the losses of all the VOAs are sequentially set to 0, 3, and 5 dB to change the channel transmission. The accumulation time is approximately 1,034 s for each scenario, during which a total of 10^{11} pulses are sent. The average down-converted mean photon number is maintained at $\mu = 0.023$. The QBERs and secure key rates are calculated from the experimental data. The detailed results are summarized in Table 1. The upper limit of the phase error rate ϕ^Z can be estimated based on the total bit error rate in the X basis, which can be inferred from the bit error rate between Alice and Bob_i in the X basis ($E^X_{AB_i}$) [67]. Therefore, the QBERs in Z basis and X basis are both provided.

Figure 4 depicts the conference key rate versus channel transmission. The maximum secure key rate of 2.11×10^4 bit/s is attained at the channel transmission of 1.64×10^{-1} with a Z-basis selection probability of 0.9. At identical channel transmission, the key rate is markedly higher in most cases for $p_z = 0.9$ compared to $p_z = 0.5$. This is because the raw keys are generated from coincidence counts in the Z basis, and intuitively, a higher p_z corresponds to an increased key rate. However, as the channel transmission decreases, the key rate when $p_z = 0.9$ decreases more rapidly than when $p_z = 0.5$. A higher p_z results in an increased number of coincidence counts in the Z basis but a reduced number in the X basis, thereby amplifying statistical uncertainties in the X-basis measurements, affecting the estimation of ϕ^Z and consequently decreasing the final secure key rate. With decreasing channel transmission, the experimental secure key rate remains at a high level, demonstrating the high efficiency and practicality of the protocol in quantum network applications.

Discussion

In summary, we have experimentally demonstrated the tripartite source-independent QCKA protocol. We establish a tripartite QCKA system, leveraging polarization-entangled photon pairs to facilitate secure multiuser communication. The experimental system is capable of generating high-quality entangled

Table 1. Summary of experimental data. A total of 10^{11} pulses are sent. η denotes the channel transmission excluding the detector efficiency between central node Eve and each user. The measured channel transmission values for all channels are approximately identical, i.e., $\eta = \eta_{EA} = \eta_{EB_1} = \eta_{EB_2}$, where η_{EA} is the channel transmission from Eve to Alice, and η_{EB_i} is the channel transmission from Eve to Bob_i. E^X_{AB1}, E^Z_{AB1} denote the experimental quantum bit error rates between Alice and Bob_1 in X basis and Z basis, respectively, and E^X_{AB2}, E^Z_{AB2} denote the corresponding quantum bit error rates between Alice and Bob_2. R_{QCKA} is the experimental conference secure key rate.

p_z	η	E^X_{AB1} (%)	E^X_{AB2} (%)	E^Z_{AB1} (%)	E^Z_{AB2} (%)	R_{QCKA} (bit/s)
0.9	1.64×10^{-1}	1.46	1.09	2.54	2.66	2.11×10^{4}
	8.24×10^{-2}	1.50	1.19	3.02	2.35	4.72×10^{3}
	5.20×10^{-2}	1.57	1.24	3.24	2.34	1.72×10^{3}
0.5	1.64×10^{-1}	1.99	1.91	1.79	1.92	6.25×10^{3}
	8.24×10^{-2}	2.04	2.18	1.99	2.08	1.55×10^{3}
	5.20×10^{-2}	2.11	2.10	2.00	2.08	6.31×10^{2}

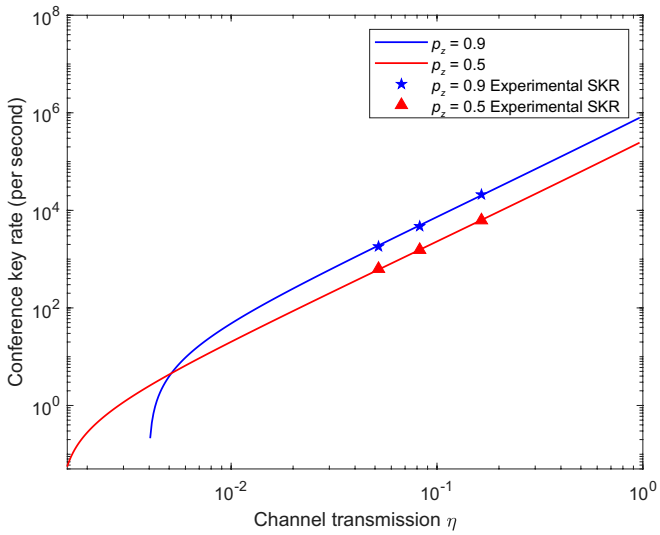


Fig. 4. Conference secure key rate as a function of channel transmission η. The 5-pointed blue stars and red triangles represent the experimental results for $p_z = 0.9$ and $p_z = 0.5$, respectively. For each p_z, the QCKA key rates are measured under 3 different channel transmission values, where the channel transmission η denotes the transmission from the central node to each user. The blue and red lines represent the simulation results for $p_z = 0.9$ and $p_z = 0.5$, respectively.

photon pairs with the fidelity of approximately 97% and the visibility exceeding 96%. Notably, we achieve a high key rate of 2.11×10^4 bits/s at the channel transmission of 1.64×10^{-1} and a Z-basis selection probability of 0.9.

Furthermore, we conduct 6 sets of experiments to explore the effects of basis selection probability and channel transmission on the secure key rate. In most scenarios, the key rate for $p_z = 0.9$ is markedly higher than for $p_z = 0.5$. Nevertheless, as channel transmission decreases, the key rate when $p_z = 0.9$ declines more rapidly, which results from the increasing statistical fluctuation of coincidence counts in the X basis. Additionally, the intensity of the source is directly correlated with the data size. While higher intensity increases coincidence counts, it also leads to higher QBERs. Therefore, it is crucial to choose an appropriate basis selection probability to optimize the key rate according to the channel transmission and the intensity of the source.

Compared to previous QCKA experiments, our approach is more efficient and scalable based on entangled photon pairs, thereby offering a feasible route for implementing multipartite QCKA in large-scale quantum networks. By incorporating technologies such as wavelength division multiplexing, the implementation can be integrated into quantum networks, including fully connected QKD networks, to accommodate larger user groups. Overall, this work marks a pivotal step toward the realization of an efficient, multiuser quantum network for next-generation secure communication systems.

Materials and Methods

Supplementary data

In this work, we have experimentally implemented the tripartite source-independent QCKA protocol, utilizing polarization-entangled photon pairs to enable scalable and secure multiuser communication. A high key rate of 2.11×10^4 bits/s is achieved with a compact experimental setup under the channel transmission of 1.64×10^{-1}. The parameters used in the calculation of the secure key rates are provided in Table 2. e_0 is the background error rate. e_d is the misalignment error rate. η_d is the detection efficiency of single photon detectors. p_d is the dark count rate per pulse. f is the error correction efficiency. ϵ_{cor} and ϵ_{sec} are the parameters of correctness and privacy. In the simulation of theoretical predictions, the parameters remain the same.

During the experiment, a total of 10^{11} pulses are sent. The detailed coincidence counts in the Z basis and X basis under varying channel transmission and key selection probabilities are presented in Tables 3 and 4. Table 3 presents the coincidence counts between Alice and Bob_1 and Table 4 provides the coincidence counts between Alice and Bob_2. The state of the detected photon pairs is expressed as $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ in the Z basis and $|\Phi^+\rangle = (|++\rangle + |--\rangle)/\sqrt{2}$ in the X basis. Notably, the theoretical prediction reveals an optimal basis selection probability, which is dependent on the down-converted mean photon number μ and the channel transmission. However, it is challenging for us to achieve the optimal ratio due to constraints imposed by the splitting ratios of BSs. Thus, there remains potential for further enhancement in the key rates. Through the coincidence counts, we can obtain the number of

entangled photon pairs detected in the Z basis n_Z and calculate the QBERs in the Z basis and X basis, which are essential for estimating the upper bound of phase error rate in the Z basis ϕ^Z and the length of the secure key L_{QCKA}. The down-converted mean photon numbers μ of the 2 entangled photon pairs are different due to the difficulty in achieving perfect splitting of laser pulses.

Table 2. The parameters involved in the secure key rate calculation. e_0 is the background error rate. e_d is the misalignment error rate. η_d is the detection efficiency of single photon detectors. p_d is the dark count rate per pulse. f is the error correction efficiency. ϵ_{cor} and ϵ_{sec} represent the parameters of correctness and privacy, respectively.

e_0	e_d	η_d	p_d	f	ϵ_{cor}	ϵ_{sec}
0.5	0.02	83%	10^{-7}	1.16	1.2×10^{-9}	1.2×10^{-9}

Computation of the 4 expectations to calculate the *S* parameter

To calculate the S parameter of the CHSH inequality, we need to calculate the normalized expectation value $E(\theta_A, \theta_B)$ based on the results of polarization measurements. The definition of the expectation is:

$$E(\theta_A, \theta_B) = \frac{N_{++} - N_{+-} - N_{-+} + N_{--}}{N_{++} + N_{+-} + N_{-+} + N_{--}} \tag{2}$$

where N_{ij} represents the coincidence counts (+ denotes parallel alignment, − denotes antiparallel alignment of the angle of the 2 users). The experimental results are presented in Fig. 3. To

Table 3. The detailed coincidence counts under different channel transmission and key selection probabilities between Alice and Bob_1. η denotes the channel transmission excluding the detector efficiency between central node Eve and each user. The Z (X) indicates that Alice and Bob_1 select the same Z basis (X basis). The subscripts (00, 01, 10, and 11) correspond to the measurement results of the detected photon pair. The down-converted mean photon number μ is approximately 0.024 per pulse.

p_z	0.9			0.5		
η	1.64×10^{-1}	8.24×10^{-2}	5.20×10^{-2}	1.64×10^{-1}	8.24×10^{-2}	5.20×10^{-2}
Z_{00}	17,559,115	4,159,589	1,610,121	5,243,818	1,376,112	563,083
Z_{01}	520,307	159,452	64,587	91,583	23,690	10,013
Z_{10}	388,668	99,534	41,610	99,125	31,773	12,752
Z_{11}	17,193,668	4,144,120	1,586,726	5,247,370	1,350,268	558,092
X_{00}	119,561	29,056	12,096	5,670,628	1,418,979	588,371
X_{01}	1,774	426	198	129,711	33,365	13,971
X_{10}	1,469	397	190	83,117	22,982	10,234
X_{11}	99,272	25,894	11,553	4,797,483	1,269,066	535,394

Table 4. The detailed coincidence counts under different channel transmission and key selection probabilities between Alice and Bob_2. η denotes the channel transmission excluding the detector efficiency between central node Eve and each user. The Z (X) means that Alice and Bob_2 choose the same Z basis (X basis). The superscripts (00, 01, 10, and 11) correspond to the measurement results of the photon pair. The down-converted mean photon number μ is approximately 0.021 per pulse.

p_z	0.9			0.5		
η	1.64×10^{-1}	8.24×10^{-2}	5.20×10^{-2}	1.64×10^{-1}	8.24×10^{-2}	5.20×10^{-2}
Z_{00}	28,787,736	6,667,492	2,749,255	7,156,545	1,743,702	731,003
Z_{01}	885,955	200,731	48,101	165,071	40,469	14,390
Z_{10}	632,049	115,341	79,320	108,417	33,147	17,489
Z_{11}	26,663,254	6,443,307	2,569,273	6,872,625	1,729,300	755,435
X_{00}	182,153	44,402	17,940	7,742,444	1,930,379	688,314
X_{01}	2,348	621	259	141,563	35,871	15,346
X_{10}	1,680	561	197	152,882	48,212	13,195
X_{11}	182,327	53,928	18,482	7,281,136	1,842,162	652,107

obtain $E(\theta_A, \theta_B)$, Alice and Bob$_i$ adjust the angle of their polarizer to measure the coincidence counts under the 4 scenarios corresponding to parallel and antiparallel alignments with a determined initial angle combination (θ_A, θ_B). The average coincidence counts measured in the experiment are shown in Tables 5 and 6.

Density matrix reconstruction via maximum likelihood estimation

To ensure that the reconstructed density matrix is physical, i.e., Hermitian, positive semi-definite, and with unit trace, a maximum likelihood estimation (MLE) method is employed [73]. This approach circumvents the issues of linear tomography, which can yield nonphysical matrices due to experimental noise.

The MLE procedure begins by constructing an explicitly physical density matrix, $\hat{\rho}_p$. First, we define an arbitrary 4×4 lower-triangular matrix $\hat{T}(t)$, which is a function of 16 independent real parameters $\{t_1, t_2, \ldots, t_{16}\}$. A matrix $\hat{\mathcal{G}} = \hat{T}^\dagger \hat{T}$ is necessarily Hermitian and positive semi-definite. By normalizing this matrix, a valid physical density matrix is constructed as:

$$\hat{\rho}_p(t) = \frac{\hat{T}^\dagger(t)\hat{T}(t)}{Tr\left\{\hat{T}^\dagger(t)\hat{T}(t)\right\}} \tag{3}$$

With this representation, the goal of the MLE method is to find the optimal set of parameters t that best describes the experimental data. This is achieved by defining a likelihood function, $\mathcal{L}(t)$, which quantifies the differences between the measured coincidence counts n_ν and the expected counts $\overline{n}_\nu(t)$ predicted by the physical density matrix $\hat{\rho}_p(t)$. Here, $\nu = 1, 2, \ldots, 16$ labels the distinct measurement settings. The expected count $\overline{n}_\nu(t)$ is defined as:

$$\overline{n}_\nu(t) = \mathcal{N}\langle\psi_\nu|\hat{\rho}_p(t)|\psi_\nu\rangle \tag{4}$$

where $\mathcal{N}$ is the normalization constant representing the total number of events for a complete basis. $\mathcal{N}$ is estimated from the experimental data as $\mathcal{N} = n_1 + n_2 + n_3 + n_4$. $|\psi_\nu\rangle$ denotes the quantum state vector representing the νth tomographic projection measurement. For example, as defined in Table 7, $|\psi_1\rangle = |HH\rangle, |\psi_2\rangle = |HV\rangle$, etc.

Assuming Gaussian probability distribution for the count noise, the optimization problem reduces to finding the minimum of the function $\mathcal{L}(t)$:

$$\mathcal{L}(t) = \sum_{\nu=1}^{16} \frac{\left[\overline{n}_\nu(t) - n_\nu\right]^2}{2\overline{n}_\nu(t)} = \sum_{\nu=1}^{16} \frac{\left[\mathcal{N}\langle\psi_\nu|\hat{\rho}_p(t)|\psi_\nu\rangle - n_\nu\right]^2}{2\mathcal{N}\langle\psi_\nu|\hat{\rho}_p(t)|\psi_\nu\rangle} \tag{5}$$

A numerical optimization algorithm is used to find the specific set of parameters, $\left\{t_1^{(\mathrm{opt})}, \ldots, t_{16}^{(\mathrm{opt})}\right\}$, that minimizes this function $\mathcal{L}$. The resulting matrix, $\hat{\rho}_p\left(t^{(\mathrm{opt})}\right)$, is then taken as the most likely physical density matrix consistent with the observed data. The coincidence counts n_ν measured in the experiment and the corresponding wave plate angles $\{q_{1,\nu}, h_{1,\nu}, q_{2,\nu}, h_{2,\nu}\}$ are provided in Tables 7 and 8. To reduce statistical fluctuations, the coincidence counts n_ν for each measurement setting are accumulated for 3 s. The notation used for the polarization states is $|D\rangle \equiv (|H\rangle + |V\rangle)/\sqrt{2}$ and $|R\rangle \equiv (|H\rangle + i|V\rangle)/\sqrt{2}$.

Table 5. The average coincidence counts N measured under different combinations of the polarization angles of Alice and Bob$_1$

(θ_A, θ_B)	$(0°, -22.5°)$	$(0°, 22.5°)$	$(-45°, -22.5°)$	$(-45°, 22.5°)$
N_{++}	15,310	11,512	12,883	66,602
N_{+-}	68,214	73,735	73,433	15,465
N_{-+}	68,063	71,460	72,430	15,258
N_{--}	15,518	10,817	10,585	67,398

Table 6. The average coincidence counts N measured under different combinations of the polarization angles of Alice and Bob$_2$

(θ_A, θ_B)	$(0°, -22.5°)$	$(0°, 22.5°)$	$(-45°, -22.5°)$	$(-45°, 22.5°)$
N_{++}	17,035	16,706	23,747	99,819
N_{+-}	98,111	101,814	96,475	19,172
N_{-+}	106,584	103,258	101,611	20,995
N_{--}	17,961	19,506	18,746	100,198

Table 7. Experimental coincidence counts (n_v) measured under the 16 tomographic projection settings for Alice and Bob_1

v	Mode 1	Mode 2	q_1	h_1	q_2	h_2	n_v
1	$\|H\rangle$	$\|H\rangle$	0°	0°	0°	0°	1,305
2	$\|H\rangle$	$\|V\rangle$	0°	0°	0°	45°	82,190
3	$\|V\rangle$	$\|V\rangle$	0°	45°	0°	45°	1,257
4	$\|V\rangle$	$\|H\rangle$	0°	45°	0°	0°	81,980
5	$\|R\rangle$	$\|V\rangle$	0°	22.5°	0°	45°	36,899
6	$\|R\rangle$	$\|H\rangle$	0°	22.5°	0°	0°	43,677
7	$\|D\rangle$	$\|H\rangle$	45°	22.5°	0°	0°	48,880
8	$\|D\rangle$	$\|V\rangle$	45°	22.5°	0°	45°	37,391
9	$\|D\rangle$	$\|R\rangle$	45°	22.5°	0°	22.5°	44,333
10	$\|D\rangle$	$\|D\rangle$	45°	22.5°	45°	22.5°	1,585
11	$\|R\rangle$	$\|D\rangle$	0°	22.5°	45°	22.5°	47,749
12	$\|R\rangle$	$\|R\rangle$	0°	22.5°	0°	22.5°	1,863
13	$\|H\rangle$	$\|D\rangle$	0°	0°	45°	22.5°	48,302
14	$\|H\rangle$	$\|R\rangle$	0°	0°	0°	22.5°	38,370
15	$\|V\rangle$	$\|R\rangle$	0°	45°	0°	22.5°	46,510
16	$\|V\rangle$	$\|D\rangle$	0°	45°	45°	22.5°	40,014

Table 8. Experimental coincidence counts (n_v) measured under the 16 tomographic projection settings for Alice and Bob_2

v	Mode 1	Mode 2	q_1	h_1	q_2	h_2	n_v
1	$\|H\rangle$	$\|H\rangle$	0°	0°	0°	0°	1,383
2	$\|H\rangle$	$\|V\rangle$	0°	0°	0°	45°	119,018
3	$\|V\rangle$	$\|V\rangle$	0°	45°	0°	45°	1,704
4	$\|V\rangle$	$\|H\rangle$	0°	45°	0°	0°	121,674
5	$\|R\rangle$	$\|V\rangle$	0°	22.5°	0°	45°	60,747
6	$\|R\rangle$	$\|H\rangle$	0°	22.5°	0°	0°	62,533
7	$\|D\rangle$	$\|H\rangle$	45°	22.5°	0°	0°	73,073
8	$\|D\rangle$	$\|V\rangle$	45°	22.5°	0°	45°	50,917
9	$\|D\rangle$	$\|R\rangle$	45°	22.5°	0°	22.5°	77,260
10	$\|D\rangle$	$\|D\rangle$	45°	22.5°	45°	22.5°	3,037
11	$\|R\rangle$	$\|D\rangle$	0°	22.5°	45°	22.5°	57,551
12	$\|R\rangle$	$\|R\rangle$	0°	22.5°	0°	22.5°	2,585
13	$\|H\rangle$	$\|D\rangle$	0°	0°	45°	22.5°	65,648
14	$\|H\rangle$	$\|R\rangle$	0°	0°	0°	22.5°	58,292
15	$\|V\rangle$	$\|R\rangle$	0°	45°	0°	22.5°	60,181
16	$\|V\rangle$	$\|D\rangle$	0°	45°	45°	22.5°	61,324

Acknowledgments

Funding: This work was supported by the National Natural Science Foundation of China (Nos. 12522419, U25D8016, and 12274223), the Fundamental Research Funds for the Central Universities, and the Research Funds of Renmin University of China (No. 24XNKJ14).

Author contributions: Z.-B.C. guided the work. H.-L.Y. conceived and supervised the research. W.-J.H., Y.-R.X., Y.B., and H.-L.Y. designed the experiments. W.-J.H., Y.-R.X., and H.-L.Y. performed the experiments and analyzed the experimental data. W.-J.H., Y.-R.X., and H.-L.Y. cowrote the manuscript, with input from the other authors. All authors have discussed the results and proofread the manuscript.

Competing interests: The authors declare that they have no competing interests.

Data Availability

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

References

1. Wehner S, Elkouss D, Hanson R. Quantum internet: A vision for the road ahead. *Science*. 2018;362(6412):eaam9288.
2. Azuma K, Economou SE, Elkouss D, Hilaire P, Jiang L, Lo H-K, Tzitrin I. Quantum repeaters: From quantum networks to the quantum internet. *Rev Mod Phys*. 2023;95(4):Article 045006.
3. Li CL, Yin HL, Chen ZB. Asynchronous quantum repeater using multiple quantum memory. *Rep Prog Phys*. 2024;87(12):Article 127901.
4. Guo X, Breum CR, Borregaard J, Izumi S, Larsen MV, Gehring T, Christandl M, Neergaard-Nielsen JS, Andersen UL. Distributed quantum sensing in a continuous-variable entangled network. *Nat Phys*. 2020;16:281–284.
5. Zhao SR, Zhang YZ, Liu WZ, Guan JY, Zhang W, CL LI, Bai B, Li MH, Liu Y, You L, et al. Field demonstration of distributed quantum sensing without post-selection. *Phys Rev X*. 2021;11(3):Article 031009.
6. Xu Y, Wang T, Huang P, Zeng G. Integrated distributed sensing and quantum communication networks. *Research*. 2024;7:0416.
7. Zhou MG, Liu ZP, Yin HL, Li CL, Xu TK, Chen ZB. Quantum neural network for quantum neural computing. *Research*. 2023;6:0134.
8. Zhong Y, Chang HS, Bienfait A, Dumur E, Chou MH, Conner CR, Grebel J, Povey RG, Yan H, Schuster DI, et al. Deterministic multi-qubit entanglement in a quantum network. *Nature*. 2021;590:571–575.
9. Zhou MG, Cao XY, Lu YS, Wang Y, Bao Y, Fu Y, Yin HL, Chen ZB. Experimental quantum advantage with quantum coupon collector. *Research*. 2022;2022:Article 9798679.
10. Zhang J, Chen T, Deng W, Tong X, Zhang X. Quantum 2-player games and realizations 350 with circuits. *Research*. 2024;7:0480.
11. Cao XY, Li BH, Wang Y, Fu Y, Yin HL, Chen. Experimental quantum E-commerce. *Sci Adv*. 2024;10(2):eadk3258.
12. Chen YA, Zhang Q, Chen TY, Cai WQ, Liao SK, Zhang J, Chen K, Yin J, Ren JG, Chen Z, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*. 2021;589:214–219.

13. Weng CX, Gao RQ, Bao Y, Li RH, Liu WB, Xie YM, Lu YS, Yin HL, Chen ZB. Beating the fault-tolerance bound and security loopholes for byzantine agreement with a quantum solution. *Research*. 2023;6:0272.
14. Jing X, Qian C, Weng CX, Li BH, Chen Z, Wang CQ, Tang J, Gu XW, Kong YC, Chen TS, et al. Experimental quantum byzantine agreement on a three-user quantum network with integrated photonics. *Sci Adv*. 2024;10(34):eadp2877.
15. Cao Z, Lu Y, Chai G, Yu H, Liang K, Wang L. Realization of quantum secure direct communication with continuous variable. *Research*. 2023;6:0193.
16. Yang Y, Li Y, Li H, Wu C, Zheng Y, Chen X. A 300-km fully-connected quantum secure direct communication network. *Sci Bull*. 2025;70(9):1445–1451.
17. Yin HL, Fu Y, Li CL, Weng CX, Li BH, Gu J, Lu Y-S, Huang S, Chen ZB. Experimental quantum secure network with digital signatures and encryption. *Natl Sci Rev*. 2023;10(4): Article nwac228.
18. Bozzio M, Crepeau C, Wallden P, Walther P. Quantum cryptography beyond key distribution: Theory and experiment. arXiv. 2024. https://doi.org/10.48550/arXiv.2411.08877
19. Pan D, Long GL, Yin L, Shen YB, Ruan D, Ng SX, Lu J, Hanzo L. The evolution of quantum secure direct communication: On the road to the qinternet. *IEEE Commun Surv Tut*. 2024;26:1898–1949.
20. Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. *Rev Mod Phys*. 2020;92(2):Article 025002.
21. Pirandola S, Andersen UL, Banchi L, Berta D, Bunandar R, Colbeck D, Englund T, Gehring C, Lupo C, Ottaviani JL, et al. Advances in quantum cryptography. *Adv Opt Photon*. 2020;12(4):1012–1236.
22. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Phys Rev Lett*. 2012;108(13): Article 130503.
23. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*. 2018;557:400–403.
24. Xie YM, Lu YS, Weng CX, Cao XY, Jia ZY, Bao Y, Wang Y, Fu Y, Yin HL, Chen ZB. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum*. 2022;3(2):Article 020315.
25. Zeng P, Zhou H, Wu W, Ma X. Mode-pairing quantum key distribution. *Nat Commun*. 2022;13:3903.
26. Ying JW, Wang JY, Xiao YX, Gu SP, Wang XF, Zhong W, Du MM LXY, Shen ST, Zhang AL, Zhou L, et al. Passive-state preparation for quantum secure direct communication. *Sci China Phys Mech Astron*. 2025;68:Article 240312.
27. Wang YZ, Sun XR, Cao XY, Yin HL, Chen ZB. Experimental coherent-state quantum secret sharing with finite pulses. *Phys Rev Appl*. 2024;22(4):Article 044018.
28. Gu J, Cao XY, Fu Y, He ZW, Yin ZJ, Yin HL, Chen ZB. Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci Bull*. 2022;67(21):2167–2175.
29. Guo M, Huang P, Huang L, Liao X, Jiang X, Wang T, Zeng G. Discrete-modulated coherent-state quantum key distribution with basis-encoding. *Research*. 2025;8:0691.
30. Liu WB, Li CL, Xie YM, Cheng CX, Gu J, Cao XY, Lu YS, Li BH, Yin HL, Chen ZB. Homodyne detection quadrature phase shift keying continuous variable quantum key distribution with high excess noise tolerance. *PRX Quantum*. 2021;2(4):Article 040334.
31. Pan D, Liu YC, Niu P, Zhang H, Zhang F, Wang M, Song XT, Chen X, Zheng C, Long GL. Simultaneous transmission of information and key exchange using the same photonic quantum states. *Sci Adv*. 2025;11(8):eadt4627.
32. Ding CW, Wang WY, Zhang WD, Zhou L, Sheng YB. Quantum secure direct communication based on quantum error correction code. *Appl Phys Lett*. 2025;126:Article 024002.
33. Sheng YB, Zhou L, Long GL. One-step quantum secure direct communication. *Sci Bull*. 2022;67(4):367–374.
34. Fang D, Zhang C, Chen W, Cui J, Huang Y, Li C, Guo G. A fast-tunable and stable fiber microcavity for coupling Ba^+ ions in quantum networks. *Chin Opt Lett*. 2025;23(12): Article 120201.
35. Shao Y, Shen Z, Xu Y, Li L, Tan Z, Liao X, Huang P, Wang T, Zeng G. Integration of classical communication and quantum key distribution using frequency division multiplexing. *Chin Opt Lett*. 2025;23:Article 032702.
36. Fu Y, Yin HL, Chen TY, Chen ZB. Long-distance measurement-device-independent multiparty quantum communication. *Phys Rev Lett*. 2015;114(9):Article 090501.
37. Pickston A, Ho J, Ulibarrena A, Grasselli F, Proietti M, Morrison CL, Barrow P, Graffitti F, Fedrizzi A. Conference key agreement in a quantum network. *NPJ Quantum Inf*. 2023;9:82.
38. Grasselli F, Kampermann H, Bruß D. Conference key agreement with single-photon interference. *New J Phys*. 2019;21:Article 123002.
39. Murta G, Grasselli F, Kampermann H, Bruß D. Quantum conference key agreement: A review. *Adv Quantum Technol*. 2020;3(11):2000025.
40. Li CL, Fu Y, Liu WB, Xie YM, Li BH, Zhou MG, Yin HL, Chen ZB. All-photonic quantum repeater for multipartite entanglement generation. *Opt Lett*. 2023;48(5):1244–1247.
41. Epping M, Kampermann H, Macchiavello C, Bruß D. Multi-partite entanglement can speed up quantum key distribution in networks. *New J Phys*. 2017;19:Article 093012.
42. Xie YM, Lu YS, Fu Y, Yin HL, Chen ZB. Multi-field quantum conferencing overcomes the network capacity limit. *Commun Phys*. 2024;7:410.
43. Wallnofer J, Pirker A, Zwerger M, Dur W. Multipartite state generation in quantum networks with optimal scaling. *Sci Rep*. 2019;9:314.
44. Miguel-Ramiro J, Pirker A, Dur W. Optimized quantum networks. *Quantum*. 2023;7:919.
45. Kuzmin VV, Vasilyev DV, Sangouard N, Dur W, Muschik CA. Scalable repeater architectures for multi-party states. *NPJ Quantum Inf*. 2019;5:115.
46. Lu YS, Yin HL, Xie YM, Fu Y, Chen ZB. Repeater-like asynchronous measurement device-independent quantum conference key agreement. *Rep Prog Phys*. 2025;88: Article 067901.
47. Hahn F, De Jong J, Pappa A. Anonymous quantum conference key agreement. *PRX Quantum*. 2020;1(2):Article 020325.
48. Cao XY, Gu J, Lu YS, Yin HL, Chen ZB. Coherent one-way quantum conference key agreement based on twin field. *New J Phys*. 2021;23:Article 043002.
49. Li Z, Cao XY, Li CL, Weng CX, Gu J, Yin HL, Chen ZB. Finite-key analysis for quantum conference key agreement with asymmetric channels. *Quantum Sci Technol*. 2021;6(4): Article 045019.

50. Grasselli F, Kampermann H, Bruß D. Finite-key effects in multipartite quantum key distribution protocols. *New J Phys*. 2018;20:Article 113014.
51. Ribeiro J, Murta G, Wehner S. Fully device-independent conference key agreement. *Phys Rev A*. 2018;97(2): Article 022307.
52. Cao XY, Lu YS, Li Z, Gu J, Yin HL, Chen ZB. High key rate quantum conference key agreement with unconditional security. *IEEE Access*. 2021;9:128870–128876.
53. Zhao S, Zeng P, Cao WF, Xu XY, Zhen YZ, Ma X, Li L, Liu NL, Chen K. Phase-matching quantum cryptographic conferencing. *Phys Rev Appl*. 2020;14(2):Article 024010.
54. Li CL, Fu Y, Liu WB, Xie YM, Li BH, Zhou MG, Yin HL, Chen ZB. Breaking universal limitations on quantum conference key agreement without quantum memory. *Commun Phys*. 2023;6:122.
55. Ho J, Moreno G, Brito S, Graffitti F, Morrison CL, Nery R, Pickston A, Proietti M, Rabelo R, Fedrizzi A, et al. Entanglement-based quantum communication complexity beyond bell nonlocality. *NPJ Quantum Inf*. 2022;8:13.
56. Cai B, Guo G, Lin S, Zuo H, Yu C. Multipartite quantum key agreement over collective noise channels. *IEEE Photonics J*. 2018;10:7600211.
57. Proietti M, Ho J, Grasselli F, Barrow P, Malik M, Fedrizzi A. Experimental quantum conference key agreement. *Sci Adv*. 2021;7(23):eabe0395.
58. Webb JW, Ho J, Grasselli F, Murta G, Pickston A, Ulibarrena A, Fedrizzi A. Experimental anonymous quantum conferencing. *Optica*. 2024;11(6):872–875.
59. Jons KD, Schweickert L, Versteegh MAM, Dalacu D, Poole PJ, Gulinatti A, Giudice A, Zwiller V, Reimer ME. Bright nanoscale source of deterministic entangled photon pairs violating bell's inequality. *Sci Rep*. 2017;7:1700.
60. Gaertner S, Kurtsiefer C, Bourennane M, Weinfurter H. Experimental demonstration of 449 four-party quantum secret sharing. *Phys Rev Lett*. 2007;98(2):Article 020503.
61. Tittel W, Zbinden H, Gisin N. Experimental demonstration of quantum secret sharing. *Phys Rev A*. 2001;63(4): Article 042301.
62. Erven C, Meyer-Scott E, Fisher K, Lavoie J, Higgings BL, Yan Z, Pugh CJ, Bourgoin JP, Prevedel R, Shalm LK, et al. Experimental three-photon quantum nonlocality under strict locality conditions. *Nat Photonics*. 2014;8:292–296.
63. Uppu R, Midolo L, Zhou X, Carolan J, Lodahl P. Quantum-dot-based deterministic photon–emitter interfaces for scalable photonic quantum technology. *Nat Nanotechnol*. 2021;16(12):1308–1317.
64. Pan JW, Zeilinger A. Greenberger-Horne-Zeilinger-state analyzer. *Phys Rev A*. 1998;57(3):2208–2211.
65. Yang KX, Mao YL, Chen H, Dong X, Zhu J, Wu J, Li ZD. Experimental measurement-device-independent quantum conference key agreement. *Phys Rev Lett*. 2024;133(21): Article 210803.
66. Du Y, Liu Y, Yang C, Zheng X, Zhu S, Xs M. Experimental measurement-device independent quantum cryptographic conferencing. *Phys Rev Lett*. 2025;134(4):Article 040802.
67. Bao Y, Xiao YR, Song YC, Cao XY, Fu Y, Yin HL, Chen ZB. Efficient source-independent quantum conference key agreement. *Opt Express*. 2024;32(14):24629–24642.
68. Ma X, Fung CHF, Lo HK. Quantum key distribution with entangled photon sources. *Phys Rev A*. 2007;76(1):Article 012307.
69. Koashi M, Preskill J. Secure quantum key distribution with an uncharacterized source. *Phys Rev Lett*. 2003;90(5):Article 057902.
70. Lu YS, Cao XY, Weng CX, Gu J, Xie YM, Zhou MG, Yin HL, Chen ZB. Efficient quantum digital signatures without symmetrization step. *Opt Express*. 2021;29(7):10162.
71. Huang Y, Qi Z, Yang Y, Zhang Y, Li Y, Zheng Y, Chen X. A sixteen-user time-bin entangled quantum communication network with fully connected topology. *Laser Photonics Rev*. 2024;19(1):Article 2301026.
72. Clauser JF, Horne MA, Shimony A, Holt RA. Proposed experiment to test local hidden variable theories. *Phys Rev Lett*. 1969;23(15):880–884.
73. James DFV, Kwiat PG, Munro WJ, White AG. Measurement of qubits. *Phys Rev A*. 2001;64(5):Article 052312.
74. Yin HL, Zhou MG, Gu J, Xie YM, Lu YS, Chen ZB. Tight security bounds for decoy-state quantum key distribution. *Sci Rep*. 2020;10:14312.