ARTICLE OPEN

Experimental demonstration of multiparty quantum secret sharing and conference key agreement

Shuaishuai Liu[1,2], Zhenguo Lu[1,2], Pu Wang[3], Yan Tian[1,2], Xuyang Wang[1,2,4] and Yongmin Li[1,2,4]✉

Quantum secret sharing (QSS) and conference key agreement (CKA) provide efficient encryption approaches for realizing multi-party secure communication, which are essential components of quantum networks. In this work, a practical, scalable, verifiable (k, n) threshold continuous variable QSS protocol secure against eavesdroppers and dishonest players are proposed and demonstrated. The protocol does not require preparing the laser source by each player and phase locking of independent lasers. The parameter evaluation and key extraction can be accomplished by only the dealer and the corresponding player. By using the multiple sideband modulation, a single heterodyne detector can extract the information of multiple players. The practical security of the system is considered. The system is versatile, it can support the CKA protocol by only modifying the classic post-processing and requiring no changes to the underlying hardware architecture. By implementing the QSS and CKA protocols with five parties over 25 km (55 km) single-mode fibers, a key rate of 0.0061 (7.14×10^{-4}) bits per pulse is observed. The results significantly reduces the system complexity and paves the way for the practical applications of QSS and CKA with efficient utilization of resources and telecom technologies.

npj Quantum Information (2023)9:92 ; https://doi.org/10.1038/s41534-023-00763-z

INTRODUCTION

In recent years, quantum communication has made significant breakthroughs, in particular, quantum key distribution (QKD)[1–3] ensures secure communication between legitimate parties based on the principles of quantum mechanics. The invention of QKD provides an effective approach to solve the point-to-point security key distribution between two users. Inspired by the idea of QKD and classical cryptography protocols[4–6], the quantum secret sharing (QSS)[7], and conference key agreement (CKA)[8] using multiparticle Greenberger-Horne-Zeilinger (GHZ) entangled states were proposed. The QSS combines quantum cryptography with classical secret sharing and uses quantum state as a secret encoding carrier. The secret message is divided into n pieces and distributed to n players in an appropriate way[7]. For a (k, n) threshold protocol, if no less than k players combine their pieces of information together, the secret message can be recovered[4]. QSS can protect secret message from the eavesdroppers and dishonest players, and has important applications in key management, identity authentication, remote voting, and quantum sealed-bid auction. The task of CKA is to establish a common secret key among n players. All players can encrypt the public messages and decrypt the encrypted public messages broadcasted by other players, whereas the eavesdroppers cannot obtain any public messages broadcasted by the players[8].

At present, a variety of QSS and CKA protocols have been proposed. They follow mainly two different paths: the multipartite entangled states based protocols and the bipartite QKD based protocols. The first path employs quantum correlations of genuine multipartite quantum resources, require no explicit QKD process, and may offer specific advantages over the latter. The latter can use mature security proofs and technology of QKD, and could bring operational advantages such as it can switch between different protocols by configuring only the classical post-processing program and no modification of hardware devices are required. Depending on the quantum resources employed, the discrete variable QSS including the entangled state QSS[7,9–13], the single qubit QSS[14–16], the single qudit QSS[17–19], and the post-selected multipartite entanglement state QSS[20] have been investigated. The continuous variable QSS with the entangled state[21–24] and coherent state[25–28] were also presented. Furthermore, CKA with multipartite entangled state (known as quantum conference key agreement (QCKA)[29])[8,29–34], three party QKD[35], and measurement-device-independent (MDI) type[20,36–38] have been reported.

The above works significantly improve the feasibility of QSS and CKA. However, there are still key limitations in security and practicability. For instance, the single qubit QSS protocol is vulnerable to Trojan horse attacks[39,40] where an eavesdropper can send a signal to the player's station and unambiguously determine the private information by measuring the output signals. The QSS[7,9–13] and CKA[8,29–34] based on the GHZ entangled state are appealing. For certain CKA networks with bottlenecks[31], the GHZ resource state can be distributed in a single use of the network for the multipartite entanglement protocol, despite the complicated quantum network coding with two-qubit gates failure rates and channel noises below certain threshold are required. Nevertheless, the practical applications of GHZ-like states are quite limited due to the difficulty of generation, manipulation, and distribution of multi-partite entangled states with very large dimension at present[20,33,41]. The post-selection GHZ entangled state QSS and CKA alleviate this issue[20,37]. However, the implementation of this scheme requires the intervention of multiple players, which increases the complexity of the experiment. Continuous variable QSS (CV-QSS) based on coherent states has good compatibility with telecom techniques[25–28]. Unfortunately, most of coherent-state CV-QSS protocols require that all players have to prepare

[1]State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China. [2]Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China. [3]School of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China. [4]Hefei National Laboratoty, Heifei 230088, China. ✉email: yongmin@sxu.edu.cn

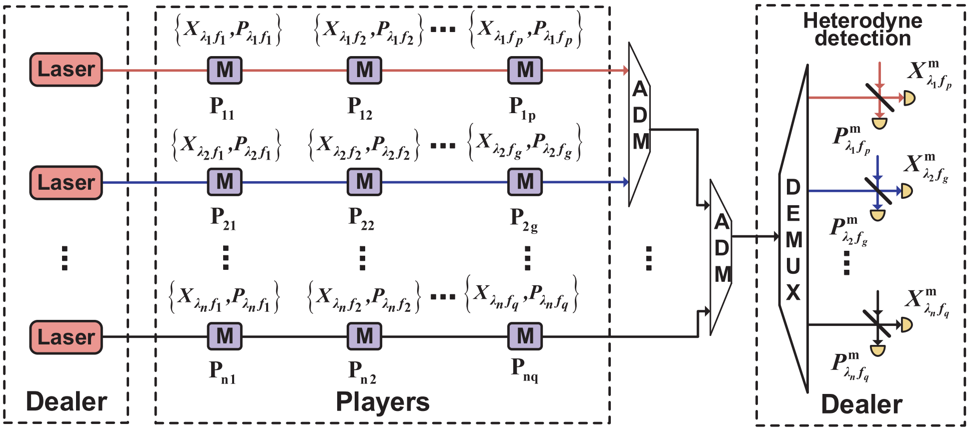
Dealer
Laser
Laser
Laser
Players
$\{X_{\lambda_1 f_1}, P_{\lambda_1 f_1}\}$
$\{X_{\lambda_1 f_2}, P_{\lambda_1 f_2}\}$
$\{X_{\lambda_1 f_p}, P_{\lambda_1 f_p}\}$
$\{X_{\lambda_2 f_1}, P_{\lambda_2 f_1}\}$
$\{X_{\lambda_2 f_2}, P_{\lambda_2 f_2}\}$
$\{X_{\lambda_2 f_g}, P_{\lambda_2 f_g}\}$
$\{X_{\lambda_n f_1}, P_{\lambda_n f_1}\}$
$\{X_{\lambda_n f_2}, P_{\lambda_n f_2}\}$
$\{X_{\lambda_n f_q}, P_{\lambda_n f_q}\}$
M
P_{11}
P_{12}
P_{1p}
P_{21}
P_{22}
P_{2g}
P_{n1}
P_{n2}
P_{nq}
ADM
ADM
DEMUX
Heterodyne detection
$X^m_{\lambda_1 f_p}$
$P^m_{\lambda_1 f_p}$
$X^m_{\lambda_2 f_g}$
$P^m_{\lambda_2 f_g}$
$X^m_{\lambda_n f_q}$
$P^m_{\lambda_n f_q}$
Dealer

Fig. 1 The QSS protocol. M modulator, ADM add/drop multiplexer, DEMUX demultiplexer. The dealer prepares a number of coherent laser source that passes through each player in sequence, and all players implement independent Gaussian modulation to encode the information in different sidebands of the laser field, then the signal fields with different wavelengths are multiplexed via ADM. After transmission, the dealer demultiplexs the signals of different players and extracts the corresponding sideband information in terms of the encoding rules of the players separately by heterodyne detection.

their own laser sources, and the phase of all players' independent lasers should be strictly locked, which adds considerable complexity and cost to the system. On the other hand, the superposition of channel excess noises from other players severely reduces the secret key rate due to the joint measurement by the dealer[25,26,28]. Furthermore, most of the existing QSS and CKA require dedicated hardware devices and many QSS are (n, n) schemes.

To solve above problems, in this paper we propose a practical, scalable, and verifiable (k, n) threshold CV-QSS protocol based on the bipartite QKD approach. In contrast to previous works with continuous variable regime, our protocol does not require each player preparing a laser source and phase locking of the overall lasers. Furthermore, the dealer can use a single heterodyne detector to extract the information of multiple players thanks to the proposed multiple sideband modulation approach, and the evaluation of the channel parameters for each player is independent. These significantly reduce the complexity and cost of QSS network system and increase the secret key rate and transmission distance. The proposed QSS scheme is versatile and flexible. It can switch between QSS and CKA just by switching the classical post-processing program and no modification of hardware devices are required. We perform strict security analysis for Trojan horse attacks and the untrusted sources intensity fluctuation and noise. The protocol is proved to be secure against eavesdroppers on the quantum channel and dishonest players. We experimentally demonstrate the QSS and CKA protocols with five-party over long-distance single-mode fiber, and investigate the excess noise variations versus the number of the players and fiber length.

RESULTS

The QSS protocol

The sketch of the QSS protocol is shown in Fig. 1, the dealer prepares a number of laser sources of different wavelengths and sends them to adjacent players. For each laser source, the players implement independent Gaussian modulation to encode their key information in different sidebands[42] of the light field and subsequently send the modulated light field to the next player. Then the signal fields with different wavelengths are multiplexed via the add/drop multiplexer (ADM) and sent to the dealer through a common quantum channel. The dealer demultiplexs the relieved signal fields via a demultiplexer (DEMUX) and measures them separately via heterodetection. The detailed steps are as follows.

Step 1. The dealer prepares n laser sources of different wavelength λ_i, $i \in \{1, 2, \ldots, n\}$. The first player P_{11} modulates the laser λ_1 and prepares a coherent state $|X_{\lambda_1 f_1} + iP_{\lambda_1 f_1}\rangle$ with weak modulation at sideband frequency f_1 of the light field and sends the modulated light field to the neighboring player P_{12}.

Step 2. The second player P_{12} prepares the coherent state $|X_{\lambda_1 f_2} + iP_{\lambda_1 f_2}\rangle$ on sideband f_2. Above procedure is repeated until the P_{1p}th player prepares the coherent state $|X_{\lambda_1 f_p} + iP_{\lambda_1 f_p}\rangle$ and sends the modulated signal fields into the common quantum channel.

Step 3. For other laser source λ_i, the corresponding players implement the same procedure as above to encode their information in different sidebands of the light field and add the modulated signal fields into the common quantum channel via ADM.

Step 4. After the quantum states of all players reach the dealer through a common quantum channel, the dealer uses a demultiplexer to separate the received quantum states and measures them using heterodyne detection. The measurement results (raw data) are denoted by $\{X^m_{\lambda_i f_j}, P^m_{\lambda_i f_j}\}$, $j \in \{1, 2, \ldots, p, \ldots, q\}$.

Step 5. Repeat the above steps until enough raw keys are accumulated.

Step 6. The dealer and each player independently evaluate the channel parameters including the quantum channel transmittance and excess noise $\{T_{\lambda_i f_j}, \varepsilon_{\lambda_i f_j}\}$ by using the same procedure as that of the continuous variable QKD (CV-QKD)[43–46]. Based on the channel parameters, the key rates between the dealer and each player can be estimated. If all of them are positive, the dealer selects the lowest key rate $K_{\min}$ among all players as the key rate of the QSS, that means the QSS works at the rate of the worst performing player. Then using the data reconciliation and privacy amplification, the secret keys $\{S_{\lambda_i f_j}\}$ are distilled.

Step 7. For a (k, n) threshold QSS, the dealer randomly selects a $k-1$ power polynomial $f(S_{\lambda_i f_j})$ in the finite field Z, where $f(S_{\lambda_i f_j}) = S + a_1 S^1_{\lambda_i f_j} + a_2 S^2_{\lambda_i f_j} + \cdots + a_{k-2} S^{k-2}_{\lambda_i f_j} + a_{k-1} S^{k-1}_{\lambda_i f_j}$. Here, the polynomial coefficients $\{S, a_1, a_2, \cdots, a_{k-1}\} \in Z$ and S is the sharing secret key. The dealer calculates $\{S_{\lambda_i f_j}, f(S_{\lambda_i f_j})\}$, and selects a Hash function $H(S_{\lambda_i f_j})$ to calculate the authentication tag $\{H(S_{\lambda_i f_j})\}$. Next, the dealer sends $f(S_{\lambda_i f_j})$, the Hash function, and the authentication tags to each player through the authenticated classical channel.

Step 8. Each player know $f(S_{\lambda_i f_j})$ and the authentication tags of all players. If k players want to reconstruct the sharing secret keys, they use the Hash function to calculate the authentication tags $\{H'(S_1), H'(S_2), \cdots, H'(S_k)\}$ and compare them with those sent by the dealer. By checking the consistency of the authentication tag, the dishonest players can be discovered. After verification, the sharing secret key S can be calculated directly using the Lagrange interpolation formula:

$$S = \sum_{h=1}^{k} f(S_h) \prod_{l=1.l \neq h}^{k} \frac{S_l}{S_l - S_h}. \tag{1}$$

Although above procedures are classical, we take each distributed key $S_{\lambda_i f_j}$ as a independent variable of a polynomial $f(S_{\lambda_i f_j})$ and combine it with a Hash function, which makes our scheme secure against eavesdroppers and dishonest players in both the quantum distribution stage and the key reconstruction stage.

The CKA protocol

For actual application scenarios, a quantum network should not support only a single protocol. On the premise of not changing the underlying architecture, it is desired that the network can support multiple protocols which can be conveniently switched according to the needs of the players. Such a network structure is flexible and versatile[20,27,37].

Our experimental system is flexible and versatile and can be used to implement CKA without modifying any hardware devices, one only need to switch the corresponding post-processing procedure. Below we present the implementation process of CKA in detail.

Step 1. By utilizing the same quantum stage as that of the QSS scheme, the dealer establishes different quantum keys $\{S_{\lambda_i f_j}\}$ with all players. The dealer selects the lowest secret key rate $K_{\min}$ among all players, that means the CKA works at the key rate of the worst performing player.

Step 2. The dealer prepares a common secret key S_c, which are encrypted using the player's quantum secret key $S_{\lambda_i f_j}$, $S_e = S_{\lambda_i f_j} \oplus S_c$, and then sent to the designated players through the authenticated classical channel. Next the players decrypt the encrypted keys with their own quantum secret key and recover the common secret key $S_c = S_e \oplus S_{\lambda_i f_j}$[31].

Our CKA scheme has following advantages. Quantum state preparation: it only requires off-the-shelf telecom components such as commercial narrow linewidth lasers, amplitude and phase modulators, thus the state preparation process is simple and low-cost. Scalability: it can be conveniently extended to plenty of players on the order of hundreds (see "Discussion" section for the details).

Security analysis

For the presented QSS scheme, similar to the theoretical framework of plug-and-play QKD[39], the transmission of the laser source from the dealer to the players can be controlled by Eve. In this case, Eve may performs potential attacks. Therefore, the practical security of the protocols under the conditions of Trojan horse attacks, untrusted source intensity fluctuation, and untrusted source noise should be analyzed. (See "Methods" section for the detailed theoretical analysis).

On the basis of the practical security analysis of QSS scheme, we derive the secret key rate in this part. The lower bound of the asymptotic secret key rate of the QSS and CKA protocols against collective attack are given by[47,48]

$$K = \beta I_{AB} - \chi_{BE}, \tag{2}$$

where β is the reconciliation efficiency, I_{AB} is the Shannon mutual information between the player and dealer, and χ_{BE} is the maximum information available to the dishonest players and eavesdroppers conditioned on dealer's measurement.

The channel added noise referred to the channel input is given by

$$\chi_{\text{line}} = \frac{1}{T_2} - 1 + \varepsilon_1, \tag{3}$$

where $1/T_2 - 1$ is introduced by the quantum channel loss, T_2 denotes the effective channel transmittance, and ε_1 denotes the effective excess noise. The detection noise referred to the dealer's input is expressed by

$$\chi_{\text{het}} = \frac{[1 + (1 - \eta) + 2\upsilon_{\text{el}}]}{\eta}, \tag{4}$$

where η and υ_{el} denote the detector efficiency and the detector electronic noise, respectively. The total noise referred to the channel input is

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T_2}. \tag{5}$$

The mutual information I_{AB} is calculated directly from the dealer's measured quadratures variance $V_B = T_2\eta(V + \xi_E + \chi_{\text{tot}})$, where $V = V_M + 1$, V_M denotes the effective modulated variance and the conditional variance $V_{B|A} = T_2\eta(1 + \xi_E + \chi_{\text{tot}})$

$$I_{AB} = \log_2 \frac{V_B}{V_{B|A}} = \log_2 \frac{(V + \xi_E + \chi_{\text{tot}})}{(1 + \xi_E + \chi_{\text{tot}})}, \tag{6}$$

where ξ_E denotes the untrusted source noise added by Eve. Eve's access information is up bounded by the Holevo quantity

$$\chi_{BE} = S(\rho_{E_0E}) - \int dm_{B_1} p(m_{B_1}) S\left(\rho_{E_0E}^{m_{B_1}}\right), \tag{7}$$

where $p(m_{B_1})$ is the probability density of the dealer's measurement outcomes m_{B_1}. $\rho_E^{m_{B_1}}$ is the quantum state of Eve and

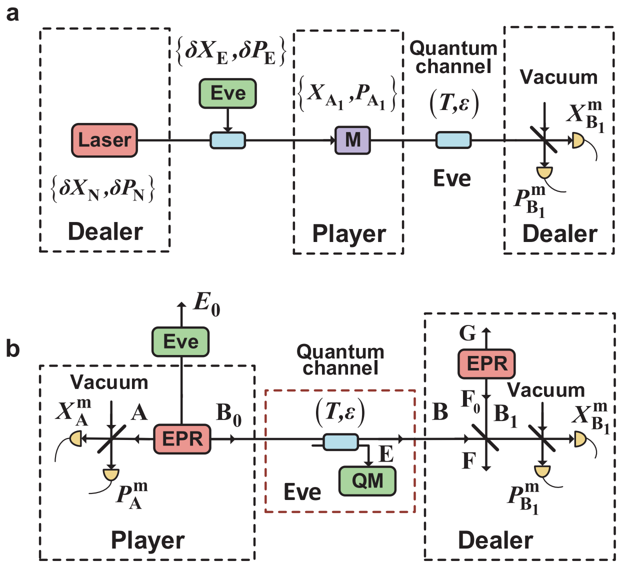

Fig. 2 PM and EB schemes of the QSS protocol with untrusted coherent source. a The PM scheme. **b** The equivalent EB scheme. Eve may introduce noises at the sidebands where the player encoding key information by modulating the laser in the PM scheme. In the equivalent EB scheme, a three-mode entangled state $\rho_{AE_0B_0}$ is generated with the mode E_0 controlled by Eve.

dishonest players conditioned on the dealer's measurement result. $S(.)$ denotes the von Neumann entropy. To calculate Eve's accessible information, we know that Eve's system can purifiy the system AE$_0$B (Fig. 2), $S\left(\rho_{E_0E}\right)=S(\rho_{AB})$, and the system AE$_0$EFG is pure after the dealer's heterodyne measurement, so that $S\left(\rho_{E_0E}^{m_{B_1}}\right)=S\left(\rho_{AFG}^{m_{B_1}}\right)$, where $S\left(\rho_{AFG}^{m_{B_1}}\right)$ is independent of m_{B_1} for the Gaussian modulated Gaussian states protocol. Now, Eq. (7) can be rewritten as

$$\chi_{BE}=S(\rho_{AB})-S\left(\rho_{AFG}^{m_{B_1}}\right). \tag{8}$$

The covariance matrix of the Gaussian state ρ_{AB}

$$\gamma_{AB}=\begin{bmatrix} VI & \sqrt{T_2\left(V^2-1\right)}\sigma_z \\ \sqrt{T_2\left(V^2-1\right)}\sigma_z & T_2(V+\xi_E+\chi_{line})I \end{bmatrix}, \tag{9}$$

where $I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ and $\sigma_z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$.

The symplectic eigenvalues of γ_{AB} have the form

$$\lambda_{1,2}^2=\frac{1}{2}\left[A\pm\sqrt{A^2-4B}\right], \tag{10}$$

where

$$\begin{aligned} A &= V^2-2T_2\left(V^2-1\right)+{T_2}^2(V+\xi_E+\chi_{line})^2, \\ B &= {T_2}^2[V(\xi_E+\chi_{line})+1]^2. \end{aligned} \tag{11}$$

The symplectic eigenvalues of $\gamma_{AFG}^{m_{B_1}}$ have the form

$$\lambda_{3,4}^2=\frac{1}{2}\left[C\pm\sqrt{C^2-4D}\right], \lambda_5=1, \tag{12}$$

where

$$\begin{aligned} C &= \frac{1}{[T_2(V+\xi_E+\chi_{tot})]^2}\{A{\chi_{het}}^2+B+1+2\chi_{het} \\ &\quad \times[V\sqrt{B}+T_2(V+\xi_E+\chi_{line})]+2T_2\left(V^2-1\right)\}, \\ D &= \left(\frac{V+\sqrt{B}\chi_{het}}{T_2(V+\xi_E+\chi_{tot})}\right)^2. \end{aligned} \tag{13}$$

The Holevo quantity χ_{BE} is given by

$$\begin{aligned} \chi_{BE} &= G\left(\tfrac{\lambda_1-1}{2}\right)+G\left(\tfrac{\lambda_2-1}{2}\right) \\ &\quad -G\left(\tfrac{\lambda_3-1}{2}\right)-G\left(\tfrac{\lambda_4-1}{2}\right), \end{aligned} \tag{14}$$

where $G(x)=(x+1)\log_2(x+1)-x\log_2 x$.

Using Eqs. (2), (6), and (10)–14), we can calculate the lower bound of the secret key rate.

Modulation

In our experiment, the weak modulation method is adopted to prepare the coherent states at the sideband modes. Before the modulation, the complex amplitude of a single frequency laser has the form

$$a(t)=\alpha_0 e^{i2\pi f_0 t}, \tag{15}$$

where α_0 and f_0 are the amplitude and frequency of the laser. When the laser is weakly modulated at frequency f_j, the sidemode of the modulated laser is given by

$$a'(t)=\alpha_0(M_x+iM_p)\left[e^{i2\pi(f_0+f_j)t}+e^{i2\pi(f_0-f_j)t}\right], \tag{16}$$

where $M_x \ll 1$ and $M_p \ll 1$ denote the amplitude and phase modulation depths respectively. Because the average photon number of the carrier satisfies $|\alpha_0|^2 \gg 1$, even if a very weak modulation can faithfully prepare a coherent state with mean photon number of a few photons at the sidemode. From Eq. (16), the sidemode states can be written as

$$|\phi_{f_j}\rangle = |X+iP\rangle_{\pm f_j}|0\rangle_{f\neq\pm f_j}, \tag{17}$$

where $X=M_x\alpha_0$, $P=M_p\alpha_0$. Therefore, under the condition of large $|\alpha_0|$ and small modulation depths, we can conveniently prepare sidemode coherent states by modulating the amplitude and phase of the laser field.

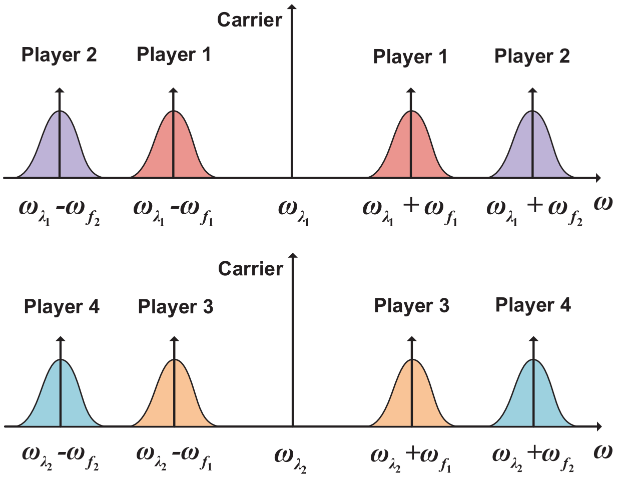
Carrier
Player 2
Player 1
Player 1
Player 2
ω_{λ_1} -ω_{f_2}
ω_{λ_1} -ω_{f_1}
ω_{λ_1}
$\omega_{\lambda_1}+\omega_{f_1}$
$\omega_{\lambda_1}+\omega_{f_2}$
ω
Carrier
Player 4
Player 3
Player 3
Player 4
ω_{λ_2} -ω_{f_2}
ω_{λ_2} -ω_{f_1}
ω_{λ_2}
$\omega_{\lambda_2}+\omega_{f_1}$
$\omega_{\lambda_2}+\omega_{f_2}$
ω

Fig. 3 Distribution of quantum signals and carrier signals in frequency domain. The player's quantum signals are generated by modulating the carrier of the lasers, thus the carrier and signals have the same phase. The phase of the signals can be determined by estimating the phase of the carrier.

Carrier phase evaluation

In our experiment, the quantum signals and local oscillators (LO) are transmitted through two different long-distance fibers to simulate the local local oscillator (LLO) scheme. In this case, there exists fast phase drifts between the quantum signals and LO. At present, several phase recovered schemes have been proposed that mainly using the pilot-aided feedforward data recovery scheme. The basic idea of the pilot-sequence scheme is to use adjacent pilot pulses to estimate the middle signal's phase drift[49]. The pilot-multiplexed scheme divides the phase drift into the fast drift and the slow drift parts, and one can implement two remapping procedures to compensate them separately[50].

In our scheme, we use a simple method to estimate the phase of the signals. As shown in Fig. 3, the quantum signals are generated by modulating the carrier of the lasers and they have fixed phase relations. Although the player's quantum signals are not generated at the same time, the quantum signals and the carrier pass through the same optical path and are subject to the same phase evolution[51,52]. Therefore, all the quantum signals for each laser have the same phase and we can infer the phase of the quantum signals by evaluating the phase of the carrier.

Experimental results

We demonstrated the proof-of-principle experiment of the proposed QSS and CKA protocols over different long-distance fiber links (see Fig. 4). The experimental parameters are shown in Table 1. To investigate the effect of different multiplexing methods on the player's excess noises, we measured the excess noises under different scenarios, only a single player, two players with sideband multiplexing, and four players with both the dense wavelength division multiplexing and sideband multiplexing. The results are shown in Fig. 5.

In Fig. 5a, the average values of the excess noise of player 1 at total transmission distance of 22 km under three cases are 0.00847

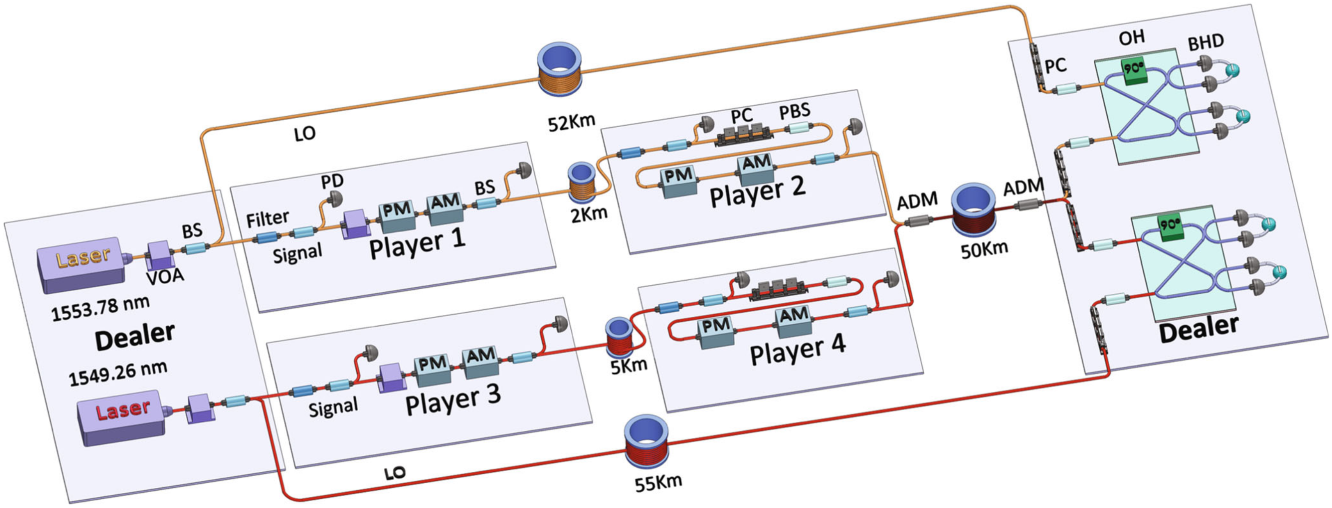

Fig. 4 Experimental setup for QSS and CKA. VOA variable optical attenuator, BS beam splitter, PM phase modulator, AM amplitude modulator, PD photoelectric detector, PC polarization controller, PBS polarizing beam splitter, OH optical hybrid, BHD balanced homodyne detector.

Table 1. The experimental parameters of the QSS and CKA system.

Players	L (km)	V_M (SNU)	I_{el}^{max}	V_{el}	V_{λ_i}	v_{el} (SNU)	η (%)	β (%)	ε_1 (SNU)	S (bits per pulse)
Player 1	22	2.14	4.70×10^{-4}	5.03×10^{-8}	1.67×10^{-7}	0.052	54	95	0.010	0.0075
Player 2	20	2.12	1.75×10^{-3}	1.87×10^{-7}	1.94×10^{-7}	0.087	54	95	0.011	0.0770
Player 3	25	2.18	5.18×10^{-4}	4.83×10^{-8}	1.49×10^{-7}	0.045	56	95	0.0079	0.0061
Player 4	20	2.08	1.97×10^{-3}	1.98×10^{-7}	1.74×10^{-7}	0.048	56	95	0.0071	0.0824
Player 1	52	2.09	4.94×10^{-4}	5.06×10^{-8}	1.64×10^{-7}	0.26	54	95	0.038	7.14×10^{-4}
Player 2	50	2.13	1.57×10^{-3}	1.82×10^{-7}	1.98×10^{-7}	0.39	54	95	0.029	0.0089
Player 3	55	2.20	4.97×10^{-4}	4.88×10^{-8}	1.53×10^{-7}	0.19	56	95	0.022	9.49×10^{-4}
Player 4	50	2.11	1.82×10^{-3}	1.89×10^{-7}	1.83×10^{-7}	0.24	56	95	0.0086	0.0130

L the length of single-mode fiber, V_M the overall modulation variance, V'_{el} the electronic noise of the photodetector that monitoring light intensity fluctuations, V'_{λ_i} the variance of light pulse intensity fluctuation, I_{el}^{max} the maximum electronic noise of the photodetector that monitoring the fluctuations of the light intensity, v_{el} the electronic noise of the homodyne detector, η the efficiency of the homodyne detector, β reconciliation efficiency, ε_1 excess noise, S secret key rate.

The lower key rates for players 1 and 3 is mainly because that their quantum signals pass through players 2 and 4, resulting in larger channel losses.

(only player 1 encoding the information), 0.0102 (both player 1 and player 2 encoding the information), and 0.0098 (all players 1–4 encoding the information), respectively. We can see that the frequency multiplexing has a slight influence on the excess noise. It is due to that the frequency multiplexing causes a little crosstalk during the modulation and demodulation of the quantum signals. For the dense wavelength division multiplexing of the quantum signals, the player's excess noise has negligible impact on each other. Above phenomenon is also confirmed by the similar results observed in Fig. 5b–d.

The experimental secret key rates of the QSS (CKA) system are shown in Fig. 6. The black line represents the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound[53]. The two purple rhombus, black triangles, blue pentagrams, and red squares correspond to the secret key rate of the players 1, 2, 3, and 4 at single-mode fiber links of (22 km, 52 km), (20 km, 50 km), (25 km, 55 km), and (20 km, 50 km), respectively. The blue and red curves represent the simulated secret key rates for the players 1, 3 and the players 2, 4, respectively. Due to the channel loss of the players 1 and 3 is larger than that of the players 2 and 4 (the players 2 and 4 are regarded as eavesdroppers from the viewpoint of the player of 1 and 3), the key rate of the players 1 and 3 are lower. After all players estimate their key rate with the dealer, the lowest key rate of all the players is set as the key rate for the QSS (CKA) system. In our case, the key rate of the QSS (CKA) at 25 and 55 km fiber links are 0.0061 and 7.14×10^{-4} bits per pulse, respectively, which are determined by the key rate of players 3 and 1.

DISCUSSION

On the basis of our presented scheme, in this section we discuss the possible construction of a network topology for metropolitan QSS and CKA network.

In our proof of principle experiment, we employ the fiber-based components such as amplitude and phase modulators, optical filter, beam-splitters. These fiber pigtailed components have relative large insertion losses, which are detrimental to the performance of the QSS and CKA protocols. In fact, the players can employ free space optical devices at their stations, which can significantly reduce the adverse insertion losses and increase the player amount.

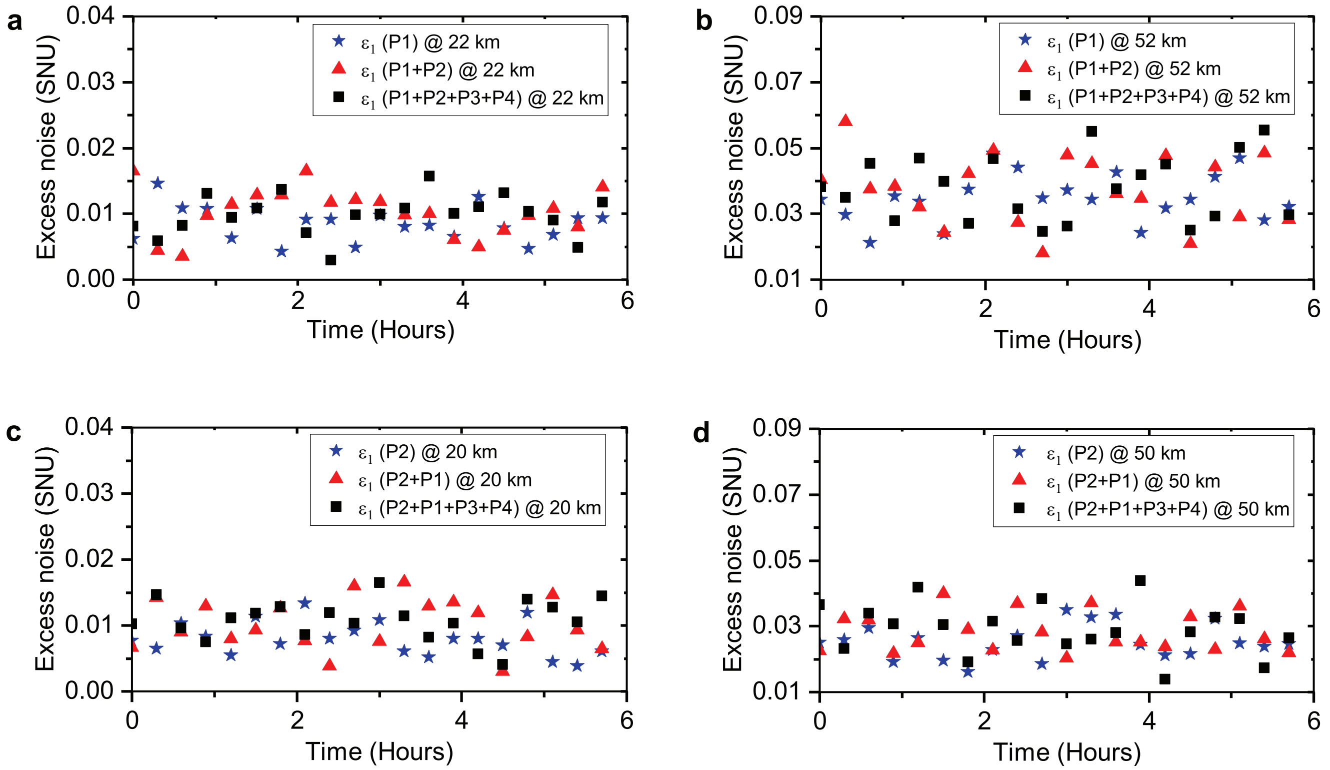

Fig. 5 Experimental excess noises of player 1 and player 2. **a**, **b** The excess noise of player 1 under different multiplexing methods for total transmission distance of 22 km and 52 km. The blue pentagrams represent the excess noise where of player 1 only player 1 encodes the information. The red triangles represent the excess noise of player 1 when both players 1 and 2 encode their information at different sidebands. The black squares represent the excess noise of player 1 when players 1, 2, 3, and 4 encode their information at different sidebands and wavelengths. **c**, **d** The excess noises of player 2 under different multiplexing methods for total transmission distance of 20 km and 50 km. The blue pentagrams represent the excess noise of player 2 where only player 2 encodes the information. The red triangles represent the excess noise of player 2 when both players 2 and 1 encoded their information at different sidebands. The black squares represent the excess noise of player 2 when players 2, 1, 3, and 4 encode their information at different sidebands and wavelengths.

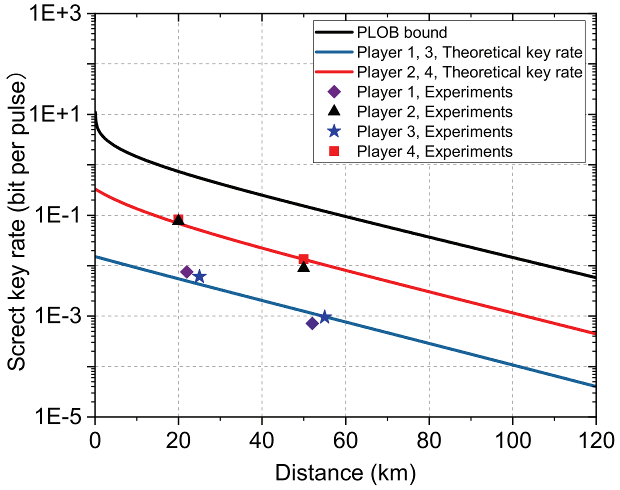

Fig. 6 Secret key rates of QSS (CKA). The black line is the PLOB bound. The two purple rhombus, black triangles, blue pentagrams, and red squares corresponds to the secret key rate of the players 1, 2, 3, and 4 at single-mode fiber links of (22 km, 52 km), (20 km, 50 km), (25 km, 55 km), and (20 km, 50 km), respectively. The blue and red curves represent the simulated secret key rates for players 1, 3 and players 2, 4, respectively. The key rate of the QSS (CKA) at 25 and 55 km fiber links are 0.0061 and 7.14×10^{-4} bits per pulse.

Table 2 shows the typical losses of state of the art optical devices that are required in our protocol. From the loss values, we can estimate the total insertion losses (d) for each player's station is around 1.35 dB. Using the estimated loss, we propose a possible network topology for metropolitan QSS and CKA network, as shown in Fig. 7. The metropolitan network consists of a backbone network and multiple access networks. The backbone network have m access points, which enables the end players to connect to the network. The upper limit value of the channel loss for each access network is assumed to be D. The construction process of the metropolitan network is as follows.

Step 1. The fiber distance between the farthest player and the dealer in each access network is defined as L, and the therefore channel linear loss is $0.2L$ for standard single-mode fiber.

Step 2. Since the insertion loss of the player's station is greater than that of the ADM, the backbone network should configure the access nodes as many as possible in order to maximize the number of the players in the metropolitan network. The number of access nodes can be given by

$$m = \frac{D - 0.2L - \mathrm{AWG}}{\mathrm{ADM}}, \tag{18}$$

where AWG and ADM denote the insertion loss of the AWG and ADM.

Table 2. The insertion loss of the optical devices.

Optical devices	Filter	PC	1/99 BS	PBS	PM	AM	Coupling efficiency	ADM	AWG 48-CH
Insertion loss (dB)	0.35	0.1	0.05	0.1	0.05	0.25	0.2	0.35	3.5

Filter fiber optical filter, *PC* fiber polarization controller, *1/99 BS* free-space 1/99 beam splitter, *PBS* free-space polarization beam splitter, *PM* free-space phase modulator, *AM* free-space amplitude modulator biased at 96% transmission point, *Coupling efficiency* the coupling efficiency of fiber to free-space (free-space to fiber), *AWG 48-CH* arrayed waveguide grating of 48-channel.

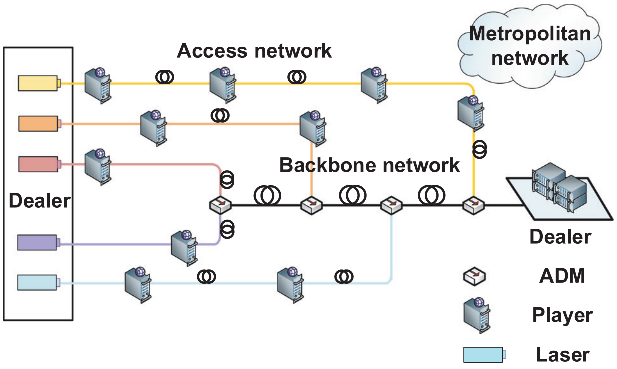

Fig. 7 The schematic diagram of the QSS and CKA network topology. The metropolitan network is composed of the access network and the backbone network.

Step 3. The number of the players in the yth access network counting from receiver is expressed as

$$n_y = \frac{D - 0.2L - y\text{ADM} - \text{AWG}}{d} + 1, \tag{19}$$

where $y \in \{1, 2, \ldots, m\}$.

Step 4. The maximum number of the players in the metropolitan network is

$$N = 1 + \sum_{y=1}^{m} n_y. \tag{20}$$

Notice that, given the fiber distance L between the farthest players of the access networks and the dealer, the position of the players in each access network is unrestricted. The span between two adjacent access points can also be freely configured as needed.

Based on the construction method mentioned above, we simulate the maximum number of the players at different transmission distances in Fig. 8. The black and blue dots represent the results of theoretical simulations under $D = 20$ dB and 30 dB. The red and black curves are the fitting curves. The network exhibits a nonlinear dependence between the transmission distance and number of the players. When the channel loss limit is set to 20 dB, we can see that the secure QSS and CKA among 180 (53) players are feasible within a metropolitan area over 20 km (50 km). If the channel loss limit increases to 30 dB, the number of the players can improve to 651 (307) accordingly. In our protocols, adding or removing users is straightforward and can be realized by inserting or removing the encoding devices of the target users, and the overall network architecture remains almost unchanged.

In conclusion, we have proposed and demonstrated a practical, scalable, verifiable (k, n) threshold continuous variable QSS and CKA protocol. Our protocol effectively eliminates the need of preparing laser source by each player, phase locking of all players' independent lasers, and excess noises superposition. Furthermore, a single heterodyne detector can be used to extract the information of multiple players by using the multiple sideband modulation approach. We strictly analyzed the practical security for the proposed QSS system under Trojan horse attack, untrusted sources intensity fluctuating, and noisy untrusted sources. The proposed system is flexible and versatile, it can realize both the QSS and CKA tasks by just switching the post-processing program. We experimentally investigated the effects of the quantum channel multiplexing of multiple players on the excess noises of the system, and verified the five-party QSS and CKA quantum communication protocols. A secure key rate of 0.0061 (7.14×10^{-4}) bits per pulse are achieved over 25 (55) km standard single-mode fiber. Our results provide a feasible solutions for practical quantum private communication network with current telecom technology.

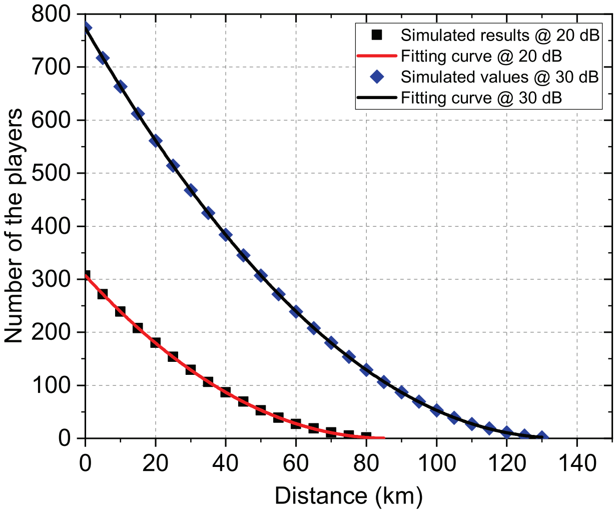

Fig. 8 The number of the players versus the transmisssion distance. The black squares and blue rhombus are the simulated number of the players. The red and black curve is the fitting according to the simulated values. Given the channel loss limits of 20 dB and 30 dB, we find that the secure QSS and CKA among 180 (53) and 651 (307) players are feasible over a metropolitan area over 20 km (50 km).

In our current proof of principle experiment, the sideband frequencies that encoding the key information are 7 MHz and 9 MHz, respectively, and the system clock rate is 250 kHz. In principle, the sideband offset can be set to higher frequencies, which are only limited by the bandwidth of the modulator and heterodyne detector that currently reaches above 20 GHz. In this case, one can use a higher system clock rate, for example, above GHz. Moreover, our network system uses Gaussian modulation to encode the information, other modulation formats such as discrete modulation can also be employed[54–57]. It is possible that the proposed sideband encoding method can be applied to other QKD schemes, for example, Twin-Field QKD (TF-QKD), which can effectively beating the PLOB bound and achieve a much longer communication distance[51,52,58–61].

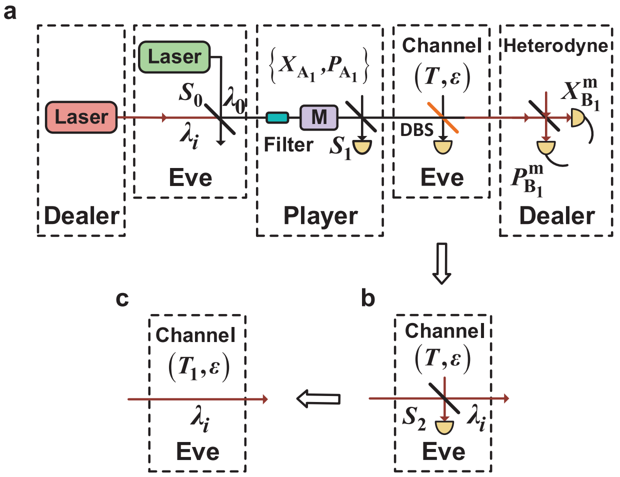

Fig. 9 Schematic diagram of the Trojan horse attack model. a Eve uses a beam splitter to inject her probe light at wavelength of λ_0 into the player's station. After being modulated by the player, the probe light is separated by a DBS at outside of the station. Then Eve can acquire the key information by measuring the probe beam. **b** We can assume $\lambda_0 = \lambda_i$, and replace the DBS with beam splitter S_2 with transmittance $S_2 = I_{\lambda_i}/(I_{\lambda_i} + I_{\lambda_0})$ at I_{λ_0}. **c** The Trojan horse attack is equivalent to decrease the transmittance of the untrusted quantum channel from T to $T_1 = TS_2$.

METHODS

Experimental setup

The schematic of the experimental setup is shown in Fig. 4. Two continuous wave single-frequency lasers with different wavelengths (1553.78 nm and 1549.26 nm) were prepared by the dealer. A small portion of the lasers are employed as the signals and the rest are acted as the LO fields. The 1553.78 nm and 1549.26 nm signals are sent to player 1 and player 3, respectively. The players 1 and 3 independently generate two sets of Gaussian random numbers at a repetition rate of 250 kHz, and mix them with a 7 MHz sine signals. Then the mixed signals are loaded on the phase and amplitude waveguide modulators to modulate two conjugate quadrature components of the signal fields. The optical filters at the input port of the players' station limit the wavelength range of Eve's Trojan horse attacks. To counter against the untrusted source intensity fluctuation attack, a small portion of the incoming signal beams is split and monitored by a photodetector (PD). The PD after the amplitude modulators (AM) monitors the modulation variance in real time by detecting the intensity of the modulated laser beam. Combine with the optical filter together, they can resist the Trojan horse attacks.

The modulated signal beams are sent to the players 2 and 4 through a 2 km and 5 km single-mode fiber (SMF-28e), respectively. After correcting the state of the polarization by the polarization controller (PC), the players 2 and 4 encode their secret key information at the 9 MHz sideband of the signal beams. By using the ADM, two signal beams are coupled into a 50 km single-mode fiber. The two LO beams are sent to the dealer though 52 km and 55 km single-mode fiber, respectively. At the dealer's station, the signal beams are decoupled by the ADM and measured by heterodyne detection. To this end, two 90° optical hybrid (Kylia) and four balanced homodyne detectors are employed to measure both the amplitude and phase quadrature of the incoming signals. The outputs of the detectors are mixed with 7 MHz and 9 MHz sine waveforms, respectively, and then filtered by two 500 kHz low pass filters. The dealer identifies and extracts the key information of each player in terms of the corresponding wavelengths and sidebands on which the players encoding their key information.

Security proof under Trojan horse attacks

Due to the bidirectional feature of the QSS scheme, the Trojan horse attack should be considered. As shown in Fig. 9a, Eve can use a beam splitter with transmittance of S_0 to couple her probe laser at wavelength of λ_0 with the laser at wavelength of λ_i, $i \in \{1, 2, \ldots, n\}$ sent by the dealer and send them to the player. The probe laser will carry the key information after being modulated by the modulators of the players. Just at the outside of the player's station, Eve uses a dichroic beam splitter (DBS) to separate the probe laser to obtain the key information.

To deal with this attack, we insert a 50-GHz narrow-band optical filter (0.4 nm bandwidth) into the player's input port, thereby limiting Eve's probe laser wavelength to $|\lambda_0 - \lambda_i| \le 0.2$ nm. A beam splitter with transmittance of S_1 is added after the modulator to monitor the modulated light fields. The measured light intensity is given by

$$I_m = \eta_{\lambda_i} I_{\lambda_i} + \eta_{\lambda_0} I_{\lambda_0} + I_{el}, \tag{21}$$

where η_{λ_i} and η_{λ_0} are the total detection efficiency of the player and Eve, respectively, including the modulator's loss, split ratio of beam splitter, and the photodiode's quantum efficiency. I_{λ_i} and I_{λ_0} are the light intensity of the player and Eve respectively, and I_{el} is the electronic noise of the monitoring detector. Since a weak electro-optic modulation is employed, the modulation variance is proportional to the light intensity of the modulated laser. The modulation variance of the player and Eve can be expressed as

$$V_A = M_{\lambda_i} I_{\lambda_i}, V_{\lambda_0} = M_{\lambda_0} I_{\lambda_0}, \tag{22}$$

where M_{λ_i} and M_{λ_0} are the modulation coefficients of the electro-optic modulators. Substituting Eq. (22) into Eq. (21) we get

$$I_m = \frac{\eta_{\lambda_i} V_A}{M_{\lambda_i}} + \frac{\eta_{\lambda_0} V_{\lambda_0}}{M_{\lambda_0}} + I_{el}. \tag{23}$$

Considering that the wavelength of the probe light is very close to the wavelength of the dealer' laser $\lambda_0 \approx \lambda_i$, we have

$$\frac{\eta_{\lambda_0}}{M_{\lambda_0}} \approx \frac{\eta_{\lambda_i}}{M_{\lambda_i}} = R. \tag{24}$$

Eq. (23) can be simplified to

$$I_m \approx R(V_A + V_{\lambda_0}) + I_{el}. \tag{25}$$

Therefore, by measuring the partial light intensity of the modulated laser, the overall variance $V_M = V_A + V_{\lambda_0}$ of the modulated light fields can be monitored.

Note that the effect of the Trojan horse attack has nothing to do with the specific value of λ_0 given that the average photon number of the probe light remains unchanged. Without loss of generality, we can choose $\lambda_0 = \lambda_i$, therefore $V_{\lambda_0} = V_{\lambda_i}$, $V_M = V_A + V_{\lambda_i}$ and replace the DBS of Eve with a beam splitter of transmittance S_2 as shown in Fig. 9b. Eq. (25) can be rewritten as

$$I_m = RV_M + I_{el}. \tag{26}$$

Therefore, the Trojan horse attack of the eavesdropper is equivalent to the increase of the attenuation of the untrusted quantum channel (Fig. 9c), i.e. $T_1 = TS_2$, where T is the original channel transmittance and $S_2 = I_{\lambda_i}/(I_{\lambda_i} + I_{\lambda_0})$. Since the quantum key distribution protocol is information-theoretical secure for untrusted quantum channel, the Trojan horse attack is discoverable and ineffective.

The measurement of the modulated laser intensity is an average of plenty of measurement data in one data block (>10^6). In this case, the effect of the electronic noise can be ignored. Eq. (26) can be rewritten as

$$\langle I_{\mathrm{m}}\rangle \approx RV_{\mathrm{M}}. \tag{27}$$

To defeat Eve's Trojan horse attack, we can estimate the channel transmittance and excess noise using the player's and dealer's data, and the monitored V_{M},

$$T_1 = \frac{\langle X_{\mathrm{A}_1} X_{\mathrm{B}_1}^{\mathrm{m}}\rangle^2}{\eta V_{\mathrm{A}} V_{\mathrm{M}}} = \frac{TV_{\mathrm{A}}}{V_{\mathrm{M}}}, \tag{28}$$

$$\varepsilon = \frac{V_{\mathrm{B}} - 1 - \upsilon_{\mathrm{el}}}{\eta T_1} - V_{\mathrm{M}}, \tag{29}$$

where $V_{\mathrm{B}} = \langle X_{\mathrm{B}_1}^{\mathrm{m}\,2}\rangle$ is the variance of the quadratures measured by dealer. η and υ_{el} are the efficiency and electronic noise of homodyne detector, respectively.

Security proof under untrusted source intensity fluctuations

Since the laser source is untrusted, Eve can also perform source intensity fluctuation attacks[62]. Supposes that the dealer plans to prepare a signal pulse with intensity I_{λ_i}, however, he actually prepares a pulse with the intensity of $I_{\lambda_i}(1+\sigma)$, where σ is the intensity fluctuation caused by the instability of the laser source with mean value zero and variance V_σ. The intensity of the signal pulse received by the player is $I_{\lambda_i}(1+\sigma+\varphi)$, where φ is the intensity fluctuation caused by Eve's intensity fluctuation attack with mean value zero and variance V_φ. The actual coherent state that encoding the Gaussian random variables $(X_{\mathrm{A}_1}, P_{\mathrm{A}_1})$ of the player is given by

$$|X_{\mathrm{A}_2} + \mathrm{i}P_{\mathrm{A}_2}\rangle = \left|\sqrt{(1+\sigma+\varphi)}X_{\mathrm{A}_1} + \mathrm{i}\sqrt{(1+\sigma+\varphi)}P_{\mathrm{A}_1}\right\rangle. \tag{30}$$

To deal with Eve's source intensity fluctuation attack, we added a photodetector at the player's input port to monitor the intensity of each light pulse and the measured signal is

$$I_{\mathrm{m}} = I_{\lambda_i} + I_{\mathrm{el}}, \tag{31}$$

where I_{el} is the electronic noise of the detector. The measured intensity fluctuation of the light pulse relative to the average light intensity is expressed as

$$\delta I_{\mathrm{m}} = \delta I_{\lambda_i} + \delta I_{\mathrm{el}}, \tag{32}$$

where δI_{λ_i} and δI_{el} are the light pulse fluctuation and electronic noise fluctuation relative to the average light intensity and they satisfy $\delta I_{\lambda_i} = \sigma + \varphi$, $\langle \delta I_{\lambda_i}\rangle = 0$, $\left\langle \delta I_{\lambda_i}{}^2\right\rangle = V_{\lambda_i}$, $\langle \delta I_{\mathrm{el}}\rangle = 0$, and $\left\langle \delta I_{\mathrm{el}}{}^2\right\rangle = V_{\mathrm{el}}$. Considering the source intensity fluctuation, the prepared coherent states can be rewritten as

$$|X_{\mathrm{A}_2} + \mathrm{i}P_{\mathrm{A}_2}\rangle = \left|\sqrt{(1+\delta I_{\lambda_i})}X_{\mathrm{A}_1} + \mathrm{i}\sqrt{(1+\delta I_{\lambda_i})}P_{\mathrm{A}_1}\right\rangle. \tag{33}$$

Notice that the fluctuations of the optical pulses cannot be accurately determined due to the electronic noise of the detector. To guarantee the security of the protocol, the player revises the data from $(X_{\mathrm{A}_1}, P_{\mathrm{A}_1})$ to

$$\begin{aligned} X_{\mathrm{A}_3} &= \left(1 + \delta I_{\mathrm{m}} + I_{\mathrm{el}}^{\max}\right)X_{\mathrm{A}_1}, \\ P_{\mathrm{A}_3} &= \left(1 + \delta I_{\mathrm{m}} + I_{\mathrm{el}}^{\max}\right)P_{\mathrm{A}_1}, \end{aligned} \tag{34}$$

where $I_{\mathrm{el}}^{\max}$ is the maximum of the electronic noise of the monitoring detector. In this case, the channel loss and excess noise will be overestimated by the dealer and players.

The channel transmittance can be

$$\begin{aligned} T_2 &= \frac{\left\langle X_{\mathrm{A}_3} X_{\mathrm{B}_2}^{\mathrm{m}}\right\rangle^2}{\left\langle 1+\delta I_{\mathrm{m}}+I_{\mathrm{el}}^{\max}\right\rangle^2 \eta V_{\mathrm{A}} V_{\mathrm{M}}} \\ &= \frac{\left\langle\sqrt{1+\delta I_{\lambda_i}}\right\rangle^2 TV_{\mathrm{A}}}{\left\langle\sqrt{1+\delta I_{\mathrm{m}}+I_{\mathrm{el}}^{\max}}\right\rangle^2 V_{\mathrm{M}}}, \end{aligned} \tag{35}$$

where $X_{\mathrm{B}_2}^{\mathrm{m}} = \sqrt{1+\delta I_{\lambda_i}} X_{\mathrm{B}_1}^{\mathrm{m}}$.

By using Taylor expansion, we can obtain

$$\sqrt{1+\delta I_{\lambda_i}} \approx 1 + \frac{\delta I_{\lambda_i}}{2} - \frac{\delta I_{\lambda_i}{}^2}{8}, \tag{36}$$

$$\sqrt{1+\delta I_{\mathrm{m}} + I_{\mathrm{el}}^{\max}} \approx 1 + \frac{\delta I_{\mathrm{m}} + I_{\mathrm{el}}^{\max}}{2} - \frac{(\delta I_{\mathrm{m}} + I_{\mathrm{el}}^{\max})^2}{8}. \tag{37}$$

Inserting Eqs. (36) and (37) into Eq. (35), we have

$$T_2 = \frac{(8 - V_{\lambda_i})^2 TV_{\mathrm{A}}}{(8 + 4I_{\mathrm{el}}^{\max} - V_{\lambda_i} - V_{\mathrm{el}})^2 V_{\mathrm{M}}}. \tag{38}$$

Using the expression of T_2, the excess noise ε_1 is written as

$$\varepsilon_1 = \frac{(V_{\mathrm{B}} - 1 - \upsilon_{\mathrm{el}})}{\eta T_2} - \left(1 + I_{\mathrm{el}}^{\max}\right)V_{\mathrm{M}}, \tag{39}$$

The fluctuation variance V_{λ_i} of the light pulse intensity cannot be directly measured. We measure the total variance $\left\langle \delta I_{\mathrm{m}}{}^2\right\rangle = V_{\lambda_i} + V_{\mathrm{el}}$ of the fluctuation of the laser and the electronic noise, and then subtract the electronic noise variance V_{el} to obtain V_{λ_i}.

Security proof under untrusted source noises

In addition to the potential Trojan horse attack and untrusted source intensity fluctuation attack, Eve can also perform source noise attacks. In the following, we present the prepare-and-measurement (PM) scheme and the equivalent entanglement-based (EB) scheme. In Fig. 2a, a PM scheme is shown. The dealer prepares a coherent state source and its sidemode quantum state is $|X_{\mathrm{N}} + iP_{\mathrm{N}}\rangle$ with $\left\langle \delta X_{\mathrm{N}}{}^2\right\rangle = \left\langle \delta P_{\mathrm{N}}{}^2\right\rangle = 1$ (shot noise units, SNU). Eve introduces Gaussian noise $\{\delta X_{\mathrm{E}}, \delta P_{\mathrm{E}}\}$ on the sidemodes where the players encoding the key information by modulating the laser, and the noise satisfies $\left\langle \delta X_{\mathrm{E}}{}^2\right\rangle = \left\langle \delta P_{\mathrm{E}}{}^2\right\rangle = \xi_{\mathrm{E}}$. The untrusted source received by the player can be expressed as

$$|\delta X_{\mathrm{I}} + \mathrm{i}\delta P_{\mathrm{I}}\rangle = |\delta X_{\mathrm{N}} + \delta X_{\mathrm{E}} + \mathrm{i}(\delta P_{\mathrm{N}} + \delta P_{\mathrm{E}})\rangle. \tag{40}$$

After encoding the key information onto the source, the quantum state of the player is given by

$$|X_{\mathrm{PM}} + \mathrm{i}P_{\mathrm{PM}}\rangle = |\delta X_{\mathrm{I}} + X_{\mathrm{A}_1} + \mathrm{i}(\delta P_{\mathrm{I}} + P_{\mathrm{A}_1})\rangle. \tag{41}$$

The variance of the quadratures for the quantum state is given by

$$\left\langle X_{\mathrm{PM}}{}^2\right\rangle = \left\langle P_{\mathrm{PM}}{}^2\right\rangle = V + \xi_{\mathrm{E}}, \tag{42}$$

where $V = V_{\mathrm{A}}+1$. The conditional variance of X_{PM} (P_{PM}) given X_{A_1} or δX_{E} are

$$V_{X_{\mathrm{PM}}|X_{\mathrm{A}_1}} = V_{P_{\mathrm{PM}}|P_{\mathrm{A}_1}} = 1 + \xi_{\mathrm{E}}, \tag{43}$$

$$V_{X_{\mathrm{PM}}|\delta X_{\mathrm{E}}} = V_{P_{\mathrm{PM}}|\delta P_{\mathrm{E}}} = V. \tag{44}$$

The equivalent EB scheme of the QSS protocol is shown in Fig. 2b, a three-mode Gaussian entangled state $\rho_{\mathrm{AE_0B_0}}$ is generated and the mode E_0 controlled by Eve. For mode $A(X_{\mathrm{A}}, P_{\mathrm{A}})$, mode $\mathrm{E}_0(X_{\mathrm{E}_0}, P_{\mathrm{E}_0})$, and mode $\mathrm{B}_0(X_{\mathrm{B}_0}, P_{\mathrm{B}_0})$, we assume the following realtions are satisfied

$$\begin{aligned} \left\langle X_{\mathrm{A}}{}^2\right\rangle &= \left\langle P_{\mathrm{A}}{}^2\right\rangle = V, \\ \left\langle X_{\mathrm{E}_0}{}^2\right\rangle &= \left\langle P_{\mathrm{E}_0}{}^2\right\rangle = 1 + \xi_{\mathrm{E}}, \\ \left\langle X_{\mathrm{B}_0}{}^2\right\rangle &= \left\langle P_{\mathrm{B}_0}{}^2\right\rangle = V + \xi_{\mathrm{E}}. \end{aligned} \tag{45}$$

The covariance matrix $\gamma_{AE_0B_0}$ charactering the state $\rho_{AE_0B_0}$ has the form

$$\begin{bmatrix} V & 0 & 0 & 0 & \sqrt{V^2-1} & 0 \\ 0 & V & 0 & 0 & 0 & -\sqrt{V^2-1} \\ 0 & 0 & c\xi_{\mathrm{E}} & 0 & \sqrt{c\xi_{\mathrm{E}}} & 0 \\ 0 & 0 & 0 & c\xi_{\mathrm{E}} & 0 & -\sqrt{c\xi_{\mathrm{E}}} \\ \sqrt{V^2-1} & 0 & \sqrt{c\xi_{\mathrm{E}}} & 0 & V+\xi_{\mathrm{E}} & 0 \\ 0 & -\sqrt{V^2-1} & 0 & -\sqrt{c\xi_{\mathrm{E}}} & 0 & V+\xi_{\mathrm{E}} \end{bmatrix} \tag{46}$$

where $c \to +\infty$ is a large real number.

The player performs a heterodyne detection on mode A and the measurement results are given by

$$X_{\mathrm{A}}^{\mathrm{m}} = \frac{1}{\sqrt{2}}(X_{\mathrm{A}} + \delta X_{\mathrm{N}}), P_{\mathrm{A}}^{\mathrm{m}} = \frac{1}{\sqrt{2}}(P_{\mathrm{A}} - \delta P_{\mathrm{N}}). \tag{47}$$

The player uses the measurement results $\left(X_{\mathrm{A}}^{\mathrm{m}}, P_{\mathrm{A}}^{\mathrm{m}}\right)$ to estimate the mode B_0,

$$\begin{aligned} X'_{\mathrm{B}_0} &= \frac{\langle X_{\mathrm{B}_0} X_{\mathrm{A}}^{\mathrm{m}} \rangle}{\langle X_{\mathrm{A}}^{\mathrm{m}2} \rangle} X_{\mathrm{A}}^{\mathrm{m}} = \sqrt{\tfrac{2(V-1)}{V+1}} X_{\mathrm{A}}^{\mathrm{m}}, \\ P'_{\mathrm{B}_0} &= \frac{\langle P_{\mathrm{B}_0} P_{\mathrm{A}}^{\mathrm{m}} \rangle}{\langle P_{\mathrm{A}}^{\mathrm{m}2} \rangle} P_{\mathrm{A}}^{\mathrm{m}} = -\sqrt{\tfrac{2(V-1)}{V+1}} P_{\mathrm{A}}^{\mathrm{m}}. \end{aligned} \tag{48}$$

From Eq. (48), we have

$$\left\langle {X'_{\mathrm{B}_0}}^2 \right\rangle = \left\langle {P'_{\mathrm{B}_0}}^2 \right\rangle = V_{\mathrm{A}}. \tag{49}$$

The conditional variances can be expressed as

$$V_{X_{\mathrm{B}_0}|X'_{\mathrm{B}_0}} = V_{P_{\mathrm{B}_0}|P'_{\mathrm{B}_0}} = \langle {X_{\mathrm{B}_0}}^2 \rangle - \frac{\langle X_{\mathrm{B}_0} X'_{\mathrm{B}_0} \rangle^2}{\langle {X'_{\mathrm{B}_0}}^2 \rangle} = 1 + \xi_{\mathrm{E}}, \tag{50}$$

$$V_{X_{\mathrm{B}_0}|X_{\mathrm{E}_0}} = V_{P_{\mathrm{B}_0}|P_{\mathrm{E}_0}} = \langle {X_{\mathrm{B}_0}}^2 \rangle - \frac{\langle X_{\mathrm{B}_0} X_{\mathrm{E}_0} \rangle^2}{\langle {X_{\mathrm{E}_0}}^2 \rangle} = V. \tag{51}$$

From Eqs. (48) and (49), mode B_0 is projected onto states with variable mean values of (X'_{B_0},P'_{B_0}) and corresponding variance of V_{A} conditioned on the player's measurement. The uncertainty on the inferred values of mode B_0 for the player (Eq. (50)) coincides with the noisy coherent state in the PM scheme (Eq. (43)). Furthermore, from Eq. (51), the uncertainty on the inferred values of mode B_0 for Eve is identical to that in the PM scheme (Eq. (44)). Therefore, the EB scheme is equivalent to the PM scheme.

DATA AVAILABILITY

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

CODE AVAILABILITY

The underlying code developed for this study is not publicly available but may be made available on reasonable request from the corresponding author.

Received: 26 May 2023; Accepted: 8 September 2023;
Published online: 19 September 2023

REFERENCES

1. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
3. Portmann, C. & Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022).
4. Shamir, A. How to share a secret. *Commun. ACM* **22**, 612–613 (1979).
5. Blakley, G. R. Safeguarding cryptographic keys. *Proc. Natl Comput. Conf.* **48**, 313–317 (1979).
6. Chiou, G.-H. & Chen, W.-T. Secure broadcasting using the secure lock. *IEEE Trans. Softw. Eng.* **15**, 929 (1989).
7. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
8. Bose, S., Vedral, V. & Knight, P. L. Multiparticle generalization of entanglement swapping. *Phys. Rev. A* **57**, 822 (1998).
9. Tittel, W., Zbinden, H. & Gisin, N. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63**, 042301 (2001).
10. Chen, Y.-A. et al. Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.* **95**, 200502 (2005).
11. Gaertner, S., Kurtsiefer, C., Bourennane, M. & Weinfurter, H. Experimental demonstration of four-party quantum secret sharing. *Phys. Rev. Lett.* **98**, 020503 (2007).
12. Bell, B. A. et al. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **5**, 5480 (2014).
13. Lu, H. et al. Secret sharing of a quantum state. *Phys. Rev. Lett.* **117**, 030501 (2016).
14. Schmid, C. et al. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.* **95**, 230505 (2005).
15. Bogdanski, J., Rafiei, N. & Bourennane, M. Experimental quantum secret sharing using telecommunication fiber. *Phys. Rev. A* **78**, 062307 (2008).
16. Ma, H. Q., Wei, K. J. & Yang, J. H. Experimental single qubit quantum secret sharing in a fiber network configuration. *Opt. Lett.* **38**, 4494–4497 (2013).
17. Yu, I.-C., Lin, F.-L. & Huang, C.-Y. Quantum secret sharing with multilevel mutually (un)biased bases. *Phys. Rev. A* **78**, 012344 (2008).
18. Smania, M., Elhassan, A. M., Tavakoli, A. & Bourennane, M. Experimental quantum multiparty communication protocols. *npj Quant. Inf.* **2**, 16010 (2016).
19. Pinnell, J., Nape, I., Oliveira, M., TabeBordbar, N. & Forbes, A. Experimental demonstration of 11-dimensional 10-party quantum secret sharing. *Laser Photon. Rev.* **14**, 2000012 (2020).
20. Fu, Y., Yin, H. L., Chen, T. Y. & Chen, Z. B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 090501 (2015).
21. Lance, A. M., Symul, T., Bowen, W. P., Sanders, B. C. & Lam, P. K. Tripartite quantum state sharing. *Phys. Rev. Lett.* **92**, 177903 (2004).
22. Kogias, I., Xiang, Y., He, Q. & Adesso, G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys. Rev. A* **95**, 012315 (2017).
23. Zhou, Y. et al. Quantum secret sharing among four players using multipartite bound entanglement of an optical field. *Phys. Rev. Lett.* **121**, 150502 (2018).
24. Walk, N. & Eisert, J. Sharing classical secrets with continuous-variable entanglement: composable security and network coding advantage. *PRX Quant.* **2**, 040339 (2021).
25. Grice, W. P. & Qi, B. Quantum secret sharing using weak coherent states. *Phys. Rev. A* **100**, 022339 (2019).
26. Wu, X., Wang, Y. & Huang, D. Passive continuous-variable quantum secret sharing using a thermal source. *Phys. Rev. A* **101**, 022301 (2020).
27. Richter, S. et al. Agile and versatile quantum communication: signatures and secrets. *Phys. Rev. X* **11**, 011038 (2021).
28. Liao, Q. et al. Practical continuous-variable quantum secret sharing using plug-and-play dual-phase modulation. *Opt. Express* **30**, 3876–3892 (2022).
29. Murta, G., Grasselli, F., Kampermann, H. & Bruß, D. Quantum conference key agreement: a review. *Adv. Quant. Technol.* **3**, 2000025 (2020).
30. Chen, K. & Lo, H.-K. Conference key agreement and quantum sharing of classical secrets with noisy GHZ states. *Quant. Inf. Comput.* **7**, 689 (2007).
31. Epping, M., Kampermann, H., macchiavello, C. & Bruß, D. Multi-partite entanglement can speed up quantum key distribution in networks. *New J. Phys.* **19**, 093012 (2017).
32. Hahn, F., de Jong, J. & Pappa, A. Anonymous quantum conference key agreement. *PRX Quant.* **1**, 020325 (2020).
33. Proietti, M. et al. Experimental quantum conference key agreement. *Sci. Adv.* **7**, eabe0395 (2021).
34. Qin, Y. et al. Continuous variable quantum conference network with a Greenberger-Horne-Zeilinger entangled state. *Photon. Res.* **11**, 533–540 (2023).
35. Matsumoto, R. Multiparty quantum-key-distribution protocol without use of entanglement. *Phys. Rev. A* **76**, 062316 (2007).
36. Das, S., Bäuml, S., Winczewski, M. & Horodecki, K. Universal limitations on quantum key distribution over a network. *Phys. Rev. X* **11**, 041016 (2021).
37. Wu, Y. et al. Continuous-variable measurement-device-independent multipartite quantum communication. *Phys. Rev. A* **93**, 022325 (2016).

38. Ottaviani, C., Lupo, C., Laurenza, R. & Pirandola, S. Modular network for high-rate quantum conferencing. *Commun. Phys.* **2**, 118 (2019).
39. Muller, A. et al. "Plug and play" systems for quantum cryptography. *Appl. Phys. Lett.* **70**, 793–795 (1997).
40. Lucamarini, M. et al. Practical security bounds against the trojan-horse attack in quantum key distribution. *Phys. Rev. X* **5**, 031030 (2015).
41. Zhao, S. et al. Phase-matching quantum cryptographic conferencing. *Phys. Rev. Appl.* **14**, 024010 (2020).
42. Shen, Y., Zou, H., Tian, L., Chen, P. & Yuan, J. Experimental study on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A* **82**, 022317 (2010).
43. Jain, N. et al. Practical continuous-variable quantum key distribution with composable security. *Nat. Commun.* **13**, 4740 (2022).
44. Tian, Y. et al. Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. *Optica* **9**, 492–500 (2022).
45. Zhang, M., Huang, P., Wang, P., Wei, S. & Zeng, G. Experimental free-space continuous-variable quantum key distribution with thermal source. *Opt. Lett.* **48**, 1184–1187 (2023).
46. Chen, Z., Wang, X., Yu, S., Li, Z. & Guo, H. Continuous-mode quantum key distribution with digital signal processing. *npj Quant. Inf.* **9**, 28 (2023).
47. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
48. Fossier, S., Diamanti, E., Debuisschert, T., TualleBrouri, R. & Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B* **42**, 114014 (2009).
49. Qi, B., Lougovski, P., Pooser, R., Grice, W. & Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **5**, 041009 (2015).
50. Wang, T., Huang, P., Zhou, Y., Liu, W. & Zeng, G. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator. *Phys. Rev. A* **97**, 012310 (2018).
51. Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photon.* **15**, 530–535 (2021).
52. Zhou, L., Lin, J., Jing, Y. & Yuan, Z. Twin-field quantum key distribution without optical frequency dissemination. *Nat. Commun.* **14**, 928 (2023).
53. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
54. Lin, J., Upadhyaya, T. & Lütkenhaus, N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X* **9**, 041064 (2019).
55. Denys, A., Brown, P. & Leverrier, A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum* **5**, 540 (2021).
56. Pan, Y. et al. Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. *Opt. Lett.* **47**, 3307-3310, (2022).
57. Wang, P., Zhang, Y., Lu, Z., Wang, X. & Li, Y. Discrete-modulation continuous-variable quantum key distribution with a high key rate. *New J. Phys.* **25**, 023019 (2023).
58. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
59. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-feld type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).
60. Wang, S. et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photon.* **16**, 154–161 (2022).
61. Liu, Y. et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.* **130**, 210801 (2023).
62. Li, C., Qian, L. & Lo, H.-K. Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources. *npj Quant. Inf.* **7**, 150 (2021).

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (62175138, 62205188); Shanxi 1331KSC; Innovation Program for Quantum Science and Technology (2021ZD0300703).

AUTHOR CONTRIBUTIONS

Y.L. conceived the research and designed the experiments. S.L. prepared the setup and implemented the experiments. All authors participated in discussions of the results. S.L. and Y.L. prepared the manuscript with assistance from all other co-authors. All authors have given approval for the final version of the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Yongmin Li.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.