nature communications

Article

https://doi.org/10.1038/s41467-025-66333-3

Fully heterogeneous prepare-and-measure quantum network for the next stage of quantum internet

Received: 18 March 2025

Accepted: 5 November 2025

Published online: 12 December 2025

Check for updates

Feng-Yu Lu[1,2,3,4,6], Ze-Hao Wang[1,2,3,6], Yao Zhou[1,2,3,6], Yu-Xuan Fan[1,2,3], Shuang Wang[1,2,3,4] ✉, Zhen-Qiang Yin[1,2,3,4] ✉, Jian Li[5], De-Yong He[1,2,3,4], Fang-Xiang Wang[1,2,3,4], Wei Chen[1,2,3,4], Kaiping Xue[4,5], Guang-Can Guo[1,2,3,4] & Zheng-Fu Han[1,2,3,4]

The quantum internet promises unparalleled capabilities that are provably impossible with the classical internet. However, current quantum networks are often designed with dedicated systems for specified tasks, which hinders the openness and diversity of future quantum internet. To address these limitations, this work proposes a fully heterogeneous quantum network accompanied with several techniques. Our proposal allows users to access the network using any mainstream systems or even partial systems. The network also enables the execution of multiple distinct quantum tasks and provides opportunities for global optimization and cost-efficient design. A five-node quantum network featuring heterogeneous nodes has been implemented, demonstrating the superiority of our proposal through tasks such as quantum key distribution, quantum digital signature, quantum Byzantine agreement, and quantum conference. Notably, the experiment represents the first demonstration of multi-malicious node quantum Byzantine agreement in a quantum network.

Quantum information[1–8] is set to revolutionize information technology, enabling provably impossible capabilities using only classical information. As networking is an inevitable part of the evolution of all information technologies, one important vision for a quantum internet[9–15] is to provide fundamentally new internet technology that facilitates quantum communication (QC)[16–18] between any two points on Earth. However, several developmental stages must be navigated before reaching the quantum internet, each presenting its own set of challenges[11–13,19–21]. As of today, significant progress has been made in the initial stage, known as the trusted repeater network[22–27]. However, this stage cannot provide end-to-end quantum communication services without trusted relays. Efforts are now focused on the next stage, the prepare-and-measure quantum network (P&M-QN)[11], which aims to eliminate the need for a trusted relay[28–32].

Although explorations have greatly promoted the second stage, there are still gaps between the demonstrations and practical applications. According to the vision for a fully realized P&M-QN, it must not only retain the properties and advantages of classical networks but also leverage the unique benefits of quantum information. More precisely, in addition to eliminating the need for trusted repeaters, such a network should support a diverse range of devices and accommodate various applications and services. In contrast, the recent explorations[22–30,32] face several limitations. Users are required to select their devices, prepare states, and process data in strict accordance

[1]Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China. [2]Anhui Province Key Laboratory of Quantum Network, University of Science and Technology of China, Hefei, Anhui 230026, China. [3]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, P. R. China. [4]Hefei National Laboratory, University of Science and Technology of China, Hefei, China. [5]School of Cyber Science and Technology, University of Science and Technology of China, Hefei, Anhui, China. [6]These authors contributed equally: Feng-Yu Lu, Ze-Hao Wang, Yao Zhou. ✉e-mail: wshuang@ustc.edu.cn; yinzq@ustc.edu.cn

with predefined constraints. Moreover, these efforts are typically focused on a single quantum task and often feature fixed, which increases networking costs and hinders scalability.

To realize the vision of a quantum internet, we present a fully heterogeneous network that addresses existing gaps and advances the P&M-QN toward its ultimate form. This heterogeneity is reflected in several key aspects. First, the degrees of freedom (DoF) are heterogeneous. Our presented DoF converter can adapt to nodes with different DoFs, thereby enabling them to access the network with any mainstream modulation schemes, such as polarization (Pol.), time-bin-phase (T.B.P.), or phase (Pha.). Second, the setups are heterogeneous. Our networking allows users to access the network with non-paired and incompatible setups and realize full connection without any trusted nodes. Finally, the execution of protocols and tasks are heterogeneous, allowing users to conduct on-demand switching among various quantum protocols[1,33–45] and quantum tasks[33,46,47], such as quantum key distribution (QKD)[1,16], quantum digital signature (QDS)[47–50], quantum Byzantine agreement (QBA)[51–54], and quantum conference[55,56]. Our network supports centralized control functions by proposing a software-defined prepare-and-measure network (SD-P&M-QN) architecture[57,57–59] and provides task selection, protocol selection, and parameter optimization via proposing a dedicated "orchestration core" in the architecture. The server can coordinate nodes with different setup types and DoFs, thereby enabling quantum communication between originally incompatible nodes. Furthermore, the server's global network view provides opportunities for integrating valuable quantum resources and optimizing the overall network performance, and brings potential advantages of flexibility, agility[33], optimization, and cost-effectiveness.

Based on the above proposal, we built a five-node heterogeneous network, which consists of a detection node and four source nodes. The detection node holds a typical Pol. measurement unit[39,40,60], and the source nodes each possess one of the common modulation systems, including Pol., T.B.P., and Pha. With this heterogeneous network, we successfully demonstrate multi-protocol switching, multi-DoF switching, and multi-task switching. Four different quantum tasks including QKD, QDS, QBA, and quantum conference, and two different protocols including BB84 and measurement-device-independent (MDI) is demonstrated among the five heterogeneous nodes. In particular, we demonstrate product traceability by our five-node QBA with two malicious nodes. This is also the first multi-malicious-nodes QBA experiment. Our heterogeneous network lays out a blueprint for the final form of the P&M-QN. Similarly, just like the first message was sent over a simple four-node network (Advanced Research Projects Agency Network) in 1969, our experiment outlines the technical process for completing the blueprint.

Results

Fully heterogeneous networking

In previous quantum networks, network nodes are typically required to hold both of transmitter and a detector with strictly limited DoF. In contrast, our network releases the requirement. The nodes only possess one of the transmission or detection. As the mainstream QC systems can be separated into weak coherent transmitter, entanglement transmitter, and single-photon detector, nodes in our network can also be divided into three fundamental types: nodes with weak coherent sources (C-type nodes), with entanglement sources (E-type nodes), and with single-photon detectors (D-type nodes). C and E-type nodes can also be referred to as source-type (S-type) collectively. As listed in Table 1, any two nodes can achieve end-to-end communication by properly selecting their protocol. For instance, a S-type node can share secret keys with a D-type node by P&M-type protocol[1,35–38]; two C-type nodes can communicate by executing the MDI-type protocol[40–42] with the assistance of D-type nodes; similarly, two D-type nodes can share secret keys by performing the entanglement-based protocols[44,45] with the assistance of E-type nodes (for entanglement distribution), the nodes can also freely select any mainstream DoF to encode their information. Two nodes with different DoFs can perform the quantum tasks by utilizing our DoF converter, which ensures precise and high-fidelity conversion of their DoF to Pol., T.B.P., or Pha.

User nodes with different fundamental types and different DoFs access the network through the topology as shown in Fig. 1. Compared with the previous networks[22–32], our network does not require full connection or centralization. User nodes with the same type do not need to be interconnected. The server consists of distributed infrastructure devices and a centralized controller. As a P&M quantum network, the server is considered as part of the channel and therefore do not introduce any additional security assumptions. The server performs path planning and node scheduling based on communication requests and optimal parameters[61–64]. Except for the direct link between S-type and D-type nodes, the server can also provide or borrow E-type or D-type nodes for entanglement distribution or Bell-state measurement (BSM) to assist the EB protocols and MDI-type protocols. These untrusted E-type and D-type nodes can belong to server or inactive user nodes. Especially, some of the D-type nodes cannot perform the BSMs independently. Thus, we propose a joint-BSM to schedule several D-type nodes to complete the BSM collaboratively (see "METHOD" for details). Notably, the BSM serves as part of the MDI-QKD protocol.

With the above schemes and designs, we have realized the hardware heterogeneity, enabling more flexible configurations, broader coverage, and lower costs. However, hardware heterogeneity alone is insufficient to classify our network as fully heterogeneous. To address this, we introduce an SD-P&M-QN architecture to enable software heterogeneity, ensuring both agility and versatility,[33,46], which are also fundamental requirements for the classical internet. Agility[33,34] refers to the resource-efficient replacement of a cryptographic core when security is compromised, while versatility allows nodes to switch tasks without requiring any knowledge of the underlying implementation details[33]. Our SD-P&M-QN architecture effectively guarantees these properties by providing a universal platform for real-time information collection and heterogeneous quantum task support. In addition, it incorporates a three-layer architecture with a centralized controller to facilitate quantum protocol switching and global optimization (see "METHOD" for details).

To summarize, our fully heterogeneous networking enables the integration of diverse setups and DoFs, enhancing flexibility, scalability, and performance. At the same time, it supports a variety of quantum tasks and protocols, ensuring agility and versatility. Given the critical role of heterogeneity in the classical Internet, our work is poised to advance the quantum Internet toward the next stage, i.e., the realization of a P&M-QN.

Experimental setup

To demonstrate the superiority of fully heterogeneous networking, we established a five-node quantum communication network, which included one D-type (David) node and four C-type nodes (Alice, Bob, Charlie, Frank). The authentication between the five nodes is realized by the pre-shared secret keys[65]. The four C-type nodes held different modulation systems and encoded quantum states in different DoFs. With the experimental network, we successfully realized the end-to-end quantum tasks among the five heterogeneous nodes without any trusted repeater. We also demonstrated how the DoF converter and orchestration core transferred DoFs, switched quantum protocols, switched quantum tasks, and optimized parameters according to the node type, requirement, hardware, and network resources. Especially, we successfully realized a five-node QBA with two malicious nodes, which is also the first multiple malicious-node QBA experiment in the world.

As illustrated in Fig. 2, each of the four C-type nodes are abstracted to several modules. The coherent pulses were initially generated by the pulse module, which consisted of a CW laser (Wavelength References Clarity-NLL-1542-HP), a $LiNbO_3$-based phase modulator (PM), and two $LiNbO_3$-based intensity modulators (IMs). The CW laser, which was frequency-locked to a molecular absorption line at a center wavelength of 1542.8 nm with an accuracy of approximately 10 MHz in the spectral domain, serves as the source. The first IM functioned as a chopper, converting the CW laser into a pulse train with a 200 ps pulse width and 1 GHz repetition rate. The subsequent PM randomized the pulse phase to ensure security. Finally, the second IM applied random modulation to generate several pre-decided intensities for the decoy-state method[66–68]. The modulators were driven by our electronic system, which consists of AWGs, homemade circuits, and RF-amplifiers.

Following the pulse module, the pulse train was fed into the encoding module to encode the quantum states. The main differences lay within this module. Alice employed Pol. modulation[60,69]. She first adjusted the Pol. of her pulses to a diagonal Pol. and then fed them into a Sagnac structure via a Pol. beam splitter (PBS). The horizontal and vertical components were split into clockwise and counterclockwise pulses, respectively, in the Sagnac ring and then sequentially propagated through the PM. As a result, the PM independently modulated the pulses and controlled the relative phase between the horizontal and vertical components. Frank held a phase modulation system[31]. He first split one pulse to the superposition of early and late T.B.P. state via an asymmetric Mach-Zehnder interferometer (AMZI) that consisted of two paths with a 500 ps optical path difference. Then, a PM was driven in 2 GHz frequency to modulate the phase difference between the two T.B.P. states. Both Bob and Charlie employed the T.B.P. encoding, but their realizations were different. Bob generated the T.B.P. superposition with an AMZI (500 ps optical path difference) and driven a PM in 2 GHz frequency to modulate the phase difference between the two T.B.P. states. An additional IM was added to eliminate the early-bin or late-bin pulses, thereby modulating the two T.B.P. eigenstates, or to halve the intensity, thereby modulating the superpositions. Different from Bob, Charlie fed his pulses to a Faraday-Michelson interferometer (FMI)[70] with also a 500 ps optical path difference to split them to the two time-bins and then drove an IM and a PM to modulate the T.B.P. states.

After that, an adapter module consists of our DoF converter and supporting components was employed, allowing nodes to select a path to maintain or transfer their DoF according to circumstances. The selection was realized by a pair of 2 × 1 optical switches (OS). The nodes directed the pulses to pass through a fiber channel to maintain their DoF, or switched the OS to feed the pulses to the DoF converter to transfer the DoF. In this experiment, a passive structure (see "METHOD" for an active structure) was employed for the DoF converter. It has a Pol. port and a T.B.P. port. Alice fed her Pol. state $a|H\rangle + be^{i\theta}|V\rangle$ to the module from the Pol. port, the $|H\rangle$ and $|V\rangle$ components were split into two different paths by a PBS, passed through different delay, and then converged in a coupler to be transferred to the T.B.P. state $a|e\rangle + be^{i\theta}|l\rangle$ and left the module from the T.B.P. port. Conversely, Bob, Charlie, and Frank fed their T.B.P. or Pha. states to the module from the T.B.P. port, split to the two paths by the BS (reverse of the coupler), pass through different delay, and then converge in the PBS to be transferred to the Pol. state $a|H\rangle + be^{i\theta}|V\rangle$. An IM following the module was employed to eliminate the excess pulses. Finally, the nodes attenuated their pulse to an optimized mean photon number by their electric variable optical attenuator (EVOA) and sent them to the

Table 1 | Protocol selections for different node types

node type	C-type node	E-type node	D-type node
C-type node	MDI-type[1]	MDI-type[2]	P&M-type[3]
E-type node	MDI-type[2]	MDI-type[4]	P&M-type[5]
D-type node	P&M-type[3]	P&M-type[5]	EB-type[6]

[1]MDI-type protocols with weak coherent transmitter[69,73,96].
[2]MDI-type protocols with hybired sources[97].
[3]The most mature P&M protocols, including decoy-state based BB84[1], RFI[35], and LT[37], et al.
[4]MDI type protocols with heralded single-photon source and passive decoy-state method[98,99].
[5]P&M protocols with heralded single-photon source and passive decoy-state method[100,101].
[6]Entanglement-based protocols, such as E91[44]and BBM92[45]protocols.

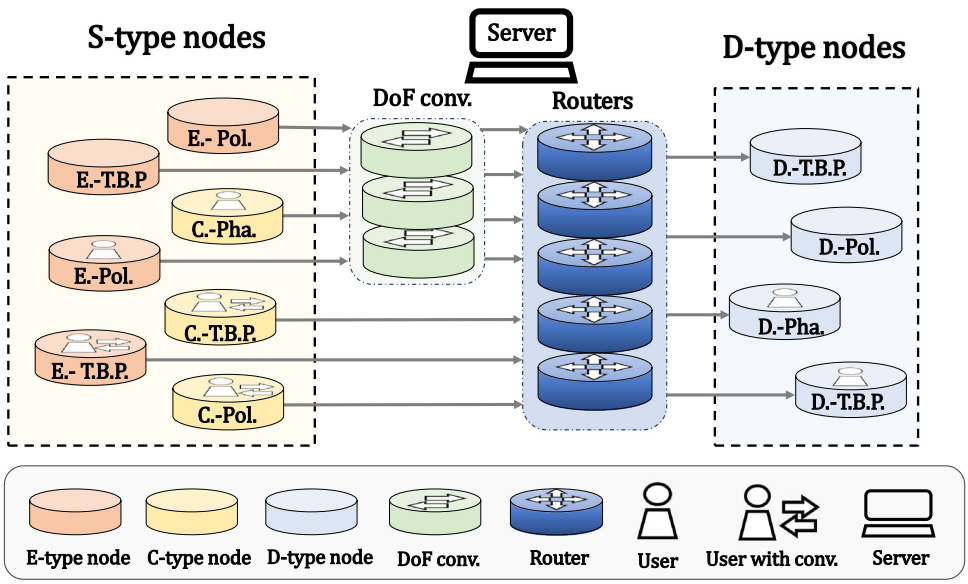


Fig. 1 | The topology of our fully heterogeneous network. Orange, yellow, and light blue cylinders: E, C, and D-type nodes; green cylinders: DoF converters; deep blue cylinders: router; gray arrows: the flow of quantum signals. Text on nodes represents their type and DoF. Only cylinders with a user icon represent user nodes. This indicates that some D-type and E-type nodes belong to the server and can be employed as untrusted relays. A cylinder with a DoF converter icon means the node has its own DoF converters. The quantum router consists of optical switches, splitters, couplers, wavelength division multiplexers, and other components.

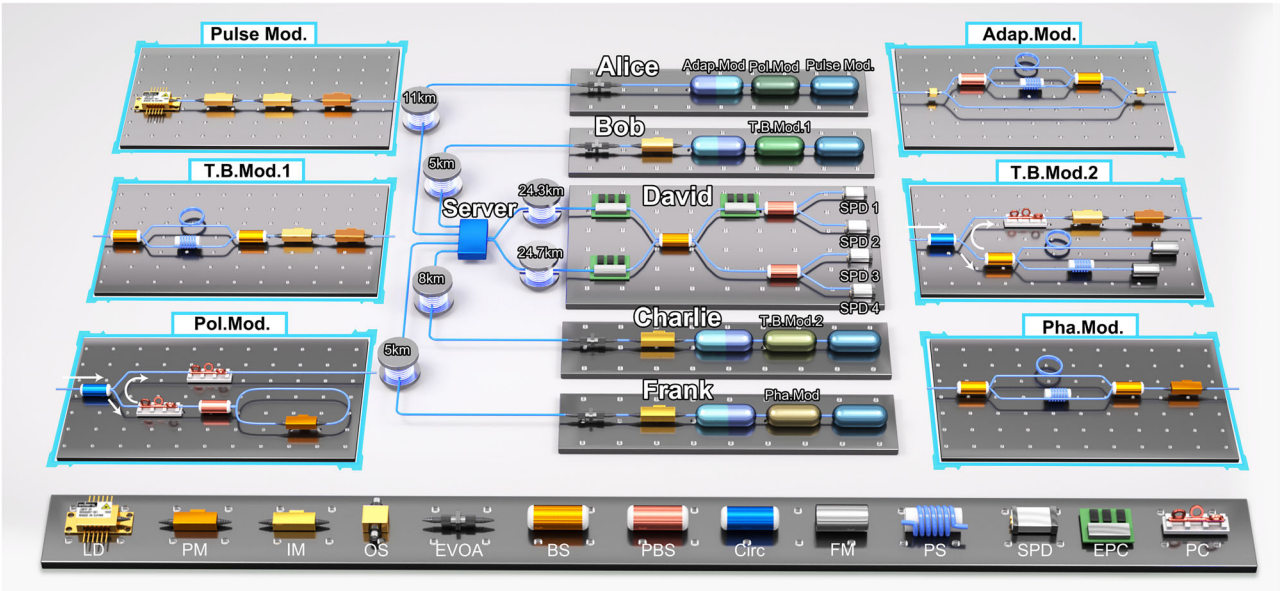


Fig. 2 | Experimental setup of our heterogeneous quantum network. LD laser diode, PM phase modulator, IM intensity modulator, OS optical switch EVOA electric variable optical attenuator, BS beam splitter, PBS polarization beam splitter, Circ circulator, FM Faraday mirror, PS phase shifter, SPD single-photon detector, EPC electric polarization controller, PC polarization controller, Mod module. Server: the server consists of the manual fiber-link switching and control programs in this experiment, Adap.Mod Adapting module, consisting of the DoF converter and supporting components.

channel. We emphasize the DoF converter can be employed by the server or nodes. In our experiment, the passive DoF converter has at least 3 dB loss, so we set them at C-type nodes for compensating the loss.

The D-type node David held a typical passive Pol. decoding system[60]. The four homemade InGaAS-based SPDs[71] worked at 1 GHz gated mode and fine-tuned to a 20% detection efficiency and a 10^{-6} level dark count rate. When David communicated with other nodes, they performed a P&M protocol. The other four nodes prepared or transferred their states on the Pol. DoF and sent them to David by the quantum channel. David used 50:50 BS and adjusted the two EPCs to realized a balanced basis selection. The four homemade SPDs were employed to measure the $|H\rangle$, $|V\rangle$, $\sqrt{2}(|H\rangle+|V\rangle)/2$, $\sqrt{2}(|H\rangle-|V\rangle)/2$, respectively. Besides, we indicate that David can also perform the BSM by adjusting the EPC and SPD delay. When the two C-type nodes wanted to establish an end-to-end communication, the server invoked David as an untrusted measurement relay. The two nodes first transferred their states to the same DoF and sent them to David for performing the MDI protocol. In our experiment, Bob-Charlie performed a T.B.P.-based MDI protocol directly. Other pairs performed a Pol.-based MDI protocol. When David assists the T.B.P.-based MDI protocol, he adjusted the delay of SPD1 and SPD3 to detect the early and late bin, respectively, while employing the other two SPDs to assist the Pol. calibration[72]. When Bob assists the Pol. based protocol, he adjusted his EPCs to perform a standard Pol. BSM[40,69,73], in which SPD1, SPD3 detected the $|H\rangle$ component, and SPD2, SPD4 detected the $|V\rangle$ component. David publicly announced his measurement results[40] and the two C-type nodes generated their raw bits according to the announcement.

Alice, Bob, Charlie, Frank, and David were connected to the server with fiber spools of 5, 11, 5, 8, and 25 km, respectively. In our control program, six different C++ classes are constructed — five for individually controlling each node and one for the server. In our experiment, a single process instantiates the six C++ classes, spawning six threads. Five threads emulate user nodes and one thread emulates the server, thereby simulating the distributed network architecture. Based on the requirements and terminal information, the orchestration core selects an appropriate quantum task and protocol according to a predefined rule. The server routed the quantum channel (Micro-electro-mechanical systems can programmatically route the quantum channel. In this setup, we manually switch the node links, which does not affect our conclusions) and informed the nodes of the channel parameters. According to the parameters of terminals and channel, the orchestration core loaded optimized parameters[63,74] (including decoy-state intensities and selection probabilities) from a pre-established optimal-parameter table. After that, the nodes and the server calibrated the phase references, Pol., mean-photon number, and time delay by adjusting their phase shifter (PSs), EPC, EVOA, and circuits. The communication generates secret keys between the two end-to-end nodes, some of the keys could be consumed by the current task, and the remained keys are saved in their pre-established key pools[75] for further applications.

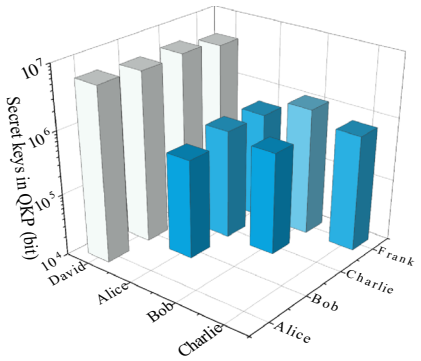
Experimental results

QKD. QKD is one of the most successful and foundational applications of quantum technology, making it the natural choice for our first demonstration. Here, we demonstrated all possible combinations of end-to-end QKD among the five nodes. Following the aforementioned process, the nodes and server exchanged terminal information, established the quantum channel, selected the protocol, loaded optimal parameters, and calibrated their systems with the assistance of the orchestration core in the SD-P&M-QN architecture. The experimental results are summarized in Fig. 3.

In accordance with the pre-defined rules in Table 1, the orchestration core selected the BB84-QKD protocol for D-C-type combinations, including Alice-David, Bob-David, Charlie-David, and Frank-David. Since David held a passive Pol. decoder, the other transmitters (except Alice) must convert their DoF to Pol. using the DoF converter before sending their pulses to David. Each pair executed QKD for 2 seconds (2×10^9 rounds) to generate enough raw key bits, mitigating the finite-key-size effect[63]. The sifted key bits were processed by cascade error correction[76] and privacy amplification[77], resulting in about 5.90×10^6, 5.38×10^6, 5.64×10^6, and 4.50×10^6 secret key bits stored in each QKP.

For C-C-type combinations, the orchestration core selected the MDI-QKD protocol, with the server designated David as the untrusted

https://doi.org/10.1038/s41467-025-66333-3



(a) Secret key length of each QKP

User pair	protocol	DoF	T (s)	L (km)	f	l_{sift} (bit)	e_b	l_{sec} (bit)
D-A	BB84	Pol.	2	35.3	1.138	16387303	0.0088	5895618
D-B	BB84	T.B.P.	2	29.3	1.138	14605700	0.0092	5382766
D-C	BB84	T.B.P.	2	32.7	1.138	16516150	0.0087	5646444
D-F	BB84	Pha.	2	29.7	1.133	12731587	0.0105	4500523
A-B	MDI	Pol. - T.B.P.	1000	64.6	1.179	25507836	0.0341	394595
A-C	MDI	Pol. - T.B.P.	1000	68.0	1.182	18425794	0.0334	566247
A-F	MDI	Pol. - Pha.	1000	65.0	1.172	20951678	0.0298	545926
B-C	MDI	T.B.P. - T.B.P.	1000	62.0	1.153	6450466	0.0162	449431
B-F	MDI	T.B.P. - Pha.	1000	59.0	1.150	27758108	0.0242	1112747
C-F	MDI	T.B.P. - Pha.	1000	62.4	1.152	24996302	0.025	729713

(b) QKD results of each user pair

Fig. 3 | QKD experiment results of each node pair. a 3D bar chart to show the secret key length of each node pair. The *x* and *y*-axis represent the two nodes. The *z*-axis denotes the secret key length. **b** Important experimental parameters and results of each node pair. A: Alice; B: Bob; C: Charlie; D: David; F: Frank; T: time for raw key accumulation; L: fiber length between the two nodes; f: error correction efficiency; l_{sift}: sifted key length; e_b: bit error rate; l_{sec}: secret key length.

measurement unit to assist communication. For the Alice-Bob, Alice-Charlie, and Alice-Frank pairs, the orchestration core opted for Pol. based MDI-QKD. Bob, Charlie, and Frank converted their DoF to Pol. using their DoF converters. For the Bob-Frank and Charlie-Frank pairs, both nodes transferred their DoF to Pol. via their DoF converters. David adjusted his EPCs to compensate for channel disturbances and performed a Pol.-based BSM. For the Bob-Charlie pair, since both of them utilized the T.B.P. encoder, their orchestration cores directly prepared T.B.P. states, which were sent to David for a T.B.P.-based BSM. David adjusted the gated times of SPD1 and SPD3 to detect early and late time bins, respectively, and optimized his EPCs to achieve high Hong-Ou-Mandel (HOM) visibility. Each C-C-type pair executed QKD for 1000 seconds (10^{12} rounds) to counteract the finite-key-size effect. They also processed their raw key bits by the aforementioned error correction and privacy amplification, resulting in 3.94×10^5, 5.66×10^5, 5.46×10^5, 1.11×10^6, 7.30×10^5, and 4.49×10^5 secret key bits stored in the respective QKPs.

QDS. QDS is another important quantum task that ensures integrity, authenticity, and non-repudiation. By leveraging the key resources generated through quantum processes such as QKD and integrating one-time universal hashing and one-time pad operations, QDS extends the computational security of classical digital signatures to information-theoretic security in a three-party quantum scenario. We took two quantum e-commerce processes[78,79] in our heterogeneous network to demonstrate the QDS. In the two demonstrations, Alice was a client who wants to online purchase some products from merchants David and Charlie, respectively.

The first demonstration was the trading between Alice and David. They first randomly designated a node from the network as a third party (TP) to assist the QDS. Without loss of generality, we designated Bob as the TP in the experiment. The Merchant David built two quantum channels with the client Alice and the TP Bob. Then their operation systems invoked the hardware to randomly modulate four Pol. based BB84-states and three optimized intensities[63] for distributing non-secret but error-corrected keys (we name them imperfect keys for simplicity). Here, Alice (Bob) and David kept the communication for 2 s and generated raw key bits with an error rate of 1.05% (0.89%). 1.276×10^7 (1.641×10^7) bits of error-corrected keys was generated by the cascade error correction algorithm[76]. The privacy amplification was executed here thus the keys were imperfect.

David prepared a 43 KB contract file C_D and selected two 900-bit imperfect quantum key strings X_A and Y_A (X_B and Y_B) from the error-corrected keys with Alice (Bob). Then he randomly generated an irreducible polynomial and performs the division hashing[80] on the contract C_D to get the hash value. By utilizing the combined key strings $X_D = X_A \oplus X_B$ and $Y_D = Y_A \oplus Y_B$ to perform the one-time pad operation on the coefficient of the polynomial and the hash value, the signature S_D of C_D was obtained. The contract and its signature were first sent to Alice. Alice checked the contract, then transfers C_D, S_D, and her corresponding imperfect key X_A and Y_A to Bob (if she accepted the contract). Bob checked the contract and sent his key strings X_B and Y_B to Alice. Both Alice and Bob independently verified the signature of the contract. Alice paid the money if both of their verification were passed. In our experiment, this group passed the verification after consuming 1800 bit keys. The maximum key generation (ignore the time of data process) and imperfect key consumption of David-Alice (David-Bob) were 6382375 bit/s and 1800 bit/times (8205939 bit/s and 1800 bit/times). The signature rate depends on the keys of a lower key rate, thus, they achieved a signature rate of 3545 times/s (David-Alice has a lower key rate).

In another trade between Alice and Charlie, another QDS protocol were selected. In this protocol, the perfect secret keys were required, thus, they randomly designated a TP (in this experiment, Frank was designated) and then took 53 bit secret key strings X_A and Y_A, X_F and Y_F from the QKP of Alice-Charlie, Frank-Charlie, respectively. Then they used the perfect secret keys to repeat the procedure of signature, transference, and verification similarly to the previous group. This group finally passed the verification after consuming 106 bit keys. The filling rates of the two QKPs were 566.247 bit/s and 729.713 bit/s, respectively, with secret key consumption of 106 bits per transaction. The signature rate depends on the keys of Alice-Charlie, thus achieved a signature rate of 5.34 times/s. The experimental results are shown in Fig. 4.

QBA. Byzantine agreement aims to enable all nodes in a decentralized network to reach consensus, and it plays a crucial role in applications such as distributed ledger, blockchain, and quality traceability. Compared to classical Byzantine agreement (CBA), QBA[53,54] offers unconditional security and surpasses the 1/3 fault-tolerance bound of CBA, thanks to the multiparty correlations provided by QDS. The general protocol steps of the QBA protocol for arbitrary N network nodes, as well as its communication complexity, consensus rate, and rigorous security proofs, can be found in ref. 53. In this demonstration, we present the distributed ledger based on the recently proposed QBA protocol[53], illustrating how users in our network reach consensus on a trading transaction. The trade is recorded by all nodes in the network through QBA, and all honest nodes will reach the same consensus. This consensus can only be disrupted if malicious nodes exceed 1/2 of the network, thereby surpassing the 1/3 fault-tolerance bound of CBA. This is also the first complete QBA experiment to showcase quantum superiority in the presence of multiple malicious nodes.

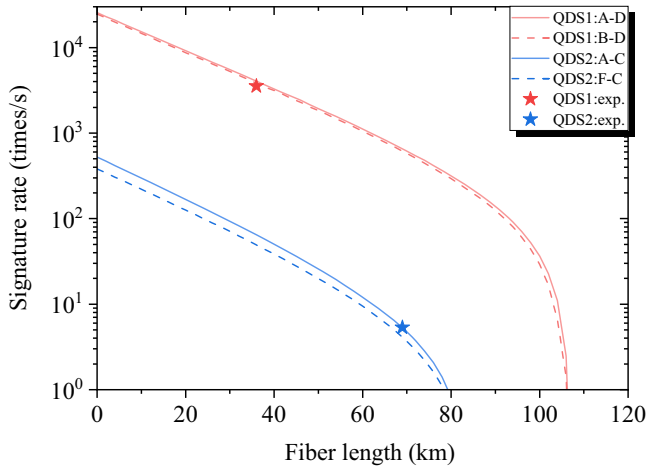


Fig. 4 | The QDS experiment result. The blue and red curves represent the simulated signature rate versus fiber length of the first QDS (with imperfect keys) and the second QDS (with secret keys), respectively. Since the QDS refers to two pairs of keys, the signature rate depends on the keys of a lower key rate. The red solid (dash) line represents the case that A-D (B-D) has a lower key rate. The blue solid (dash) line represents A-C (F-C) has a lower key rate. The red and blue stars denote the first and second QDS experiment results, corresponding to the key rates of A-D and A-C, respectively.

In this demonstration, we presented two trading transactions in the network. In the first case, Alice, as an honest signer, attempted to record a 0.1 MB trading file, while Charlie and Frank, as malicious nodes, attempted to disrupt the recording process. In the second case, Alice was a malicious signer who wants to cheat other nodes, with Bob as her collaborator. The QBA protocol operates based on the recursion of multicast rounds and QDS. In each multicast round, there was a primary node, and the others acted as backups. The primary sent the file and its signature to the backups, one of which was chosen as the forwarder, while the others became verifiers. The primary, forwarder and one verifier performed a three-party QDS to transmitted the message. The signing was successful only if both the forwarder and verifier accepted the signature. This process repeated until all backups had served as forwarders. Ultimately, there ware 5 broadcasting rounds of the two demonstrations respectively, including 72 round QDS in total, and the consumption of the secure keys in the QKP was shown in Fig. 5.

Quantum conference. Quantum conference is a quantum task for establishing a common secret key with unconditional security between multi-parties. Notably, here we realize the quantum conference by the QKD-based key delivery[55,56] rather than the multiparty agreement[43,81–86], as this approach offers simpler implementation, higher efficiency, and better compatibility with our network architecture while maintaining information-theoretic security. In our demonstration, David is the sponsor of the meeting. He first generates a quantum random number series by his local quantum random number. Then he independently distributes equal-length symmetric secret keys with all other participants by QKD, encrypts the quantum random number by one-time-pad with the secret keys, and sends it to the corresponding participant by public channel. The participant decrypts the ciphertext using the secret keys to obtain the quantum random number, which is exploited as the conference keys.

In this experiment, David generated 10 Kbit quantum random numbers by our quantum random number generator (QRNG)[87] with a 1.34 Mbps random number generation rate. Then he extracted 10 Kbit secret keys from each of his four QKPs, encrypted the random number separately with each key, and sent them to the corresponding nodes. Alice, Bob, Charlie, and Frank decrypted the ciphertext with their own secret keys and obtained the 10 Kbit quantum random number as the secret conference keys.

Discussion

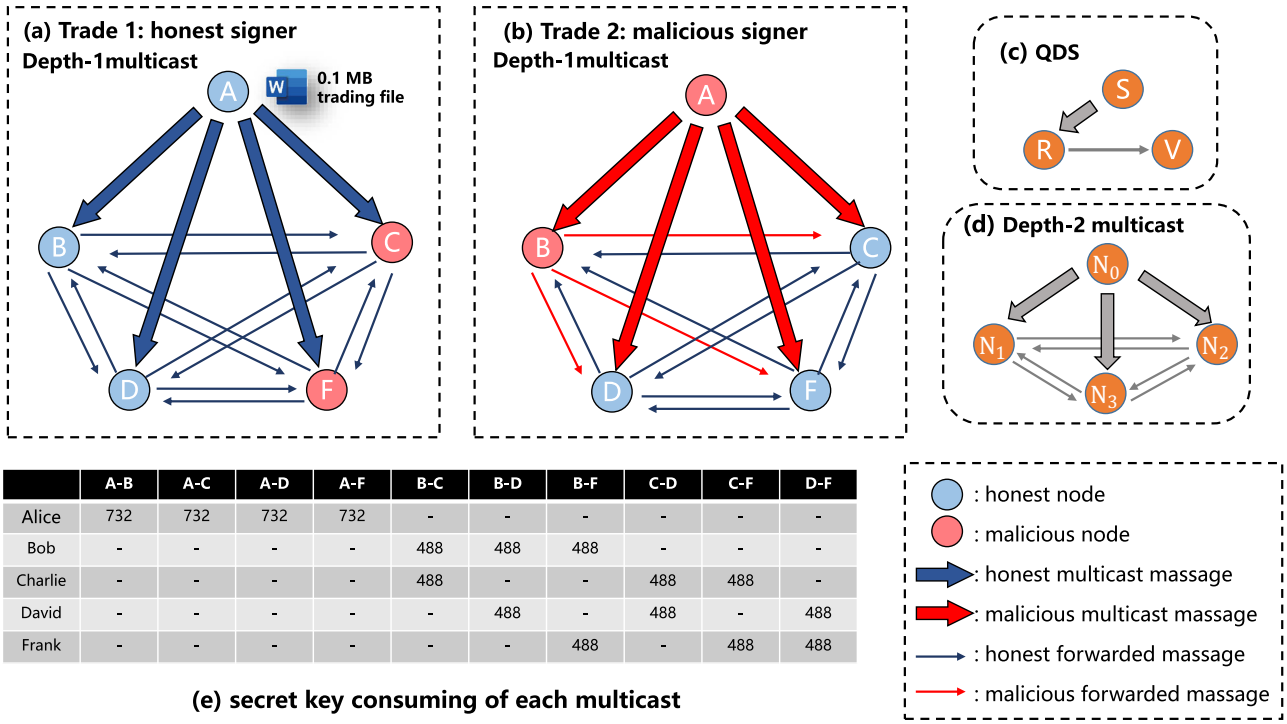
In this work, we proposed a fully heterogeneous network, accompanied by several key techniques to promote quantum internet to its next stage. The "heterogeneity" is reflected at both the hardware and software levels. At the hardware level, users can access the network with any mainstream devices and DoFs. At the software level, the network supports a variety of quantum tasks and protocols. We introduced two key techniques- the "DoF converter" and "joint BSM" - which are experimentally demonstrated to achieve heterogeneity with improved efficiency and performance. In addition, we designed an SD-P&M-QN architecture for the heterogeneous network. The SD-P&M-QN architecture enables nodes to distribute quantum keys without relying on trusted nodes, while the "orchestration core" in the control layer collects device, channel, and network information to select the appropriate tasks, protocols, and optimized parameters, enhancing the agility and versatility of the network.

To validate the advantages of our network, we established an experimental network with five heterogeneous user nodes for demonstrating various quantum tasks and protocols. Using BB84 and MDI protocols, we successfully distributed quantum keys between each pair of heterogeneous nodes. Our DoF converter and joint BSM were shown to effectively adapt the DoF and assist in the MDI protocol. We then demonstrated two QDS protocols for an e-commerce scenario, followed by two QBA experiments showcasing a distributed ledger with quantum advantages. Notably, the QBA experiment is the first complete QBA with multiple malicious nodes. Finally, we demonstrated a quantum conference experiment, successfully distributing conference keys among the five nodes using our QRNG and pre-distributed quantum keys. The heterogeneous network is a critical piece of a fully functional quantum internet, one that is sure to generate widespread interest.

The features of our network provide some potential superiorities such as flexibility, agility, optimization, and cost-effectiveness. The flexibility means the network can dynamically adapt its resource allocation through programmable control interfaces, and the multi-protocol support allows nodes to switch optimal protocols according to the channel condition. Besides, as discussed in ref. 33, quantum devices capable of executing multiple protocols and tasks can switch to avoid potential attacks for improving the implementation security. Our network is also multiple protocols and tasks supported so it also has opportunity to be agility. In addition, the network performance could be optimized since the global network view of the centralized control architecture allows the server to set its network performance optimizing target and globally allocate the network resources. Finally, the network could be cost-efficient since the heterogeneous structure allows for the integration of existing quantum communication networks and the upgrade of existing single-function trusted-node quantum networks to versatile prepare-and-measure quantum networks without requiring large-scale replacement of encoding and decoding equipment. These potential superiorities further indicate the network's promising prospects.

Except for the demonstrated tasks, it is worth noting that, with appropriate extensions, our network architecture holds potential for implementing other fundamental quantum communication protocols, such as twin-field QKD[88], quantum teleportation[89,90], and quantum secure direct communication (QSDC)[91,92]. While these protocols are not realized in the present work, their future integration would further enrich the capabilities of our system and expand its applicability to a broader class of quantum network applications[93]. Furthermore, although quantum repeaters are currently unsupported at the P&M quantum network stage, once quantum repeater technology matures,

https://doi.org/10.1038/s41467-025-66333-3



	A-B	A-C	A-D	A-F	B-C	B-D	B-F	C-D	C-F	D-F
Alice	732	732	732	732	-	-	-	-	-	-
Bob	-	-	-	-	488	488	488	-	-	-
Charlie	-	-	-	-	488	-	-	488	488	-
David	-	-	-	-	-	488	-	488	-	488
Frank	-	-	-	-	-	-	488	-	488	488

(e) secret key consuming of each multicast

Fig. 5 | The QBA experiment diagram. The blue and red colors emphasize honesty and maliciousness, respectively. The circles represent the user nodes. The thick arrows and thin arrows denote the multicast messages and forward messages, respectively. The depth of the five-node QBA is two. Sub-figure (**a**) and (**b**) represent the depth-1 multicast in the two trades, respectively. **a** depth-1 multicast of the trade one (honest signer). **b** depth-1 multicast of the trade two (malicious signer). **c** QDS as the basic unit of a QBA experiment. **d** depth-2 multicast among the remaining four nodes. There are four multicast rounds in depth-2. We define the four nodes as N_i ($i = 0, 1, 2, 3$). N_0 is the primary node and N_0 = B, C, D, F in the four multicast rounds, respectively. N_1 to N_2 are remained three nodes in each multicast round. **e** consumption of each QKP in each multicast round (unit: bit). The columns of the table indicate the multicast corresponding to the primary node, and the rows indicate the corresponding QKP.

it can be seamlessly integrated into our architecture, thereby advancing the system to its next developmental stage.

Four different quantum tasks, QKD, QDS, QBA, and quantum conference, are demonstrated in our network. The realization of these four tasks is interdependent to some extent, demonstrating our principle of network resource multiplexing. For instance, QKD enables two communicating parties to share a secret key string with information-theoretic security. QDS and QBA utilize such secure key resources to achieve information-theoretic security. Although QDS and QBA can theoretically be implemented using alternative quantum resources, using the QKD-based key implementation in our network remains the most cost-effective and efficient approach. In addition, QDS enables the construction of an asymmetric multiparty relationship among three participants, where the roles of the forwarder and the verifier are symmetric and do not rely on a trusted third party. Building upon QDS as the fundamental primitive, the QBA protocol employs multi-round broadcasting and a recursive loop structure. Based on a binary tree model, QBA can rigorously prove the existence of a secure path, thereby achieving information-theoretic security while also surpassing the classical 1/3 fault-tolerance bound for Byzantine consensus. Similarly, we realize the quantum conference by the QKD-based key delivery[55,56] rather than the multiparty agreement[43,81–86], as this multiplexing can maximize the resource utilization rate.

The scaling issue is also important for the network upgrade. A feasible approach to scale our network to large-scale deployments involves organizing nearby nodes within the same local area into local-area quantum networks (LAQNs), which are then interconnected to form a wide-area quantum network (WAQN). In addition, the authentication in our experiment is realized by pre-shared secret keys. It may not be convenient for large-scale networks. A possible countermeasure is employing a hybrid quantum-classical authentication scheme. More details about the scaling issue are introduced in the Supplementary Material.

Notably, to distinguish from our previous network experiment, we emphasize that ref. 32 is a homogeneous network in which all users must equip the same equipment and follow the same protocols. Its main purpose is to realize a robust and non-blocking network without the trusted relay assumption.

Methods

DoF converter for heterogeneous networking

Our heterogeneous structure allows users to access the network with different DoFs, which greatly expands the application scenarios and reduces usage costs. To enable quantum communication between the nodes with different DoFs, we designed a methodology for transforming the DoFs with high fidelity.

The DoF converter consists of a Pol. path conversion module and a path-time converter. A node can translate its Pol. states to T.B.P. or Pha. states by first sending their Pol. signals into different paths via the Pol.-path converter, and then utilizing the path-time converter to convert different paths into different time bins. In this process, the two orthogonal Pol., without loss of generality, horizontal and vertical, are translated to early and late time bins, with their relative phase converted to the relative phase between the time bins. Similarly, a node can convert T.B.P. or Pha. information back to Pol. by reversing this process. The two time-bins and their relative phase are then converted to the two Pol. and their relative phase (see Supplementary Material for the detailed physical model with practical imperfections and different physical realizations).

In our experiment, the DoF converter is physically realized via a passive structure. When a node wants to transfer T.B.P. or Pha. DoF to Pol. DoF, the superposition $a|e\rangle + b|l\rangle$ (b is a complex number) is fed to

the DoF converter from the time-bin port. Then the state is transferred to a path superposition. As an additional delay that equals the time difference of the two time bins is added to the up-path, the superposition is represented as $\frac{\sqrt{2}}{2}(a|u\rangle + b|d\rangle) + \frac{\sqrt{2}}{2}|\varnothing\rangle$, where $|u\rangle$ and $|d\rangle$ represent the up and the down-paths respectively, $|\varnothing\rangle$ represents the discarded state. After that, the polarization beam splitter transfers the path DoF to the Pol. DoF as $\frac{\sqrt{2}}{2}(a|H\rangle + b|V\rangle) + \frac{\sqrt{2}}{2}|\varnothing\rangle$. The $|\varnothing\rangle$ is discarded so the final output state is $a|H\rangle + b|V\rangle$ (We emphasize that since all channel operations are security-preserving, if DoF conversion is performed via the server or other nodes, $|\varnothing\rangle$ should be regarded as loss. This incurs a 3 dB reduction in the secret key rate.). In addition, two active structures are introduced in the Supplementary Material. The active converters eliminate the $|\varnothing\rangle$ term, thereby exhibiting greater potential. However, the high loss of electro-optical devices limits their current effectiveness.

Joint Bell-state measurement

Our heterogeneous network allows D-type nodes to connect using any form of the regular detection unit[60,94,95]. However, most BB84 detection units are incapable of performing BSMs and therefore cannot directly assist with MDI-type protocols. To address this limitation, we propose a joint BSM, enabling the server and multiple D-type nodes to collaboratively perform a BSM. The key idea is enable distributed nodes to each contribute part of their idle detector resources and collectively forming a BSM setup. The signals of the two S-type nodes converge at the server, which provides a BS for the interference. Then the server forwards the two interfered signals to two different assisted nodes. The two nodes collectively form a BSM unit (see Supplementary Information for more details). In MDI-QKD, the joint-BSM model can be easily equivalent to a regular BSM-model. Regarding the channel between server and D-type nodes, the symmetric part (L) can be equivalently interpreted as the channel between the user node and the untrusted measurement node. Besides, the asymmetric part (ΔL) can be regarded equivalently interpreted as an additional detection efficiency $\eta_{\Delta L}$. So the MDI-QKD with the joint-BSM can be equivalently regarded as a conventional MDI-QKD with non-identical SPDs. As MDI-QKD makes no assumptions about the detection system, asymmetrical detection efficiencies are in fact a prevalent scenario in practical MDI-QKD implementations.

We also experimentally validate the joint BSM. In this experiment, we suppose Bob and Charlie wish to perform MDI-QKD, but David is occupied, the server then recalls two other D-type nodes, George and Henry, to collaboratively perform the BSM. Each of them provides two SPDs, operating in 1 GHz gated mode, to detect the early and late time bins, respectively. Bob and Charlie prepare T.B.P. states to perform a regular T.B.P.-based MDI-QKD. The main difference between the joint and the regular BSM is the interfered signals are detected after passing two different long fiber channels, Which may lead to additional calibration and delay adjustment. In this demonstration, Bob and Charlie accumulated 10^{12} round in 1000 seconds and reached a 331062 secret key length, with a 0.018 error rate.

Software-defined prepare-and-measure network

In this work, we propose an SD-P&M-QN architecture to coordinate nodes and optimize network performance in our fully heterogeneous quantum network (see Supplementary Information for more details). horizontally, the SD-P&M-QN consists of nodes and a server, where the nodes are heterogeneous and the server contains distributed infrastructure devices (such as a quantum router, DoF converters) and a centralized controller. Vertically, the SD-P&M-QN consists of an application layer, a control layer, and an infrastructure layer, whose functions are listed as follows:

1. Application layer: The user node of this layer facilitates the execution of quantum tasks by acting as a client, which independently submits their requirement to the server. This interaction is handled by an agent, which abstracts the details of the underlying communication process, allowing users to focus solely on their tasks without needing to understand the technical details. For the network, the application layer includes platform management and task management functionalities. Platform management involves network configuration and access authentication, enabling the server to enable or disable specific quantum tasks and controlling user access. Task management involves aggregating user requests, analyzing task requirements, and mapping resources to ensure efficient execution. All user requests are submitted to the server (referred to as the platform), which coordinates and manages the tasks.
2. Control layer: This layer plays a critical role in managing both user-side operations and network-wide functionalities. For user nodes, it provides local control and management, which includes configuring local devices (such as device usage, protocols, and parameter settings) and managing local resources (such as key resources in the quantum key pool (QKP)[75], including storage, lifecycle checks, and usage). For the network, the control layer encompasses resource allocation and routing control. The orchestration core is the key component for software heterogeneity, responsible for resource allocation, protocol selection, and parameter optimization. Specifically, it treats all nodes and network devices as a unified pool of resources, allocating and optimizing them based on the tasks issued by the application layer. This process effectively maps tasks to specific physical devices. Once resources are allocated, the control layer selects appropriate protocols and parameters for each node device and instructs the devices to operate accordingly. Routing control determines the paths through which quantum signals are transmitted, enabling end-to-end quantum communication between any two nodes in the network. Finally, the network hypervisor oversees the status of all nodes and manages network devices, ensuring smooth and efficient network operations. This layer ensures both user-side functionality and network-wide coordination, enabling seamless quantum communication.
3. Infrastructure layer: This layer is the foundational component that supports both user-side operations and network-wide functionalities. For the user terminal, it consists of classical devices, such as synchronization and post-processor. In addition, it includes quantum devices, such as the various types of setups proposed in this work, corresponding to the heterogeneous users. For network infrastructure, this layer comprises classical devices, including networking equipment (such as switches and routers) and centralized controllers, which establish the classical communications and execute SD-P&M-QN control functions. Furthermore, it incorporates quantum devices, such as the DoF converters and quantum routers. This layer ensures the seamless integration of classical and quantum components, providing the necessary support for both node operations and network management.

Data availability

The data that support the plots within this paper are deposited on Zenodo https://zenodo.org/records/17504715.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179 (IEEE, 1984).
2. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004 (2017).
3. DiVincenzo, D. P. Quantum computation. *Science* **270**, 255–261 (1995).

4. Komar, P. et al. A quantum network of clocks. *Nat. Phys.* **10**, 582–587 (2014).
5. Degen, C. L., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
6. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5**, 222–229 (2011).
7. Gisin, N. *Quantum Chance: Nonlocality, Teleportation and Other Quantum Marvels* (Springer, 2014).
8. Kollmitzer, C. & Pivk, M. *Applied Quantum Cryptography* (Springer, 2010).
9. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
10. Castelvecchi, D. The quantum internet has arrived (and it hasn't). *Nature* **554**, 289–293 (2018).
11. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018).
12. Singh, A., Dev, K., Siljak, H., Joshi, H. D. & Magarini, M. Quantum internet-applications, functionalities, enabling technologies, challenges, and research directions. *IEEE Commun. Surv. Tutor.* **23**, 2218–2247 (2021).
13. Li, Z. et al. Entanglement-assisted quantum networks: Mechanics, enabling technologies, challenges, and research directions. *IEEE Commun. Surv. Tutor.* **25**, 2133–2189 (2023).
14. Gösta, F. *The Quantum Internet: Ultrafast and Safe from Hackers* (Springer, 2020).
15. Delle Donne, C. et al. An operating system for executing applications on quantum network nodes. *Nature* **639**, 321–328 (2025).
16. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
17. Cariolaro, G. *Quantum Communications* (Springer, 2015).
18. Wolf, R. *Quantum Key Distribution* (Springer, 2021).
19. Kozlowski, W., Dahlberg, A. & Wehner, S. Designing a quantum network protocol. In *Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies*, 1–16 (2020).
20. Dahlberg, A. & Wehner, S. SimulaQron-a simulator for developing quantum internet software. *Quantum Sci. Technol.* **4**, 015001 (2018).
21. Dahlberg, A. et al. NetQASM-a low-level instruction set architecture for hybrid quantum–classical programs in a quantum internet. *Quantum Sci. Technol.* **7**, 035023 (2022).
22. Salvail, L. et al. Security of trusted repeater quantum key distribution networks. *J. Comput. Secur.* **18**, 61–87 (2010).
23. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *N. J. Phys.* **11**, 075001 (2009).
24. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. *Opt. Exp.* **19**, 10387–10409 (2011).
25. Wang, S. et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Exp.* **22**, 21739–21756 (2014).
26. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
27. Ribezzo, D. et al. Deploying an inter-european quantum network. *Adv. Quantum Technol.* **6**, 2200061 (2023).
28. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* **6**, 011024 (2016).
29. Joshi, S. K. et al. A trusted node–free eight-user metropolitan quantum communication network. *Sci. Adv.* **6**, eaba0959 (2020).
30. Wengerowsky, S., Joshi, S. K., Steinlechner, F., Hübel, H. & Ursin, R. An entanglement-based wavelength-multiplexed quantum communication network. *Nature* **564**, 225–228 (2018).
31. Fan-Yuan, G.-J. et al. Measurement-device-independent quantum key distribution for nonstandalone networks. *Photon. Res.* **9**, 1881–1891 (2021).
32. Fan-Yuan, G.-J. et al. Robust and adaptable quantum key distribution network without trusted nodes. *Optica* **9**, 812–823 (2022).
33. Richter, S. et al. Agile and versatile quantum communication: Signatures and secrets. *Phys. Rev. X* **11**, 011038 (2021).
34. De Marco, I. et al. Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter. *Optica* **8**, 911–915 (2021).
35. Laing, A., Scarani, V., Rarity, J. G. & O'Brien, J. L. Reference-frame-independent quantum key distribution. *Phys. Rev. A* **82**, 012304 (2010).
36. Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89**, 037902 (2002).
37. Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **90**, 052314 (2014).
38. Pereira, M., Kato, G., Mizutani, A., Curty, M. & Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **6**, eaaz4487 (2020).
39. Wang, W. et al. Fully passive quantum key distribution. *Phys. Rev. Lett.* **130**, 220801 (2023).
40. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
41. Wang, C. et al. Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **115**, 160502 (2015).
42. Bian, J.-W., Li, B.-H., Xie, Y.-M., Yin, H.-L. & Chen, Z.-B. Asynchronous measurement-device-independent quantum digital signatures. *Phys. Rev. A* **110**, 012609 (2024).
43. Yang, Y.-G. et al. Measurement-device-independent quantum key agreement based on entanglement swapping. *Quantum Inf. Process.* **22**, 438 (2023).
44. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
45. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.* **68**, 557 (1992).
46. Roberts, G. et al. Experimental measurement-device-independent quantum digital signatures. *Nature Communications* **8**, 1098 (2017).
47. Yin, H.-L. et al. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **10**, nwac228 (2023).
48. Gottesman, D. & Chuang, I. Quantum digital signatures. Preprint at https://doi.org/10.48550/arXiv.quant-ph/0105032 (2001).
49. Dunjko, V., Wallden, P. & Andersson, E. Quantum digital signatures without quantum memory. *Physical Review Letters* **112**, 040502 (2014).
50. Li, B.-H. et al. One-time universal hashing quantum digital signatures without perfect keys. *Phys. Rev. Appl.* **20**, 044011 (2023).
51. Fitzi, M., Gisin, N. & Maurer, U. Quantum solution to the byzantine agreement problem. *Phys. Rev. Lett.* **87**, 217901 (2001).
52. Sun, X., Kulicki, P. & Sopek, M. Multi-party quantum Byzantine agreement without entanglement. *Entropy* **22**, 1152 (2020).
53. Weng, C.-X. et al. Beating the fault-tolerance bound and security loopholes for byzantine agreement with a quantum solution. *Research* **6**, 0272 (2023).
54. Jing, X. et al. Experimental quantum Byzantine agreement on a three-user quantum network with integrated photonics. *Sci. Adv.* **10**, eadp2877 (2024).
55. Mehic, M. et al. Quantum key distribution: a networking perspective. *ACM Comput. Surv.* **53**, 1–41 (2020).
56. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).

57. Quantum key distribution networks - software-defined networking control. https://www.itu.int/rec/T-REC-Y.3805-202112-I/en (2025).
58. Kreutz, D. et al. Software-defined networking: A comprehensive survey. *Proc. IEEE* **103**, 14–76 (2014).
59. Aguado, A. et al. The engineering of software-defined quantum key distribution networks. *IEEE Commun. Mag.* **57**, 20–26 (2019).
60. Grünenfelder, F., Boaron, A., Rusca, D., Martin, A. & Zbinden, H. Performance and security of 5 GHz repetition rate polarization-based quantum key distribution. *Appl. Phys. Lett.* **117**, 144003 (2020).
61. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **93**, 042324 (2016).
62. Jiang, C., Yu, Z.-W., Hu, X.-L. & Wang, X.-B. Higher key rate of measurement-device-independent quantum key distribution through joint data processing. *Phys. Rev. A* **103**, 012402 (2021).
63. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
64. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
65. Wegman, M. N. & Carter, J. L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **22**, 265–279 (1981).
66. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
67. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
68. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
69. Da Silva, T. F. et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
70. Lu, F.-Y. et al. Experimental demonstration of fully passive quantum key distribution. *Phys. Rev. Lett.* **131**, 110802 (2023).
71. He, D.-Y. et al. Sine-wave gating ingaas/inp single photon detector with ultralow afterpulse. *Appl. Phys. Lett.* **110**, 111104 (2017).
72. Liu, H. et al. Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. *Phys. Rev. Lett.* **122**, 160501 (2019).
73. Comandar, L. et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photon.* **10**, 312 (2016).
74. Wang, W., Xu, F. & Lo, H.-K. Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks. *Phys. Rev. X* **9**, 041012 (2019).
75. Cao, Y. et al. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Commun. Surv. Tutor.* **24**, 839–894 (2022).
76. Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. In *Advances in Cryptology — EUROCRYPT '93*, 410–423 (1994).
77. Zhang, C.-M. et al. Fast implementation of length-adaptive privacy amplification in quantum key distribution. *Chin. Phys. B* **23**, 090310 (2014).
78. Schiansky, P. et al. Demonstration of quantum-digital payments. *Nat. Commun.* **14**, 3849 (2023).
79. Cao, X.-Y. et al. Experimental quantum e-commerce. *Sci. Adv* **10**, eadk3258 (2024).
80. Shoup, V. On fast and provably secure message authentication based on universal hashing. In *Advances in Cryptology — CRYPTO '96*, 313–328 (Springer Berlin Heidelberg, 1996).
81. Murta, G., Grasselli, F., Kampermann, H. & Bruß, D. Quantum conference key agreement: A review. *Adv. Quantum Technol.* **3**, 2000025 (2020).
82. Hahn, F., de Jong, J. & Pappa, A. Anonymous quantum conference key agreement. *PRX Quantum* **1**, 020325 (2020).
83. Proietti, M. et al. Experimental quantum conference key agreement. *Sci. Adv.* **7**, eabe0395 (2021).
84. Pickston, A. et al. Conference key agreement in a quantum network. *NPJ Quantum Inf.* **9**, 82 (2023).
85. Li, C.-L. et al. Breaking universal limitations on quantum conference key agreement without quantum memory. *Commun. Phys.* **6**, 122 (2023).
86. Xie, Y.-M., Lu, Y.-S., Fu, Y., Yin, H.-L. & Chen, Z.-B. Multi-field quantum conferencing overcomes the network capacity limit. *Commun. Phys.* **7**, 410 (2024).
87. Lin, X. et al. Certified randomness from untrusted sources and uncharacterized measurements. *Phys. Rev. Lett.* **129**, 050506 (2022).
88. Lucamarini, M., Yuan, Z., Dynes, J. & Shields, A. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018).
89. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).
90. Hu, X.-M., Guo, Y., Liu, B.-H., Li, C.-F. & Guo, G.-C. Progress in quantum teleportation. *Nat. Rev. Phys.* **5**, 339–353 (2023).
91. Long, G.-L. & Liu, X.-S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
92. Pan, D. et al. The evolution of quantum secure direct communication: On the road to the qinternet. *IEEE Commun. Surv. Tutor.* **26**, 1898–1949 (2024).
93. Huang, J., Chen, X., Li, X. & Wang, J. Chip-based photonic graph states. *AAPPS Bulletin* **33**, 14 (2023).
94. Agnesi, C. et al. Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. *Optica* **7**, 284–290 (2020).
95. Hu, C., Wang, W., Chan, K.-S., Yuan, Z. & Lo, H.-K. Proof-of-principle demonstration of fully passive quantum key distribution. *Phys. Rev. Lett.* **131**, 110801 (2023).
96. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Revi. Lett.* **117**, 190501 (2016).
97. Deng, J.-J. et al. Measurement-device-independent quantum key distribution with asymmetric sources. *Phys. Rev. Appl.* **24**, 044045 (2025)
98. Wang, Q. & Wang, X.-B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. *Phys. Rev. A* **88**, 052332 (2013).
99. Zhan, X.-H. et al. Measurement-device-independent quantum key distribution with practical spontaneous parametric down-conversion sources. *Phys. Rev. Appl.* **20**, 034069 (2023).
100. Wang, Q., Wang, X.-B. & Guo, G.-C. Practical decoy-state method in quantum key distribution with a heralded single-photon source. *Phys. Rev. A* **75**, 012312 (2007).
101. Schiavon, M., Vallone, G., Ticozzi, F. & Villoresi, P. Heralded single-photon sources for quantum-key-distribution applications. *Phys. Rev. A* **93**, 012331 (2016).

Acknowledgements
This work was supported in part by the National Natural Science Foundation of China under Grant 62425507, Grant 62301524, Grant 62105318, Grant 62271463 and Grant 62171424, in part by the Fundamental Research Funds for the Central Universities under Grant WK2030250122, and in part by China Postdoctoral Science Foundation under Grant 2022M723064, in part by the Natural Science Foundation of Anhui under Grant 2308085QF216, and in part by the Innovation Program for Quantum Science and Technology under Grant 2021ZD0300700.

Author contributions
F.-Y.L., Z.-H.W., and S.W. developed the experimental setup, performed the experiments; F.-Y.L., Z.Y., and Z.-Q.Y. performed the simulation, collected and analyzed the data; F.-Y.L., J.L., and K.X. did the network designment; Y.-X.F. and D.-Y.H. provided the electric technique support; F.-X.W., W.C., G.-C.G., and Z.-F.H. supervised the project; F.-Y.L. wrote the manuscript with input from all authors.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-025-66333-3.

Correspondence and requests for materials should be addressed to Shuang Wang or Zhen-Qiang Yin.

Peer review information *Nature Communications* thanks Yongli Zhao and the other anonymous reviewer(s) for their contribution to the peer review of this work. A peer review file is available.