SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2026, Vol. 69, Iss. 8, 180502:1–180502:10
https://doi.org/10.1007/s11432-026-4996-4

Special Topic: Quantum Information

Scalable and highly fault-tolerant circular quantum Byzantine agreement

Chen-Xun WENG[1,2†], Ming-Yang LI[1,2†], Shi-Gen LI[1,2], Mengya ZHU[3], Xiao-Ran SUN[1,2], Hua-Lei YIN[2,1*] & Zeng-Bing CHEN[1,3*]

[1]*National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*
[2]*School of Physics and Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, Beijing 100872, China*
[3]*MatricTime Digital Technology Co. Ltd., Nanjing 211899, China*

Received 3 February 2026/Revised 30 March 2026/Accepted 11 June 2026/Published online 16 July 2026

Abstract Quantum Byzantine agreement (QBA), a cornerstone of quantum blockchain, offers inherent advantages in security and fault tolerance over classical protocols, guaranteed by the laws of quantum mechanics. However, existing multiparty QBA protocols face challenges for large-scale deployment due to exponential communication complexity or reliance on complex multi-particle entanglement. To address this, we propose a multiparty circular QBA protocol that adopts a semi-decentralized architecture, leveraging circular message gathering and quantum digital signatures to achieve quadratic communication complexity and enhanced fault tolerance. Our protocol is experimentally feasible, requiring only weak coherent states, and is compatible with existing star-shaped quantum networks. Simulations conducted on a global satellite-to-ground network demonstrate that the protocol sustains high consensus rates among multiple users, even when employing different key generation protocols under realistic conditions. This work presents a scalable framework for large-scale QBA networks, establishing the foundation for a practical quantum blockchain that enables secure and fault-tolerant decentralized services.

Keywords quantum Byzantine agreement, quantum blockchain, semi-decentralized, high fault-tolerance, polynomial communication complexity, blockchain trilemma

Citation Weng C-X, Li M-Y, Li S-G, et al. Scalable and highly fault-tolerant circular quantum Byzantine agreement. Sci China Inf Sci, 2026, 69(8): 180502, https://doi.org/10.1007/s11432-026-4996-4

1 Introduction

Originating from the Byzantine generals problem [1], Byzantine agreement protocols enable all honest nodes to reach consensus on a value even in the presence of malicious nodes [2–4]. This task is fundamental to decentralized applications such as blockchain, distributed databases, and the metaverse [5–7]. Classical protocols rely on computational assumptions that are increasingly threatened by advances in quantum algorithms and quantum computers [8–11]. In addition, classical protocols where nodes are linked via point-to-point channels are rigorously constrained by the 1/3 fault-tolerance bound, which means the system could tolerate at most 1/3 of the nodes being malicious [12–14].

Quantum Byzantine agreement (QBA) leverages quantum resources to provide quantum advantages in both security and fault tolerance for consensus mechanisms. The first QBA protocol, based on entangled qutrit states (Aharonov state), is proposed to achieve a three-party consensus that is unattainable by classical protocols [15], and is experimentally demonstrated using tailored four-photon polarization-entangled states [16]. Currently, feasible detectable QBA protocols remain limited to three-party consensus and lack a clear, practical framework for extending beyond three-party scenarios because of their reliance on multi-particle entanglement or high-dimensional qudits [17–20]. Generally, a "detectable" QBA protocol satisfies Byzantine conditions only when it terminates successfully, as honest players will abort the process upon detecting malicious inconsistencies. Recently, a multiparty recursive QBA protocol has been proposed [21], which exploits recursive structures together with one-time universal hashing quantum digital signatures (OTUH-QDS) [22–27]. The term "recursive" refers to a layered message-passing

* Corresponding author (email: hlyin@ruc.edu.cn, zbchen@nju.edu.cn)
† These authors contributed equally to this work.

structure where a three-party OTUH-QDS is recursively utilized to relay signed messages layer by layer throughout the network to ensuring consistency. Unlike detectable approaches relying on multipartite entangled states or high-dimensional qudits, recursive QBA requires only weak coherent states and can, in principle, be extended to an arbitrary number of participants. Owing to the asymmetric properties of three-party QDS [28–34], the protocol achieves information-theoretic security and a fault tolerance approaching one half, thereby surpassing the classical 1/3 fault-tolerance bound and demonstrating a quantum advantage in distributed consensus. It has been experimentally demonstrated in a three-party setting using an integrated photonic circuit [35], and further extended to a five-party scenario based on a fully heterogeneous prepare-and-measure quantum network [36].

With the rapid development of quantum networks [37–39], it is intriguing to explore whether multiparty QBA can be deployed on large-scale quantum networks for practical applications, such as metropolitan and satellite-to-ground quantum networks. If realized, such a QBA network could serve as a core consensus mechanism for constructing quantum blockchains that provide information-theoretically (i.-t.) secure and highly fault-tolerant decentralized information services for real-world applications, such as quantum-blockchain-based federated learning [40], distributed data trust management [41], distributed finance [42], Internet of Things [43], and secure authenticated message delivery in vehicular networks [44–46].

However, current QBA protocols face three main limitations for large-scale deployment. (1) Detectable QBA requires multi-particle entanglement or high-dimensional qudits, making it difficult to scale beyond three parties [47–49]. (2) Although recursive QBA [21] and QKD-based QBA [50] use practical weak coherent states, their communication complexity scales exponentially with the number of participants. This occurs because both methods rely on recursive structures, where the recursion depth depends on the number of malicious nodes. (3) Current protocols all assume a fully connected network. For an N-party system using point-to-point QKD, this requires $N(N-1)/2$ quantum channels. In practice, large-scale quantum networks usually use star or ring topologies rather than full connections.

To address these issues, we propose a semi-decentralized, i.-t. secure circular QBA protocol. Our motivation is to provide a consensus mechanism that is secure, scalable, and compatible with existing quantum network architectures. Our main contributions are as follows. (1) Our protocol uses OTUH-QDS based on weak coherent states instead of multi-particle entanglement, which enables efficient multi-bit signature generation and verification. It requires only two honest nodes to reach consensus (i.e., $N \geqslant f+2$, where f is the number of malicious nodes). (2) We replace the recursive structure with a circular message-gathering process. This reduces the communication complexity from exponential to polynomial $\mathcal{O}(N^2)$ while ensuring unforgeability and non-repudiation. (3) Our semi-decentralized architecture simplifies the network topology by requiring only N quantum channels to distribute keys for OTUH-QDS. This design fits satellite-to-ground quantum networks, where the satellite acts as a certificate authority (CA). Simulations show that our protocol achieves a high consensus rate under realistic satellite-to-ground conditions, demonstrating its feasibility for practical deployment.

2 Semi-decentralized QBA design

Our QBA protocol employs the three-party OTUH-QDS [22,23] as the core component, which provides i.-t. secure non-repudiation and unforgeability. OTUH-QDS involves three roles: signer ($\mathbb{S}$), forwarder ($\mathbb{F}$), and verifier ($\mathbb{V}$), with two phases: the distribution phase and the messaging phase. In the distribution phase, the three parties utilize a key generation protocol (KGP, see Appendix A) such as QKD or quantum secret sharing to establish correlated secret key strings, denoted by $\{X_k, Y_k, Z_k\}$ for user $k \in \{\mathbb{S}, \mathbb{F}, \mathbb{V}\}$. These keys satisfy the XOR correlation where the signer's key equals the bitwise sum of the others: $X_{\mathbb{S}} = X_{\mathbb{F}} \oplus X_{\mathbb{V}}$, $Y_{\mathbb{S}} = Y_{\mathbb{F}} \oplus Y_{\mathbb{V}}$, and $Z_{\mathbb{S}} = Z_{\mathbb{F}} \oplus Z_{\mathbb{V}}$.

In the messaging phase, the signer defines a linear-feedback shift register (LFSR)-based Toeplitz hash function $H_{X_{\mathbb{S}},p_{\mathrm{s}}}$ determined by key $X_{\mathbb{S}}$ and a random parameter p_{s}. For a message Mes, the signer computes the digest $\mathrm{Dig} = H_{X_{\mathbb{S}},p_{\mathrm{s}}}(\mathrm{Mes})$. This digest is encrypted to generate the signature $\mathrm{Sig} = \mathrm{Dig} \oplus Y_{\mathbb{S}}$, while p_{s} is encrypted as $p = p_{\mathrm{s}} \oplus Z_{\mathbb{S}}$. The signer transmits $\{\mathrm{Mes}, \mathrm{Sig}, p\}$ to the forwarder.

Upon receiving the data, the forwarder transmits $\{\mathrm{Mes}, \mathrm{Sig}, p\}$ along with keys $\{X_{\mathbb{F}}, Y_{\mathbb{F}}, Z_{\mathbb{F}}\}$ to the verifier. The verifier recovers the signer's keys by calculating the XOR between the received keys and their own (e.g., $K_{X_{\mathbb{V}}} = X_{\mathbb{V}} \oplus X_{\mathbb{F}}$) and verifies the signature by comparing the decrypted digest against the locally computed hash of Mes. If successful, the verifier sends keys $\{X_{\mathbb{V}}, Y_{\mathbb{V}}, Z_{\mathbb{V}}\}$ to the forwarder. The forwarder then reconstructs the signer's keys (e.g., $K_{Y_{\mathbb{F}}} = Y_{\mathbb{F}} \oplus Y_{\mathbb{V}}$), decrypts Sig and p, and computes the actual digest using the hash function derived from $K_{X_{\mathbb{F}}}$. The signature is accepted only if both the forwarder and the verifier confirm that the computed digest matches the decrypted one.

In our scalable multi-party QBA framework, we introduce a designated entity, the certificate authority (CA),

which exclusively assumes the role of the verifier in every QDS transaction. The role of the CA is strictly confined to providing a cryptographic service: it verifies the validity of signatures upon request from the players. Crucially, the CA serves as an impartial assistant that does not actively participate in the consensus process. It neither generates nor relays messages between players, contributes to the final decision, nor provides any information to a player other than the binary result of a signature verification (i.e., valid or invalid). Such an assumption is also consistent with classical Byzantine agreement protocols that rely on digital signatures, where a trusted setup such as a public-key infrastructure is typically required to distribute and authenticate public keys [1,2]. In this sense, the CA in our protocol plays a similar role as a supporting cryptographic infrastructure, rather than a decision-making entity. This architecture leads to our semi-decentralized model, where we achieve a profound simplification in network topology and a reduction in communication complexity, thereby enabling scalability that would be difficult in a fully decentralized QBA network. The detailed steps and security analysis of OTUH-QDS can be found in Appendix B.

3 Protocol description

The Byzantine generals' problem is typically framed with a commanding general S and several lieutenants R_i [1]. A protocol is considered successful only if it satisfies two interactive consistency (**IC**) conditions: (1) all honest lieutenants agree on the same value ($\mathbf{IC}_1$); and (2) if the commanding general is honest, then all honest lieutenants adopt the correct general's value ($\mathbf{IC}_2$).

In our circular QBA, a commanding general S is randomly selected from N participants, with the other $N-1$ serving as lieutenants R_i ($i \in \mathbb{Z}_{N-1}^{+}$, where $\mathbb{Z}_{N-1}^{+} = \{1, 2, \cdots, N-1\}$). The protocol has three phases: order distribution, where the general sends orders to lieutenants; circular gathering, where lieutenants collect messages from each other; and consensus output, where each honest lieutenant independently outputs the final value according to what they collected before. Figure 1 illustrates the steps of our circular QBA. The details of the three phases are as follows.

(1) Order distribution. For each lieutenant R_i ($i \in \mathbb{Z}_{N-1}^{+}$), the commanding general S signs an m-bit order m_i with an n-bit signature σ_i in Figure 1(a). This pair $\{m_i; \sigma_i\}$ is sent to R_i via a three-party OTUH-QDS, with S, R_i, and the CA as the signer, forwarder, and verifier. Each OTUH-QDS session is shown in Figure 1(b): first, a KGP where S, R_i, and the CA establish their correlated keys; second, the classical signing and verification procedure. Upon verification completes, R_i stores its order list $O^i = \{m_i; \sigma_i\}$. If the general is loyal, all orders received by R_i are identical: $m_i = m_0$ ($\forall i \in \mathbb{Z}_{N-1}^{+}$).

(2) Circular gathering. Each of the $N-1$ lieutenants initiates a clockwise circular gathering of $N-1$ steps (Figure 1(c)). We take the circular gathering started by R_i as an example. The gathering follows a clockwise cycle, denoted by the sequence ($i \to i+1 \to \cdots \to N-1 \to 1 \to \cdots \to i$). The first information package delivered from R_i to R_{i+1} is R_i's initial message list O^i signed with $\sigma^i_{i\to i+1}$, which is denoted by $G^i_{i\to i+1} = \{m_i; \sigma_i; \sigma^i_{i\to i+1}\}$. In the clockwise cycle, one of the participants, lieutenant R_j ($j \neq i$), who receives $G^i_{j-1\to j}$ from R_{j-1} and sends $G^i_{j\to j+1}$ to R_{j+1}, combines $G^i_{j-1\to j}$ with its own initial message list ($O^j = \{m_j; \sigma_j\}$), and signs them with signature $\sigma^i_{j\to j+1}$, which means that $G^i_{j\to j+1} = G^i_{j-1\to j} \cup O^j \cup \{\sigma^i_{j\to j+1}\} = \{m_i, \cdots, m_j; \sigma_i, \cdots, \sigma_j; \sigma^i_{i\to i+1}, \cdots, \sigma^i_{j\to j+1}\}$. The information packages are delivered via three-party OTUH-QDS as shown in Figure 1(d), which is similar to the QDS in the order distribution.

After the clockwise gathering, R_i will receive the final list $G^i_{i-1\to i}$ which contains three parts: (1) all the lieutenants' received order $\{m_1, m_2, \ldots, m_{N-1}\}$, (2) the signatures signed by the commanding general $\{\sigma_1, \sigma_2, \ldots, \sigma_{N-1}\}$, and (3) the signatures generated during the circular gathering by lieutenants $\{\sigma^i_{i\to i+1}, \sigma^i_{i+1\to i+2}, \ldots, \sigma^i_{N-1\to 1}, \ldots, \sigma^i_{i-1\to i}\}$.

Note that in each step of circular gathering, CA verifies all the signatures in the information package. First, CA verifies the validity of $\sigma^i_{j\to j+1}$ as the regular QDS process and records it if valid. Second, CA further verifies that the signatures of all previous steps are unchanged and valid according to the record of CA, i.e., $\{\sigma_i, \cdots, \sigma_j; \sigma^i_{i\to i+1}, \cdots, \sigma^i_{j-1\to j}\}$. Because CA maintains the records of correlated quantum keys and signatures of each OTUH-QDS process, the verification is straightforward. Any failure of verification will restart a new round of circular gathering initiated by R_i.

(3) Consensus output. After the circular gathering, each lieutenant R_i ($\forall i \in \mathbb{Z}_{N-1}^{+}$) gets the completely identical message list, namely $F^i = \{m_1, m_2, \ldots, m_{N-1}\}$, and puts it into a pre-selected deterministic function D to produce the final output $m^{R_i} = D(m_1, m_2, \ldots, m_{N-1})$. Note that a deterministic function is a function that always produces the same output for the same input.

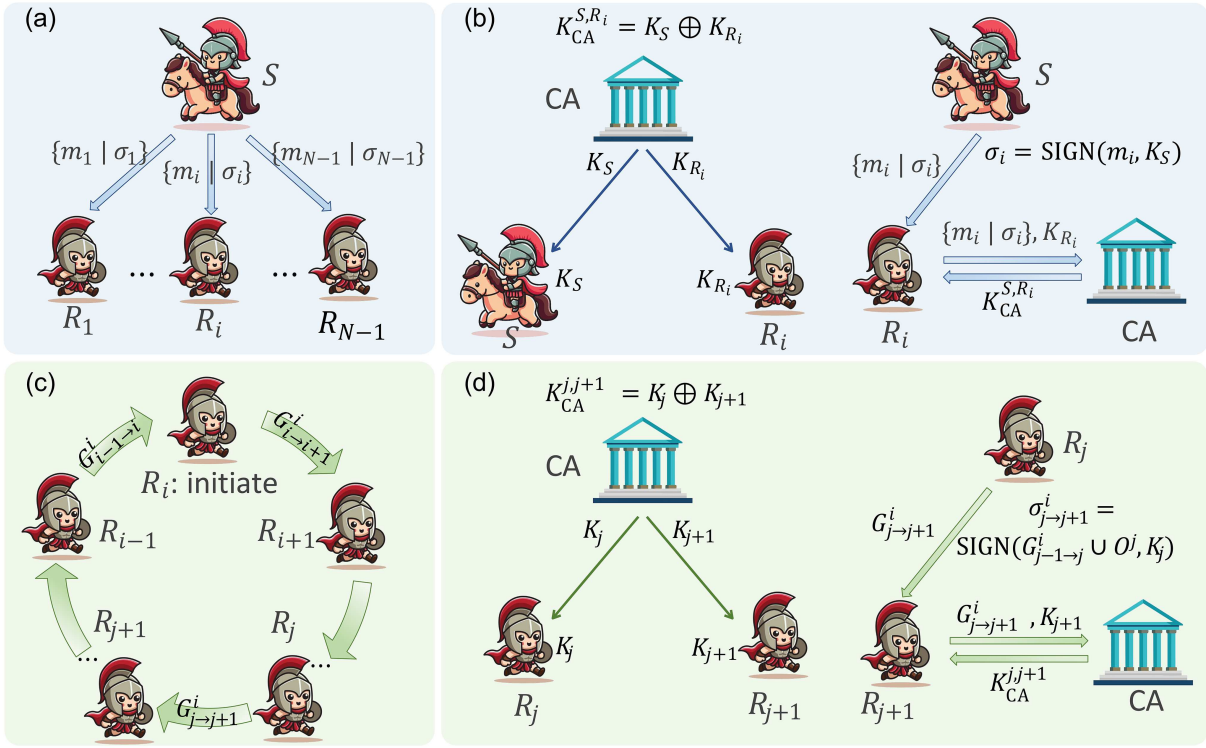

Figure 1 (Color online) Schematic of our circular QBA protocol. (a) Order distribution. The commanding general S distributes message m_i to each lieutenant R_i with signature σ_i through three-party OTUH-QDS ($\forall i \in \mathbb{Z}_{N-1}^+$). (b) Message distribution step between S, R_i, and CA in the order distribution phase. S, R_i, and the CA share correlated quantum keys through a KGP first (left). Then they conduct the signing and verifying procedure (right). R_i's initial message list is $O^i = \{m_i, \sigma_i\}$. CA records the signature σ_i and related quantum keys of this QDS. (c) Circular gathering started by R_i ($\forall i \in \mathbb{Z}_{N-1}^+$). The gathering follows a clockwise sequence, and each step is completed using OTUH-QDS. (d) The information delivery step from R_j to R_{j+1}. R_j combines the information package received from the previous lieutenant R_{j-1}, which is G_{j-1}^i, and its initial message list, which is O^j, and takes it as a whole and signs it with a signature $\sigma_{j\to j+1}^i$. Thus $G_{j\to j+1}^i = G_{j-1\to j}^i \cup O^j \cup \{\sigma_{j\to j+1}^i\}$. The OTUH-QDS process is similar to those in order distribution. CA acts as the verifier of QDS, records $\sigma_{j\to j+1}^i$ and checks the validity of all signatures in $G_{j\to j+1}^i$. Icons Copyright 2026 Vecteezy.

4 Security analysis of circular QBA

In this part, we analyze the i.-t. security and fault-tolerance ability of our circular QBA protocol. The details of the security analysis can be found in Appendix C.

(a) Overall security. The security of our protocol rests on the i.-t. secure non-repudiation and unforgeability of its underlying cryptographic primitive, the OTUH-QDS. As demonstrated in [22], repudiation is impossible, while the probability of a successful forgery is bounded by

$$\varepsilon_{\mathrm{for}}(\mathcal{M}, \mathcal{N}) = \mathcal{M} \cdot 2^{1-\mathcal{N}}, \tag{1}$$

where $\mathcal{M}$ and $\mathcal{N}$ are the lengths of the message and signature, respectively.

To ensure the protocol satisfies the two **IC** conditions, all QDS steps must be secure against forgery. The overall failure probability of the QBA, $\varepsilon_{\mathrm{QBA}}$, is therefore determined by the cumulative risk of forgery across all vulnerable communication steps, i.e., all the QDS steps with dishonest nodes. Crucially, the forgery probability in (1) depends on the message length $\mathcal{M}$, which varies and grows during the circular gathering phase. Therefore, our security analysis adopts a conservative, worst-case approach: we assume malicious players will always target the QDS steps involving the longest possible messages. The final bound also accounts for different scenarios based on the general's honesty, as this affects the number of malicious lieutenants. This reasoning leads to an upper bound on the total failure probability, expressed as

$$\varepsilon_{\mathrm{QBA}} = \max\{f\left[\varepsilon_{\mathrm{for}}(m,n) + (N-f-1)\cdot\varepsilon_{\mathrm{for}}(L_{N-1},n)\right], (f-1)(N-f)\cdot\varepsilon_{\mathrm{for}}(L_{N-1},n)\}, \tag{2}$$

where $L_{N-1} = (N-1)m + (2N-3)n$ is the length of the longest message signed in a circular gathering. A detailed derivation of this bound is provided in Appendix C.

Furthermore, we consider composable security by accounting for imperfections in the KGPs used to establish the shared keys [51, 52]. The overall security of the protocol is thus modeled by the sum of the protocol's QBA failure probability and that of the underlying KGPs,

$$\varepsilon_{\text{all}} = \varepsilon_{\text{QBA}} + \varepsilon_{\text{KGP}}, \tag{3}$$

where ε_{KGP} represents the total failure probability of all KGPs involved.

(b) Fault-tolerance. Here we consider two cases where the commanding general S is honest or not according to $\mathbf{IC}_1$ and $\mathbf{IC}_2$. When S is honest, the distribution of the message m_0 is guaranteed with unforgeability because at least two honest participants (S and CA) record the message distribution and its signature. Only the correct message m_0 appears in the circular gathering phase and ensures that all honest lieutenants reach a unanimous decision based on $N-1$ copies of m_0. When S is dishonest, although $N-1$ distinct messages $\{m_1, m_2, \cdots, m_{N-1}\}$ are distributed, the CA still records them to prevent any forgeries when an honest lieutenant performs a circular gathering. All honest lieutenants gather the same set of messages $\{m_1, m_2, \cdots, m_{N-1}\}$. This ensures that all honest lieutenants output the same result. As a result, our protocol requires at least two honest participants in the system, which means that

$$N \geqslant f + 2. \tag{4}$$

5 Scalability analysis of circular QBA

Here, we analyze the communication complexity and the number of required quantum channels of our circular QBA protocol.

(a) Communication complexity. We define the communication complexity, $C(N)$, as the minimum times of communication (QDS in our protocol) to reach consensus for a distributed system of N players with f malicious ones. In our work, the order distribution phase comprises $N-1$ distribution steps from the commanding general S, the circular gathering phase comprises $N-1$ lieutenants independently initiating circular gathering, and each circular gathering contains $N-1$ message delivery steps. Therefore, the communication complexity of circular QBA is

$$C(N) = (N-1) + (N-1)(N-1) = N^2 - N. \tag{5}$$

In Figure 2, we compare the communication complexity (measured by the number of communication rounds) of our protocol with detectable QBA [15] and two existing i.-t. secure multiparty QBA protocols, QKD-based QBA [50] and recursive QBA [21]. The figure presents lower bounds on communication complexity, determined by minimizing the total number of nodes while maintaining security for a given number of malicious participants. The results demonstrate that, except in the single-malicious-node case ($f = 1$), our protocol exhibits significantly superior scalability and fault tolerance, particularly for large-scale systems. Specifically, for $f = 10$ malicious nodes, QKD-based QBA [50] requires at least 2.30×10^{15} rounds, and the recursive QBA protocol [21] requires at least 7.44×10^{12} rounds, whereas our protocol requires only 132 rounds, achieving a reduction of more than ten orders of magnitude.

(b) Number of quantum channels. Our protocol's architecture reduces quantum channel requirements. The three-party correlated keys needed for OTUH-QDS are established efficiently: with the CA acting as a verifier, it performs two separate QKD processes with the other participants (signer and forwarder) and locally computes its key via bitwise XOR. This star-shaped model simplifies the network from a fully-connected mesh requiring $N(N-1)/2$ quantum channels [21, 50] to a star-shaped network with only N channels connecting players to the CA. Such a configuration is well-suited for a satellite-based implementation, where the satellite naturally serves as the central CA, overcoming the attenuation limits of terrestrial fiber. We present this satellite architecture in detail in the following section.

6 Satellite-based large-scale circular QBA networks

The successful demonstration of satellite-to-ground QKD has established a viable path towards a global quantum internet, overcoming the distance limitations imposed by fiber attenuation [53–55]. However, these pioneering networks fundamentally serve for some information tasks involving trusted nodes, primarily for point-to-point secure links. While sufficient for quantum key distribution involving two trusted parties, this poses a critical limitation on multiparty distributed applications, such as blockchain where nodes may be untrusted with each other. The

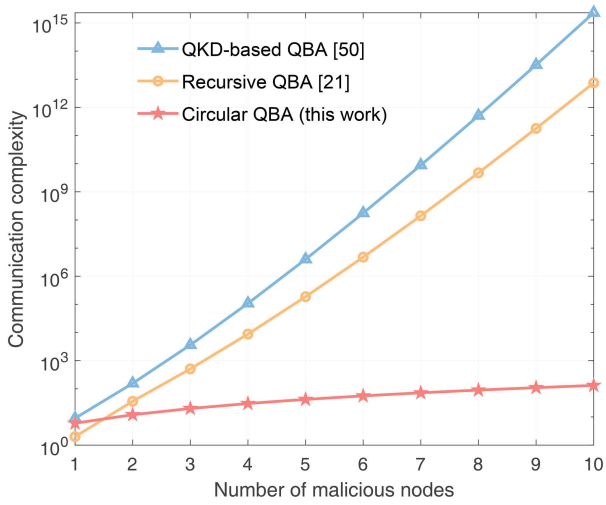

Figure 2 (Color online) Comparison of lower bounds on communication complexity (number of communication rounds) for QKD-based QBA [50], recursive QBA [21] and this work. For each protocol, the total number of nodes is minimized according to its fault-tolerance capability. For the number of malicious players $f \geqslant 2$, our protocol provides an obvious advantage over the previous schemes.

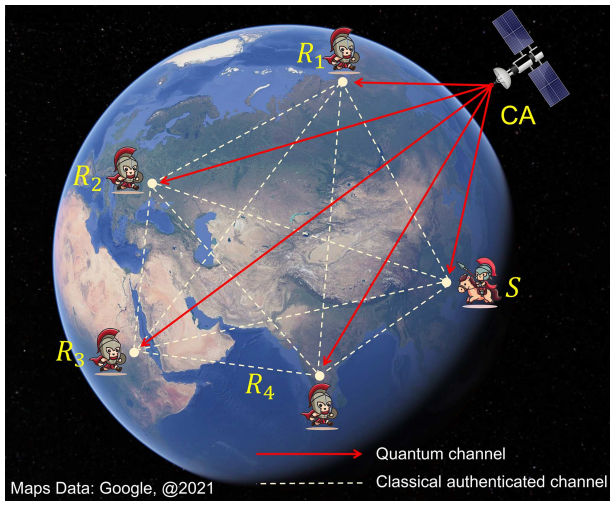

Figure 3 (Color online) Illustration of the satellite-to-ground five-user QBA network employing our circular QBA protocol. The satellite acts as the CA, distributing quantum keys to ground-based players via satellite-to-ground quantum channels (red solid lines) and verifying validity in each three-party QDS. Authenticated classical channels (yellow dashed lines) are employed for communication among users, avoiding the need for quantum channels between ground stations. Note that classical authenticated channels between a player and CA are needed for the communication during QDS.

next step for the applications of quantum networks, whether terrestrial or space-based, is to develop towards fault-tolerant decentralized systems. QBA is the foundational protocol for achieving such a system. With a polynomial communication complexity and linear scaling of the number of quantum channels, our circular QBA protocol is practical when applied in large-scale satellite-to-ground star-shaped quantum networks.

Satellite-to-ground communication involves signal transmission through the atmosphere instead of optical fibers, enabling long-distance communication [56]. Depending on the receiver's position, the channel is categorized as either downlink or uplink. Here we focus on the downlink, where the receiver (player) is located on the ground, as shown in Figure 3. Atmospheric effects on the optical signal can be classified into attenuation, turbulence, and deflection. Attenuation is primarily caused by aerosol and molecular scattering, while turbulence and deflection result from the uneven spatiotemporal distribution of the atmosphere. As the laser beam travels through the atmosphere, this unevenness causes the beam waist to broaden and the beam's direction to deviate randomly. All of these effects, together with possible laser misalignment, contribute to a reduction in total transmittance, which is described in Appendix D. The extent of these effects depends on many factors, most of which are determined by the environment. Here, we focus on the satellite's altitude and zenith angle in subsequent simulations, considering controllability.

Here, to present the efficiency, we simulate the consensus rate (CR) of our protocol, defined as the number of

Table 1 Comparison between our protocol and other QBA protocols. We mainly consider three aspects: security, scalability, and decentralization. Detectable: detectable QBA has a nonzero probability of avoidable failure, where the events should be disregarded. $P_r^n = \frac{n!}{(n-r)!}$ is r-permutations of n. N/A: not applicable.

Performance index		Fitzi et al. [15]	Rahaman et al. [19]	Smania et al. [20]	Kiktenko et al. [50]	Weng et al. [21]	This work
Security	Fault-tolerance	$f=1, N=3$	$f=1, N=3$	$f=1, N=3$	$N \geqslant 3f+1$	$N \geqslant 2f+1$	$N \geqslant f+2$
	Security level	Detectable	Detectable	Detectable	i.-t. secure	i.-t. secure	i.-t. secure
Scalability	Communication complexity	N/A	N/A	N/A	$\sum_{r=1}^{f+1} P_r^{N-1}$	$\sum_{r=0}^{f-1} P_{r+2}^{N-1}$	N^2-N
	Number of quantum channels	3	3	3	$N(N-1)/2$	$N(N-1)/2$	N
	Experimental requirement	Entangled Aharonov states	Entangled Hardy states	Single qutrit	Coherent states	Coherent states	Coherent states
	Message type	Single bit	Single bit	Single bit	Single bit	Multi-bit	Multi-bit
Decentralization		Full	Full	Full	Full	Full	Semi
Cryptography tool		Quantum entanglement	Quantum entanglement	High-dimension quantum state	QKD	QDS	QDS

successful consensuses that can be achieved per second. Since OTUH-QDS are required for each consensus at least $C(N) = N^2 - N$ times, the CR is proportional to the signature rate (SR, see Appendix B for details). CR can be expressed as [21]

$$CR = \frac{\min(SR)}{C(N)} = \frac{\min(SR)}{(N^2-N)}, \tag{6}$$

where the minimum function (min) accounts for variations in the quantum channels between parties, leading to different channel losses and varying signature rates.

We first simulate the performance of our circular QBA using the satellite-to-ground discrete-modulated continuous-variable (DM-CV) QKD [56], under the conditions of both homodyne detection [57] and heterodyne detection [58]. In these simulations, we optimize the performance by setting the intensity of the coherent state $\alpha = 0.72$ and the post-selection parameters $\Delta_c = 0.42$, $\Delta_a = 0.52$, and $\Delta_p = 0$. The repetition rate is 10^9 Hz, and the detectors' noise is $\xi_{\text{het}} = 2\xi_{\text{hom}} = 2\xi_{\text{det}} = 0.02$. Figure 4 presents the consensus rate achieved using the two detection methods with different numbers of participants, noise levels, and the types of detectors(trusted or untrusted). All simulations are conducted under the downlink condition to model the scenario where the satellite (CA) distributes the quantum keys. The results demonstrate high efficiency under various conditions, especially for low Earth orbit (LEO) satellites with an altitude of around 200–900 km. A consensus rate of more than 10^2–10^5 times per second can be achieved for multi-party consensus, demonstrating the excellent performance in various practical conditions of our QBA protocol.

We further simulate the consensus rate when using BB84 KGP adopted from the asymmetric coding BB84 QKD [59–61], as shown in Figure 5. Simulations employed the following parameters: detector efficiency of 70%, dark count rate of 10^{-8}, misalignment error rate of 0.02, and error correction efficiency of 1.1. Besides different numbers of participants, we additionally calculate the consensus rates for different sizes of the message (1 kb, 1 Mb, and 100 Mb). The consensus rate exceeds 10^3 times per second in a 7-party QBA with a 100 Mb message for LEO satellites. These simulations demonstrate the practicality of our QBA protocol, since the experimental requirements of BB84 KGP are simple, and BB84 QKD has been implemented in the satellite-to-ground system recently [55]. All the simulation details can be found in Appendix D.

Note that in our simulations of the circular QBA protocol on satellite-to-ground networks, we employ the commonly used BB84 and DM-CV protocols for key distribution. While adopting more efficient QKD protocols with higher key rates, such as twin-field QKD [62,63] and asynchronous measurement-device-independent QKD [64,65], would naturally increase the signature generation rate and the overall consensus rate, this improvement is straightforward.

7 Discussion and outlook

The blockchain trilemma describes the challenge of balancing three fundamental aspects of a distributed system: decentralization, scalability, and security. Achieving all three optimally is impossible for classical distributed systems, as improving one aspect often comes at the cost of another. This trade-off also persists in all known QBA protocols, as shown in Table 1. We also compare our protocol with other QBA protocols in terms of the three aspects of the blockchain trilemma to show the practicality of our work. In addition, the blockchain trilemma also

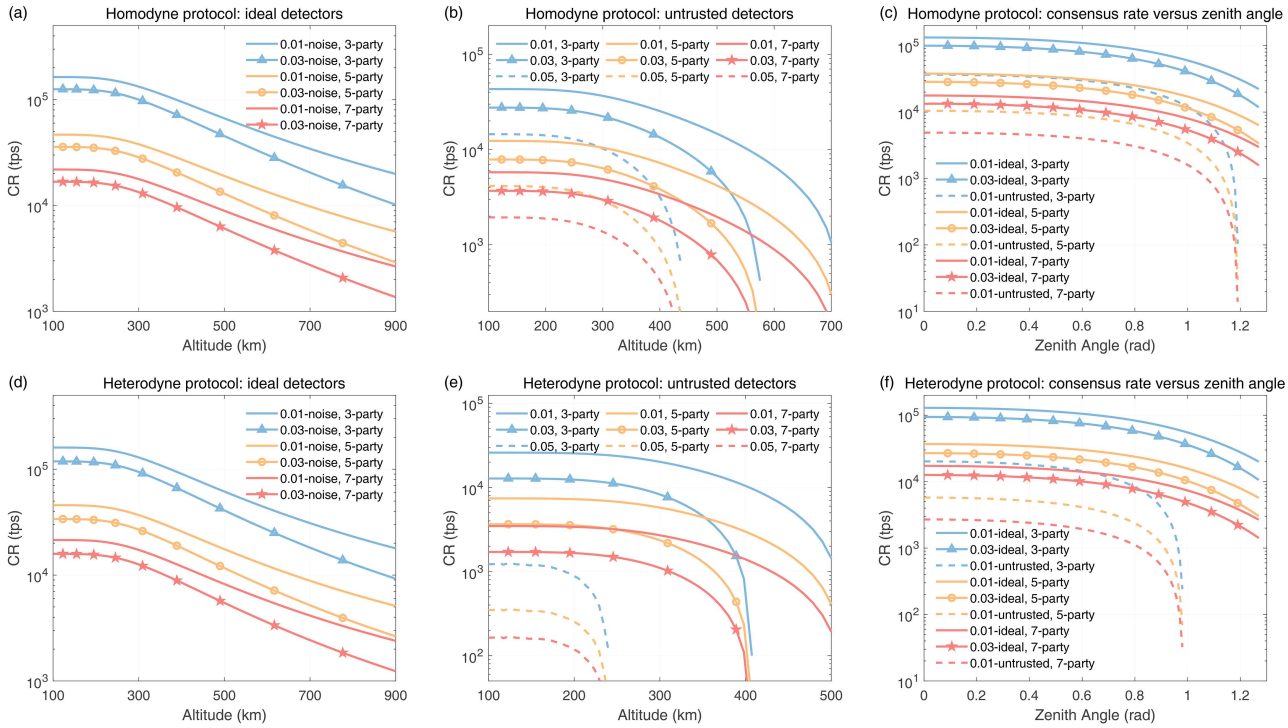

Figure 4 (Color online) Simulation of the consensus rate of circular QBA using satellite-to-ground DM-CV KGP scheme. The consensus rate versus altitude of the satellite (CA) at a zenith angle of 0 rad with (a) ideal detectors, (b) untrusted detectors, and (c) the consensus rate versus the zenith angle at an altitude of 300 km, when using the homodyne protocol. (d)–(f) The corresponding results when using the heterodyne protocol. All simulations are performed under downlink conditions, as the proposed QBA scheme requires the CA to distribute quantum keys. We consider different noise levels ($\xi_{\mathrm{ch}} = 0.01,\ 0.03,\ 0.05$) with both ideal and untrusted detectors. The size of the message is fixed at 1 Mb. These results comprehensively demonstrate the high efficiency of our protocol in a satellite-to-ground system.

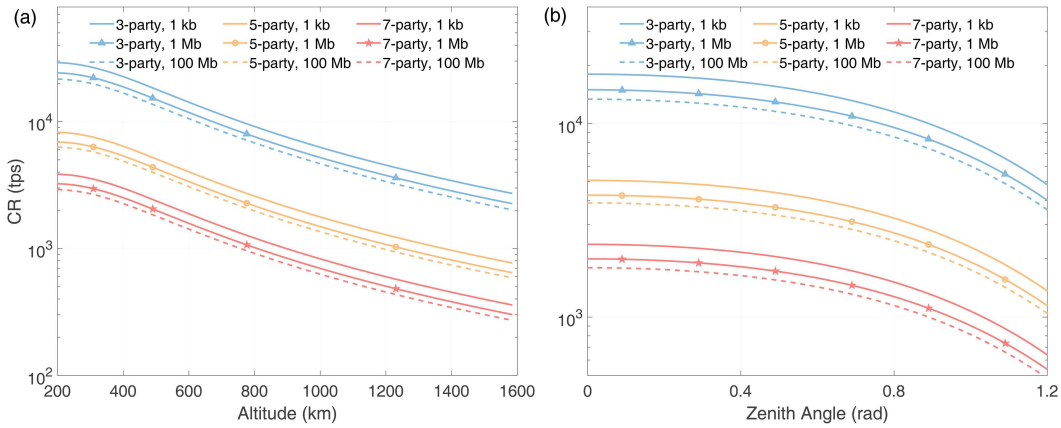

Figure 5 (Color online) Performance of the QBA protocol using BB84 KGP adapted from asymmetric coding BB84 QKD. (a) Consensus rate versus satellite altitude (zenith angle = 0 rad). (b) Consensus rate versus zenith angle (at a fixed altitude of 300 km). Results are shown for various numbers of participants and message sizes (1 kb, 1 Mb, and 100 Mb).

remains for our circular QBA due to the relaxation of decentralization. To date, whether a QBA protocol can overcome the blockchain trilemma remains an open question.

Interestingly, our approach demonstrates that breaking the trilemma may not be necessary. Our results indicate that by partially relaxing decentralization to optimize security and scalability, it is possible to design an i.-t, secure multiparty QBA protocol with quadratic communication complexity, a fault tolerance of $N \geqslant f + 2$, and requiring only N quantum channels, making it suitable for large-scale deployment.

It is worth noting that the introduction of the CA in our framework is a deliberate design choice to navigate the blockchain trilemma. While the CA is a designated entity, its role is strictly confined to signature verification as a supporting cryptographic infrastructure, rather than acting as a decision-making participant in the consensus process. Furthermore, although the current work assumes a single CA for simplicity, the framework could be

extended to multi-CA scenarios in practical network topologies. In such a setup, security against partially corrupted CAs could be achieved through redundancy or threshold-based verification techniques. Exploring the multi-CA architecture for circular QBA remains an interesting open direction for future QBA networks.

This work paves the way for practical, efficient, and scalable QBA networks compatible with current quantum network topologies, and lays the foundation for future quantum blockchain systems capable of delivering i.-t. secure and fault-tolerant decentralized information services, even under the potential threats of quantum computing in the quantum era.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. U25D8016, 12522419, 12274223), Program for Innovative Talents, Entrepreneurs in Jiangsu (Grant No. JSSCRC2021484), and Fundamental Research Funds for the Central Universities and the Research Funds of Renmin University of China (Grant No. 24XNKJ14). We gratefully acknowledged the icons designed by Vecteezy from www.vecteezy.com.

Supporting information Appendixes A–D The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans Program Lang Syst, 1982, 4: 382–401
2 Castro M, Liskov B, et al. Practical Byzantine fault tolerance. In: Proceedings of OSDI, 1999. 173–186
3 Aublin P L, Mokhtar S B, Quéma V. RBFT: redundant Byzantine fault tolerance. In: Proceedings of 2013 IEEE 33rd International Conference on Distributed Computing Systems, 2013. 297–306
4 Guo B, Lu Z, Tang Q, et al. Dumbo: faster asynchronous BFT protocols. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020. 803–818
5 Bodkhe U, Tanwar S, Parekh K, et al. Blockchain for Industry 4.0: a comprehensive review. IEEE Access, 2020, 8: 79764–79800
6 Jiang C S, Xu C X, Chen J, et al. Blockchain-based immunization against kleptographic attacks. Sci China Inf Sci, 2024, 67: 172102
7 Miao Y, Gai K K, Zhu L H. Blockchain-assisted multi-keyword searchable provable data possession for cloud storage. Sci China Inf Sci, 2026, 69: 132101
8 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev, 1999, 41: 303–332
9 Grover L K. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett, 1997, 79: 325–328
10 Fedorov A K, Kiktenko E O, Lvovsky A I. Quantum computers put blockchain security at risk. Nature, 2018, 563: 465–467
11 Zhou M G, Cao X Y, Lu Y S, et al. Experimental quantum advantage with quantum coupon collector. Research, 2022, 2022: 9798679
12 Dolev D, Halpern J Y, Strong H R. On the possibility and impossibility of achieving clock synchronization. J Comput Syst Sci, 1986, 32: 230–250
13 Fischer M J, Lynch N A, Merritt M. Easy impossibility proofs for distributed consensus problems. Distrib Comput, 1986, 1: 26–39
14 Feng L L, Fu X, Wang H M, et al. From PBFT to the present: a thorough overview of blockchain consensus protocols. Sci China Inf Sci, 2026, 69: 111102
15 Fitzi M, Gisin N, Maurer U. Quantum solution to the Byzantine agreement problem. Phys Rev Lett, 2001, 87: 217901
16 Gaertner S, Bourennane M, Kurtsiefer C, et al. Experimental demonstration of a quantum protocol for Byzantine agreement and liar detection. Phys Rev Lett, 2008, 100: 070504
17 Iblisdir S, Gisin N. Byzantine agreement with two quantum-key-distribution setups. Phys Rev A, 2004, 70: 034306
18 Neigovzen R, Rodó C, Adesso G, et al. Multipartite continuous-variable solution for the Byzantine agreement problem. Phys Rev A, 2008, 77: 062307
19 Rahaman R, Wieśniak M, Żukowski M. Quantum Byzantine agreement via Hardy correlations and entanglement swapping. Phys Rev A, 2015, 92: 042302
20 Smania M, Elhassan A M, Tavakoli A, et al. Experimental quantum multiparty communication protocols. npj Quantum Inf, 2016, 2: 16010
21 Weng C X, Gao R Q, Bao Y, et al. Beating the fault-tolerance bound and security loopholes for Byzantine agreement with a quantum solution. Research, 2023, 6: 0272
22 Yin H L, Fu Y, Li C L, et al. Experimental quantum secure network with digital signatures and encryption. Natl Sci Rev, 2023, 10: nwac228
23 Li B H, Xie Y M, Cao X Y, et al. One-time universal hashing quantum digital signatures without perfect keys. Phys Rev Appl, 2023, 20: 044011
24 Xiong S, Tang B, Han H, et al. Efficient arbitrated quantum digital signature with multi-receiver verification. Adv Quantum Tech, 2024, 7: 2400110
25 Bian J W, Li B H, Xie Y M, et al. Asynchronous measurement-device-independent quantum digital signatures. Phys Rev A, 2024, 110: 012609
26 Qin J Q, Yu Z W, Wang X B. Efficient quantum digital signatures over long distances with likely bit strings. Phys Rev Appl, 2024, 21: 024012
27 Du Y, Li B H, Hua X, et al. Chip-integrated quantum signature network over 200 km. Light Sci Appl, 2025, 14: 108
28 Gottesman D, Chuang I. Quantum digital signatures. 2001. arXiv:quant-ph/0105032
29 Dunjko V, Wallden P, Andersson E. Quantum digital signatures without quantum memory. Phys Rev Lett, 2014, 112: 040502
30 Yin H L, Fu Y, Chen Z B. Practical quantum digital signature. Phys Rev A, 2016, 93: 032316
31 Amiri R, Wallden P, Kent A, et al. Secure quantum signatures using insecure quantum channels. Phys Rev A, 2016, 93: 032325
32 Roberts G L, Lucamarini M, Yuan Z L, et al. Experimental measurement-device-independent quantum digital signatures. Nat Commun, 2017, 8: 1098
33 Richter S, Thornton M, Khan I, et al. Agile and versatile quantum communication: signatures and secrets. Phys Rev X, 2021, 11: 011038
34 Qin J Q, Jiang C, Yu Y L, et al. Quantum digital signatures with random pairing. Phys Rev Appl, 2022, 17: 044047
35 Jing X, Qian C, Weng C X, et al. Experimental quantum Byzantine agreement on a three-user quantum network with integrated photonics. Sci Adv, 2024, 10: eadp2877
36 Lu F Y, Wang Z H, Zhou Y, et al. Fully heterogeneous prepare-and-measure quantum network for the next stage of quantum internet. Nat Commun, 2025, 16: 11487
37 Wehner S, Elkouss D, Hanson R. Quantum Internet: a vision for the road ahead. Science, 2018, 362: eaam9288
38 Azuma K, Economou S E, Elkouss D, et al. Quantum repeaters: from quantum networks to the quantum internet. Rev Mod Phys, 2023, 95: 045006
39 Bozzio M, Crépeau C, Wallden P, et al. Quantum cryptography beyond key distribution: theory and experiment. Rev Mod Phys, 2025, 97: 045006

40 Liu H W, Liu Z P, Yin H L, et al. Quantum-enhanced blockchain federated learning via quantum Byzantine agreement. Sci China Inf Sci, 2025, 68: 180503
41 Qu Z, Zhang Z, Liu B, et al. Quantum detectable Byzantine agreement for distributed data trust management in blockchain. Inf Sci, 2023, 637: 118909
42 Liu S, Zhang Y, Ren S, et al. Experimental demonstration of complete quantum e-commerce based on an efficient quantum digital payment. Photon Res, 2025, 13: 572–582
43 Zhao Z, Li X, Luan B, et al. Secure Internet of Things (IoT) using a novel Brooks Iyengar quantum Byzantine agreement-centered blockchain networking (BIQBA-BCN) model in smart healthcare. Inf Sci, 2023, 629: 440–455
44 Dharminder D, Kumar U, Gupta P. Edge based authentication protocol for vehicular communications without trusted party communication. J Syst Architecture, 2021, 119: 102242
45 Yadav D K, Sahu H, Chaudhary D, et al. NTRU lattice-based blockchain consensus-assisted vehicle-to-vehicle authenticated message delivery in Internet of vehicles. Int J Communication, 2025, 38: e70089
46 Singh R, Das L, Chaudhary D. Building scalable and quantum attack resistant authenticated message delivery system for Internet of vehicles with blockchain consensus mechanism. Concurrency Computation, 2025, 37: e70071
47 Sun X, Kulicki P, Sopek M. Multi-party quantum Byzantine agreement without entanglement. Entropy, 2020, 22: 1152
48 Li L, Sun X, Zhu J. Quantum Byzantine agreement against full-information adversary. 2024. ArXiv:2409.01707
49 Paing S N, Setiawan J W, Ullah M A, et al. Counterfactual quantum Byzantine consensus for human-centric metaverse. IEEE J Sel Areas Commun, 2024, 42: 905–918
50 Kiktenko E O, Pozhar N O, Anufriev M N, et al. Quantum-secured blockchain. Quantum Sci Technol, 2018, 3: 035004
51 Yin H L, Wang W L, Tang Y L, et al. Experimental measurement-device-independent quantum digital signatures over a metropolitan network. Phys Rev A, 2017, 95: 042338
52 Korzh B, Lim C C W, Houlmann R, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. Nat Photon, 2015, 9: 163–168
53 Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution. Nature, 2017, 549: 43–47
54 Chen Y A, Zhang Q, Chen T Y, et al. An integrated space-to-ground quantum communication network over 4600 kilometres. Nature, 2021, 589: 214–219
55 Li Y, Cai W Q, Ren J G, et al. Microsatellite-based real-time quantum key distribution. Nature, 2025, 640: 47–54
56 Li S, Li C, Liu W, et al. Discrete-modulated continuous-variable quantum key distribution in satellite-to-ground communication. Adv Quantum Tech, 2024, 7: 2400140
57 Liu W B, Li C L, Xie Y M, et al. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. PRX Quantum, 2021, 2: 040334
58 Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Phys Rev X, 2019, 9: 041064
59 Lo H K, Chau H F, Ardehali M. Efficient quantum key distribution scheme and a proof of its unconditional security. J Cryptology, 2005, 18: 133–165
60 Lim C C W, Curty M, Walenta N, et al. Concise security bounds for practical decoy-state quantum key distribution. Phys Rev A, 2014, 89: 022307
61 Yin H L, Zhou M G, Gu J, et al. Tight security bounds for decoy-state quantum key distribution. Sci Rep, 2020, 10: 14312
62 Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature, 2018, 557: 400–403
63 Wang X B, Yu Z W, Hu X L. Twin-field quantum key distribution with large misalignment error. Phys Rev A, 2018, 98: 062323
64 Xie Y M, Lu Y S, Weng C X, et al. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. PRX Quantum, 2022, 3: 020315
65 Zeng P, Zhou H, Wu W, et al. Mode-pairing quantum key distribution. Nat Commun, 2022, 13: 3903