

Quantum NETwork: from theory to practice

Kun FANG*, Jingtian ZHAO, Xiufan LI, Yifei LI & Runyao DUAN*

Institute for Quantum Computing, Baidu Research, Beijing 100193, China

Received 3 January 2023/Revised 12 May 2023/Accepted 16 May 2023/Published online 5 July 2023

Abstract The quantum internet is envisioned as the ultimate stage of the quantum revolution, which surpasses its classical counterpart in various aspects, such as the efficiency of data transmission, the security of network services, and the capability of information processing. Given its disruptive impact on the national security and the digital economy, a global race to build scalable quantum networks has already begun. With the joint effort of national governments, industrial participants, and research institutes, the development of quantum networks has advanced rapidly in recent years, bringing the first primitive quantum networks within reach. In this work, we aim to provide an up-to-date review of the field of quantum networks from both theoretical and experimental perspectives, contributing to a better understanding of the building blocks required for the establishment of a global quantum internet. We also introduce a newly developed quantum network toolkit to facilitate the exploration and evaluation of innovative ideas. Particularly, it provides dual quantum computing engines, supporting simulations in both the quantum circuit and measurement-based models. It also includes a compilation scheme for mapping quantum network protocols onto quantum circuits, enabling their emulations on real-world quantum hardware devices. We showcase the power of this toolkit with several featured demonstrations, including a simulation of the Micius quantum satellite experiment, a testing of a four-layer quantum network architecture with resource management, and a quantum emulation of the CHSH game. We hope this work can give a better understanding of the state-of-the-art development of quantum networks and provide the necessary tools to make further contributions along the way.

Keywords quantum network, quantum internet, quantum network architecture, quantum network protocol, quantum network simulation, quantum software toolkit

Citation Fang K, Zhao J T, Li X F, et al. Quantum NETwork: from theory to practice. Sci China Inf Sci, 2023, 66(8): 180509, <https://doi.org/10.1007/s11432-023-3773-4>

1 Introduction

The internet has become a truly global phenomenon that drives the growth of the digital economy across international borders and alters our way of life in ways that nothing else has. We can attend international conferences online, read news from around the world, and even compute on the cloud. The idea of the quantum internet aims to expand these possibilities further with the integration of quantum technologies. With the proper use of quantum features, such as interference, superposition, and entanglement, quantum internet can greatly improve the capability of information processing, the security of information transmission, the precision of information synchronization, and even accomplish tasks impossible in classical networks [1–12]. Particularly, it is anticipated that the creation of a fully-fledged quantum internet will have a wide range of fascinating applications. The most well-known is quantum key distribution (QKD), a cryptographic paradigm whose security is ensured by the laws of physics [13, 14]. It can also support other security-related applications, such as blind quantum computation, which enables users to delegate a computational task to a quantum computer without disclosing the computation details to the cloud server [15]. Given long-distance quantum entanglement, a quantum internet would also enable more precise time synchronization that would help to improve the current navigation systems [16] and facilitate new fundamental tests for a deeper understanding of the universe [17]. Distributed quantum computation is also promising in the long run. As the computational power grows exponentially with the number of quantum computers connected, we may exploit such power to handle computationally

* Corresponding author (email: fangkun02@baidu.com, duanrunyao@baidu.com)

demanding problems, such as weather forecasts and protein folding, that are beyond the capabilities of classical computers or individual quantum computers [18–20].

Given the potential impact that a quantum internet could have on the economy and society, national governments, industrial participants, and research institutes are currently conducting extensive research and development on quantum networks worldwide. It is clear that quantum internet research has reached a national level. In 2016, China launched the world's first quantum communications satellite [21–23] and established the world's first trunk line for secure quantum communications between Beijing and Shanghai [24, 25], contributing to the initial steps to make the global quantum internet a reality. China has also included quantum internet technology in its 14th Five-Year Plan for National Informatization as one of the strategic core technologies for future development¹⁾. Since 2019, all 27 EU Member States have signed the European Quantum Communication Infrastructure Declaration, demonstrating their support for the initiative and aiming to boost the European capabilities in quantum technology, cybersecurity, and industrial competitiveness²⁾. In 2020, the National Quantum Coordination Office in the White House published A Strategic Vision for America's Quantum Networks, outlining five-year and twenty-year objectives for the development of quantum internet³⁾. Besides, countries such as Australia, Japan, and Russia, have all actively made their moves for the quantum internet. The potential of quantum internet has also attracted numerous industrial participants. Among these are the traditional tech giants such as Baidu and Amazon, the world's biggest telecommunication companies such as AT&T, BT, and NTT, manufacturing companies such as Toshiba and Cisco, and a series of start-ups including Qunnect, evolutionQ, Aliro Quantum, Xanadu, and QuantumCTek. A majority of these companies are concentrating their efforts on developing quantum cryptography applications that are ready to implement with current quantum technologies, such as quantum random number generation and QKD. Part of them also plan for the long run and study use cases in a more advanced stage of the quantum internet. A more detailed list of global efforts in quantum networks is summarized in Appendix A.

There is a comprehensive review paper by Wehner et al. [2] giving a roadmap for the development of quantum internet, that includes six phases. We are currently stepping from the first stage to the second. The state-of-the-art quantum networks are mostly aimed at proof-of-concept experiments for quantum physics and the preliminary demonstration of quantum cryptography tasks. The scalability of such networks is largely based on trusted repeaters, where no end-to-end quantum communication actually happens. Compared to a classical network, we are still at a primitive stage where we can merely start to entangle different quantum devices at a small distance in the laboratory [26]. Fully functional quantum networks capable of transmitting and controlling entangled quantum states in the field are still under development, the success of which requires sustained and concerted efforts in physics, computer science, and engineering. Recently, extensive studies have been done to connect multiple quantum devices and improve their efficiency and scalability. There is also a Quantum Internet Research Group established in the well-known Internet Engineering Task Force by leading experts, focusing on the design of quantum network architectures and core topics such as routing, resource allocation, connection establishment, interoperability, security, and API (application programming interface) design [27–29].

The structure of a quantum internet can be much more complex than its classical counterpart. In addition to the usual network performance metrics such as bandwidth, delay, throughput, and packet loss rate, quantum factors such as fidelity, success probability, and coherence time should also be considered. The interplay of tons of parameters makes the designing and testing of quantum network protocols beyond the scope of conventional mathematical frameworks. To address this, various quantum network simulators have been released, among which are the general simulators such as NetSquid [30], SeQÜeNCe [31], QuISP [32], and SQUANCH [33], as well as specialized simulators such as qkdX [34] and QuNet [35]. As quantum networks are still being explored, there are numerous unknowns, but also ample opportunities for innovation. Quantum network simulators can operate on both classical and quantum devices, supporting higher-level quantum network applications. They serve as efficient testbeds for verifying ideas and can significantly reduce trial-and-error costs. Furthermore, they offer an effective approach to making quantum technology more accessible, particularly since quantum hardware devices are typically unaffordable

1) 14th Five-Year Plan for National Informatization. <https://www.gov.cn/xinwen/2021-12/28/5664873/files/1760823a103e4d75ac681564fe481af4.pdf>.

2) The European Quantum Communication Infrastructure (EuroQCI) Initiative. <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>.

3) A Strategic Vision for America's Quantum Networks. <https://www.quantum.gov/wp-content/uploads/2021/01/A-Strategic-Vision-for-Americas-Quantum-Networks-Feb-2020.pdf>.

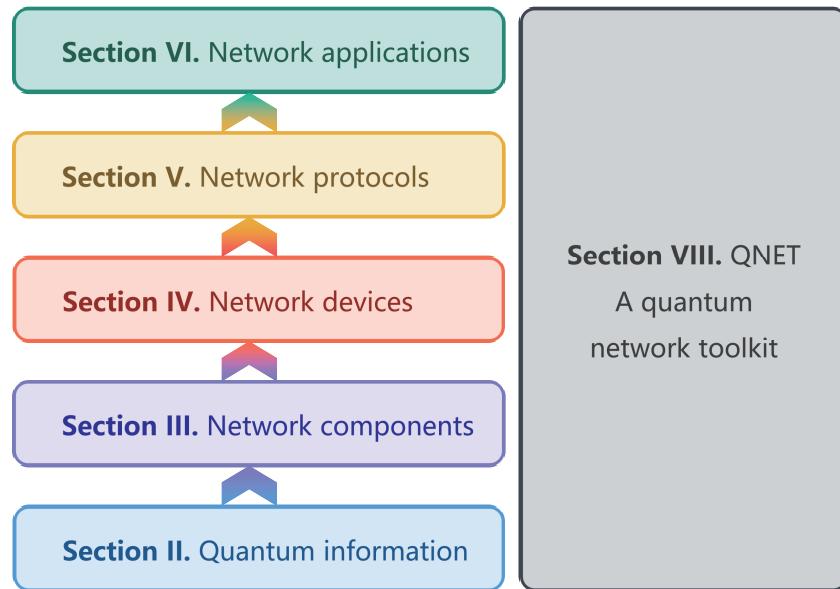


Figure 1 (Color online) Structure of key contents in this work. The left part is a review of quantum networks, from the underlying principles all the way to the applications. The right part is the introduction of our software practice in quantum network simulation.

for most users.

This work aims to provide an up-to-date review of the field of quantum networks from both theoretical and experimental perspectives. As the building blocks for more advanced quantum networks are still under development in the laboratory, and the corresponding applications are still being explored, we introduce a newly developed software toolkit called QNET⁴⁾. This toolkit serves as an efficient testbed for quantum network innovations. We hope that this work can offer a better understanding of the state-of-the-art development of quantum networks and provide the necessary tools to make further contributions along the way. It should be useful to people unfamiliar with the field and can also serve as a reference for those already working within it. The remainder of the content is organized as follows (see also the structure in Figure 1). In Section 2, we give a gentle introduction to the basic concepts of quantum information science, laying the theoretical foundations for the understanding of quantum networks. In Section 3, we introduce the key components that make up a quantum network, including different categories of quantum nodes and the communication links connecting them. Quantum networks necessarily operate on a set of infrastructures comprising hardware, software, and applications. In Section 4, we introduce the hardware part of a quantum network by some essential devices. In Section 5, we go to the software part by discussing quantum network architectures and relevant protocols. In Section 6, we discuss some representative applications in quantum cryptography, quantum computing, and quantum sensing. In Section 7, we give a brief summary of the challenges of developing a fully functional quantum network. In Section 8, we introduce the key techniques in QNET, its basic usage, and several featured demonstrations. Finally, a conclusion is given in Section 9, and some technical details in the main text are delegated to the appendices.

2 Quantum information in a nutshell

In this section, we discuss some prerequisites of quantum information that are necessary for understanding the working mechanism of quantum networks. Readers who are already familiar with these concepts may skip this part and jump to the later sections.

Quantum bit and superposition. Central to the superiority of a quantum internet is the ability to process quantum bits (qubits). A qubit is a two-level quantum system that can be physically implemented by different approaches, such as the polarization of a photon [36], the current of a Josephson junction [37], and the spin of an electron [38]. Every qubit is associated with a state, which represents the current

4) The name QNET is derived from the abbreviation of Quantum NETwork.

status of the system. But different from the binary choice of a classical bit, a qubit can possess a state beyond 0 or 1. This phenomenon is called quantum superposition, one of the fundamental principles of quantum mechanics. More specifically, besides the state of 0 or 1 (or $|0\rangle$ or $|1\rangle$ in the Dirac notation), a qubit can possess a state that is the linear combination of these isolated states, such as $\alpha|0\rangle + \beta|1\rangle$ for any complex numbers α and β with $|\alpha|^2 + |\beta|^2 = 1$. Simply speaking, any unit vector in a two-dimensional complex vector space represents a state of the qubit. We can also map these states to points on the unit sphere, known as the Bloch sphere. In this perspective, a classical bit could only be at one of the two poles, where $|0\rangle$ and $|1\rangle$ are located; but a qubit can appear at any point on the sphere. This difference can become even more significant as the number of qubits increases. Generally, while n classical bits can only encode one of the 2^n possible states at a time, n qubits can coherently encode all 2^n states through superposition. This remarkable phenomenon enables the possibility of parallel information processing and eventually underpins the speedup of quantum computation [39–44].

Quantum entanglement. Quantum entanglement is another striking feature of quantum mechanics, revealing the quantum nature in the multipartite scenario. Two features of entanglement make it an ideal resource for quantum networks. First, entangled states can be strongly correlated such that the measurement outcomes of two qubits can always be matched, even though their outcomes are completely random. For example, if two parties share a Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$, by measuring each of the two qubits independently, one obtains a random distribution of 0 and 1 with equal probability. However, if the outcomes of the two independent measurements are compared, one observes that every time the measurement of a qubit yielded 0, so did the measurement of the other qubit, and the same happened with outcome 1. Remarkably, such coordination is independent of the distance between the separated parties, making entanglement an ideal resource for data synchronization (e.g., in entanglement-based QKD [14], clock synchronization [16]) and transmission (e.g., in the quantum teleportation protocol [45]). Second, due to the inherent property of monogamy, entanglement cannot be shared with a third party. This underpins the security of entanglement-based or device-independent types of QKD and many other quantum cryptography applications [46]. Despite being spooky and counter-intuitive, the existence of quantum entanglement has been rigorously confirmed by plenty of experiments [47–55]. Notably, a Nobel Prize in Physics was awarded in 2022 to Alain Aspect, John F. Clauser, and Anton Zeilinger for their pioneering work in this direction⁵⁾.

Quantum measurement. Quantum measurement is a fundamental operation that helps to extract information from a quantum system [56, 57]. A quantum measurement, according to the postulate of quantum mechanics, will collapse the measured quantum state and return a random outcome, the probability of which depends on the measurement operation and the state itself. For instance, if the outcome of measuring a superposed quantum state $\alpha|0\rangle + \beta|1\rangle$ (in the computational basis) is zero, then the qubit collapses into the corresponding state $|0\rangle$ and any further measurement will give zero as the outcome with certainty, regardless of the parameters α, β in the superposed state. As a result, although the superposition principle permits a qubit to retain more than one bit of information, only one bit can be retrieved at a time by measurement. The disruptive nature of quantum measurement makes it difficult to extract information from a quantum state without causing a disturbance. This, however, happens to make qubit an ideal information carrier for the defense against attackers. Besides information extraction, quantum measurement can also be leveraged to steer quantum computation in the measurement-based model [58], which lays the foundation for blind quantum computation, one of the most important applications in a quantum internet [15].

No-cloning theorem. Unlike classical information that can be readily duplicated, the no-cloning theorem states that it is impossible to create an identical copy of an arbitrary and unknown quantum state [59]. That is, there exists no unitary transformation U such that $U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle$ for any $|\varphi\rangle$, where $|0\rangle$ is a blank quantum state. This results in both advantages and limitations. On the one hand, the no-cloning theorem guarantees that information embedded in a quantum state cannot be easily stolen by a malicious party because the intercepted qubits cannot be copied, and extracting the information by quantum measurement will inevitably disturb the state and be detected. This underpins the security of many quantum network applications, such as QKD [13]. On the other hand, no-cloning makes quantum information processing much more challenging than its classical counterpart. For instance, techniques for classical information processing, such as signal amplification and retransmission, cannot be directly applied to quantum networks, making it necessary to find new schemes to counteract losses and errors.

5) The Nobel Prize in Physics 2022. <https://www.nobelprize.org/prizes/physics/2022/press-release/>.

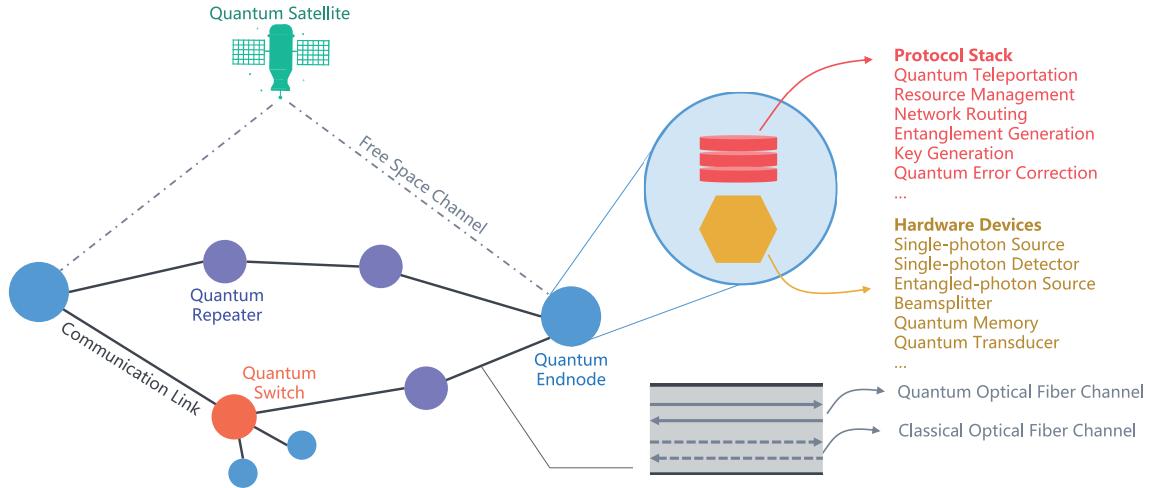


Figure 2 (Color online) Illustration of a quantum network and its key components. A quantum network comprises a collection of quantum nodes and communication links between them. Typical quantum nodes include quantum endnodes, quantum repeaters, quantum switches/routers, and quantum satellites. Each node is equipped with a protocol stack and relevant hardware devices that work together to provide network services. Communication links can consist of both classical and quantum channels connecting two ends for data transmission.

3 Quantum network components

A quantum network will work synergistically with the existing classical internet, but it also demands some extra quantum components to support new applications and services. These primarily include different categories of quantum nodes and communication links connecting them. Depending on the role it plays, a quantum node can be a quantum endnode, quantum repeater, quantum switch, quantum router, and quantum satellite. As classical information processing is always indispensable, we assume that every quantum node has the capability of classical computation built-in. On top of this, every quantum node should contain both the software and hardware parts, particularly a protocol stack defining the rules of information exchange and quantum hardware devices responsible for the implementation of specific requests. As for the communication links, they may consist of classical or quantum channels, depending on the type of information to propagate. In the following, we highlight the basic components required to construct a quantum network. An illustrative diagram of these components and their relationships is depicted in Figure 2.

Quantum endnode. The quantum endnode usually represents a user or client who can send or receive quantum information. It can also be a cloud server that provides quantum computing services to the public. These nodes typically play the role of the source or destination of a service request. For instance, a request is started by a quantum endnode and travels through intermediary nodes before reaching the destination endnode. This request is subsequently handled by the target endnode in accordance with the applicable protocols, and it is then sent back to the initiator. Finally, end-to-end quantum services can be accomplished by repeating these transactions back and forth. A quantum endnode (as well as other nodes) typically contains two types of qubits: communication qubits for generating entanglement with distant nodes and memory qubits for data storage and computation. Depending on the use cases, a quantum endnode can be equipped with very simple devices consisting of barely a photon source or a photon detector. Such an endnode can work with applications like QKD. To support sophisticated applications such as blind quantum computation, a quantum endnode may require durable quantum memories and fault-tolerant quantum computers.

Quantum repeater. Because of the environmental noise and channel attenuation, information can readily be contaminated and get lost over a long distance transmission. In particular, quantum communication requires the transmission of fragile photons that cannot travel indefinitely in fibers or through the air. The longer the distance, the more likely they will be absorbed or scattered. This issue is resolved in classical networks by repeaters that can copy and amplify the received signals for further transmission. As for quantum networks, information carried in qubits cannot be copied or amplified due to the no-cloning theorem [59], making classical repeaters not applicable for quantum communication. To overcome the barrier of long-distance qubit transmission, quantum repeaters were introduced [60].

These nodes are deployed in the middle of endnodes to divide the whole transmission line into smaller segments, thereby reducing the distance of direct transmission to an acceptable range. Depending on the underlying mechanism, there are at least two types of quantum repeaters in principle [61–69]. The first type starts with the generation of long-range entanglement through a combination of protocols, such as herald entanglement generation, entanglement swapping, and entanglement distillation. Then quantum information is transferred via quantum teleportation with the established entanglement (more discussions on these protocols will be given in Section 5). The second type relies on the techniques of quantum error correction that directly encode the quantum information in a block of physical qubits and send it toward the next hop. For the time being, the practical use of quantum repeaters is still hindered by the challenges of simultaneously realizing and integrating all the key capabilities [70]. In particular, the first type of quantum repeater requires entanglement generation for the elementary links in a heralded way; that is, one has to know when the entanglement has been successfully established. It also requires durable quantum memories to temporarily store the established short-range entanglement so as to perform entanglement swapping when two adjacent entangled pairs are both ready. The second type of quantum repeater can be much more efficient in time but requires joint manipulation of numerous qubits and higher initial fidelity of the transmitted states (refer to the threshold theorem [71]). Besides what has been mentioned, a hybrid quantum repeater that combines different approaches can also be considered [62, 72]. Although practical quantum repeaters do not yet exist, several lab experiments involving networks of two or three nodes have made some progress [26, 73–75]. It is also worth noting that trusted repeaters are frequently used as a temporary solution at the current stage, for example, in the Beijing-Shanghai Trunk Line, the Tokyo QKD network, and many other networks in the field, where no end-to-end quantum communication actually happens [76]. Photons that arrive at the trusted repeaters are measured, and fresh photons in the right state are sent toward the next repeater station in the chain. While trusted repeaters do help to extend the applicable distances for specific applications, they are essentially classical and will compromise the security of the network.

Quantum satellite. Due to the photon loss, the effective distance of photon transmission in optical fibers or terrestrial free space is limited to a few hundred kilometers. Quantum repeaters on the ground may extend the communication distance to a few thousand kilometers. To further expand the coverage of quantum networks and realize a truly global quantum internet, quantum satellites and space-based links should be exploited [77, 78]. In this case, most of the photons' propagation paths are in a vacuum, and thus the photon loss and decoherence can be significantly reduced. In 2016, China launched the first quantum communications satellite, successfully demonstrating its integration with ground-based networks and the distribution of secure keys and quantum entanglement at space scales [21]. In 2022, the first micro-nano quantum satellite has also been launched by China, which is smaller but more efficient in its performance⁶⁾. Stimulated by these outstanding results, other countries such as Austria [79], Germany [80], French [81], Singapore [82], Canada⁷⁾, and the United Kingdom⁸⁾, are all making efforts in building and launching their quantum satellite missions, especially nanosatellites that helps to reduce cost and development time. Despite significant progress, there remains plenty of room for improvement in both science and engineering aspects [21]. First, the propagation of quantum signals through free space is prone to atmospheric turbulence and weather conditions, significantly limiting the practical application of quantum satellites. New technologies to release the constraints of working conditions for quantum satellites are desired. Second, compared to the classical satellite, quantum satellites require adapting the existing optical tracking techniques to the needs of quantum communication and building devices that can operate in a satellite without the need for heavy maintenance. Third, a constellation combining low-earth-orbit and high-earth-orbit quantum satellites is necessary for constructing a global-scale quantum network. While more satellites with varying orbital altitudes should be launched, the cost of manufacture is also an important consideration to take into account.

Quantum switch/router. In a classical network, information can be transmitted when two users are directly connected by a communication link. However, as the number of users grows, it becomes impractical to connect every pair of users via a physical link. Switches are then created as central nodes to facilitate information exchange by connecting various network users. A quantum switch would play a

6) China's new quantum satellite now operational. <http://english.news.cn/20220728/5c79b61cc5084819994ee3d5479fc160/c.html>.

7) Quantum Encryption and Science Satellite (QEYSSat). <https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp>.

8) Satellite quantum key distribution for space. <https://www.quantumcommshub.net/wp-content/uploads/2020/09/QCH-Satellite-Quantum-Key-Dist-for-Space.pdf>.

similar role by linking several users to it and attempting to establish multipartite quantum entanglement, such as Bell states or general Greenberger-Horne-Zeilinger (GHZ) states [83], among them. The entanglement switching mainly involves two steps. First, bipartite entanglement between the user and the switch is created in parallel. Second, local operations and measurements are carried out on the bipartite entangled states to produce multipartite entanglement for a set of users. In this sense, a quantum switch can be considered a multipartite generalization of a quantum repeater, but it should also include routing logic to determine the best route to switch and the capability of resource management to handle multiple requests. Because of the decoherence and limited size of quantum memories, prioritizing entanglement switching affects the switch's performance, such as the fidelity of the distributed entanglement, the latency of the entanglement requests, and the throughput of the switch. Some analytical studies on the interplay of these factors have been given in [84–87].

Communication link. A link represents the connection between two nodes in the network. It is usually referred to as a topological concept and should contain specific classical or quantum channels for the actual information transmission. Classical channels in a quantum network are the same as those in a classical network and are responsible for transmitting classical messages between the nodes they connect to. Quantum channels, however, are responsible for transmitting quantum information. Given that quantum teleportation allows the transmission of quantum states by consuming shared entanglement, a link may also refer to the nonlocal correlation of quantum entanglement between different nodes.

4 Quantum network devices

In this section, we investigate the hardware part of a quantum network, which is responsible for the physical implementation of all kinds of quantum services and applications. We will put our focus on the discussion of quantum devices, particularly, sources for photon emission and entanglement generation, detectors for information readout, quantum transducers for signal conversion, quantum memories for data storage, and quantum channels for photon transmission. Before proceeding to their details, we remark that devices responsible for classical computation and communication also play a significant part in quantum networks and that their performance can constitute a bottleneck for the overall efficiency of the network⁹⁾. However, these are beyond the scope of this work. More in-depth discussions on the hardware aspect of quantum networks can refer to [7, 12] and references therein.

Single-photon source. Different from coherent or thermal light sources, a single-photon source is a device that emits single photons. Such a device is needed in QKD and other quantum cryptography applications because multi-photon pulses would compromise security by allowing eavesdroppers to collect information, e.g., by the photon-number-splitting attack [88]. An ideal single-photon source should meet the following criteria: a single photon can be emitted with certainty and on demand; vacuum or multiple-photon emission occurs with zero probability; successively emitted photons are indistinguishable; and the repetition rate is arbitrarily large. Apparently, deviations from these ideal features are always present in reality. These deviations lead to the performance metrics, most importantly, the frequency that determines the repetition rate of the light pulse emission, the wavelength and bandwidth that define the intrinsic attributes of the released photons, and the mean photon number that represents the average number of photons per signal pulse. In terms of physical realizations, two distinct technologies have been explored [89, 90]. The first one is deterministic sources, also referred to as on-demand sources, that can be realized in systems such as semiconductor quantum dots [91–94], mesoscopic quantum wells [95], single molecules [96–98], single atoms [99], single ions [100, 101], and color centers [102–104]. The other is probabilistic sources, which can be realized by weak lasers [105], atomic cascades [106], and parametric down-conversion [107, 108]. These sources emit photons in pairs so that the detection of one photon heralds another photon. The distinction between deterministic and probabilistic sources can be blurred in practice. Deterministic sources can become more probabilistic with the decrease of extraction loss and coupling efficiency, and probabilistic sources can become more deterministic by multiplexing [109]. Although perfect sources are not achievable in reality, significant advancements have been made towards ever-improving approximations [110, 111]. The state-of-the-art source can generate a single photon on demand with a probability of 57% at a repetition rate of 1 GHz and with average two-photon interference visibility of 97.5% [112]. Another recent experiment successfully yields single-photon source characteristics

9) A coordinated approach to quantum networking research. <https://www.quantum.gov/wp-content/uploads/2021/01/A-Coordinated-Approach-to-Quantum-Networking.pdf>.

such as a single-photon purity of 99.8% and indistinguishability of 92.6% by tailoring solid-state single-photon sources with stimulated emissions [113].

Single-photon detector. A photon detector is a highly sensitive device that converts incoming photons into electrical signals and is capable of detecting and specifying the arrival times of individual photons [90, 114]. An ideal detector should meet the following criteria: the probability that the detector successfully detects a photon when it arrives is one hundred percent; the rate at which the detector is triggered in the absence of any incident photons is zero; the time after a photon-detection event during which the detector is incapable of detecting a photon is zero; and the variation from event to event in the delay between the input of the optical signal and the output of the electrical signal is zero. Deviations from these ideals negatively impact experiments in various ways, and thereby the performance of a detector is usually characterized by a set of metrics, including detection efficiency, dark count rate, dead time, and timing jitter. Besides photon detection, an ideal photon detector should be able to distinguish the number of photons in an incident pulse, which is referred to as the photon-number resolution. While non-photon-number-resolving detectors can be realized by the quantum dot [115], single-photon avalanche photodiode [116], superconducting nanowire [117], and up-conversion technique [118], the more demanding photon-number resolving detectors can be realized by the superconducting-tunnel-junction [119], transition-edge sensor [120], charge-integration technique [121], and quantum-dot optically gated field-effect transistor [122]. The state-of-the-art detectors are made by the cryogenic superconducting nanowire single-photon detectors, whose efficiency can be as high as 98% [123] and timing jitter below 3ps [124].

Entangled photon source. An entangled photon source is a device that produces the entangled states, required for reliable quantum communication and the majority of quantum network applications. An ideal entangled photon source should satisfy the following criteria: at a given time, only one pair of entangled photons is emitted; the emitted two-photon state is exactly the standard Bell state; individual photons emitted in different trials should be indistinguishable from each other; and the photons can be extracted and collected from the source with certainty [125]. There are at least two approaches that are frequently used in realizing entangled photon sources in practice. The first approach is by using the technique of spontaneous parametric down-conversion (SPDC) [126–128], which is a nonlinear optical process in which a strong pump field induces the spontaneous emission of two lower-energy photons (referred to as signal and idler photons). Because SPDC is fundamentally a probabilistic process, the correlations of entangled photon pairs can be revealed only after post-selection, and the conversion efficiency is typically as low as 10^{-6} [129]. Nevertheless, probabilistic entangled pair generation via SPDC remains the most widely used approach, owing mainly to its relative simplicity and versatility. The other approach for making an entangled photon source is using the radiative cascades in single quantum emitters, such as atoms [130] and quantum dots [131, 132]. A state-of-the-art entangled photon source based on quantum dots has been reported in [133] that achieves an entanglement fidelity of 90%, the pair generation rate of 59%, pair extraction efficiency of 62%, and photon indistinguishability of 90%, simultaneously.

Quantum transducer. Transducers are devices that can convert a signal from one physical platform to another. Examples are microphones that convert air pressure into an electrical signal and antennae that convert propagating electromagnetic waves into conducted electrical signals. Quantum transducers are designed to play a similar role by faithfully converting quantum information between different platforms. Extensive efforts have been made in the physics community to investigate schemes and technologies enabling such an interface [8, 134–136]. Of particular importance is the microwave-to-optical transducer [137–139]. On the one hand, superconducting quantum computers, which manipulate quantum information via microwave signals, are one of the most developed approaches to implementing quantum computers. On the other hand, there is broad consensus in the field that optical photons should be used as the information carrier for long-distance communication due to their advantages, such as low interaction with the environment, ease of control with standard optical devices, and high-speed low-loss transmissivity. As a result, a scalable quantum network that connects disparate quantum computers requires a quantum transducer that reliably converts quantum signals between microwave modes and optical modes (used in quantum computing and quantum communication, respectively). However, because the energy (frequency) gap between these two domains exceeds five orders of magnitude, such a microwave-to-optical conversion can be incredibly challenging. The quality of an ideal quantum transducer can be evaluated by its high conversion efficiency, broad bandwidth, low added noise, and high quantum capacity [140]. In terms of conversion efficiency, a state-of-the-art experiment is reported in [141] that achieves a conversion efficiency of 47%. For a more comprehensive summary of quantum transducers, please refer to the recent

review paper [142] and references therein.

Quantum memory. Quantum memory is a quantum analog of classical memory, used to store and retrieve quantum states. It can be of significant use in multiple contexts. One of the simple but potentially important applications is to enhance the efficiency of a single-photon source. Given a probabilistic single-photon source such as parametric down-conversion, one can realize a deterministic source of single photons by detecting a heralding photon in a pair while storing the other one in memory and releasing it on demand. Quantum memories are also indispensable for developing long-distance quantum communication via quantum repeaters. As photons from different entangled sources do not always arrive at the repeater stations simultaneously, quantum memories can be used as a synchronization tool by storing the first arriving qubits and waiting for the later ones, allowing for the effective implementation of entanglement swapping. Moreover, quantum memories can also serve as an essential component in advanced quantum computers to store the intermediate computational results and synchronize data in a distributed computational task. As for physical implementations, quantum memories can be realized through a variety of approaches, such as atomic ensembles [143–146], cold neutral atoms [147], doped crystals [148, 149], and particularly in photonic systems [145, 150–158]. The performance of a quantum memory can be evaluated by metrics such as the probability that the stored information can be successfully retrieved, the fidelity of the retrieved information compared to the original one, the storage time that information can be faithfully retained, and the bandwidth that determines the achievable repetition rates. A state-of-the-art quantum memory that uses silicon vacancies in diamond has been reported in [159] that achieves a lifetime exceeding 2 s at temperatures up to 4.3 K.

Quantum channel. The propagation of quantum information in a network from one end to the other relies on the quantum channels connecting them. These channels can be either optical fiber channels or free-space channels, each of which has advantages and limitations. The former can leverage the well-established network of telecommunication fibers and has the advantage that the environment inside the fiber is relatively stable, thus preserving the coherence of photons. Nevertheless, the distance of direct transmission of quantum states in fibers is significantly restricted because the probability of photon loss grows exponentially with the channel distance [70, 160, 161]. As an example, it would take nearly three hundred years to successfully deliver one photon over a thousand kilometers using a typical standard telecom optical fiber with a loss of about 0.2 dB/km [70]. In contrast, free-space optical communication is less developed but does not have to account for polarization scrambling induced by optical fibers and can typically allow for higher transmission rates. Particularly in satellite communication, most of the photon loss happens lower than 10 km in the atmosphere, leaving most of the photon path as a vacuum with negligible loss of photons and decoherence. Once photons leave the atmosphere, only the dispersion effect is dominated [162]. Thus, the satellite free-space optical channel keeps the quantum information in photons intact and increases the system fidelity and channel capacity, making it an ideal approach to establishing long-distance connections [163]. The drawback of free-space communication is that it is more susceptible to environmental disturbances on the photons (e.g., weather changes), as well as the challenge of stabilizing the free-space coupling using pointing and tracking methods. However, many of these challenges have been overcome in a series of free-space quantum communication demonstrations [164–173]. It is also worth noting that the quality and efficiency of the transmission of quantum information depend not only on the communication channel but also on the coding scheme we use. The ultimate capability of a quantum channel to transmit quantum information is characterized by its channel capacity, which is a fundamental research topic in quantum Shannon theory. Unlike the classical theory, there is currently no efficient algorithm for calculating quantum channel capacity in general. Plenty of efforts have been made in this direction. In particular, the quantum capacity of a lossy channel was determined in [174]. For general quantum channel models, the state-of-the-art results are given by [175–184].

5 Quantum network protocols

Designing a quantum network capable of providing both efficient and stable quantum services to a massive number of users would require the development of a quantum-updated version of the network architecture. In this architecture, the network functionalities should be organized as a stack of layers, each containing specific protocols and interfaces that all hardware and software must comply with. Since quantum networks are still in the early stages of development, there is currently no consensus on a standard architecture yet. Different architectures have been proposed in [27, 29, 185–190], and the fundamental

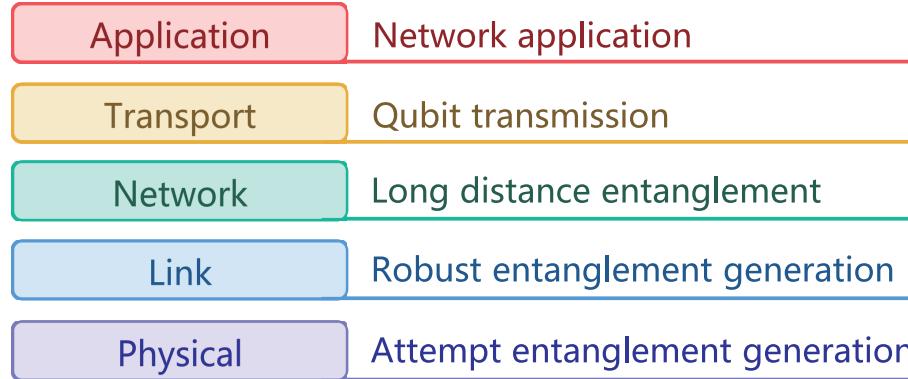


Figure 3 (Color online) Illustration of the TCP/IP (transmission control protocol/internet protocol) architecture used in classical networks and its quantum generalization proposed in [185].

principles have been outlined in [28].

One possible quantum network architecture is similar to the idea of circuit switching in the classical network, where a dedicated communication path is established before the actual data transfer happens [185] (see also Figure 3). More specifically, the lowest element will be the physical layer, which includes all classical and quantum hardware devices and is responsible for the attempt at entanglement generation. The link layer runs on top of the physical layer, aiming to produce robust entanglement between neighboring stations. The network layer will be responsible for creating long-distance entanglement between nodes that are not directly connected, by means of entanglement swapping over short-distance entanglement established from the link layer. The transport layer will be responsible for reliable qubit transmission using quantum teleportation. Finally, the application layer will enable services and applications to use both classical and quantum network capabilities. Besides circuit switching, a different approach widely used in today's internet is called packet switching, in which a message is divided into many parts which are sent independently over whatever route is optimum for each packet, and then get reassembled at the destination (see Figure 4). However, the incapability of quantum cloning and the difficulty of performing quantum error correction make it hard to apply this idea to quantum networks. Nevertheless, a conceptual design for a packet switching quantum network has been recently proposed in [188]. Quantum network protocols and architectures based on quantum graph states and the measurement-based quantum computation (MBQC) model have also been considered in [27, 189, 191, 192].

How future quantum networks will be deployed is yet to be known. But given the nature of quantum information processing and our experience with classical networks, it is conceivable that several building blocks would be necessary. In the following, we introduce some of the most important quantum protocols that could serve as critical components for future quantum network stacks.

Quantum teleportation. In classical packet switching networks, data is duplicated before transmission; if the data is lost, retransmission is done with no harm beyond a performance penalty (refer to the Transmission Control Protocol [193]). With only one copy of quantum data and the restrictions of the no-cloning theorem, we must treat that data with extreme caution. Given the risk of data loss in direct transmission, quantum teleportation provides a technique for reliable transmission of quantum information without physical movement of the object itself [45]. With local operations and shared entanglement resources, quantum teleportation allows transmitting unknown quantum states between two disparate quantum nodes regardless of their physical distance, thereby providing a fascinating strategy for the remote transmission of quantum information in the network. Suppose that the data qubit to teleport is $|\psi\rangle_A$ held by Alice and the shared entanglement between Alice and Bob is given by $|\Phi\rangle_{AB}$. The teleportation starts with Alice's implementation of a Bell state measurement on her data qubit and half of the entangled pair in her possession. Then Alice sends the measurement outcomes, i.e., two random bits of classical information, to Bob. Upon receiving the classical message, Bob performs a corresponding correction that locally restores his state to $|\psi\rangle$. Notably, the information that completely characterizes the data qubit is locally destroyed on Alice's side and reconstructed on Bob's side, ensuring that the no-cloning theorem is not violated. Moreover, as the exchange of classical information from Alice to Bob is necessary, quantum teleportation does not violate the speed of light either. Owing to the noise and errors of direct transmission, quantum teleportation will serve as one of the main approaches to trans-

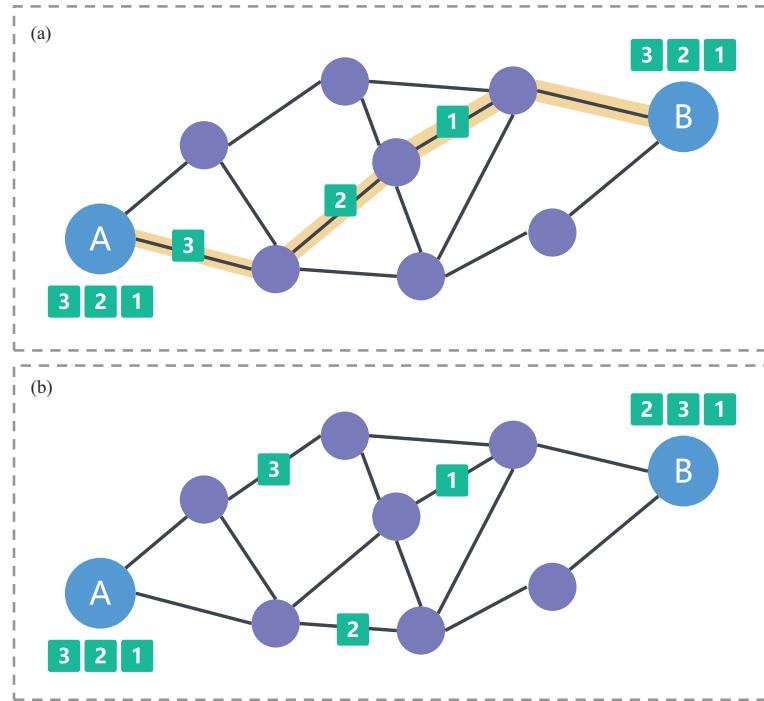


Figure 4 (Color online) Illustration of (a) the circuit switching and (b) the packet switching used in classical networks. Suppose node A wants to send information to node B. In circuit switching, a dedicated circuit path is established before communication occurs. Once set up, all communication takes place over this circuit. In packet switching, no circuit is set up prior to the data transmission. A message is divided into many parts, each of which is routed from the source to the destination as individual packets.

mitting qubits across a quantum network. Experimental determinations of quantum teleportation have been made in different physical systems [194–197] such as photons [198], atoms [199], and electrons [200]. Utilizing the Micius satellite for space-based quantum communication, the cutting-edge experiment sets a record for quantum teleportation at a distance of 1400 km [172].

Entanglement swapping. Quantum teleportation provides a promising approach for remote state transmission by consuming pre-shared entanglement resources. But the preparation of long-range entanglement remains to be solved. Since the distance of direct transmission of entanglement is severely limited by the channel loss, entanglement swapping was introduced to extend the distance by converting multiple neighboring entangled pairs into one long-distance entangled pair [45, 60, 201]. Technically, entanglement swapping can be understood as a variant of quantum teleportation. For instance, given two independent entangled pairs, say, entangled state $|\Phi\rangle_{AB_1}$ between Alice and Bob and entangled state $|\Phi\rangle_{B_2C}$ between Bob and Charlie, a new entangled pair between Alice and Charlie can be created by performing a Bell state measurement on Bob's two qubits, such that qubit B_1 is teleported to Charlie using the entangled link $|\Phi\rangle_{B_2C}$ and its entanglement with qubit A is maintained. After a suitable correction by Charlie upon receiving Bob's measurement outcomes, an entangled pair between Alice and Charlie can be established. Notably, entanglement swapping can be recursively applied in practice to extend the effective distance of entanglement as demanded. Entanglement swapping has received significant attention since its initial proposal in 1998 as a subroutine of a quantum repeater [60], and has been experimentally demonstrated in different platforms under both lab and field conditions up to one hundred kilometers [26, 202–212].

Entanglement routing. Since two endnodes in a network may not be directly connected by a communication channel, data traveling between them would have to pass through a series of intermediary stations. Routing is the procedure used to determine the best route for data transmission across a network. Particularly, given that Bell pairs can be prepared between two adjacent nodes, entanglement routing considers choosing a specific network path to establish long-distance entanglement from the adjacent Bell pairs. Because quantum information suffers from noise and decoherence, some quantum factors, such as fidelity, coherence time, and success probability, should be considered when designing entanglement routing protocols, making them much more involved than their classical counterpart. Routing protocols based on the idea of classical techniques such as the Dijkstra's algorithm are proposed, which should be easy to implement in the near term [213–216]. The essential strategy employed in these studies is first

to create a path using a path selection algorithm with cost metrics tailored to quantum networks. Then entanglement can be distributed along the path. Most of these are centralized algorithms that work under the assumption that each node has information about the entire network, whereas global knowledge about the nodes or the properties of the entangled links may not always be available in practice. Decentralized routing schemes that use only local knowledge about the nodes and their neighbors have been considered in [217–219]. More efforts in considering the scalability and practical limitations of entanglement routing can be found in [220–223].

Entanglement distillation. Quantum entanglement is a critical resource in quantum networks for teleporting quantum information [45], reducing communication complexity [224], and performing quantum cryptography tasks [13, 14]. The reliability of quantum entanglement, however, may be undermined by environmental noise and faulty controls. To counteract such detrimental effects, entanglement distillation, also referred to as entanglement purification, was introduced, aiming to extract high-quality entangled states better suited for application from many copies of the noisy ones [225]. More specifically, entanglement distillation usually starts with sharing many copies of entangled pairs between different parties and then performing unitary transformations on their individual quantum systems. After that, quantum measurements are performed on a portion of the entangled pairs, and the outcomes are shared through classical communication. Unitary transformations can again be performed on the rest of the entangled pairs, conditioned on the measurement outcomes. These processes can be applied recursively as needed. Note that entangled pairs being measured will be destroyed in the process, and when the test fails, the tested state must also be discarded. Consequently, there are three parameters of particular relevance in entanglement distillation: the rate of transformation of primitively entangled pairs into the final pairs, r , the success probability of distillation, p , and the fidelity of the final pairs, F . The interplay of these parameters has been extensively studied in quantum information theory [226–238]. Notably, an “uncertainty” type of relation between the success probability and the fidelity has been recently discovered in [239], indicating that ideal distillation where $p = 1$, $F = 1$ is generically impossible. Experimental advances of entanglement distillation can be found in [240–242].

Quantum error correction. Quantum error correction is a set of techniques used to protect quantum information against noise and errors in both computation and communication. Its main idea is to utilize the redundancy of physical qubits to protect the information of logical qubits. More specifically, quantum error correction maps k qubits into n qubits, where $n > k$. The k qubits are the logical qubits that we want to protect from error, and the extra $n - k$ qubits help to encode the k logical qubits redundantly so that the encoded information is not easily contaminated. Quantum error correction is more sophisticated than its classical counterpart due to the no-cloning theorem, the disturbance of quantum measurement, and the involved quantum error models. In general, error correction codes cannot protect against all possible errors, and they need to be designed to match the most likely types of noise. One of the most famous quantum error correction codes was given by Shor in 1995, which encodes the information of one logical qubit onto a highly entangled state of nine physical qubits, capable of correcting both bit flip and phase flip errors. Since then, quantum error correction has been an extremely active field of research [243–247]. Although the theory of quantum error correction has been worked out in great detail, the experimental difficulties of implementing it remain formidable. Several proof-of-concept implementations have been recently demonstrated in [248–252].

6 Quantum network applications

It is believed that the quantum internet in the future will significantly improve the capabilities of the existing internet in areas such as cryptography, computing, and sensing. Although it is difficult to foresee all its use cases, several representative applications have been identified. In this section, we discuss several quantum internet applications that are of particular interest.

6.1 Applications in quantum cryptography

6.1.1 Quantum key distribution

Public key cryptosystems, such as RSA (Rivest-Shamir-Adleman), are commonly employed for secure data transmission over the internet [253]. However, the security of such systems relies on computational

assumptions, such as factoring large integers is hard for an eavesdropper. Unfortunately, these assumptions can be threatened by advances in hardware and unanticipated algorithms for computation. Shor's quantum algorithm [254] for efficient factorization represents a milestone in this regard. As primitive small-scale quantum computers have already been constructed and their computational power is rapidly growing every year (refer to the quantum Moore's law), the implementation of Shor's algorithm would be expected to happen in the near future, putting the conventional key distribution method and, consequently, the security of relevant applications in great danger. A countermeasure to this is QKD, which encodes secret keys into quantum information carriers for transmission [13]. Thanks to the no-cloning theorem and the disruptive nature of quantum measurement, any eavesdropping on the distributed quantum states will unavoidably be detected. It has been proven that QKD is information-theoretically secure, meaning that the probability of any information leakage can be made arbitrarily small. Such a level of security is solely based on the fundamental laws of quantum physics and is unaffected by future advancements in computing power or algorithms.

While the application of QKD in large-scale quantum networks and high-security scenarios has a promising future (see [255] for a review of the national deployment of QKD networks), there are still numerous theoretical and experimental hurdles to overcome before its widespread commercial use can be realized. In particular, the unconditional security of QKD is based on ideally perfect single-photon sources and detectors. However, ideal devices do not exist in practice, which introduces security risks in the practical implementation of QKD protocols [256]. Designing secure protocols with imperfect devices, such as decoy-state protocols [257–259] and device-independent protocols [260] is of particular importance. The security proof under different attacks and with imperfect devices should also be continuously strengthened [261–264]. Another challenge is the implementation of long-range key distribution with high key rates. One solution to fix the issue is to split a long-distance channel into multiple short-distance channels and connect them with quantum repeaters to expand the effective distance [70]. However, quantum repeaters impose stringent demands on quantum memories, which only provide limited performance at the moment and thus cannot meet the requirements of quantum repeaters yet. An alternative scheme is to replace quantum repeaters with trusted repeaters, but this will sacrifice the security at the middle stations. Another solution to extending the distance of key distribution is given by the technique of twin-field QKD [265, 266], but the distance is still limited to a few hundreds of kilometers. To take the advantage of high secret key rates for continuous-variable QKD systems and long distance for discrete-variable QKD systems, a hybrid approach has also been considered in [267].

6.1.2 *Blind quantum computing*

Blind quantum computing (BQC), also known as secure delegated quantum computing, is a cloud-based quantum computing scheme that enables users to conduct calculations privately without disclosing any information to the server (see [268]). At the very least, there are two ways in which BQC benefits. First, most users will not own large devices (classical or quantum) due to the high cost and the requirement for specialized facilities to host them, making cloud computing the primary delivery mechanism for future quantum computing services. Second, as computational activities may involve sensitive information that the user does not want a third party to know, the blindness of BQC assures that no one in the network, even the service provider, cannot see what algorithm you are running or what data you are trying to process. This is advantageous for governments, non-governmental organizations, and corporations that want to solve computational problems that are politically or commercially sensitive. For example, a manufacturer can simulate an original material design without worrying that the service provider will figure out its secret.

The ideal scenario for implementing BQC would be a verifiable protocol between a client without any quantum capabilities (purely classical client) and a single quantum server. However, it has been shown that one-round perfectly secure BQC in this setting is impossible, i.e., the protocol cannot satisfy both the correctness of the result and the perfect blindness of the client's privacy [269]. There is also negative evidence that BQC is impossible with a purely classical client and a single quantum server [270], even though the problem itself remains open. With these in mind, two relaxed scenarios are considered: a client with minor quantum capability (quantum state preparation or quantum measurement) remotely accesses one quantum server [15, 271–273] or a completely classical client remotely accesses multiple non-communicating quantum servers [274, 275]. The latter is very similar to the source-replacement technique used in entanglement-based QKD, that is, to prepare a quantum state by measuring part of the entangled

states. But the non-communicating assumption might be difficult to guarantee. Some proof-of-concept demonstrations of BQC have been given in [276–278]. However, the lack of practical quantum memories and quantum computers makes it hard to implement large-scale BQC algorithms at present. The frequent classical communication between the client and service may also hamper the performance of BQC in practice, necessitating further improvements on both classical and quantum infrastructures.

6.2 Applications in quantum computing

6.2.1 Quantum leader election

Leader election is a primitive subroutine in distributed computing to avoid data inconsistencies and operation conflicts. It is intimately connected to several fundamental problems in distributed computing, such as the construction of spanning trees and the computation of functions on distributed inputs [279]. The objective of the leader election problem is to select a single leader from a collection of distributed parties. For instance, when there is a writing request, we hope that only one processor in the distributed system will perform this task. If each party possesses a unique identifier, the problem can be handled deterministically by designating the party with the largest identifier as the leader. In the case of anonymous networks, the leader election problem can be handled probabilistically by tossing a coin [280]. However, this approach cannot solve the problem exactly, i.e., in bounded time and with zero error, due to the chance that all parties would receive the same result from independent random bit generators. In fact, it has been proven that there exist an infinite number of graphs for which the problem cannot be exactly solved even with an unbounded (but finite) amount of communication [281–283]. Quantum leader election aims to complete the leader election task with the help of quantum resources. It has been shown that the leader election problem can be exactly solved in $O(n^2)$ rounds with $O(n^4)$ bits of communication for the number n of parties, assuming quantum computation and communication are permitted [280]. This result was further improved in [284] which achieves a round complexity linear in the number of parties, demonstrating significant superiority in the computational power of distributed quantum computing over its classical counterpart. Experimental demonstration of quantum leader election has been conducted in linear optics [285].

6.2.2 Distributed quantum computing

Distributed quantum computing usually refers to the act of performing a quantum computational task on two or more distinct quantum processors and combining the results to produce a complete output [18, 20, 286–289]. Consider a quantum computational task that is divisible into several subroutines. Each of them can be executed on a distinct quantum processor, which may be located at different nodes in a computational network and may exchange data with a central processor. Each processor operates on a partial input with a fixed size, which may be uncorrelated, correlated, or even entangled. When the computation is finished, the central processor collects partial outputs from the other processors and integrates them into a final solution. In a sense, distributed quantum computing effectively combines multiple quantum computers into a single, more powerful system, thereby considerably improving the capability of information processing. When classical computers are unified by means of cloud-based distributed architectures, the net computational capacity is equal to the sum of the components. Quantum computers, however, have fundamentally distinct scaling characteristics: the power of a quantum computer increases exponentially with the number of quantum bits it processes. Consequently, upon integrating quantum devices via a quantum internet, we are left with something significantly more powerful than the sum of its parts. Distributed quantum computing is also applicable at the nanoscale, specifically in designing quantum chips. As the architecture of a single quantum processor approaches its limits, combining multiple processors with classical and quantum communication links could provide a promising solution [288]. In IBM's recent development roadmap, it is considered that getting beyond single-chip processors is the key to overcoming the scalability problem [290, 291]. Nevertheless, the distributed architecture would also introduce new challenges, particularly, the compilation of a quantum algorithm into a distributed manner and the realization of multi-qubit gates across different quantum processing units. Some frameworks for compiling distributed quantum programs have been recently proposed in [292–295], where non-local operations are replaced with local operations on shared entanglement [296, 297]. Advances in the implementation of nonlocal gates across different modules have been reported in [298–300]. From another perspective, distributed quantum computing may also refer to computational tasks that are inherently

distributed [301–305]. One representative example is quantum fingerprinting, where a third-party needs to check the consistency of the other two parties' input. Utilizing quantum superposition, the amount of communication can be exponentially smaller than the comparable classical case [306, 307].

6.3 Applications in quantum sensing

6.3.1 Clock synchronization

A wide range of technologies, such as data transfer networks, financial trading, airport traffic control, telecommunication networks, global positioning systems, and long baseline interferometry, rely heavily on access to a globally agreed-upon standard time, making clock synchronization a critical task on the internet. Conventionally, there are two basic techniques for synchronizing clocks. The usual procedure is Einstein synchronization, which requires an operational line-of-sight exchange of light pulses between two observers [308]. A less popular alternative is Eddington's slow clock transport [309], in which the two clocks A and B are first synchronized locally and then transported adiabatically to their separate destinations. One obvious drawback of these methods is that either light or matter is physically exchanged, making them vulnerable to the quality of the intervening medium (e.g., the atmosphere). In 2000, Jozsa et al. [16] proposed a clock synchronization scheme based on quantum entanglement that leverages pre-shared entanglement between two clocks located at different spatial locations. The intrinsic correlation in quantum entanglement makes it a reliable method for synchronizing clocks regardless of the intervening medium or distance, distinguishing it from the conventional methods. The original two-partite quantum clock synchronization protocol has been improved and generalized to the multi-partite scenarios [310–313]. Experimental verifications of these protocols have been reported in [314–317]. In particular, experimental tests with quantum clock synchronization have shown timing precision up to 51 ps [318]. It is believed that a highly accurate and secure global time distribution network in the future quantum internet would enable many terrestrial applications for scientific exploration, commercial utility, and national defense [319].

6.3.2 Longer-baseline telescopes

For a better understanding of the universe, we need to observe smaller and finer details of astronomical objects. This can be achieved by enlarging the primary mirror of a telescope and thereby increasing its resolution. However, the diameter of mirrors we can manufacture is limited. An alternative approach is using the interferometry technique, which combines telescope arrays into a virtual instrument with a diameter equivalent to the size of the separation between the individual telescopes. By interfering with the light gathered at sites across the array, a synthetic aperture with resolution proportional to the length of the array can be realized [320]. Nonetheless, due to the photon loss during transmission, the baseline lengths of the interferometers are constrained, which subsequently restricts the resolution of the telescopes. One potential method to circumvent the limit is to adopt quantum teleportation-based interference, which was first suggested by Gottesman et al. [17]. Utilizing post-selected quantum teleportation, one can measure the interference visibility (which is a function of the baseline and, according to the van Cittert-Zernike theorem, is the Fourier transform of the intensity distribution of the light source [321]) of all baselines of telescope arrays and image the light source. By introducing quantum repeaters, the photon loss during transmission can be effectively reduced, thus extending the baseline of interferometers. The scheme proposed by Gottesman et al. [17], however, faces several technical challenges. For instance, it demands an extremely high rate of entanglement distribution as well as detectors with high efficiency and time resolution, which seems not feasible at the current stage. To provide a more practicable solution, new schemes have been proposed to reduce the technical requirements [322, 323].

7 Challenges

Despite the promising future of the quantum internet, there are still plenty of problems to overcome before a large-scale quantum network can be realized. These problems can come from various aspects, the most important of which are hardware, software, applications, and ecosystems. In this section, we will have a brief discussion on some of the most important issues.

Hardware. The functionality of future quantum network services and applications depends on the coordinated development of both quantum and classical hardware. Generally, the present quantum

network components have mostly been tested in a lab setting and have not yet been put to use in a full network configuration. However, it can be inferred from classical networks that to create wide-area, operational quantum networks, more capable devices satisfying suitable requirements for reliability, scalability, and maintenance are needed. These include high-rate quantum entanglement sources; robust quantum memory buffers; highly efficient photon detectors; high-speed, low-loss quantum switches; and transducers from optical and telecommunications regimes to quantum computer-relevant domains and vice versa. In addition, the development of classical communication is also important for quantum networks, as classical control information is indispensable for the functionality of quantum network protocols. For instance, the implementation of entanglement swapping and quantum teleportation requires the classical message to do suitable correction; QKD requires the classical message to do key sifting and parameter estimation; and BQC requires the classical message to control the measurement angles of computation. Besides the hardware performance, another thing to consider is the cost. The fact is that current quantum-related devices are extremely expensive and apparently beyond the reach of most users. To make quantum network services widely accessible to the public, their operating and maintenance costs need to be significantly reduced.

Software. The nature of quantum information determines that fundamental operations like information readout and duplication in quantum networks are fundamentally different from those in classical networks. Consequently, a one-to-one mapping from classical network architecture (e.g., TCP/IP or OSI (open systems interconnection)) to quantum networks appears implausible. Instead, a significant paradigm shift is required for the design of a quantum network architecture that exploits the peculiarities of quantum mechanics. This leaves us with tons of challenges in building quantum network architectures for efficient and robust services, developing quantum operating systems for resource and error management, and designing software interfaces for network users [324]. Challenges also include entanglement generation over multiple users, as well as the integration of the existing networks with quantum network technologies for optimal control and management. Despite the fact that several architecture principles have been proposed, it is not yet possible to evaluate, compare, and determine exactly which one is superior in terms of network performance, readiness for implementation, and scalability for large networks. A systematic benchmarking framework with relevant simulation and evaluation tools is in high demand.

Applications. Quantum networks are proven to provide advantages in various aspects, such as computation, communication, and sensing. However, most of the existing applications are hard to realize on current devices with limited performance. Based on the experience with classical networks, the development of network applications and network infrastructure are strongly intertwined. On the one hand, the development of network infrastructure facilitates the creation of suitable applications, while on the other hand, the pursuit of better applications will stimulate the development of network infrastructure. Instead of waiting until the quantum network infrastructure is fully built, it is more important to design applications that work at different stages. This demands the collaboration of theorists and experimentalists, as well as innovations from both network designers and users. The currently known applications are more on the theoretical side to demonstrate the superiority of quantum networks. Yet these are just the tip of the iceberg, and there are tons of real-world application scenarios and use cases in all walks of life that remain to be explored.

Ecosystem. Several prototype quantum networks have been demonstrated in the lab environment. But the transition from the demonstration to the operational infrastructure requires the collaborative efforts of all communities. Particularly, it requires scientific researchers to lay the foundation of quantum network principles; governments and business investors to finance the construction of network infrastructures; and users and customers to actually make use of the services and propose new demands on applications. It is anticipated that existing technologies will be significantly disrupted by the future quantum internet. But from another perspective, the introduction of new things inevitably results in the emergence of new challenges. When large-scale quantum networks become a reality, new issues about security, privacy, ethics, and legislation will arise. For instance, many quantum network applications are proven to be unconditionally secure in principle. But they may not be hack-proof in practice [325]. Before a large-scale quantum network emerges, post-quantum cryptography may also serve as a nice transition to the quantum future [326–331]. With this in mind, an open and sustainable quantum network ecosystem is demanded along with the development of quantum network technologies.

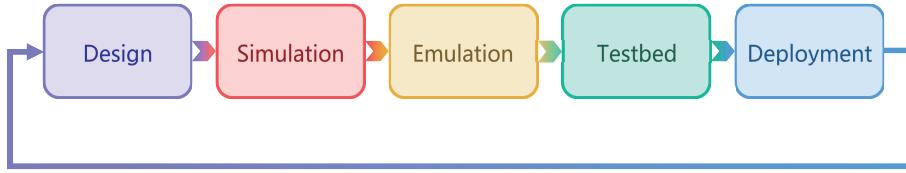


Figure 5 (Color online) Life cycle of a network protocol. A network protocol is born from an initial design and then goes through simulation and emulation steps. After that, the protocol will be evaluated in a small testbed and finally go through the deployment and standardization processes. Sometimes it may also go back to the design step for further calibrations and improvements.

8 QNET: a quantum network toolkit

In the preceding sections, we have discussed the essential components of a quantum network, their current status, and the potential challenges for future development. With these insights in mind, we now introduce a newly developed simulation toolkit that empowers users to gain hands-on experience with quantum networks and explore innovative ideas.

A network protocol, whether classical or quantum, usually goes through several stages from its initial design to the final deployment [332]. As depicted in Figure 5, once a network protocol is born, it will first undergo simulation-level testing to ensure that it performs as expected. The process then advances to the emulation phase, which entails a more comprehensive simulation of both functionality and execution logic. The emulation of a protocol should simulate the working environment of the protocol as precisely as possible and incorporate related hardware devices, either virtually or physically. The protocol will subsequently be implemented on a small testbed to check whether it works properly in practice. If everything goes as expected, the protocol will be deployed and standardized on a large-scale network. Of course, a protocol may also return to the design phase for more calibrations and improvements.

As quantum networks are still under development, a simulation toolbox would be essential for verifying new ideas and reducing possible trial-and-error costs. Here we introduce QNET, a quantum network toolkit [333], which aims to stimulate the design of quantum network protocols, accelerate the testing of quantum network architectures, and facilitate the deployment of quantum internet standards. QNET is an open-source project implemented in Python. An overview of its key modules is presented in Figure 6. The current version (v1.2.0) of QNET mainly contains three layers of functional modules. The bottom layer provides core engines for both quantum computation and network simulation. The middle layer offers tools such as virtual devices and protocols for designing quantum networks with customized topologies. The top layer provides various frequently-used model templates to help speed up the workflow of the research and development on quantum networks. QNET, in particular, contains a fully-featured discrete-event simulation (DES) framework for precise and efficient tracking of quantum network status during simulation. It also features dual quantum computing engines that support simulations in both the quantum circuit model and the MBQC model. Furthermore, QNET provides detailed modeling of the underlying physical devices. Its simulation is fine-grained down to the photon level, enabling verification of real-world quantum network experiments. QNET also provides a solution for compiling quantum network protocols into standard quantum circuits, supporting the simulation of network protocols on real-world quantum hardware devices. With its modular design, QNET can serve as a sandbox for testing different quantum network architectures.

In the remainder of this section, we will go through QNET in more detail. We will first discuss the key techniques for its implementation, followed by a quick-start guide to help to understand its basic usage. Lastly, we will use several featured demonstrations to show how QNET can be used in practice.

8.1 Key techniques

8.1.1 DES

DES is a well-studied modeling technique widely used in problems such as dispatching, resource allocation, capacity planning, and particularly network simulations [332]. A schematic diagram of DES is depicted in Figure 7. In this framework, all changes in the network are regarded as a series of events occurring at discrete time points. These events are then scheduled and processed in chronological order along the timeline. In general, DES has the following characteristics: (1) randomness, i.e., state variables of the simulation system contain random factors; (2) dynamicity, i.e., the time evolution dynamically affects the system status, which may create new events in the future as the current event is executed;

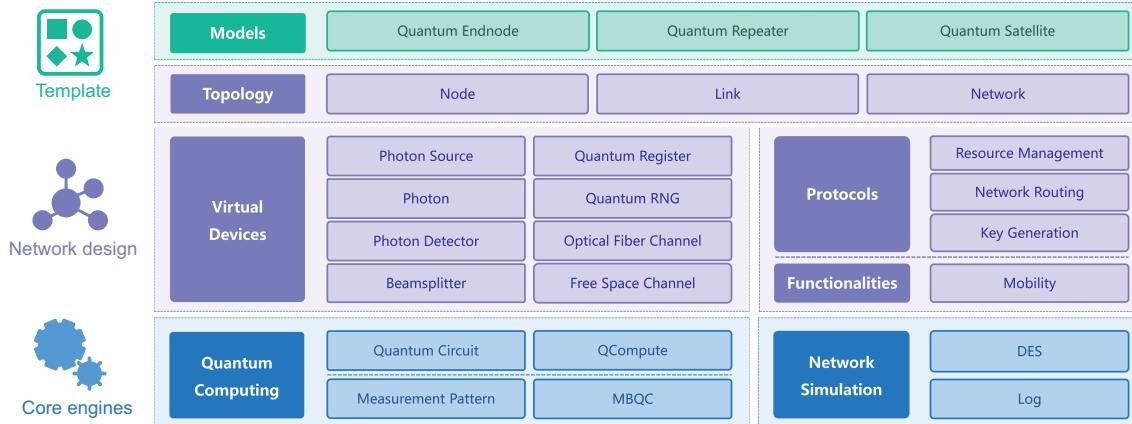


Figure 6 (Color online) Overview of QNET’s key modules (based on version 1.2.0). The bottom layer provides core engines for both quantum computation and network simulation. The middle layer offers tools such as virtual devices and protocols for designing a quantum network with customized topology. The top layer provides the users with various easy-to-use model templates for convenience. A UML (unified modeling language) class diagram laying out the structure of QNET with more details is given in Appendix B. Note that QNET is under active development, and the latest version can be accessed at [333].

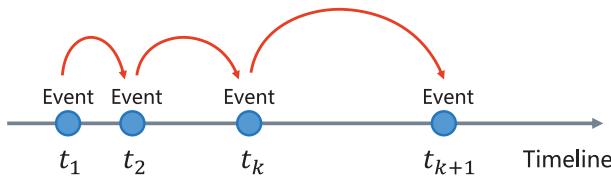


Figure 7 (Color online) Schematic diagram of DES. Every change in the network status is modeled as an event on the timeline. The simulation proceeds from event to event and holds still until the next event happens. The simulation terminates when all events are executed or a termination condition is reached.

(3) discreteness, i.e., the system status only changes when the corresponding event is executed and holds still until the next event happens.

Given that DES is well-suited to network simulation, we develop a fully-featured DES engine in QNET to accurately and efficiently track the system status in quantum network simulation. The design philosophy of our DES engine mostly refers to [332]. In particular, it contains the following key elements: (1) “DESEnv”, i.e., the simulation environment with a built-in timeline that drives the simulation forward; (2) “Entity”, i.e., the main object of the system to simulate, such as an endnode or a physical device; (3) “Event”, i.e., the change of the system status at a particular time, which may include the message transmission and reception among network users; (4) “EventHandler”, i.e., the specific action of an entity or protocol, such as emitting a photon from the photon source; (5) “Scheduler”, i.e., a scheduler that schedules events onto a timeline, usually included as a component in objects that need to schedule events, such as entities or protocols.

The DES technique has been adopted by many quantum network simulators. Unlike SeQUENCe, which delegates event scheduling entirely to the timeline, or NetSquid that regards protocols as virtual entities and allows them to interact directly with the timeline, QNET uses the design of on-demand event schedulers that can be embedded into any object as needed, leaving the flexibility of event scheduling to the users. By default, all components in a quantum network and the network itself are considered entities, each with a built-in scheduler for event scheduling. As a network protocol typically changes the network status and thus needs to schedule events, we set by default that each protocol has a built-in scheduler as well.

A flow chart of the DES algorithm is depicted in Figure 8. This algorithm takes network topology, protocols, and some characteristic parameters as input and finally outputs the statistical results and log files for network analysis. In the beginning, the simulation environment is initialized. This will automatically trigger the initialization of all entities in the environment. Meanwhile, relevant events will be written into the future event list, which is maintained as a specialized tree-based data structure (i.e., heap). An event with the top priority is then fetched from the future event list and gets executed according to the given instructions. In the meantime, new events can be scheduled and pushed into the future event list. Once the processing of an event is complete, the next event is fetched from the

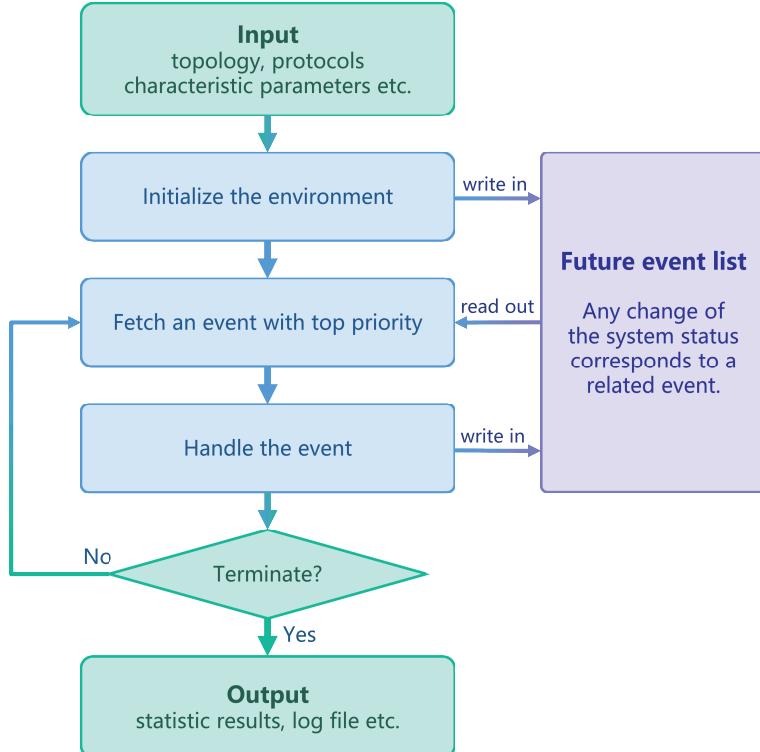


Figure 8 (Color online) Flow chart of the algorithm for the DES. This algorithm takes network topology, protocols, and some characteristic parameters as input and finally outputs the statistical results and log files for network analysis. In the main loop, the algorithm interacts with a future event list that maintains the evolution of the network. At each step, an event with the highest priority is fetched from the future event list and executed according to the given instructions. In the meantime, new events can be scheduled and pushed into the future event list.

future event list and gets executed. The main loop of this algorithm will keep running until all events are executed, or a termination condition is reached.

8.1.2 Dual quantum computing engines

Quantum computation utilizes the peculiar laws of the quantum world and provides a novel and promising way of processing information. The essence of quantum computation is to evolve the initially prepared quantum state into another expected one and then make measurements to obtain the required classical results. However, the approaches to quantum state evolution vary in different computation models. The widely used quantum circuit model completes the evolution by performing quantum gate operations, which can be regarded as a quantum analog of the classical computing model [334, 335]. Another completely different approach is given by MBQC, which is a unique quantum computation model with no classical analog. This model steers the computation by measuring part of the qubits of an entangled state, with those remaining unmeasured undergoing the evolution correspondingly. By controlling measurements, we can complete any desired evolution. More specifically, the computation in MBQC is mainly divided into three steps. The first step is to prepare a resource state, which is a highly entangled many-body quantum state. This state can be prepared offline and independent of specific computational tasks. The second step is to sequentially perform single-qubit measurements on each qubit of the prepared resource state, where subsequent measurements can depend on previous measurement outcomes; that is, measurements can be adaptive. The third step is to perform classical data processing on measurement outcomes to obtain the required computation results. A schematic illustration of MBQC algorithms is shown in Figure 9. The grid represents a commonly used quantum resource state (called cluster state). Each vertex on the grid represents a qubit, while the entire grid represents a highly entangled quantum state. We measure each qubit one by one in a specific measurement basis to drive the computation.

Quantum network architectures based on different computation models have been proposed [27–29, 185, 186, 189, 191, 192], and each architecture admits its own features. For instance, the quantum circuit model has been widely used in current quantum technology. Its working mechanism nicely matches

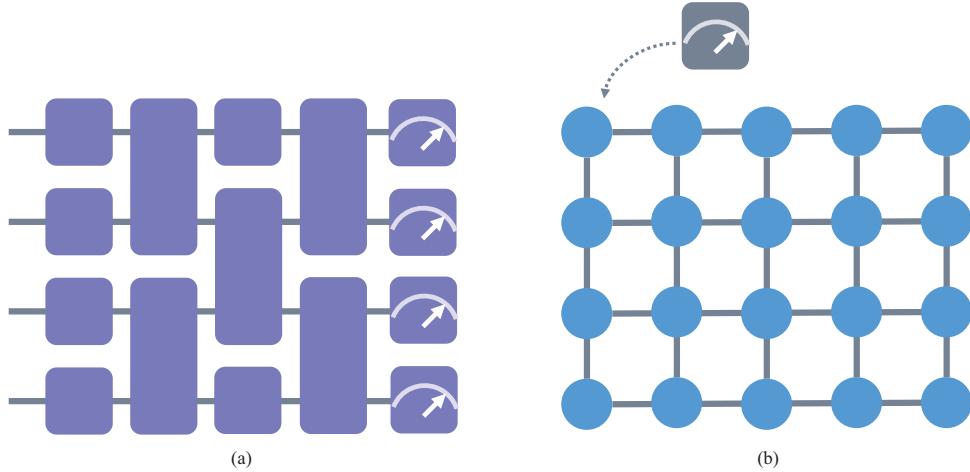


Figure 9 (Color online) Schematic diagrams of two quantum computation models. (a) The quantum circuit model, where computation is accomplished by performing quantum gates, and results are read out by the final quantum measurements; (b) the MBQC model, where the computation is realized by measuring each qubit on a prepared graph state.

our intuition, which facilitates the migration of classical network architectures to quantum networks. On the other hand, the single-qubit measurements in MBQC are much easier to implement in practice, and non-adaptive quantum measurements can be carried out simultaneously, dramatically reducing the computational depth and consequently the effect of decoherence on fidelity. Moreover, the resource states in MBQC can be independent of specific computational tasks, which can be applied in BQC (or secure delegated quantum computing in some literature) for privacy preservation [15, 336, 337]. To better utilize the characteristics of different computational models, it is likely that a hybrid approach will be adopted in the future quantum internet. Therefore, we develop dual quantum computation engines in QNET to support the simulation of both models. In particular, as far as we are concerned, QNET is the first quantum network toolkit that supports the implementation of MBQC algorithms.

As mentioned, MBQC processes the computation in three steps: resource state preparation, single-qubit measurement, and data post-processing. Each resource state corresponds to a graph $G = (V, E)$ where V is the set of vertices and E is the set of edges representing the entangling correlation in the state. Suppose we have a n -qubit resource state on systems V whose m qubits are initialized as $|\varphi\rangle$ on systems $I \subseteq V$ and the rest qubits on $V \setminus I$ are initialized as plus states $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Then the computation can be represented as

$$\left(\prod_{k \in V} M_k \right) \left(\prod_{(i,j) \in E} CZ_{ij} \right) (|\varphi\rangle_I \otimes |+\rangle^{\otimes n-m}), \quad (1)$$

where $CZ_{i,j}$ is a controlled-phase gate on qubits i and j , and M_k is a measurement on qubit k . After the measurements, we obtain a sequence of outcomes and then perform classical post-processing. To simulate the computation according to (1), it is necessary to store the resource state in a vector with a size of 2^n . This exponential memory cost can be a problem when n is larger than several dozen, which is usually the case in practice. To simulate the computational process more efficiently, we design a vertex dynamic classification algorithm (see Algorithm 1) that divides all the vertices into three categories (active, pending, measured) and dynamically maintains these vertex sets as the computation runs forward [338]. The intuition behind this is that single-qubit measurements only affect the evolution of their neighboring qubits. So we can postpone the activation of irrelevant qubits at the current step. It can also be understood as changing the execution order of entanglement and measurement operations to reduce the number of effective qubits involved in the computation and thereby improve storage and computational efficiency. This technique helps to support the simulation of MBQC algorithms up to thousands of qubits in certain cases. More details of our MBQC simulator and its usage can be found in [333]. A quantum machine learning framework on MBQC can also be found in the website¹⁰.

10) Baidu Quantum. Paddle Quantum. <https://qml.baidu.com/tutorials/measurement-based-quantum-computation/measurement-based-quantum-computation-module.html>.

Algorithm 1 Vertex dynamic classification

Input: Graph $G = (V, E)$ of the resource state, initial input state $|\varphi\rangle$ on systems I , measurement operations M_1, \dots, M_n .

Output: Measurement outcomes o_1, \dots, o_n .

```

1. Initialize three empty lists,  $V_p, V_a, V_m$ ;
2. Let  $V_a = I$ ,  $V_p = V \setminus I$ , and the background state  $|\psi\rangle = |\varphi\rangle$ ;
foreach  $k \in V$  do
    3. If  $k \in V_p$ , then append  $k$  to  $V_a$  and remove it from  $V_p$ ;
    4. Find all neighbors of  $k$  in  $G$ , denoted as  $N(k)$ , and compute  $W = N(k) \setminus (V_m \cup V_a)$ ;
    5. Append  $W$  to  $V_a$  and remove it from  $V_p$ ;
    6. Initialize the newly added qubits  $W$  as plus states, take tensor product with  $|\psi\rangle$ , and update the background state  $|\psi\rangle$ ;
    7. Perform quantum gate  $CZ_{j,k}$  on  $|\psi\rangle$  for any  $j \in W$  and update the background state  $|\psi\rangle$ ;
    8. Perform measurement on qubit  $k$  by  $M_k$  and record the measurement outcome  $o_k$ ;
    9. Append  $k$  to  $V_m$  and remove it from  $V_a$ .
end
```

8.1.3 Compilation of quantum network protocols

As mentioned at the beginning of Section 8, a network protocol needs to pass through a number of development stages before it can be deployed to the network infrastructures (see the life cycle of a network protocol in Figure 5). Emulation, which runs quantum network protocols in the actual quantum environment, is a crucial stage that comes before the testbed. By utilizing the power of quantum computers, we can remove the computational bottleneck of simulating quantum networks with classical computers while also optimizing relevant parameters and checking the protocol's performance in the quantum environment.

A number of commercially available quantum computers, such as those based on superconducting or trapped-ion qubits, can now support the implementation of standard quantum circuit programs, consisting of initial state preparation, quantum gate evolution, and final quantum measurement. However, a quantum circuit program is not the same as a quantum network protocol, which features both classical and quantum communications between different nodes (not native to quantum circuit programs). This makes it hard to run a quantum network protocol on the current quantum computers. To solve this, we propose a compilation scheme that maps quantum network protocols onto standard quantum circuits in two steps [339], as shown in Figure 10. In the first step, we compile the quantum network protocols into dynamic quantum circuits with conditional operations. In the second step, we use the principle of deferred measurement to replace classically controlled operations with quantum-controlled operations [56]. Finally, the resulting circuit is a standard quantum circuit that can be delegated to a quantum computer. The difficulty of protocol compilation mainly comes from the first step, as we need to emulate quantum communication on a single quantum device. Here, we propose to treat the spatial transmission of a qubit as the transfer of its ownership from the sender to the receiver. That is, Alice sending a qubit to Bob through a quantum channel can be viewed as Alice handing over the ownership of this qubit to Bob. A pictorial description is shown in Figure 11. In this way, we can simulate the qubit transmission through an identity channel. As for more general noisy quantum channels, they can be simulated by adding suitable gate operations before and after the transmission.

Let us take quantum teleportation as an example. This protocol involves three parties: Alice, Bob, and Charlie. Each of them has its own local operations and will interact through classical or quantum communications (see Figure 10(a)). First, Charlie prepares a Bell state on his two local registers and sends the first qubit to Alice and the second to Bob. Alice prepares a qubit to send (e.g., by a rotation-x gate) and receives the qubit from Charlie, then she takes a Bell state measurement on both qubits and sends the classical outcomes to Bob. Once receiving the qubit from Charlie and classical messages from Alice, Bob performs conditional Pauli operations to restore the qubit that Alice wants to send. By using the idea in Figure 11, QNET automatically compiles this tripartite network protocol into a dynamic quantum circuit, which contains all information about the local operations as well as classical and quantum communications (see Figure 10(b)). Then this circuit will be compiled into an equivalent standard circuit, which can be delegated to a quantum computer (see Figure 10(c)). Notably, all of these compilations are automatically handled in QNET, and users only need to focus on the native descriptions of the network protocols. More technical details about the compilation can be found in Appendix C. To the best of our knowledge, QNET is the first quantum network simulator that supports the compilation of quantum network protocols to quantum circuits as well as the emulation on quantum hardware devices. The other project capable of interacting with quantum hardware is NetQASM, whose public interface to hardware is still under development at the time of writing this manuscript [340].

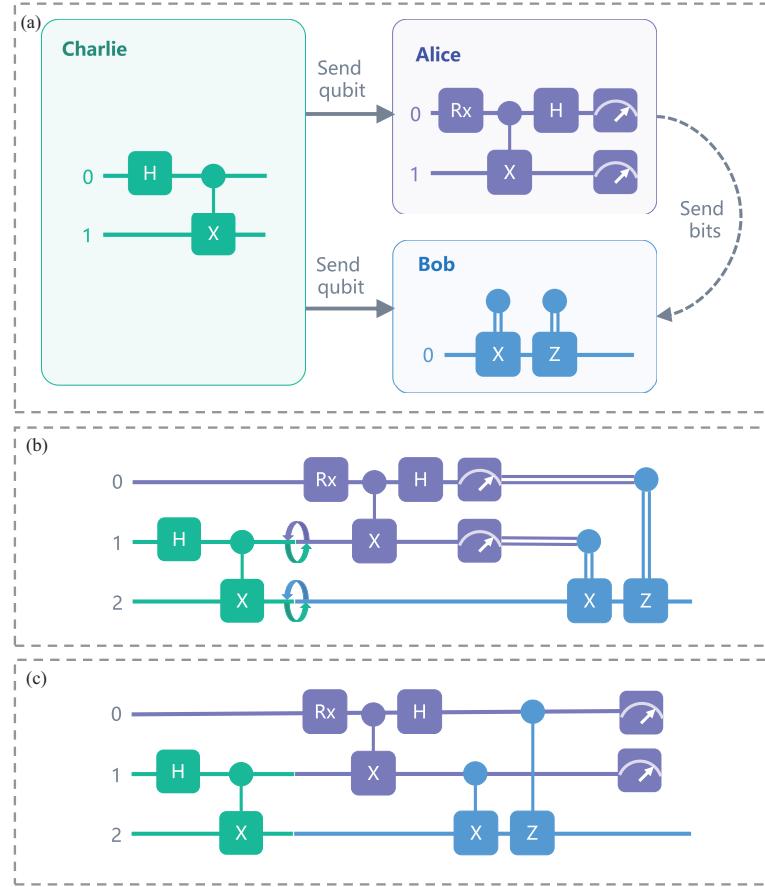


Figure 10 (Color online) Illustrative example of compiling a quantum network protocol into a standard quantum circuit. The first step is realized by replacing the spatial transmission of a qubit with the transfer of its ownership. The second step is done by using the principle of deferred quantum measurement. (a) Quantum teleportation; (b) dynamic quantum circuit; (c) standard quantum circuit.

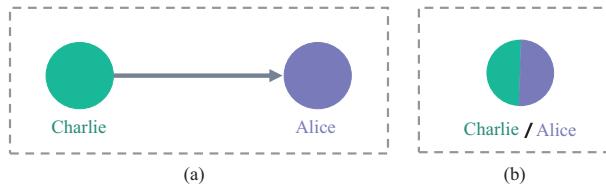


Figure 11 (Color online) Illustration of the qubit transmission in the protocol compilation scheme. (a) The spatial transmission of a qubit from Charlie to Alice through a quantum channel. (b) The perspective of the receiver, Alice. The qubit can be considered to hold its position still, and the transmission corresponds to the transfer of its ownership.

8.2 Quick start guide

In this subsection, we introduce the basic usage of QNET with the corresponding code demonstrations. Note that all the syntax highlighted in the shaded box (e.g., `ABC`) corresponds to the Python codes in QNET. As with a classical network, a quantum network comprises nodes and links. Nodes can install specific physical devices and operate in accordance with the loaded protocol stack, whereas network links usually contain classical and quantum channels between nodes. A quantum network and its components all belong to DES entities in QNET, that is, the corresponding classes, including `Network`, `Node`, `Link`, `Channel`, and other physical devices, all inherit from the class `Entity`. Every entity can add its components using the `install` method. A network, for example, can install nodes and links; a link can install physical channels, and so on. Moreover, we remark that each entity has a built-in scheduler for event scheduling. As a scheduler needs to find the corresponding simulation environment to schedule events on the timeline, users are required to specify the simulation environment whenever instantiating an entity. Otherwise, it will be attached to the default environment. With these basic settings, we can proceed

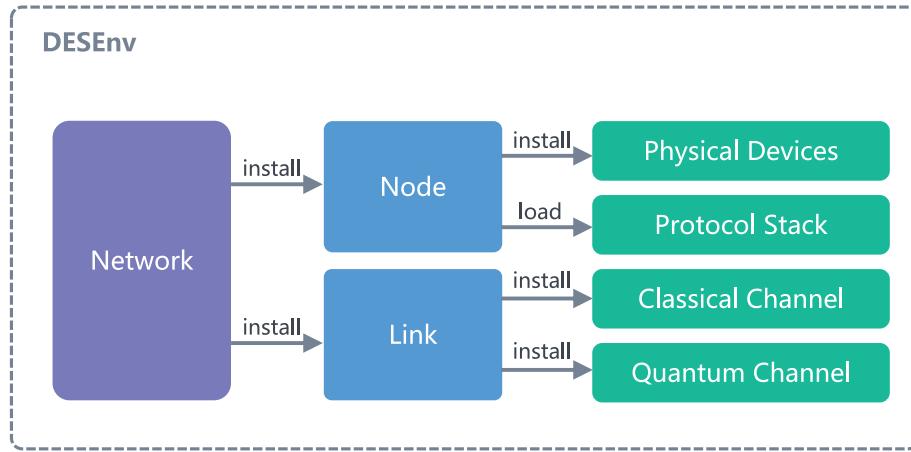


Figure 12 (Color online) Relationship between different network components. DESEnv is the simulation environment underlying all network components. A network is composed of nodes and links, where each node needs to install the necessary physical devices and load a protocol stack, and each link should contain classical and/or quantum channels.

```

from qcompute_qnet.core.des import DESEnv
env = DESEnv("Simulation Env", default=True)
env.set_log(path="./filename.log", level="INFO")
  
```

Figure 13 (Color online) Code example for creating a simulation environment.

```

env.init()
env.run(end_time=8e9, logging=True)
  
```

Figure 14 (Color online) Code example for running the simulation.

to introduce each component in further detail and show how to put them together to form a quantum network. The relationship between different network components is summarized in Figure 12.

8.2.1 Simulation environment

Here we begin with the simulation environment. Before running a simulation, we need first to create a DES environment `DESEnv` that is responsible for driving the simulation of the entire network. Moreover, we can set the simulation environment to default (i.e., set the parameter `default=True`) to allow the entities to attach themselves to the default environment automatically. This can be done by calling the method `set_default_env` as well. In addition, the simulation environment provides a logging function to record critical information during the simulation. We can also specify parameters of the logging function, such as the path of the output file or the level of log records, by `set_log`. A code example is given in Figure 13.

Now we have successfully created a simulation environment and set its configuration. The next step is to construct the quantum network we want to simulate, which will be detailed in subsequent sections. Once this is done, we need to call the `init` method to initialize the environment. This step is mandatory, and it will automatically call the `init` method of each `Entity` for initialization. After this, we can launch the network simulation by calling the `run` method of `DESEnv`. The duration of the simulation can be specified by passing the parameter `end_time` (the time unit is picosecond by default, and the time we talk about here is not the actual CPU time but a virtual time). If no `end_time` is specified, the `run` method will take its default value (which is infinity), meaning that the simulation will keep running until all future events are executed. Moreover, we can set the boolean value of the parameter `logging`, which is `False` by default, to decide whether to output the log files of the simulation. A code example is given in Figure 14.

8.2.2 Network

After the simulation environment, we need to construct a `Network` to group nodes and links. The `Network` inherits from the class `Entity` and will be automatically attached to the default simulation

```
from qcompute_qnet.topology import Network

network = Network("My First Network")
# Approach 1: add nodes and links via the install method
network.install([node1, node2, link])
# Approach 2: load the network topology from a JSON file
network.load_topology_from("filename.json")
```

Figure 15 (Color online) Code example for quantum network configuration.

```
from qcompute_qnet.topology import Node

alice = Node("Alice")
network.install(alice)
...
alice.send_classical_msg(dst=bob, msg=cmsg)
alice.send_quantum_msg(dst=bob, msg=qmsg)
```

Figure 16 (Color online) Code example for creating nodes and sending classical/quantum messages.

```
from qcompute_qnet.devices.source import PhotonSource
from qcompute_qnet.devices.detector import
PolarizationDetector

source = PhotonSource("Photon source")
detector = PolarizationDetector("Polarization detector")
alice.install([source, detector])
```

Figure 17 (Color online) Code example for creating network devices and installing them to a node.

```
from qcompute_qnet.models.qkd.key_generation import BB84
from qcompute_qnet.models.qkd.routing import QKDRouting
from qcompute_qnet.protocols.protocol import ProtocolStack

bb84 = BB84("BB84")
routing = QKDRouting("QKD Routing")
stack = ProtocolStack("QKD Network Stack")
stack.build([(routing, bb84)])
alice.load_protocol(stack)
```

Figure 18 (Color online) Code example for building a protocol stack and loading it onto a node.

environment once instantiated if no specific environment is assigned. The `Network` will be initialized with the environment, which checks relevant network configurations and calculates the routing tables. In this version, we use static routing via the shortest-path algorithm.

QNET provides two approaches to constructing the quantum network topology. The first approach is to create nodes and links manually and add them via the `install` method. The second approach is to load the network topology from a saved JSON file by using the `load_topology_from` method, which installs nodes and links according to the descriptions therein. For users' convenience, the `Network` class allows printing its topology by calling the `print_classical_topology` or `print_quantum_topology` method. A code example is given in Figure 15.

Now we have constructed the framework of a quantum network. The next step is to fill in the nodes and links.

8.2.3 Node

Nodes, such as users and routers in a network, are implemented by `Node` in QNET, which are entities capable of information processing and communication. We can call the `install` method of `Network` to add nodes to it. A node can send classical or quantum messages to the other node by calling the `send_classical_msg` or `send_quantum_msg` method with a specified destination node parameter `dst`. In a DES, calling these methods will actually schedule the corresponding events whose actions are calling methods of `receive_classical_msg` or `receive_quantum_msg` in the destination node for message's receiving. A code example is given in Figure 16.

Install physical devices. After creating nodes, we need to add physical devices to them according to their usage scenarios. For instance, a node for QKD usually contains at least a photon source (e.g., `PhotonSource`) for key encoding or a photon detector (e.g., `PolarizationDetector`) for information readout. These physical devices can be added to a `Node` by calling the `install` method. A code example is given in Figure 17.

Load a protocol stack. Aside from the physical devices, we need to provide the node with relevant software, i.e., protocol stack (`ProtocolStack`), which consists of a collection of protocols (`Protocol`) in a layered structure. As with a classical network, each layer of the protocol stack relates to specific functions that determine the rules of classical and quantum communication. A protocol stack can be customized by splicing different protocols. In QNET, the `ProtocolStack` class provides a `build` method, which allows for building a protocol stack and defining its hierarchical relationships. Once a protocol stack is built,

```

from qcompute_qnet.topology import Link

# Approach 1: use connect to set the ends of a link
link = Link("Alice_Bob")
link.connect(alice, bob)

# Approach2: set ends at the instantiation
link = Link("Alice_Bob", ends=(alice, bob))
...
network.install(link)

```

```

from qcompute_qnet.devices.channel import
    ClassicalFiberChannel, QuantumFiberChannel

# Create channels and connect to the nodes
c1 = ClassicalFiberChannel("c_A2B", distance=1e3)
c1.connect(alice, bob)
c2 = ClassicalFiberChannel("c_B2A", distance=1e3)
c2.connect(bob, alice)

# Create channels with the specified sender and receiver
q1 = QuantumFiberChannel("q_A2B",
    sender=alice, receiver=bob, distance=1e3)
q2 = QuantumFiberChannel("q_B2A",
    sender=bob, receiver=alice, distance=1e3)

link_ab.install([c1, c2, q1, q2])

```

Figure 19 (Color online) Code example for creating a link between Alice and Bob, and installing it to the network.

Figure 20 (Color online) Code example for creating classical and quantum channels between Alice and Bob, and installing it to the link.

it can be loaded onto a `Node` via the `load_protocol` method. A code example is given in Figure 18. Note that protocol stacks do not belong to entities and, thereby, should not be loaded via the `install` method.

Frequently-used node templates. As stated above, nodes can be manually created, followed by the installation of physical devices and the loading of a protocol stack. This gives the most flexibility in designing a specific node. Besides, we also provide some frequently-used node templates, which can be directly used or inherited for further customization. For example, we provide `QKDNode` that can be used for QKD. In a `QKDNode`, a photon source and a photon detector are pre-installed. These physical devices can be accessed through the corresponding attributes. Besides, an empty protocol stack is also loaded by default, leaving the flexibility of setting the key generation protocol (e.g., the `BB84` protocol) to the user. Please refer to the API documentation for more node templates and their detailed usage [333].

Now we know how to create nodes in a network. The next step is to link them together, so they can communicate.

8.2.4 Link

The link, implemented as `Link` in QNET, is the connection between nodes that usually contains specific classical or quantum channels. We can either call the `connect` method to set the ends of a link or specify the ends at instantiation. As with the nodes, we can add `Link` to a `Network` via the `install` method. A code example is given in Figure 19.

As the link is merely a topological concept, we need to further install the classical and quantum channels (`Channel`) for actual communications. In QNET, a classical fiber channel or a quantum fiber channel can be created by instantiating `ClassicalFiberChannel` (inherited from `ClassicalChannel`) or `QuantumFiberChannel` (inherited from `QuantumChannel`). As with links, we can either call the `connect` method to set the sender and receiver of a channel or specify this information at instantiation. Note that both the `ClassicalFiberChannel` and `QuantumFiberChannel` are both unidirectional channels, so the call of `connect` method has to set the sender and receiver in the right order. In addition to the unidirectional fiber channels, QNET also provides duplex channels (`DuplexChannel`) and free-space channels (`FreeSpaceChannel`); please refer to the API documentation for more details [333]. Once created, channels can be added to a `Link` via the `install` method. A code example is given in Figure 20.

8.2.5 A complete example

So far, we have covered all the basic components for constructing a quantum network. A vanilla example of running a quantum network simulation using QNET is given in Figure 21. Notably, all demonstrations in this subsection have merely constructed the skeleton of a quantum network; the heart of network simulation lies in the design of network protocols, the development of protocol stacks, and the modeling

```

from qcompute_qnet.core.des import DESEnv
from qcompute_qnet.topology import Network, Node, Link

# Create a simulation environment
env = DESEnv("Simulation Env", default=True)
# Create a network
network = Network("My First Network")
# Create a node named Alice
alice = Node("Alice")
# Create another node named Bob
bob = Node("Bob")
# Create a link between Alice and Bob
link = Link("Alice_Bob", ends=(alice, bob))
# Build up the network from nodes and links
network.install([alice, bob, link])
# Initialize the simulation environment
env.init()
# Run the network simulation
env.run()

```

Figure 21 (Color online) Code example for running a quantum network simulation using QNET. A simulation typically contains the creation of a simulation environment, the construction of a quantum network, and the initialization and running of the environment.

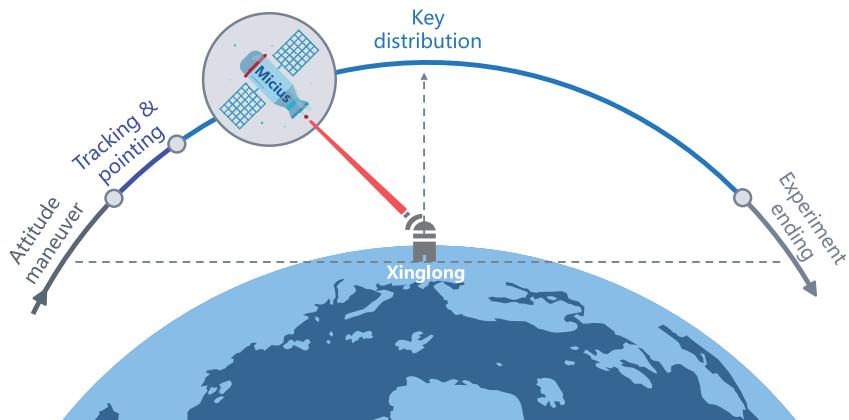


Figure 22 (Color online) Schematic diagram for the satellite-to-ground QKD experiment [22]. The experiment uses the down-link strategy, in which the Micius satellite sends quantum signals to the ground station at Xinglong. Before performing the key distribution, the satellite needs to perform the attitude maneuver and tracking & pointing procedures. The effective time for key distribution is around five minutes.

of physical devices. QNET seeks to provide the building blocks and the simplest set of usage guidelines while leaving users with complete flexibility for innovation. In Subsection 8.3, we will showcase some featured examples implemented with QNET.

8.3 Featured demonstrations

8.3.1 Micius quantum satellite experiment

Due to ground limitations, many places cannot lay the dedicated fibers for quantum communication. But using quantum satellites for relaying can overcome the effects of many negative factors, such as obstacles and ground curvature, making long-distance quantum communication easier to achieve and aiding in the establishment of a global-scale quantum network. The Micius quantum satellite is the world's first quantum communication satellite, launched in 2016 by China. It has conducted various pioneering experiments, including satellite-to-ground bidirectional entanglement distribution over thousands of kilometers, high-speed satellite-to-ground QKD, and high-speed ground-to-satellite quantum teleportation. In this example, we simulate Micius' QKD experiment to showcase the power of QNET in verifying realistic experiments.

A schematic diagram for the experimental procedure is presented in Figure 22. Before the key distribution, the satellite needs to go through the processes of attitude maneuver (adjusting the attitude of

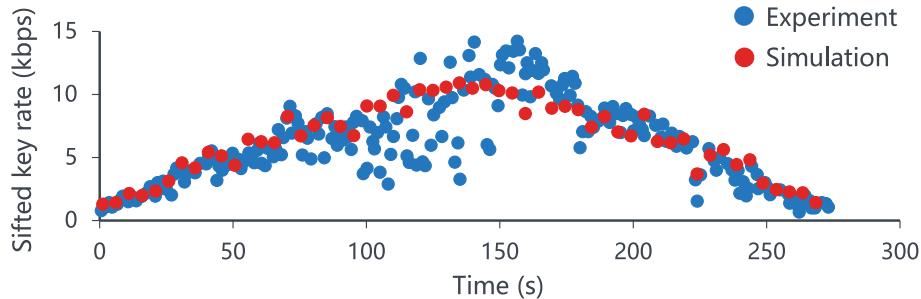


Figure 23 (Color online) Comparison between the simulation results and the experimental data. The horizontal axis is the time of key distribution, and the vertical axis is the sifted key rate.

the satellite and pointing to the ground station) and tracking & pointing (ensuring the transmitter and receiver are firmly locked throughout the orbit) for preparation. Then, the key distribution experiment adopts the decoy-state BB84 protocol to guarantee the security of the key and the down-link strategy for higher link efficiency (more details can be found in [333]). The entire key distribution process lasts for around five minutes. The difficulty in carrying out quantum satellite experiments and simulations stems from the fact that the satellite-to-ground distance varies in real-time as the satellite travels. The variation in communication distance affects photon loss and thus the sifted key rate. Generally, the longer the distance, the higher the photon loss rate and the lower the sifted key rate. In QNET, we provide templates for quantum satellites as well as free-space quantum channels. More broadly, we consider mobility to be a functionality that can be loaded onto a node, such as a quantum satellite, to enable its ability to move (see [333] for further details).

In the simulation, we use the same parameters as the original experiment in [22]. The comparison between our simulation results and the experimental data is given in Figure 23. It is clear that the simulation results closely match the experimental data, thus validating the Micius quantum satellite experiment at the software level. This example demonstrates the benefit of using a simulation tool for verifying quantum experiments. Even without real hardware devices, simulation allows us to swiftly examine protocol performance and adjust settings. This can greatly lower the cost of protocol testing and can be necessary for the standardization of quantum network architectures and expensive projects such as quantum satellites.

8.3.2 Quantum network architecture with resource management

Most of the existing quantum network infrastructure is still in the experimental testing stage and is not yet ready to serve large volumes of users. To make these facilities and technologies operational in the future, we need a network architecture with efficient resource management. In this example, we propose a quantum network architecture, i.e., a four-layer protocol stack that cooperates with a pooling scheme in the repeater stations, capable of processing large numbers of concurrent requests [341,342]. Note that this architecture is presented in the context of QKD, but it should be readily adapted to other scenarios, such as entanglement distribution.

Key pool. Given limited resources, generating keys for a specific request will inevitably block the processing of other requests in the network. To cope with multiple requests, we propose the use of the key pool, which is a battery-like queuing structure that stores and manages the keys generated between two directly connected repeater stations. As shown in Figure 24(a), a key pool has a maximum volume (capacity) V_m indicating the maximum number of keys it can accommodate, a current volume V_c for the currently available keys it holds, a service interruption volume V_i as the threshold for stopping the service, and a service recovery volume V_r for recovering the service. After delivering keys to user requests, a key pool will check its current volume, V_c . If it is less than V_i (see Figure 24(b)), the key pool will stop processing new requests and will call the key generation protocol to replenish the pool with new keys until it reaches the service recovery volume V_r (see Figure 24(c)).

Network architecture. The four-layer quantum network architecture we propose is depicted in Figure 25. Each endnode is equipped with a four-layer protocol stack, with the following protocols running from top to bottom: QKDApp protocol that generates and receives user requests; QKDRMP protocol that is responsible for resource management; QKDRouting protocol that determines the path of key distribution; KeyGeneration protocol that performs key generation with directly connected nodes.

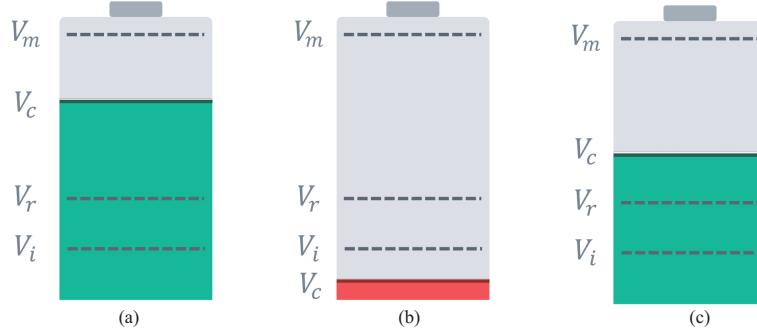


Figure 24 (Color online) Illustration of the key pool structure. Each key pool has a maximum volume V_m , a current volume V_c , a service interruption volume V_i , and a service recovery volume V_r . (a) Key pool on service; (b) key pool to replenish; (c) key pool ready to serve.

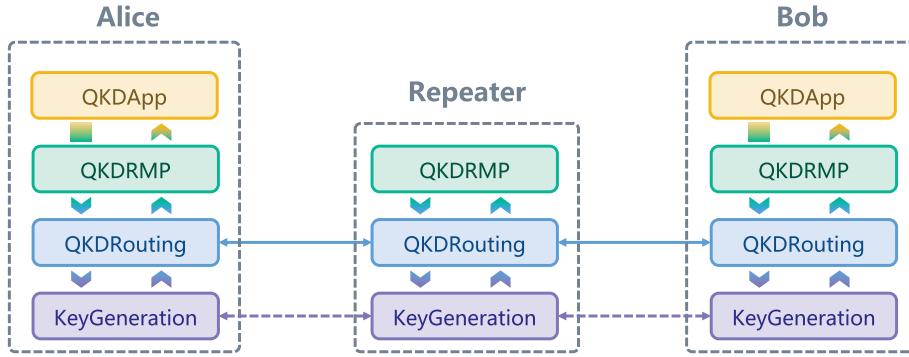


Figure 25 (Color online) Four-layer quantum network architecture. The protocol stack for each endnode has four layers of protocols, and the protocol stack for each repeater has three layers of protocols.

Each repeater has the same protocol stack as an endnode node, except for the application layer. The protocol on each layer is not restricted and can be specified as needed. For example, the routing protocol can be either static or dynamic, and the key generation protocol can be any protocol from BB84, E91, B92.

The process of an end-to-end key request from Alice to Bob is outlined as follows: (1) Alice initiates a key request and sends it to her connected repeater (the message will be directly sent to Bob if there is a direct channel between Alice and Bob). (2) Repeater stations receive the request and choose to forward or reject this message depending on the resource requirements. (3) Bob receives the request message and locally sets his key generation protocol to be ready to generate keys with the upstream node, then he returns an acceptance message. (4) Repeater stations along the path receive the acceptance message and decide, depending on the node's current status, whether to process the request or append the request to the request queue. When a request is processed, the repeater will generate a ciphertext message after key swapping and send it to Bob. (5) Alice receives the acceptance message and locally sets the key generation protocol to generate keys with the downstream node. (6) Alice and Bob save the generated keys with their downstream and upstream nodes locally. (7) Bob receives the ciphertext message and returns an acknowledgment to the repeater. (8) Upon receiving the ciphertexts from all the intermediate stations on the path, Bob combines all the information to decrypt the ciphertexts, and finally obtains the end-to-end keys with Alice. He then sends a done message to Alice to finalize the key request. (9) The repeater stations directly forward the done message once receiving it. (10) Alice receives the done message and sets the end-to-end keys, then finishes the request. It is worth noting that this end-to-end process can occur concurrently among different network users. Particularly in step (4), the repeater station will add the request to a queue if it cannot process it at the moment of acceptance. This request queue will then collaborate with the key pool for an overall scheduling. A request will wait to be called and get processed until there are enough keys in the pool.

We use this architecture to examine the capability of request processing with different key pool capacities on the Beijing Quantum Metropolitan Area Network [24]. In our experiment, we select the receiver and the time at which each endnode creates key requests at random. The amount of each key request

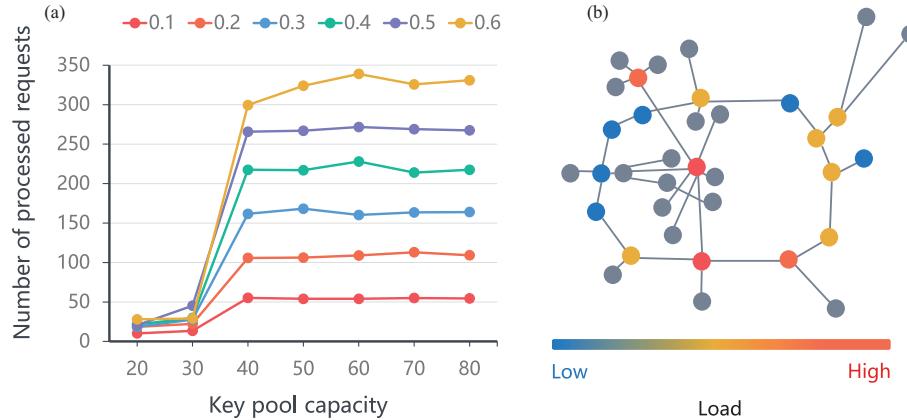


Figure 26 (Color online) Experiment results from the simulation of quantum network architecture with resource management. (a) The relationship between the number of processed requests and the key pool capacity; (b) the virtualization of the network load at each repeater station. The higher the load, the closer the color is to red.

is fixed to be 10 keys, each of length 32. In the key pool, we set $V_i = V_m/4 = V_r/4$, and the maximum volume (capacity) is chosen from 20 to 80 keys with step size 10; each key is of length 32. The simulation time is chosen from 0.1 to 0.6 s with step size 0.1. The relationship between the average number of processed requests and key pool capacity is depicted in Figure 26. We observe that increasing the key pool capacity increases the number of processed requests and thus the network throughput. However, after a threshold of around 40 keys, the network throughput barely improves, even if we increase the key pool capacity further. This is because the larger the capacity of the key pool, the more keys it can cache, and thereby the more requests it can process. However, once the key pool capacity reaches a certain point, the capacity of the key pool saturates the demand for keys in the network, leaving the throughput unchanged. This example shows how QNET can be used to assess the performance of a network architecture and quickly determine the best performance settings. Besides, QNET can also be used to monitor network status visually. For example, in Figure 26, the colored nodes are repeater stations, and the closer to red they are, the busier they can be. It is clear that some of them are significantly busier than others and might end up being the bottleneck for the network throughput. This suggests that we might be able to balance the load on the network by giving these nodes more resources.

8.3.3 CHSH game and its quantum emulation

The CHSH game is derived from the CHSH inequality by Clauser, Horne, Shimony, and Holt in 1969 [343]. This game is commonly used to illustrate quantum advantage. By using quantum entanglement, we can go beyond the limitations of classical information processing. It is worth noting that Aspect, Clauser, and Zeilinger were awarded the Nobel Prize in 2022 for their seminal work on the Bell tests, which can be considered an equivalency of the CHSH game mentioned here. The game features three parties: one referee and two cooperating players, Alice and Bob. The rules are as follows (see Figure 27): (1) The referee chooses two questions $x, y \in \{0, 1\}$ at random and sends one to each player. (2) Alice and Bob must respond to the questions x and y separately and send their answers $a, b \in \{0, 1\}$ to the referee. (3) The referee determines whether the equation $x \cdot y = a \oplus b$ is satisfied. If this is the case, the players win this round; otherwise, they lose. Alice and Bob are allowed to discuss an appropriate strategy before the game begins to increase their chances of victory. However, no communication between them is permitted during the game. It can be easily checked that an optimal classical strategy is provided by Alice and Bob both returning 0 as their answers regardless of the questions posed to them. In this case, the winning probability, which is also the optimal probability, of this game is 75%. The players lose if and only if both questions x and y are equal to 1.

If Alice and Bob are quantum players and are allowed to share quantum entanglement before the game begins, this winning probability can be increased to 85%, far exceeding the classical scenario and exhibiting the quantum advantage. The optimal quantum strategy of the CHSH game is as follows [344]: before the game starts, Alice and Bob need to share an EPR pair $|\Phi\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$ which can be created from an entanglement source. Once receiving the questions from the referee, Alice and Bob take measurements on their qubits A and B, respectively. Alice measures her qubit A in the Z -basis if

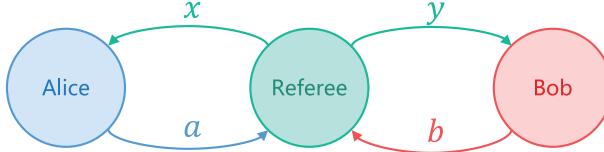


Figure 27 (Color online) Illustration of the CHSH game, which involves one referee and two cooperating players, Alice and Bob. The referee sends questions $x, y \in \{0, 1\}$ to Alice and Bob, respectively, and they need to respond with their answers $a, b \in \{0, 1\}$.

CHSHGame_x0y0:

```
--H----*---M-----  
|  
-----X---Ry---M---
```

CHSHGame_x0y1:

```
--H----*---M-----  
|  
-----X---Ry---M---
```

CHSHGame_x1y0:

```
--H----*---H---M---  
|  
-----X---Ry---M---
```

CHSHGame_x1y1:

```
--H----*---H---M---  
|  
-----X---Ry---M---
```

Figure 28 (Color online) Quantum circuits compiled from the optimal quantum strategy of the CHSH game. Note that the R_y gates in the case of $x = 0, y = 0$ and $x = 1, y = 0$ have a rotation angle $-\pi/4$, whereas the other two cases have a rotation angle $\pi/4$.

the question is $x = 0$ and in the X -basis if the question is $x = 1$. She then replies to the referee with her measurement outcome as the answer a . Bob measures his qubit B in the $(Z + X)/\sqrt{2}$ -basis if the question is $y = 0$ and in the $(Z - X)/\sqrt{2}$ -basis if the question is $y = 1$. Then he replies to the referee with his measurement outcome as the answer b .

Using the protocol compilation in Subsection 8.1.3, we can compile this three-party protocol into the corresponding quantum circuits (see Figure 28) and submit them to Baidu’s Qian Shi (a highly-integrated industry-level superconducting quantum computer¹¹) for evaluation. We observe an average winning probability of around 81.45%, surpassing the optimal classical value of 75%. More details about this implementation can be found at [333]. We remark that this demonstration differs from the actual long-distance Bell test experiments and cannot avoid the causality loophole. But the point is that we can test network protocols in quantum environment through QNET, which can serve as a stepping stone to the next stage, where everything is operated in the actual testbed.

8.4 Comparison with related work

A comparison of QNET to other quantum network simulators is summarized in Figure 29, from which we can draw the following conclusions. First, most simulators are open-source and implemented in Python, but QuISP [32] and qkdX [34] are written in C++ as they are built upon OMNeT++ (a modular, component-based C++ simulation framework that is widely used in classical network simulation). Second, most simulators are designed for general quantum networks, except for QuNet [35], which utilizes a method called “quantum cost-vector analysis” to simulate and benchmark entanglement routing in multi-user entanglement networks, and qkdX which is specialized for QKD. Third, QNET, NetSquid [30], SeQUENCe [31], and QuISP are the four general-purpose simulators that utilize the DES framework, which allows for accurate and efficient system tracking. Among these, QuISP makes use of the existing framework from OMNeT++, whilst the other three simulators build their own standalone simulation engines. There are some distinctions in their DES designs. In particular, SeQUENCe schedules events for entities and protocols by calling the method of a global timeline, NetSquid allows event scheduling for all entities and treats protocols as virtual entities, but QNET allows the flexibility of installing an

¹¹ Baidu Quantum. <https://quantum.baidu.com/>.

Year	Simulator	Developer	Language	Open-Source	DES	Generality	Hardware	MBQC
2022	QNET	Baidu Quantum	Python	Y	Y	Y	Y	Y
2022	AliroNet	Aliro Quantum	?	N	?	Y	?	?
2021	QuNet	UTS	Julia	Y	N	N	N	N
2020	NetSquid	QuTech	Python	N	Y	Y	N	N
2020	SeQUENCe	Argonne National Lab.	Python	Y	Y	Y	N	N
2020	QuNetSim	TUM Munchen	Python	Y	N	Y	N	N
2019	QuISP	Keio University	C++	Y	Y	Y	N	N
2018	SimulaQron	QuTech	Python	Y	N	Y	N	N
2018	SQUANCH	AT&T and Caltech	Python	Y	N	Y	N	N
2015	qkdX	AFIT, USA	C++	Y	Y	N	N	N

Figure 29 (Color online) Comparison of different quantum network simulators. “Y” means the feature is supported, “N” means it is not, and a question mark “?” means that we are not sure if it is supported or not.

event scheduler to any object on-demand. Finally, while the previous simulators remain at the level of simulation with classical devices, QNET provides the compilation of quantum network protocols and supports their emulation in quantum environments. Moreover, QNET also features the ability to run both quantum circuits and MBQC models.

9 Conclusion

In this work, we provide a brief review of the field of quantum networks from both theoretical and experimental perspectives, covering the fundamental ideas, core structures, state-of-the-art developments, and major challenges. Moreover, we introduce a newly developed quantum network toolkit, making it easier for the research and development of this topic. It is the first quantum network toolkit with dual quantum computing engines, making it applicable to the design and simulation of quantum network architectures based on different principles. It also provides the first method for compiling quantum network protocols into quantum circuits so as to interface with quantum hardware devices.

Recalling the history of the internet, we might expect that before we can genuinely build a quantum internet, we first need to build full-fledged quantum computers that operate with millions of qubits. However, there is no cause-and-effect relationship between quantum computing and quantum networking. In particular, the quantum internet is not just about speeding up computations and solving hard problems. It can also be used to improve communication security and provide services that would be impossible in a classical network. Depending on the hardware requirements, quantum internet can have many types of applications at different phases of development [2]. It is highly possible that we would first construct a functional quantum internet before we have large-scale quantum computers, despite the fact that the range of applications may be limited. A notable example is QKD, which requires only single qubits to be created and detected but is sufficient to demonstrate the superiority of the quantum internet over its classical counterpart. There is no doubt that large-scale quantum computers would further enhance the capability of information processing in the quantum internet, but they are just not indispensable for all useful applications.

The future of the quantum internet is promising and significant. However, given the numerous obstacles it faces, its development is still in its early stages, necessitating collaborative efforts from various communities. Future advances in quantum networks include longer-distance quantum communication, larger-scale quantum testbed construction, broader access to quantum services, and the development of more useful applications. In retrospect, the internet’s success and diversity were largely due to creative inventors who had access to the technology and wrote programs to make it do fantastic things like remote chatting, online shopping, and cloud computing. In contrast, existing protocols and applications for a quantum internet are primarily developed by quantum scientists. But this is not how successful applications usually come into existence. People must be able to interact hands-on with a quantum internet and play around with it to develop and try out new applications. An open and sustainable quantum ecosystem involving people from different fields will facilitate new innovations and applications. We hope that this work will give interested readers a basic grasp of quantum networks and that QNET as well as

its future upgrades can serve as a key platform for further explorations and innovations.

Acknowledgements We would like to thank Yu-Ao CHEN, Shusen LIU, Jingbo WANG, Kun WANG, Xin WANG, and Zihe WANG for discussions on the development of QNET. We also thank Jie LIN for suggesting relevant references on single-photon sources and detectors.

References

- 1 Kimble H J. The quantum internet. *Nature*, 2008, 453: 1023–1030
- 2 Wehner S, Elkouss D, Hanson R. Quantum internet: a vision for the road ahead. *Science*, 2018, 362:
- 3 Caleffi M, Cacciapuoti A S, Bianchi G. Quantum internet: from communication to distributed computing! In: Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication, 2018. 1–4
- 4 Castelvecchi D. The quantum internet has arrived (and it hasn't). *Nature*, 2018, 554: 289–292
- 5 Kozlowski W, Wehner S. Towards large-scale quantum networks. In: Proceedings of the 6th Annual ACM International Conference on Nanoscale Computing and Communication, 2019. 1–7
- 6 Singh A, Dev K, Siljak H, et al. Quantum internet-applications, functionalities, enabling technologies, challenges, and research directions. *IEEE Commun Surv Tut*, 2021, 23: 2218–2247
- 7 Wei S, Jing B, Zhang X, et al. Towards real-world quantum networks: a review. *Laser Photon Rev*, 2022, 16: 2100219
- 8 Awschalom D, Berggren K K, Bernien H, et al. Development of quantum interconnects (QuICs) for next-generation information technologies. *PRX Quantum*, 2021, 2: 017002
- 9 Gyongyosi L, Imre S. Advances in the quantum internet. *Commun ACM*, 2022, 65: 52–63
- 10 Rohde P P. The Quantum Internet: The Second Quantum Revolution. Cambridge: Cambridge University Press, 2021
- 11 Pirandola S, Braunstein S L. Physics: unite to build a quantum internet. *Nature*, 2016, 532: 169–171
- 12 Ramakrishnan R K, Ravichandran A B, Kaushik I, et al. The quantum internet: a hardware review. *J Ind Inst Sci*, 2022, doi: 10.1007/s41745-022-00336-7
- 13 Bennett C, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 1984. 175–179
- 14 Ekert A K. Quantum cryptography based on Bell's theorem. *Phys Rev Lett*, 1991, 67: 661–663
- 15 Broadbent A, Fitzsimons J, Kashefi E. Universal blind quantum computation. In: Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, 2009. 517–526
- 16 Jozsa R, Abrams D S, Dowling J P, et al. Quantum clock synchronization based on shared prior entanglement. *Phys Rev Lett*, 2000, 85: 2010–2013
- 17 Gottesman D, Jennewein T, Croke S. Longer-baseline telescopes using quantum repeaters. *Phys Rev Lett*, 2012, 109: 070503
- 18 Cirac J I, Ekert A K, Huelga S F, et al. Distributed quantum computation over noisy channels. *Phys Rev A*, 1999, 59: 4249–4254
- 19 Crépeau C, Gottesman D, Smith A. Secure multi-party quantum computation. In: Proceedings of the 34th Annual ACM Symposium on Theory of Computing, 2002. 643–652
- 20 Cuomo D, Caleffi M, Cacciapuoti A S. Towards a distributed quantum computing ecosystem. *IET Quantum Commun*, 2020, 1: 3–8
- 21 Lu C Y, Cao Y, Peng C Z, et al. Micius quantum experiments in space. *Rev Mod Phys*, 2022, 94: 035001
- 22 Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution. *Nature*, 2017, 549: 43–47
- 23 Castelvecchi D. China's quantum satellite clears major hurdle on way to ultrasecure communications. *Nature*, 2017, doi: 10.1038/nature.2017.22142
- 24 Chen Y A, Zhang Q, Chen T Y, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 2021, 589: 214–219
- 25 Courtland R. China's 2,000-km quantum link is almost complete [News]. *IEEE Spectr*, 2016, 53: 11–12
- 26 Pompili M, Hermans S L N, Baier S, et al. Realization of a multinode quantum network of remote solid-state qubits. *Science*, 2021, 372: 259–264
- 27 Pirker A, Dür W. A quantum network stack and protocols for reliable entanglement-based networks. *New J Phys*, 2019, 21: 033003
- 28 Kozlowski W, Wehner S, Meter R V, et al. Architectural Principles for a Quantum Internet. RFC 9340. 2022
- 29 Van Meter R, Satoh R, Benchasattabuse N, et al. A quantum internet architecture. 2021. ArXiv:2112.07092
- 30 Coopmans T, Knegjens R, Dahlberg A, et al. NetSquid, a NETwork simulator for quantum information using discrete events. *Commun Phys*, 2021, 4: 164
- 31 Wu X, Kolar A, Chung J, et al. SeQUENCe: a customizable discrete-event simulator of quantum networks. *Quantum Sci Technol*, 2021, 6: 045027
- 32 Satoh R, Hajdušek M, Benchasattabuse N, et al. QuISP: a quantum internet simulation package. 2021. ArXiv:2112.07093
- 33 Bartlett B. A distributed simulation framework for quantum networks and channels. 2018. ArXiv:1808.07047
- 34 Mailloux L O, Morris J D, Grimalta M R, et al. A modeling framework for studying quantum key distribution system implementation nonidealities. *IEEE Access*, 2015, 3: 110–130

- 35 Leone H, Miller N R, Singh D, et al. QuNet: cost vector analysis & multi-path entanglement routing in quantum networks. 2021. ArXiv:2105.00418
- 36 Slussarenko S, Pryde G J. Photonic quantum information processing: a concise review. *Appl Phys Rev*, 2019, 6: 041303
- 37 Krantz P, Kjaergaard M, Yan F, et al. A quantum engineer's guide to superconducting qubits. *Appl Phys Rev*, 2019, 6: 021318
- 38 Brzczewicz C D, Chiaverini J, McConnell R, et al. Trapped-ion quantum computing: progress and challenges. *Appl Phys Rev*, 2019, 6: 021314
- 39 Hillery M. Coherence as a resource in decision problems: the Deutsch-Jozsa algorithm and a variation. *Phys Rev A*, 2016, 93: 012111
- 40 Hayashi M, Fang K, Wang K. Finite block length analysis on quantum coherence distillation and incoherent randomness extraction. *IEEE Trans Inform Theory*, 2021, 67: 3926–3944
- 41 Díaz M G, Fang K, Wang X, et al. Using and reusing coherence to realize quantum processes. *Quantum*, 2018, 2: 100
- 42 Fang K, Wang X, Lami L, et al. Probabilistic distillation of quantum coherence. *Phys Rev Lett*, 2018, 121: 070404
- 43 Regula B, Fang K, Wang X, et al. One-shot coherence distillation. *Phys Rev Lett*, 2018, 121: 010401
- 44 Ahnefeld F, Theurer T, Egloff D, et al. Coherence as a resource for Shor's algorithm. *Phys Rev Lett*, 2022, 129: 120501
- 45 Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys Rev Lett*, 1993, 70: 1895–1899
- 46 Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks. *Phys Rev Lett*, 2007, 98: 230501
- 47 Bell J S. On the Einstein Podolsky Rosen paradox. *Phys Phys Fizika*, 1964, 1: 195–200
- 48 Freedman S J, Clauser J F. Experimental test of local hidden-variable theories. *Phys Rev Lett*, 1972, 28: 938–941
- 49 Aspect A, Dalibard J, Roger G. Experimental test of Bell's inequalities using time-varying analyzers. *Phys Rev Lett*, 1982, 49: 1804–1807
- 50 Ou Z Y, Mandel L. Violation of Bell's inequality and classical probability in a two-photon correlation experiment. *Phys Rev Lett*, 1988, 61: 50–53
- 51 Hensen B, Bernien H, Dréau A E, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 2015, 526: 682–686
- 52 Giustina M, Versteegh M A M, Wengerowsky S, et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys Rev Lett*, 2015, 115: 250401
- 53 Shalm L K, Meyer-Scott E, Christensen B G, et al. Strong loophole-free test of local realism. *Phys Rev Lett*, 2015, 115: 250402
- 54 Handsteiner J, Friedman A S, Rauch D, et al. Cosmic Bell test: measurement settings from milky way stars. *Phys Rev Lett*, 2017, 118: 060401
- 55 Yin J, Cao Y, Li Y H, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 2017, 356: 1140–1144
- 56 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2012
- 57 Xiao Y, Fang K, Gour G. The complementary information principle of quantum mechanics. 2019. ArXiv:1908.07694
- 58 Briegel H J, Browne D E, Dür W, et al. Measurement-based quantum computation. *Nat Phys*, 2009, 5: 19–26
- 59 Wootters W K, Zurek W H. A single quantum cannot be cloned. *Nature*, 1982, 299: 802–803
- 60 Briegel H J, Dür W, Cirac J I, et al. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys Rev Lett*, 1998, 81: 5932–5935
- 61 Duan L M, Lukin M D, Cirac J I, et al. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 2001, 414: 413–418
- 62 Muralidharan S, Li L, Kim J, et al. Optimal architectures for long distance quantum communication. *Sci Rep*, 2016, 6: 20463
- 63 Zwerger M, Pirker A, Dunjko V, et al. Long-range big quantum-data transmission. *Phys Rev Lett*, 2018, 120: 030503
- 64 Brand S, Coopmans T, Elkouss D. Efficient computation of the waiting time and fidelity in quantum repeater chains. *IEEE J Sel Areas Commun*, 2020, 38: 619–639
- 65 Li B, Coopmans T, Elkouss D. Efficient optimization of cutoffs in quantum repeater chains. *IEEE Trans Quantum Eng*, 2021, 2: 1–15
- 66 Rozpędek F, Noh K, Xu Q, et al. Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes. *npj Quantum Inf*, 2021, 7: 102
- 67 Rozpędek F, Goodenough K, Ribeiro J, et al. Parameter regimes for a single sequential quantum repeater. *Quantum Sci Technol*, 2018, 3: 034002
- 68 Coutinho B C, Munro W J, Nemoto K, et al. Robustness of noisy quantum networks. *Commun Phys*, 2022, 5: 105
- 69 Zhou Z. A multiplexed quantum repeater based on absorptive quantum memories. *Sci China Inf Sci*, 2021, 64: 217501
- 70 Sangouard N, Simon C, de Riedmatten H, et al. Quantum repeaters based on atomic ensembles and linear optics. *Rev Mod Phys*, 2011, 83: 33–80
- 71 Gottesman D. An introduction to quantum error correction and fault-tolerant quantum computation. 2009. ArXiv:0904.2557

- 72 Munro W J, Azuma K, Tamaki K, et al. Inside quantum repeaters. *IEEE J Sel Top Quantum Electron*, 2015, 21: 78–90
- 73 Lago-Rivera D, Grandi S, Rakonjac J V, et al. Telecom-heralded entanglement between multimode solid-state quantum memories. *Nature*, 2021, 594: 37–40
- 74 Liu X, Hu J, Li Z F, et al. Heralded entanglement distribution between two absorptive quantum memories. *Nature*, 2021, 594: 41–45
- 75 Pu Y F, Zhang S, Wu Y K, et al. Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments. *Nat Photon*, 2021, 15: 374–378
- 76 Cao Y, Zhao Y, Wang Q, et al. The evolution of quantum key distribution networks: on the road to the qinternet. *IEEE Commun Surv Tut*, 2022, 24: 839–894
- 77 Sidhu J S, Joshi S K, Gündoğan M, et al. Advances in space quantum communications. *IET Quantum Commun*, 2021, 2: 182–217
- 78 Belenchia A, Carlesso M, Bayraktar Ö, et al. Quantum physics in space. *Phys Rep*, 2022, 951: 1–70
- 79 Neumann S P, Joshi S K, Fink M, et al. Q³Sat: quantum communications uplink to a 3U CubeSat-feasibility & design. *EPJ Quantum Technol*, 2018, 5: 4
- 80 Knips L, Auer M, Baliuka A, et al. QUBE – towards quantum key distribution with small satellites. In: *Proceedings of Quantum 2.0*. Optica Publishing Group, 2022
- 81 Kerstel E, Gardelein A, Barthelemy M, et al. Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technol*, 2018, 5: 6
- 82 Dalibot C, Tustain S. The preliminary thermal design for the SPEQTRE CubeSat. In: *Proceedings of International Conference on Environmental Systems*, 2020
- 83 Greenberger D M, Horne M A, Zeilinger A. Going beyond Bell's theorem. In: *Proceedings of Bell's Theorem, Quantum Theory and Conceptions of the Universe*, 1989. 69–72
- 84 Dai W, Rinaldi A, Towsley D. Entanglement swapping in quantum switches: protocol design and stability analysis. 2021. ArXiv:2110.04116
- 85 Nain P, Vardoyan G, Guha S, et al. On the analysis of a multipartite entanglement distribution switch. *Proc ACM Meas Anal Comput Syst*, 2020, 4: 1–39
- 86 Vardoyan G, Nain P, Guha S, et al. On the capacity region of bipartite and tripartite entanglement switching. 2019. ArXiv:1901.06786
- 87 Vardoyan G, Guha S, Nain P, et al. On the stochastic analysis of a quantum entanglement switch. *SIGMETRICS Perform Eval Rev*, 2019, 47: 27–29
- 88 Lütkenhaus N, Jahma M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New J Phys*, 2002, 4: 44
- 89 Eisaman M D, Fan J, Migdall A, et al. Invited review article: single-photon sources and detectors. *Rev Sci Instrum*, 2011, 82: 071101
- 90 Migdall A, Polyakov S V, Fan J, et al. *Single-photon Generation and Detection: Physics and Applications*. New York: Academic Press, 2013
- 91 Senellart P, Solomon G, White A. High-performance semiconductor quantum-dot single-photon sources. *Nat Nanotech*, 2017, 12: 1026–1039
- 92 Arakawa Y, Holmes M J. Progress in quantum-dot single photon sources for quantum information technologies: a broad spectrum overview. *Appl Phys Rev*, 2020, 7: 021309
- 93 Strauf S, Stoltz N G, Rakher M T, et al. High-frequency single-photon source with polarization control. *Nat Photon*, 2007, 1: 704–708
- 94 Shields A J. Semiconductor quantum light sources. *Nat Photon*, 2007, 1: 215–223
- 95 Kim J, Benson O, Kan H, et al. A single-photon turnstile device. *Nature*, 1999, 397: 500–503
- 96 Chu X L, Götzinger S, Sandoghdar V. A single molecule as a high-fidelity photon gun for producing intensity-squeezed light. *Nat Photon*, 2017, 11: 58–62
- 97 De Martini F, Di Giuseppe G, Marrocco M. Single-mode generation of quantum photon states by excited single molecules in a microcavity trap. *Phys Rev Lett*, 1996, 76: 900–903
- 98 Kako S, Santori C, Hoshino K, et al. A gallium nitride single-photon source operating at 200 K. *Nat Mater*, 2006, 5: 887–892
- 99 Kuhn A, Hennrich M, Rempe G. Deterministic single-photon source for distributed quantum networking. *Phys Rev Lett*, 2002, 89: 067901
- 100 Blinov B B, Moehring D L, Duan L M, et al. Observation of entanglement between a single trapped atom and a single photon. *Nature*, 2004, 428: 153–157
- 101 Maurer C, Becher C, Russo C, et al. A single-photon source based on a single Ca⁺ ion. *New J Phys*, 2004, 6: 94
- 102 Kurtsiefer C, Mayer S, Zarda P, et al. Stable solid-state source of single photons. *Phys Rev Lett*, 2000, 85: 290–293
- 103 Babinec T M, Hausmann B J M, Khan M, et al. A diamond nanowire single-photon source. *Nat Nanotech*, 2010, 5: 195–199
- 104 Alléaume R, Treussart F, Messin G, et al. Experimental open-air quantum key distribution with a single-photon source. *New J Phys*, 2004, 6: 92

- 105 Pittman T B, Franson J D, Jacobs B C. Investigation of a single-photon source based on quantum interference. *New J Phys*, 2007, 9: 195
- 106 Grangier P, Roger G, Aspect A. Experimental evidence for a photon anticorrelation effect on a beam splitter: a new light on single-photon interferences. *Europhys Lett*, 1986, 1: 173–179
- 107 Hong C K, Mandel L. Experimental realization of a localized one-photon state. *Phys Rev Lett*, 1986, 56: 58–60
- 108 Fasel S, Alibart O, Tanzilli S, et al. High-quality asynchronous heralded single-photon source at telecom wavelength. *New J Phys*, 2004, 6: 163
- 109 Meyer-Scott E, Silberhorn C, Migdall A. Single-photon sources: approaching the ideal through multiplexing. *Rev Sci Instrum*, 2020, 91: 041101
- 110 Wang H, Qin J, Ding X, et al. Boson sampling with 20 input photons and a 60-mode interferometer in a 60-mode interferometer in a 10^{14} -dimensional Hilbert space. *Phys Rev Lett*, 2019, 123: 250503
- 111 Thomas S, Senellart P. The race for the ideal single-photon source is on. *Nat Nanotechnol*, 2021, 16: 367–368
- 112 Tomm N, Javadi A, Antoniadis N O, et al. A bright and fast source of coherent single photons. *Nat Nanotechnol*, 2021, 16: 399–403
- 113 Wei Y, Liu S, Li X, et al. Tailoring solid-state single-photon sources with stimulated emissions. *Nat Nanotechnol*, 2022, 17: 470–476
- 114 Hadfield R H. Single-photon detectors for optical quantum information applications. *Nat Photon*, 2009, 3: 696–705
- 115 Komiyama S, Astafiev O, Antonov V, et al. A single-photon detector in the far-infrared range. *Nature*, 2000, 403: 405–407
- 116 Cova S, Ghioni M, Lotito A, et al. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *J Modern Opt*, 2004, 51: 1267–1288
- 117 Rosfjord K M, Yang J K W, Dauler E A, et al. Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating. *Opt Express*, 2006, 14: 527–534
- 118 Takesue H, Diamanti E, Langrock C, et al. 1.5- μ m single photon counting using polarization-independent up-conversion detector. *Opt Express*, 2006, 14: 13067–13072
- 119 Peacock A, Verhoeve P, Rando N, et al. Single optical photon detection with a superconducting tunnel junction. *Nature*, 1996, 381: 135–137
- 120 Rosenberg D, Lita A, Miller A, et al. Noise-free high-efficiency photon-number-resolving detectors. *Phys Rev A*, 2005, 71: 061803
- 121 Fujiwara M, Sasaki M. Direct measurement of photon number statistics at telecom wavelengths using a charge integration photon detector. *Appl Opt*, 2007, 46: 3069–3074
- 122 Gansen E J, Rowe M A, Greene M B, et al. Photon-number-discriminating detection using a quantum-dot, optically gated, field-effect transistor. *Nat Photon*, 2007, 1: 585–588
- 123 Reddy D V, Nerem R R, Nam S W, et al. Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550 nm. *Optica*, 2020, 7: 1649–1653
- 124 Korzh B, Zhao Q Y, Allmaras J P, et al. Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector. *Nat Photon*, 2020, 14: 250–255
- 125 Lu C Y, Pan J W. Push-button photon entanglement. *Nat Photon*, 2014, 8: 174–176
- 126 Burnham D C, Weinberg D L. Observation of simultaneity in parametric production of optical photon pairs. *Phys Rev Lett*, 1970, 25: 84–87
- 127 Pan J W, Chen Z B, Lu C Y, et al. Multiphoton entanglement and interferometry. *Rev Mod Phys*, 2012, 84: 777–838
- 128 Anwar A, Perumangatt C, Steinlechner F, et al. Entangled photon-pair sources based on three-wave mixing in bulk crystals. *Rev Sci Instrum*, 2021, 92: 041101
- 129 Bock M, Lenhard A, Chunnillall C, et al. Highly efficient heralded single-photon source for telecom wavelengths based on a PPLN waveguide. *Opt Express*, 2016, 24: 23992–24001
- 130 Aspect A, Grangier P, Roger G. Experimental tests of realistic local theories via Bell's theorem. *Phys Rev Lett*, 1981, 47: 460–463
- 131 Young R J, Stevenson R M, Atkinson P, et al. Improved fidelity of triggered entangled photons from single quantum dots. *New J Phys*, 2006, 8: 29
- 132 Akopian N, Lindner N H, Poem E, et al. Entangled photon pairs from semiconductor quantum dots. *Phys Rev Lett*, 2006, 96: 130501
- 133 Wang H, Hu H, Chung T H, et al. On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability. *Phys Rev Lett*, 2019, 122: 113602
- 134 Hammerer K, Sørensen A S, Polzik E S. Quantum interface between light and atomic ensembles. *Rev Mod Phys*, 2010, 82: 1041–1093
- 135 Stannigel K, Rabl P, Sørensen A S, et al. Optomechanical transducers for long-distance quantum communication. *Phys Rev Lett*, 2010, 105: 220501
- 136 Lauk N, Sinclair N, Barzanjeh S, et al. Perspectives on quantum transduction. *Quantum Sci Technol*, 2020, 5: 020501
- 137 Bochmann J, Vainsencher A, Awschalom D D, et al. Nanomechanical coupling between microwave and optical photons. *Nat*

- Phys, 2013, 9: 712–716
- 138 Andrews R W, Peterson R W, Purdy T P, et al. Bidirectional and efficient conversion between microwave and optical light. *Nat Phys*, 2014, 10: 321–326
- 139 Jiang W, Sarabalis C J, Dahmani Y D, et al. Efficient bidirectional piezo-optomechanical transduction between microwave and optical frequency. *Nature Commun*, 2020, 11: 1166
- 140 Wang C H, Li F, Jiang L. Quantum capacities of transducers. *Nat Commun*, 2022, 13: 6698
- 141 Higginbotham A P, Burns P S, Urmey M D, et al. Harnessing electro-optic correlations in an efficient mechanical converter. *Nat Phys*, 2018, 14: 1038–1042
- 142 Han X, Fu W, Zou C L, et al. Microwave-optical quantum frequency conversion. *Optica*, 2021, 8: 1050–1064
- 143 Julsgaard B, Kozhekin A, Polzik E S. Experimental long-lived entanglement of two macroscopic objects. *Nature*, 2001, 413: 400–403
- 144 Chou C W, de Riedmatten H, Felinto D, et al. Measurement-induced entanglement for excitation stored in remote atomic ensembles. *Nature*, 2005, 438: 828–832
- 145 Vernaz-Gris P, Huang K, Cao M, et al. Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble. *Nat Commun*, 2018, 9: 1–6
- 146 Heller L, Farrera P, Heinze G, et al. Cold-atom temporally multiplexed quantum memory with cavity-enhanced noise suppression. *Phys Rev Lett*, 2020, 124: 210504
- 147 Choi K S, Deng H, Laurat J, et al. Mapping photonic entanglement into and out of a quantum memory. *Nature*, 2008, 452: 67–71
- 148 Usmani I, Clausen C, Bussières F, et al. Heralded quantum entanglement between two crystals. *Nat Photon*, 2012, 6: 234–237
- 149 Ortú A, Holzapfel A, Etesse J, et al. Storage of photonic time-bin qubits for up to 20 ms in a rare-earth doped crystal. *npj Quantum Inf*, 2022, 8: 29
- 150 Lvovsky A I, Sanders B C, Tittel W. Optical quantum memory. *Nat Photon*, 2009, 3: 706–714
- 151 Simon C, Afzelius M, Appel J, et al. Quantum memories. *Eur Phys J D*, 2010, 58: 1–22
- 152 Heshami K, England D G, Humphreys P C, et al. Quantum memories: emerging applications and recent advances. *J Modern Opt*, 2016, 63: 2005–2028
- 153 Bussières F, Sangouard N, Afzelius M, et al. Prospective applications of optical quantum memories. *J Modern Opt*, 2013, 60: 1519–1537
- 154 Novikova I, Walsworth R L, Xiao Y. Electromagnetically induced transparency-based slow and stored light in warm atoms. *Laser Photon Rev*, 2012, 6: 333–353
- 155 Ma L, Slattery O, Tang X. Optical quantum memory based on electromagnetically induced transparency. *J Opt*, 2017, 19: 043001
- 156 Wang Y, Li J, Zhang S, et al. Efficient quantum memory for single-photon polarization qubits. *Nat Photon*, 2019, 13: 346–351
- 157 Ma L, Slattery O, Tang X. Optical quantum memory and its applications in quantum communication systems. *J Res Natl Inst Stan*, 2020, 125: 125002
- 158 Zhu T X, Liu C, Jin M, et al. On-demand integrated quantum memory for polarization qubits. *Phys Rev Lett*, 2022, 128: 180501
- 159 Stas P J, Huan Y Q, Machielse B, et al. Robust multi-qubit quantum network node with integrated error detection. *Science*, 2022, 378: 557–560
- 160 Inagaki T, Matsuda N, Tadanaga O, et al. Entanglement distribution over 300 km of fiber. *Opt Express*, 2013, 21: 23241
- 161 Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys Rev Lett*, 2016, 117: 190501
- 162 Villoresi P, Jennewein T, Tamburini F, et al. Experimental verification of the feasibility of a quantum channel between space and Earth. *New J Phys*, 2008, 10: 033038
- 163 Hughes R J, Nordholt J E. Quantum space race heats up. *Nat Photon*, 2017, 11: 456–458
- 164 Buttler W T, Hughes R J, Kwiat P G, et al. Practical free-space quantum key distribution over 1 km. *Phys Rev Lett*, 1998, 81: 3283–3286
- 165 Ma X S, Herbst T, Scheidl T, et al. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 2012, 489: 269–273
- 166 Steinlechner F, Ecker S, Fink M, et al. Distribution of high-dimensional entanglement via an intra-city free-space link. *Nat Commun*, 2017, 8: 1–7
- 167 Valivarthi R, Puigibert M G, Zhou Q, et al. Quantum teleportation across a metropolitan fibre network. *Nat Photon*, 2016, 10: 676–680
- 168 Sun Q C, Mao Y L, Chen S J, et al. Quantum teleportation with independent sources and prior entanglement distribution over a network. *Nat Photon*, 2016, 10: 671–675
- 169 Pugh C J, Kaiser S, Bourgoin J P, et al. Airborne demonstration of a quantum key distribution receiver payload. *Quantum*

- Sci Technol, 2017, 2: 024009
- 170 Wang J Y, Yang B, Liao S K, et al. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat Photon*, 2013, 7: 387–393
- 171 Liu H Y, Tian X H, Gu C, et al. Drone-based entanglement distribution towards mobile quantum networks. *Natl Sci Rev*, 2020, 7: 921–928
- 172 Ren J G, Xu P, Yong H L, et al. Ground-to-satellite quantum teleportation. *Nature*, 2017, 549: 70–73
- 173 Liao S K, Cai W Q, Handsteiner J, et al. Satellite-relayed intercontinental quantum network. *Phys Rev Lett*, 2018, 120: 030501
- 174 Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental limits of repeaterless quantum communications. *Nat Commun*, 2017, 8: 1–5
- 175 Pirandola S. Capacities of repeater-assisted quantum communications. 2016. ArXiv:1601.00966
- 176 Wang X, Fang K, Tomamichel M. On Converse bounds for classical communication over quantum channels. *IEEE Trans Inform Theory*, 2019, 65: 4609–4619
- 177 Wang X, Fang K, Duan R. Semidefinite programming converse bounds for quantum communication. *IEEE Trans Inform Theory*, 2018, 65: 2583–2592
- 178 Fang K, Fawzi H. Geometric Rényi divergence and its applications in quantum channel capacities. *Commun Math Phys*, 2021, 384: 1615–1677
- 179 Fang K, Gour G, Wang X. Towards the ultimate limits of quantum channel discrimination. 2021. ArXiv:2110.14842
- 180 Fawzi H, Fawzi O. Defining quantum divergences via convex optimization. *Quantum*, 2021, 5: 387
- 181 Fawzi O, Shayeghi A, Ta H. A hierarchy of efficient bounds on quantum capacities exploiting symmetry. *IEEE Trans Inform Theory*, 2022, 68: 7346–7360
- 182 Wang X, Xie W, Duan R. Semidefinite programming converse bounds for classical communication over quantum channels. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), 2017. 1728–1732
- 183 Fang K, Wang X, Tomamichel M, et al. Quantum channel simulation and the channel's smooth max-information. *IEEE Trans Inform Theory*, 2019, 66: 2129–2140
- 184 Fang K, Fawzi O, Renner R, et al. Chain rule for the quantum relative entropy. *Phys Rev Lett*, 2020, 124: 100501
- 185 Dahlberg A, Skrzypczyk M, Coopmans T, et al. A link layer protocol for quantum networks. In: Proceedings of the ACM Special Interest Group on Data Communication, 2019. 159–173
- 186 Kozłowski W, Dahlberg A, Wehner S. Designing a quantum network protocol. In: Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies, 2020. 1–16
- 187 Illiano J, Caleffi M, Manzalini A, et al. Quantum internet protocol stack: a comprehensive survey. *Comput Netw*, 2022, 213: 109092
- 188 DiAdamo S, Qi B, Miller G, et al. Packet switching in quantum networks: a path to quantum internet. 2022. ArXiv:2205.07507
- 189 Pirker A, Wallnöfer J, Dür W. Modular architectures for quantum networks. *New J Phys*, 2018, 20: 053054
- 190 Zhang H, Li Y, Zhang C, et al. Connection-oriented and connectionless quantum internet considering quantum repeaters. 2022. ArXiv:2208.03930
- 191 Zwerger M, Dür W, Briegel H J. Measurement-based quantum repeaters. *Phys Rev A*, 2012, 85: 062326
- 192 Zwerger M, Briegel H J, Dür W. Measurement-based quantum communication. *Appl Phys B*, 2016, 122: 1–5
- 193 Cerf V, Kahn R. A protocol for packet network intercommunication. *IEEE Trans Commun*, 1974, 22: 637–648
- 194 Boschi D, Branca S, De Martini F, et al. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys Rev Lett*, 1998, 80: 1121–1125
- 195 Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. *Nature*, 1997, 390: 575–579
- 196 Pirandola S, Eisert J, Weedbrook C, et al. Advances in quantum teleportation. *Nat Photon*, 2015, 9: 641–652
- 197 Liu S, Lou Y, Jing J. Orbital angular momentum multiplexed deterministic all-optical quantum teleportation. *Nat Commun*, 2020, 11: 3875
- 198 Ursin R, Jennewein T, Aspelmeyer M, et al. Quantum teleportation across the Danube. *Nature*, 2004, 430: 849
- 199 Riebe M, Häffner H, Roos C F, et al. Deterministic quantum teleportation with atoms. *Nature*, 2004, 429: 734–737
- 200 Leuenberger M N, Flatté M E, Awschalom D D. Teleportation of electronic many-qubit states encoded in the electron spin of quantum dots via single photons. *Phys Rev Lett*, 2005, 94: 107401
- 201 Zukowski M, Zeilinger A, Horne M A, et al. “Event-ready-detectors” Bell experiment via entanglement swapping. *Phys Rev Lett*, 1993, 71: 4287–4290
- 202 Pan J W, Bouwmeester D, Weinfurter H, et al. Experimental entanglement swapping: entangling photons that never interacted. *Phys Rev Lett*, 1998, 80: 3891–3894
- 203 Kaltenbaek R, Prevedel R, Aspelmeyer M, et al. High-fidelity entanglement swapping with fully independent sources. *Phys Rev A*, 2009, 79: 040302
- 204 Jennewein T, Weihs G, Pan J W, et al. Experimental nonlocality proof of quantum teleportation and entanglement swapping. *Phys Rev Lett*, 2001, 88: 017903

- 205 de Riedmatten H, Marcikic I, van Houwelingen J A W, et al. Long-distance entanglement swapping with photons from separated sources. *Phys Rev A*, 2005, 71: 050302
- 206 Wu Q L, Namekata N, Inoue S. High-fidelity entanglement swapping at telecommunication wavelengths. *J Phys B-At Mol Opt Phys*, 2013, 46: 235503
- 207 Halder M, Beveratos A, Gisin N, et al. Entangling independent photons by time measurement. *Nat Phys*, 2007, 3: 692–695
- 208 Xue Y, Yoshizawa A, Tsuchida H. Polarization-based entanglement swapping at the telecommunication wavelength using spontaneous parametric down-conversion photon-pair sources. *Phys Rev A*, 2012, 85: 032337
- 209 Takesue H, Miquel B. Entanglement swapping using telecom-band photons generated in fibers. *Opt Express*, 2009, 17: 10748–10756
- 210 Sun Q C, Jiang Y F, Mao Y L, et al. Field test of entanglement swapping over 100-km optical fiber with independent 1-GHz-clock sequential time-bin entangled photon-pair sources. 2017. ArXiv:1704.03960
- 211 Huang C X, Hu X M, Guo Y, et al. Entanglement swapping and quantum correlations via symmetric joint measurements. *Phys Rev Lett*, 2022, 129: 030502
- 212 Liu S, Lou Y, Chen Y, et al. All-optical entanglement swapping. *Phys Rev Lett*, 2022, 128: 060503
- 213 van Meter R, Satoh T, Ladd T D, et al. Path selection for quantum repeater networks. *NetwSci*, 2013, 3: 82–95
- 214 Caleffi M. Optimal routing for quantum networks. *IEEE Access*, 2017, 5: 22299–22312
- 215 Schouten E, Mancinska L, Islam T, et al. Shortcuts to quantum network routing. 2016. ArXiv:1610.05238
- 216 Bugalho L, Coutinho B C, Monteiro F A, et al. Distributing multipartite entanglement over noisy quantum networks. 2021. ArXiv:2103.14759
- 217 Gyongyosi L, Imre S. Decentralized base-graph routing for the quantum internet. *Phys Rev A*, 2018, 98: 022310
- 218 Gyongyosi L, Imre S. Entanglement-gradient routing for quantum networks. *Sci Rep*, 2017, 7: 14255
- 219 Chakraborty K, Rozpedek F, Dahlberg A, et al. Distributed routing in a quantum internet. 2019. ArXiv:1907.11630
- 220 Perseguers S, Lapeyre Jr G J, Cavalcanti D, et al. Distribution of entanglement in large-scale quantum networks. *Rep Prog Phys*, 2013, 76: 096001
- 221 Hahn F, Pappa A, Eisert J. Quantum network routing and local complementation. *npj Quantum Inf*, 2019, 5: 76
- 222 Pant M, Krovi H, Towsley D, et al. Routing entanglement in the quantum internet. *npj Quantum Inf*, 2019, 5: 1–9
- 223 Shi S, Qian C. Concurrent entanglement routing for quantum networks: model and designs. In: Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication, 2020. 62–65
- 224 Bennett C H, Wiesner S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys Rev Lett*, 1992, 69: 2881–2884
- 225 Bennett C H, DiVincenzo D P, Smolin J A, et al. Mixed-state entanglement and quantum error correction. *Phys Rev A*, 1996, 54: 3824–3851
- 226 Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys Rev Lett*, 1996, 76: 722–725
- 227 Deutsch D, Ekert A, Jozsa R, et al. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys Rev Lett*, 1996, 77: 2818–2821
- 228 Buscemi F, Datta N. Distilling entanglement from arbitrary resources. *J Math Phys*, 2010, 51: 102201
- 229 Brandao F G S L, Datta N. One-shot rates for entanglement manipulation under non-entangling maps. *IEEE Trans Inform Theory*, 2011, 57: 1754–1760
- 230 Datta N, Leditzky F. Second-order asymptotics for source coding, dense coding, and pure-state entanglement conversions. *IEEE Trans Inform Theory*, 2015, 61: 582–608
- 231 Rozpędek F, Schiet T, Thinh L P, et al. Optimizing practical entanglement distillation. *Phys Rev A*, 2018, 97: 062333
- 232 Fang K, Liu Z W. No-go theorems for quantum resource purification: new approach and channel theory. *PRX Quantum*, 2022, 3: 010337
- 233 Regula B, Fang K, Wang X, et al. One-shot entanglement distillation beyond local operations and classical communication. *New J Phys*, 2019, 21: 103017
- 234 Fang K, Wang X, Tomamichel M, et al. Non-asymptotic entanglement distillation. *IEEE Trans Inform Theory*, 2019, 65: 6454–6465
- 235 Zhao X, Zhao B, Wang Z, et al. Practical distributed quantum information processing with LOCCNet. *npj Quantum Inf*, 2021, 7: 159
- 236 Fang K, Fawzi H. The sum-of-squares hierarchy on the sphere and applications in quantum information theory. *Math Program*, 2021, 190: 331–360
- 237 Regula B, Takagi R. Fundamental limitations on distillation of quantum channel resources. *Nat Commun*, 2021, 12: 4411
- 238 Zhang H, Xu X, Zhang C, et al. Variational quantum circuit learning of entanglement purification in multi-degree-of-freedom. 2022. ArXiv:2209.08306
- 239 Fang K, Liu Z W. No-go theorems for quantum resource purification. *Phys Rev Lett*, 2020, 125: 060405
- 240 Kalb N, Reiserer A A, Humphreys P C, et al. Entanglement distillation between solid-state quantum network nodes. *Science*,

- 2017, 356: 928–932
- 241 Abdelkhalek D, Syllwasschy M, Cerf N J, et al. Efficient entanglement distillation without quantum memory. *Nat Commun*, 2016, 7: 1–7
- 242 Ecker S, Sohr P, Bulla L, et al. Experimental single-copy entanglement distillation. *Phys Rev Lett*, 2021, 127: 040506
- 243 Gottesman D. Stabilizer codes and quantum error correction. 1997. ArXiv:quant-ph/9705052
- 244 Gaitan F. Quantum Error Correction and Fault Tolerant Quantum Computing. Boca Raton: CRC Press, 2008
- 245 Lidar D A, Brun T A. Quantum Error Correction. Cambridge: Cambridge University Press, 2013
- 246 Terhal B M. Quantum error correction for quantum memories. *Rev Mod Phys*, 2015, 87: 307–346
- 247 Suter D, Álvarez G A. Colloquium: protecting quantum information against environmental noise. *Rev Mod Phys*, 2016, 88: 041001
- 248 Ofek N, Petrenko A, Heeres R, et al. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature*, 2016, 536: 441–445
- 249 Linke N M, Gutierrez M, Landsman K A, et al. Fault-tolerant quantum error detection. *Sci Adv*, 2017, 3: e1701074
- 250 Wootton J R, Loss D. Repetition code of 15 qubits. *Phys Rev A*, 2018, 97: 052313
- 251 Harper R, Flammia S T. Fault-tolerant logical gates in the IBM quantum experience. *Phys Rev Lett*, 2019, 122: 080504
- 252 Livingston W P, Blok M S, Flurin E, et al. Experimental demonstration of continuous quantum error correction. *Nat Commun*, 2022, 13: 2307
- 253 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM*, 1978, 21: 120–126
- 254 Shor P. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994. 124–134
- 255 Travagnin M, Lewis A. Quantum Key Distribution In-field Implementations. EUR 29865 EN, Publications Office of the European Union. 2019
- 256 Zhang Q, Xu F, Chen Y A, et al. Large scale quantum key distribution: challenges and solutions [Invited]. *Opt Express*, 2018, 26: 24260
- 257 Hwang W Y. Quantum key distribution with high loss: toward global secure communication. *Phys Rev Lett*, 2003, 91: 057901
- 258 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys Rev Lett*, 2005, 94: 230503
- 259 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. *Phys Rev Lett*, 2005, 94: 230504
- 260 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Phys Rev Lett*, 2012, 108: 130503
- 261 Zhang G W, Chen W, Fan-Yuan G J, et al. Polarization-insensitive quantum key distribution using planar lightwave circuit chips. *Sci China Inf Sci*, 2022, 65: 200506
- 262 Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices. *Rev Mod Phys*, 2020, 92: 025002
- 263 Pirandola S, Andersen U L, Banchi L, et al. Advances in quantum cryptography. *Adv Opt Photon*, 2020, 12: 1012
- 264 George I, Lin J, van Himbeeck T, et al. Finite-key analysis of quantum key distribution with characterized devices using entropy accumulation. 2022. ArXiv:2203.06554
- 265 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
- 266 Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre. *Nat Photon*, 2022, 16: 154–161
- 267 Ren S, Wang Y, Su X. Hybrid quantum key distribution network. *Sci China Inf Sci*, 2022, 65: 200502
- 268 Fitzsimons J F. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Inf*, 2017, 3: 23
- 269 Morimae T, Koshiya T. Impossibility of perfectly-secure one-round delegated quantum computing for classical client. *Quantum Inform Comput*, 2019, 19: 214–221
- 270 Aaronson S, Cojocaru A, Gheorghiu A, et al. Complexity-theoretic limitations on blind delegated quantum computation. 2017. ArXiv:1704.08482
- 271 Mantri A, Demarie T F, Fitzsimons J F. Universality of quantum computation with cluster states and (X, Y) -plane measurements. *Sci Rep*, 2017, 7: 42861
- 272 Morimae T, Fujii K. Blind quantum computation protocol in which Alice only makes measurements. *Phys Rev A*, 2013, 87: 050301
- 273 Shan R T, Chen X, Yuan K G. Multi-party blind quantum computation protocol with mutual authentication in network. *Sci China Inf Sci*, 2021, 64: 162302
- 274 Reichardt B W, Unger F, Vazirani U. Classical command of quantum systems. *Nature*, 2013, 496: 456–460
- 275 McKague M. Interactive proofs for BQP via self-tested graph states. *Theor Comput*, 2016, 12: 1–42
- 276 Barz S, Kashefi E, Broadbent A, et al. Demonstration of blind quantum computing. *Science*, 2012, 335: 303–308
- 277 Huang H L, Zhao Q, Ma X, et al. Experimental blind quantum computing for a classical client. *Phys Rev Lett*, 2017, 119: 050503
- 278 Greganti C, Roehsner M C, Barz S, et al. Demonstration of measurement-only blind quantum computing. *New J Phys*,

- 2016, 18: 013020
- 279 Lynch N A. *Distributed Algorithms*. San Francisco: Morgan Kaufmann Publishers Inc., 1996
- 280 Tani S, Kobayashi H, Matsumoto K. Exact quantum algorithms for the leader election problem. *ACM Trans Comput Theory*, 2012, 4: 1–24
- 281 Angluin D. Local and global properties in networks of processors (extended abstract). In: *Proceedings of the 12th Annual ACM Symposium on Theory of Computing*, 1980. 82–83
- 282 Itai A, Rodeh M. Symmetry breaking in distributed networks. *Inf Comput*, 1990, 88: 60–87
- 283 Yamashita M, Kameda T. Computing on anonymous networks. I. Characterizing the solvable cases. *IEEE Trans Parallel Distrib Syst*, 1996, 7: 69–89
- 284 Kobayashi H, Matsumoto K, Tani S. Simpler exact leader election via quantum reduction. *Chicago J Theor Comp Sci*, 2014, 20: 1–31
- 285 Okubo Y, Wang X B, Jiang Y K, et al. Experimental demonstration of quantum leader election in linear optics. *Phys Rev A*, 2008, 77: 032343
- 286 van Meter R, Nemoto K, Munro W. Communication links for distributed quantum computation. *IEEE Trans Comput*, 2007, 56: 1643–1653
- 287 Buhrman H, Röhrig H. Distributed quantum computing. In: *Mathematical Foundations of Computer Science*. Berlin: Springer, 2003
- 288 van Meter R, Devitt S J. The path to scalable distributed quantum computing. *Computer*, 2016, 49: 31–42
- 289 Beals R, Brierley S, Gray O, et al. Efficient distributed quantum computing. *Proc R Soc A*, 2013, 469: 20120686
- 290 Bravyi S, Dial O, Gambetta J M, et al. The future of quantum computing with superconducting qubits. *J Appl Phys*, 2022, 132: 160902
- 291 Piveteau C, Sutter D. Circuit knitting with classical communication. 2022. ArXiv:2205.00016
- 292 DiAdamo S, Ghibaudo M, Cruise J. Distributed quantum computing and network control for accelerated VQE. *IEEE Trans Quantum Eng*, 2021, 2: 1–21
- 293 Parekh R, Ricciardi A, Darwish A, et al. Quantum algorithms and simulation for parallel and distributed quantum computing. 2022. ArXiv:2106.06841
- 294 Häner T, Steiger D S, Hoefer T, et al. Distributed quantum computing with QMPI. In: *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, 2021. 1–13
- 295 Ferrari D, Cacciapuoti A S, Amoretti M, et al. Compiler design for distributed quantum computing. *IEEE Trans Quantum Eng*, 2021, 2: 1–20
- 296 Eisert J, Jacobs K, Papadopoulos P, et al. Optimal local implementation of nonlocal quantum gates. *Phys Rev A*, 2000, 62: 052317
- 297 Gottesman D, Chuang I L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 1999, 402: 390–393
- 298 Chou K S, Blumoff J Z, Wang C S, et al. Deterministic teleportation of a quantum gate between two logical qubits. *Nature*, 2018, 561: 368–373
- 299 Wan Y, Kienzler D, Erickson S D, et al. Quantum gate teleportation between separated qubits in a trapped-ion processor. *Science*, 2019, 364: 875–878
- 300 Daiss S, Langenfeld S, Welte S, et al. A quantum-logic gate between distant quantum-network modules. *Science*, 2021, 371: 614–617
- 301 Cleve R, Dam W V, Nielsen M, et al. Quantum entanglement and the communication complexity of the inner product function. In: *Proceedings of NASA International Conference on Quantum Computing and Quantum Communications*, 1998. 61–74
- 302 Buhrman H, Cleve R, Wigderson A. Quantum vs. classical communication and computation. In: *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, 1998. 63–68
- 303 Anshu A, Touchette D, Yao P, et al. Exponential separation of quantum communication and classical information. In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, 2017. 277–288
- 304 Brukner Č, Żukowski M, Pan J W, et al. Bell's inequalities and quantum communication complexity. *Phys Rev Lett*, 2004, 92: 127901
- 305 Wei K, Tischler N, Zhao S R, et al. Experimental quantum switching for exponentially superior quantum communication complexity. *Phys Rev Lett*, 2019, 122: 120504
- 306 Buhrman H, Cleve R, Watrous J, et al. Quantum fingerprinting. *Phys Rev Lett*, 2001, 87: 167902
- 307 Zhong X, Xu F, Lo H K, et al. Efficient experimental quantum fingerprinting with channel multiplexing and simultaneous detection. *Nat Commun*, 2021, 12: 4464
- 308 Einstein A. Zur elektrodynamik bewegter Körper. *Ann Phys*, 1905, 322: 891–921
- 309 Eddington A S. *The Mathematical Theory of Relativity*. Cambridge: Cambridge University Press, 1923
- 310 Yurtsever U, Dowling J P. Lorentz-invariant look at quantum clock-synchronization protocols based on distributed entanglement. *Phys Rev A*, 2002, 65: 052317

- 311 Krčo M, Paul P. Quantum clock synchronization: multiparty protocol. *Phys Rev A*, 2002, 66: 024305
- 312 Ben-Av R, Exman I. Optimized multiparty quantum clock synchronization. *Phys Rev A*, 2011, 84: 014301
- 313 Kómár P, Kessler E M, Bishof M, et al. A quantum network of clocks. *Nat Phys*, 2014, 10: 582–587
- 314 Quan R, Zhai Y, Wang M, et al. Demonstration of quantum synchronization based on second-order quantum coherence of entangled photons. *Sci Rep*, 2016, 6: 30453
- 315 Giovannetti V, Lloyd S, Maccone L. Quantum-enhanced positioning and clock synchronization. *Nature*, 2001, 412: 417–419
- 316 Valencia A, Scarcelli G, Shih Y. Distant clock synchronization using entangled photon pairs. *Appl Phys Lett*, 2004, 85: 2655–2657
- 317 Kong X, Xin T, Wei S, et al. Implementation of multiparty quantum clock synchronization. 2017. ArXiv:1708.06050
- 318 Lee J, Shen L, Ceré A, et al. Symmetrical clock synchronization with time-correlated photon pairs. *Appl Phys Lett*, 2019, 114: 101102
- 319 Troupé J, Haldar S, Agullo I, et al. Quantum clock synchronization for future NASA deep space quantum links and fundamental science. 2022. ArXiv:2209.15122
- 320 Lawson P. Principles of long baseline stellar interferometry. *JPL*, 2000. <https://hdl.handle.net/1813/41240>
- 321 Zernike F. The concept of degree of coherence and its application to optical problems. *Physica*, 1938, 5: 785–795
- 322 Khabiboulline E T, Borregaard J, De Greve K, et al. Optical interferometry with quantum networks. *Phys Rev Lett*, 2019, 123: 070504
- 323 Khabiboulline E T, Borregaard J, De Greve K, et al. Quantum-assisted telescope arrays. *Phys Rev A*, 2019, 100: 022316
- 324 Cacciapuoti A S, Caleffi M, Tafuri F, et al. Quantum internet: networking challenges in distributed quantum computing. *IEEE Netw*, 2020, 34: 137–143
- 325 Satoh T, Nagayama S, Suzuki S, et al. Attacking the quantum internet. *IEEE Trans Quantum Eng*, 2021, 2: 1–17
- 326 Bernstein D J, Lange T. Post-quantum cryptography. *Nature*, 2017, 549: 188–194
- 327 Wang J, Liu L, Lyu S, et al. Quantum-safe cryptography: crossroads of coding theory and cryptography. *Sci China Inf Sci*, 2022, 65: 111301
- 328 Huang Y, Zhang F, Liu Z, et al. Pseudorandom number generator based on supersingular elliptic curve isogenies. *Sci China Inf Sci*, 2022, 65: 159101
- 329 Tao Y, Ji Y, Zhang R. Generalizing Lyubashevsky-Wichs trapdoor sampler for NTRU lattices. *Sci China Inf Sci*, 2022, 65: 159103
- 330 Liu J, Yu Y, Bi H, et al. Post quantum secure fair data trading with deterability based on machine learning. *Sci China Inf Sci*, 2022, 65: 170308
- 331 Bavdekar R, Chopde E J, Agrawal A, et al. Post quantum cryptography: a review of techniques, challenges and standardizations. In: Proceedings of International Conference on Information Networking (ICOIN), 2023. 146–151
- 332 Wehrle K, Günes M, Gross J. Modeling and Tools for Network Simulation. Berlin: Springer, 2010
- 333 Baidu Quantum. QNET. 2022. Official website at <https://quantum-hub.baidu.com/qnet/>, Source code available at <https://github.com/baidu/QCompute/tree/master/Extensions/QuantumNetwork>
- 334 Deutsch D E. Quantum computational networks. *Proc Royal Soc London A*, 1989, 425: 73–90
- 335 Barenco A, Bennett C H, Cleve R, et al. Elementary gates for quantum computation. *Phys Rev A*, 1995, 52: 3457–3467
- 336 Morimae T. Verification for measurement-only blind quantum computing. *Phys Rev A*, 2014, 89: 060302
- 337 Li X, Fang K. Methods, devices and electronic apparatus for quantum computing. Patent No. CN202210324719.5, 2022
- 338 Fang K, Li X. Method and device for operating quantum system of one-way quantum computer calculation model. Patent No. CN202210858691.3, 2022
- 339 Fang K, Zhao J. Methods, devices and electronic apparatus for simulating quantum network protocols. Patent No. CN202210885409.0, 2022
- 340 Dahlberg A, van der Vecht B, Donne C D, et al. NetQASM-a low-level instruction set architecture for hybrid quantum-classical programs in a quantum internet. *Quantum Sci Technol*, 2022, 7: 035023
- 341 Fang K, Li Y. Request processing methods, apparatus and electronic device. Patent No. CN2022114860192, 2022
- 342 Fang K, Li Y. Quantum key distribution method, apparatus and electronic device. Patent No. CN2022114862164, 2022
- 343 Clauser J F, Horne M A, Shimony A, et al. Proposed experiment to test local hidden-variable theories. *Phys Rev Lett*, 1969, 23: 880–884
- 344 Montanaro A, de Wolf R. A survey of quantum property testing. 2013. ArXiv:1310.2035

Appendix A Global efforts in quantum networks

Year	Nation	Plan/Strategy/Project
2022	Singapore	National Quantum-Safe Network in the Quantum Engineering Program
2022	US	The Quantum Cybersecurity Preparedness Act
2021	China	The 14th Five-Year Plan for National Informatization
2021	Japan	Quantum Networks Whitepaper
2021	EU	The European Quantum Communication Infrastructure (EuroQCI) Initiative
2021	Australia	Digital Economy Strategy 2030
2021	US	Quantum Network Infrastructure and Workforce Development Act of 2021
2021	US	A Coordinated Approach To Quantum Networking Research
2021	UK	Quantum Communications Hub
2020	US	Quantum Internet Blueprint
2020	US	A Strategic Vision For America's Quantum Networks
2020	Russia	Quantum Communication Roadmap
2019	Germany	QuNET-Initiative
2019	UK	Cambridge Quantum Network
2019	EU	Quantum Technologies in Space Policy White Paper
2019	EU	European Industry White Paper on the European Quantum Communication Infrastructure
2018	Russia	Russian Digital Economy
2018	EU	Quantum Technologies Flagship
2017	China	Beijing-Shanghai Trunk Line
2016	China	Micius Quantum Satellite
2016	EU	Quantum Technology in Space, QTSPACE
2010	Japan	Tokyo QKD network
2009	Switzerland	Geneva Area Network
2009	China	Chinese Hierarchical Network, Wuhu
2003	Austria	SECOCQ QKD Network
2001	US	DARPA Quantum Network

Figure A1 (Color online) Partial list of the national plans/strategies/projects of quantum networks.

Year	Nation	Company	Year	Nation	Company
2022	US	Amazon	2017	US	Qunnect
2021	US	Cisco	2017	UK	Arqit
2021	UK	BT	2017	UK	Craft Prospect
2021	UK	nodeQ	2016	Canada	Crypto4A
2020	Canada	Xanadu	2016	UK	KETS
2019	China	Qudoor	2016	Canada	QEYnet
2019	Canada	Quantum Bridge Technologies	2015	Canada	evolutionQ
2019	US	Aliro Quantum	2009	China	QuantumCTek
2018	China	Baidu	2008	Australia	QuintessenceLabs
2017	China	XT Quantum	2003	Japan	Toshiba
2017	Japan	NTT	2001	Switzerland	ID Quantique
2017	US	AT&T	1999	US	MagiQ

Figure A2 (Color online) Partial list of the industrial participants working on quantum networks.

Appendix B UML class diagram of QNET

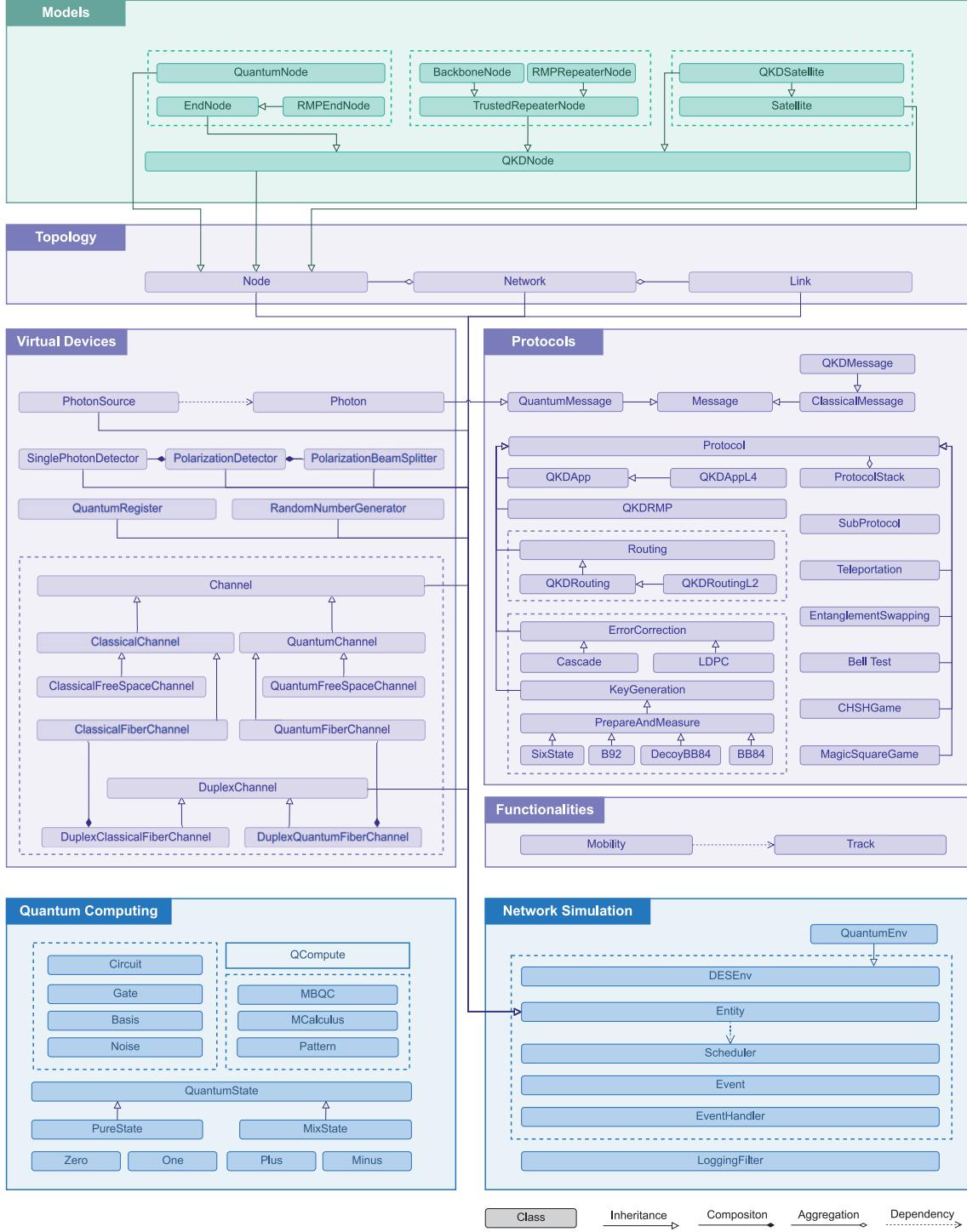


Figure B1 (Color online) UML class diagram laying out the structure of QNET (based on version 1.2.0). The main classes in each module are highlighted in shaded boxes, and their relationship in terms of inheritance, composition, aggregation, and dependency are depicted by different types of arrows.

Appendix C Compilation of quantum network protocols

In this section, we discuss the compilation techniques used to convert quantum network protocols into quantum circuits in further detail. We start by discussing the instructions that are usually used in quantum circuits. Then we introduce the design of the local quantum register and its instructions. Based on these instructions, we introduce the algorithms that compile local operations as

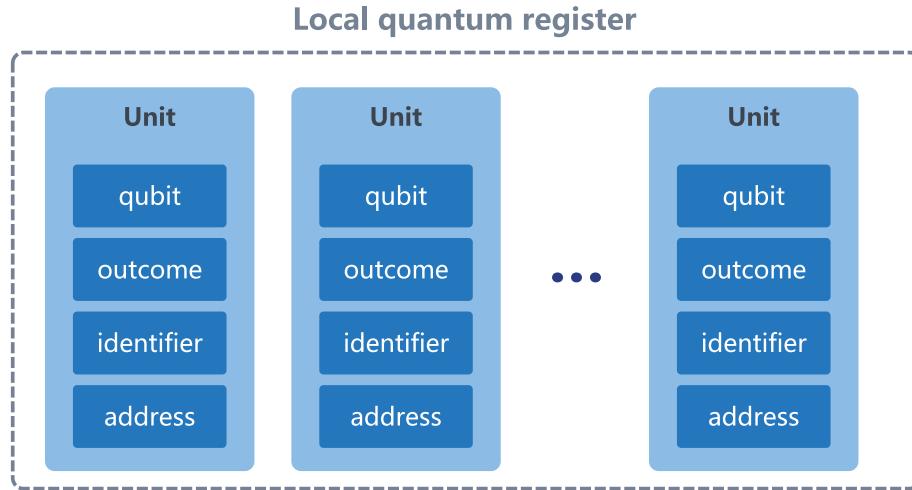


Figure C1 (Color online) Structure of a local quantum register that has several units. Each unit has four attributes, qubit, outcome, identifier, and address.

well as qubit transmission to quantum circuit instructions. Putting them together, we can eventually compile a quantum network protocol that involves different parties into one single quantum circuit in general.

Quantum circuit and its instructions. A quantum circuit usually contains quantum gates and quantum measurements. It is called a standard quantum circuit if all measurements are performed at the end of the circuit. According to the execution order, a quantum circuit can be represented as an ordered list of instructions. Each instruction is identified by a triplet [NAME, REG, PAR], indicating the name of the operation, the quantum register it acts on, and the relevant parameters (set to none if no parameters). For example, [rx, 2, pi] means that an R_x rotation gate is applied to qubit 2, and the rotation angle is π ; [cnot, [1, 3], none] means that a controlled-NOT gate is applied to qubits 1 and 3, where qubit 1 is the control qubit and qubit 3 is the target qubit; and [measure, 2, none] means that qubit 2 is measured in the computational basis. More generally, in some quantum circuits, a quantum gate on one qubit can be conditioned on the measurement outcome of the other qubit. Such circuits are called dynamic quantum circuits. The classically controlled quantum gate in a dynamic quantum circuit can be represented by a quadruple [NAME, REG, PAR, COND], where the COND indicates that the operation is controlled by the measurement outcome of the qubit to which it points. For example, [x, 2, none, 4] means that a Pauli-X gate is applied to qubit 2 if the measurement outcome of qubit 4 is one; otherwise, the gate is not applied.

Local quantum register and its instructions. Quantum network protocol is different from the quantum circuit. It involves not only local operations at each node but also the transmission of quantum and classical information between different nodes. To formulate the local operations of each node, we propose a design of the local quantum register, which contains multiple units and each unit has four attributes, qubit, outcome, identifier, and address (see Figure C1). The default values for qubit and outcome are set to be empty, and the default value for the identifier is the node itself. Any instruction on the local register can be identified by a quadruple [NAME, ADDR, PAR, COND], indicating the name of the instruction, the address of the unit to operate (if the instruction is a double-qubit gate, then the ADDR is a list, whose first element is the control qubit and the second element is the target qubit), the relevant parameters of the instruction, and the classically controlled condition of the instruction. For example, the instruction [x, 1, none, none] means that a Pauli-X gate is performed on unit 1 of the local register. Note that the instructions on the quantum circuit and the local quantum register are both characterized by quadruples. But ADDR and REG have completely different meanings. The former refers to the address of a local register at a network node, whereas the latter refers to the register of a global quantum circuit. The idea of our compilation is trying to build a connection between them.

Compilation of local operations and qubit transmission. Now we present how instructions for local registers are compiled into instructions for a global quantum circuit. The compilation of single-qubit operation is given in Algorithm C1, and the compilation of double-qubit operation is given in Algorithm C2.

Algorithm C1 Compiling single-qubit operation

Input: A local operation [NAME, ADDR, PAR, COND], and the current list of quantum circuit instructions circuit.

Output: A list of updated circuit instructions.

```

1. if the qubit attribute in the local unit of address ADDR is empty then
   | 1.1 Get the largest REG index x among all instructions of the input circuit 1.2 write x + 1 into the qubit attribute of the local
   | unit of address ADDR;
end
2. Get the qubit value of the local unit of address ADDR, and record it as REG;
3. Append the circuit instruction [NAME, REG, PAR, COND] to the end of circuit and return it;
4. if NAME is measure then
   | Write the value of REG into the outcome attribute of the local unit of address ADDR.
end

```

Note that if the local operation is a quantum measurement, the REG needs to be written into the outcome attribute of the local unit of address ADDR. Since the quantum circuit is not yet implemented at this point, the outcome here stores the register to be measured rather than an actual measurement outcome.

Similar to the single-qubit operation, we can compile a double-qubit operation as follows.

Algorithm C2 Compiling double-qubit operation

Input: A local operation [NAME, ADDR, PAR, COND], and the current list of quantum circuit instructions circuit.
Output: A list of updated circuit instructions.

1. Set ADDR0 and ADDR1 to be the first and second elements of ADDR, respectively;
2. Get the largest REG index x among all instructions of the input circuit and set f to be x ;
3. **if** the qubit attribute in the local unit of address ADDR0 is empty **then**
| Set f to be $f + 1$ and then write f into the qubit attribute of the local unit of address ADDR0;
end
4. **if** the qubit attribute in the local unit of address ADDR1 is empty **then**
| Set f to be $f + 1$ and then write f into the qubit attribute of the local unit of address ADDR1;
end
5. Get the qubit value of the local unit of address ADDR0, and record it as REG0; get the qubit value of the local unit of address ADDR1, and record it as REG1;
6. Append the circuit instruction [NAME, [REG0, REG1], PAR, COND] to the end of circuit and return it.

The compilation of qubit transmission is given in Algorithm C3. Note that the transmission of a qubit does not change the global quantum circuit, but updates the information of local quantum registers at both the source and destination nodes. The qubit stored in the register unit is not really a qubit, but its corresponding register index in the global quantum circuit. By sending this information from source to destination, we effectively transfer the right to manipulate this qubit on the quantum circuit. It is also important that we reset a local unit once the qubit is sent so that the no-cloning theorem is not violated. When the destination receives a quantum message, it is stored in the available unit with the smallest address as default, and the identifier records the source of this qubit.

Algorithm C3 Compiling qubit transmission

Input: Source node src, destination node dst, address of local register unit ADDR.
Output: Updated quantum registers at the source and destination nodes.

1. Get the qubit value of the register unit of address ADDR and record it as qmsg;
2. Reset the unit of address ADDR, i.e., rewrite its qubit value as empty and rewrite its identifier value as the node itself;
3. Send the qubit information qmsg to the node dst, i.e., find an empty unit with the smallest address at the node dst, set the qubit value of this unit as the received qmsg and set its identifier as src.

Combining Algorithms C1–C3, we can compile a complete quantum network protocol into one single quantum circuit. This is demonstrated in Algorithm C4.

Algorithm C4 Compiling quantum network protocol to dynamic quantum circuit

Input: A list of instructions of the network protocol.
Output: A list of instructions of the dynamic circuit.

1. Create an empty list of instructions circuit;
2. **foreach** instruction from the input **do**
| Using Algorithms C1–C3 to compile this instruction to a circuit instruction and update the list circuit;
end
3. Return the list of circuit instructions circuit.

Dynamic quantum circuits provide an accurate and logical description of quantum protocols, but their implementation can still be challenging. Therefore, we will use the principle of deferred measurement to replace a classically controlled quantum gate with a quantum-controlled gate to obtain an equivalent standard quantum circuit. This is presented in the following Algorithm C5.

Algorithm C5 Deferring quantum measurement

Input: A list of circuit instructions circuit.
Output: A list of updated circuit instructions.

1. **foreach** instruction from the input **do**
 - if COND of this instruction is not empty **then**
| Replace this instruction with [CNAME, [COND, REG], PAR], where CNAME is the controlled version of the instruction (e.g., CNAME = cnot if NAME = x);
end
 - if the current gate is a measurement operation **then**
| Add it to the measured_gates list;
end**end**
2. Move all measurement instructions to the end of the list while leaving the remaining items unchanged;
3. Return the list of instructions circuit.
