

DOI:10.1145/3524455

A deep dive into the quantum Internet's potential to transform and disrupt.

BY LASZLO GYONGYOSI AND SANDOR IMRE

Advances in the Quantum Internet

QUANTUM INFORMATION WILL not only reformulate our view of the nature of computation and communication but will also open up fundamentally new possibilities for realizing high-performance computer architecture and telecommunication networks. Since our data will no longer remain safe in the traditional Internet when commercial quantum computers become fully available,^{1,2,8,15,34} there will be a need for a fundamentally different network structure: the quantum Internet.^{22,25,32,33,45,47} While *quantum computational supremacy* refers to tasks and problems that quantum computers can solve but are beyond the capability of classical computers, the *quantum supremacy of the quantum Internet* identifies the properties and attributes that the quantum Internet offers but are unavailable in the traditional Internet.^a

^a While “supremacy” is a concept used to describe the theory of computational complexity^{1,15} and not a specific device (like a quantum computer), the supremacy of the quantum Internet in the current context refers to the collection of those advanced networking properties and attributes that are beyond the capabilities of the traditional Internet.

The quantum Internet uses the fundamental concepts of quantum mechanics for networking (see Sidebars 1–7 in the online Supplementary Information at <https://dl.acm.org/doi/10.1145/3524455>). The main attributes of the quantum Internet are **advanced quantum phenomena and protocols** (such as quantum superposition and quantum entanglement, quantum teleportation, and advanced quantum coding methods), **unconditional security** (quantum cryptography), and an **entangled network structure**.

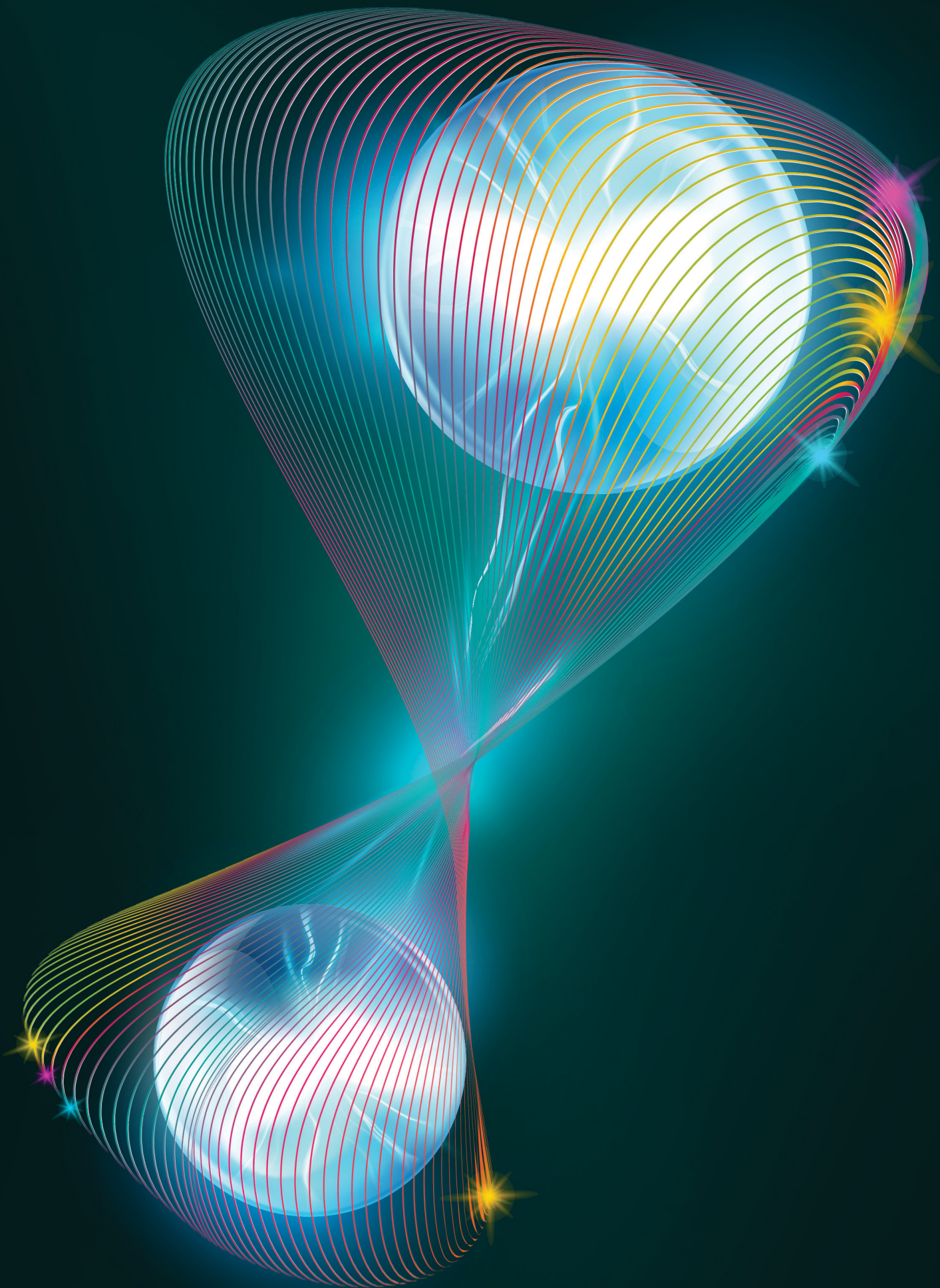
In contrast to traditional repeaters,^b quantum repeaters cannot apply the receive–copy–retransmit mechanism because of the so-called no-cloning theorem, which states that it is impossible to make a perfect copy of a quantum system (see Sidebar 4). This fundamental difference between the nature of classical and quantum information does not just lead to fundamentally different networking mechanisms; it also necessitates the definition of novel networking services in a quantum Internet scenario. Quantum memories in quantum repeater units are a fundamental part of any global-scale quantum Internet. A challenge connected to quantum memory units is the noise quantum memories adds to storing quantum systems. However, while quantum repeaters can be realized without requiring quantum memories, these units are, in fact, necessary to guarantee optimal performance in any high-performance quantum-networking scenario.

In 2019, the National Quantum

^b Traditional repeaters rely on signal amplification.

» key insights

- The quantum Internet is an adequate answer to the security issues that will become relevant as commercial quantum computers hit the market.
- The quantum Internet is based on the fundamentals of quantum mechanics to provide advanced, high-security network communications.
- The quantum Internet gives users many capabilities and services not available in a traditional Internet setting.



Initiative Act (NQIA)²⁸ established quantum research funding via the U.S. government, while European Union (EU) member countries participate in the European Quantum Communications Infrastructure (EuroQCI) initiative,⁴³ which follows the launch of the Quantum Technologies Flagship 2018,³⁷ according to the European Quantum Manifesto 2016.³⁶ EuroQCI focuses primarily on quantum key distribution (QKD) networks across Europe, which can later be extended to the quantum Internet to deliver

quantum information among quantum computers. EuroQCI networks consist of two main segments. The **ground segment** connects optical fiber-based countrywide systems with cross-border links and contains satellite-receiver ground stations. Test-bed networks are being deployed.^{5,44} The **space segment** will share quantum secret key materials between distant ground stations, either via low earth orbit (LEO)/medium earth orbit (MEO) satellites using prepare and measure protocols, or via geostationary earth orbit (GEO) satellites

applying entanglement-based protocols.³⁸ In 2017, China began researching the implementation of a global-scale QKD network.⁵⁰

The novel contributions of this article include a review of the quantum Internet's fundamental structural properties, a discussion of quantum Internet's advantages over the traditional Internet, a summarization of basic concepts and enabling technologies of the quantum Internet, and a study of the recent implementation basis and open problems in a near-term setting. Additional material is included in the tables and online sidebars.

Preliminaries

In a quantum Internet setting, one main task is to distribute quantum entanglement from a quantum source node to a quantum target node via a set of intermediate quantum nodes called quantum repeaters. Entanglement distribution is achieved in a step-by-step manner by the generation of short-distance, entangled connections between quantum nodes. An entangled connection characterizes an entangled state prepared at the nodes, not the physical link between them.

Next, the entanglement level (see the supplemental online sidebars) of the entangled connections is increased to generate longer-distance entangled connections. The entanglement level of an entangled connection determines the *hop distance* (the number of quantum nodes spanned by the entangled connection) between the source node and the target node of the given entangled connection. The increment level is realized by the so-called *entanglement purification and swapping* (entanglement improvement and extension) procedure applied in the intermediate quantum repeaters (see a description of these terms later in the article).

Quantum-state implementation. In the physical layer, a quantum state can be implemented via several different technologies. Table 1 depicts the relevant properties of these technologies, with related works. The discussion focuses on a near-term setting; therefore, related technologies implement qubit systems.

Entanglement generation. Quantum entanglement can be generated via several different probabilistic physical

Table 1. Technologies for quantum-state implementation.

Quantum-state implementation technology	Attributes
Photonic qubits	Uses photons as qubits and optical devices. Photons can be controlled and manipulated by standard optical devices. Low-cost implementations for optical fibers and wireless optical channels, optical communications, entanglement generation and distribution, quantum cryptography, and optical quantum computations.
Solid-state technology	Uses electron spins and superconducting circuits and interacts with standard RF and microwave devices. Allows efficient implementation via current semiconductor devices to realize large-scale computing applications, quantum memories, and quantum computers.
Superconducting technology	Uses Josephson junctions, interconnects, passive elements, inductors, and capacitors. Allows high-fidelity implementations for fault-tolerant quantum computing, high-speed quantum gates, and large-scale quantum computers, and supports microwave technology interaction.
Cavity quantum electrodynamics	Uses a coherent interaction between a quantum matter system (quantum dot system, trapped ion, and so on) and the field of an optical or microwave resonator. Allows the coupling of atoms with photons in cavities to generate atom-atom, atom-photon, and photon-photon entanglement.
Trapped ions	Uses trapped ions to implement quantum states. Allows high-fidelity implementations for fault-tolerant quantum computing, high-speed quantum gates, and large-scale quantum computing applications with high connectivity in the physical layer.

Table 2. Methods of entanglement generation.

Entanglement generation method	Attributes
Spontaneous parametric down conversion (photon-photon entanglement)	Uses a laser beam and crystal. Photons are employed for entanglement generation and distribution via the incidence of the laser beam on a crystal. Photon transmission between distant points can be implemented via optical fiber with a low attenuation. High success rate.
Single-atom excitation by laser beam (photon-atom entanglement)	Uses an optical cavity and a laser beam. Atoms are coupled with an optical cavity. In the emission phase, a laser beam results in atom-entangled photons in the cavity of the sender. In the absorption phase, photons are absorbed and mapped onto the state of remote atoms in the cavity of the receiver. Sender and receiver atoms are entangled by photons, and the communication channel can be implemented via an optical channel. Lower success rate.
Two-atom simultaneous excitation by laser beam (atom-atom entanglement)	Uses a laser beam, optical cavity, and measurement on the quantum channel between the sender and the receiver. In the cavities of the sender and receiver, two atoms are simultaneously excited by a laser beam, resulting in two atom-entangled photons. They are transmitted from the cavities of the sender and receiver over an optical channel, and the photons are measured on the optical channel between them. The communication channel between the sender and receiver can be implemented via an optical channel. Lower success rate.

Table 3. Entanglement distribution schemes.

Entanglement distribution method	Entanglement distribution requirements	Interaction dynamics	Implementation
Direct interaction	Direct interaction between Alice's particle A and Bob's particle B .	Closed (unitary) or open dynamics, A and B interact directly via Hamiltonian H_{AB} .	Direct interaction between A and B , and direct transmission of entangled subsystem A or B .
Indirect interaction	An ancillary system (called flag) C mediates interactions between A and B .	A and B do not interact directly (that is, there is no Hamiltonian H_{AB}).	Indirect interaction between A and B , transmission of entangled or separable ancillary system C .
Discrete interaction	Indirect only, operations or discrete interactions on objects A and C at Alice, then C is sent to Bob, Bob performs operations on B and C to entangle A and B .	A and B do not interact directly (that is, there is no Hamiltonian H_{AB}).	Entangled ancillary system C : Alice entangles A and C , and then Bob performs entanglement swapping on B and C to entangle A and B . Separable (unentangled) ancillary system C : For a separable C , entanglement gain is bounded by a non-classical correlation (called quantum discord) between AB and the ancillary C .
Continuous interaction	Indirect, continuous (in time) interactions between A and C at Alice, and between B and C at Bob.	A and B do not interact directly (that is, there is no Hamiltonian H_{AB}).	Ancillary system C mediates continuous interactions between A and B^{23} to entangle separable A and B .

procedures. Table 2 summarizes the main attributes of these approaches, with related works.

Entanglement distribution. Table 3 summarizes the features of different entanglement distribution schemes, which are illustrated in Figure 1. Entanglement distribution methods use a quantum channel \mathcal{N} that can be implemented via optical fiber or a wireless optical channel (see Sidebar 4). Direct transmission of an entangled state (*quantum correlation*) requires a high-fidelity quantum channel, while the direct transmission of a separable state (*classical correlation*) can be implemented via more noisy quantum channels due to the fundamental characteristics of quantum and classical correlations.¹⁴

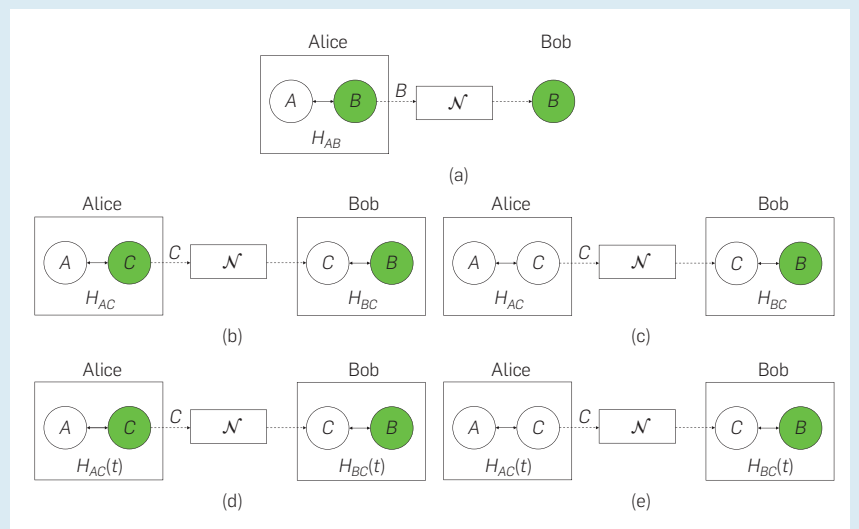
Enabling technologies. The main properties of enabling technologies for the quantum Internet are summarized in the online sidebars, as depicted in Table 4.

Unentangled and Entangled Structures of the Quantum Internet

Quantum communication networks can be classified into two main classes: *unentangled* and *entangled*. In an unentangled quantum network, connections between quantum nodes are formulated via unentangled quantum states. In an entangled quantum network, connections between quantum nodes are formulated via entangled states. The entangled states are stored within the internal quantum memories of the quantum nodes, such that the entangled connections span several hops

Figure 1. Entanglement distribution schemes.

- (a) **Direct interaction.** Quantum states A and B are in the same location. At Alice, two quantum states A and B are interacting via Hamiltonian H_{AB} . Alice sends the entangled B (in green) to Bob over a quantum channel \mathcal{N} . Bob receives B .
- (b) **Indirect, discrete interaction with entangled flag C** (in green). Quantum states A and B are at different locations. At Alice, quantum state A and flag system C are interacting via Hamiltonian H_{AC} , such that C becomes entangled with A . Alice sends the entangled flag C to Bob over \mathcal{N} . Bob receives C and applies a local Hamiltonian H_{BC} on B and C , resulting in the entangled state AB .
- (c) **Indirect, discrete interaction with separable flag C .** Quantum states A and B are at different locations. At Alice, quantum state A and flag system C are interacting via Hamiltonian H_{AC} , such that C will not be entangled with A or B . Alice sends the separable flag C to Bob over \mathcal{N} . Bob receives C and applies a local Hamiltonian H_{BC} on B and C , resulting in the entangled state AB .
- (d) **Indirect, continuous interaction with entangled flag C** (in green). Quantum states A and B are at different locations. At Alice, quantum state A and flag system C interact for a particular time t via a Hamiltonian H_{AC} , such that C becomes entangled with A . Alice sends the entangled flag C to Bob over \mathcal{N} . Bob receives C and applies a local Hamiltonian H_{BC} for a particular time t on B and C , resulting in the entangled state AB .
- (e) **Indirect, continuous interaction with separable flag C .** Quantum states A and B are at different locations. At Alice, quantum state A and flag system C are interacting for a particular time t via a Hamiltonian H_{AC} , such that C will not be entangled with A or B . Alice sends the separable flag C to Bob over \mathcal{N} . Bob receives C and applies a local Hamiltonian H_{BC} for a particular time t on B and C , resulting in the entangled state AB .



and are established over long distances. The characteristics and aims of the two types of quantum network models are fundamentally different.

While the main purpose in an unentangled quantum network is to implement a standard (unentangled) QKD protocol (see Sidebar 5) between the nodes in a point-by-point manner (or random number generation between nodes), the main task in an entangled quantum network is to distribute quantum entanglement over long distances. The services of unentangled and entangled quantum networks can be used to supplement the tasks of traditional networks—to ensure stronger encryption and security services, such as Internet Protocol Security (IPSec) or Transport Layer Security (TLS), with QKD; to reduce dependency on public-key methods and one-way functions; and to reduce the computational complexities of cryptographic methods, authentications, and privacy services. However, while unentangled quantum networks can only provide these supplemental services to traditional networks over short distances due to point-by-point, QKD-based quantum communication, the structure of entangled quantum networks allows us to construct a more complex network, called the quantum Internet.

In a quantum Internet scenario, the core network is an entangled quantum network, and the main aim is to provide



The experimental quantum Internet is currently in the development phase and exists in physics laboratories and as theoretical approaches.



Table 4. Sidebars of enabling technologies for the quantum Internet (see online Supplemental Information).

Enabling technology	Sidebar
Quantum entanglement	1
Entanglement fidelity	2
Quantum superposition	3
Quantum teleportation	3
Quantum dense coding	3
Quantum channel	4
No-cloning theorem	4
Quantum key distribution	5
Quantum repeater	6
Entanglement swapping	6
Entanglement purification	6
Entanglement levels	7
Doubling architecture	7

a general network structure for quantum computers (legal users) to establish reliable and secure long-distance quantum communications. Quantum entanglement and quantum repeaters are, therefore, fundamental to the concept of the quantum Internet. Quantum repeaters serve as intermediate quantum node transmitters between a sender node (Alice) and a receiver node (Bob) in the entanglement distribution process (EDP). Quantum entanglement enables communication distances to be extended over long spans (unlimited, in theory) via the EDP.

The entangled connections of entangled quantum networks span multiple nodes—that is, these are multi-hop connections. An entangled connection is created via the EDP, through many physical links. A given physical link, such as optical fiber or a wireless optical link, serves only temporarily in the distribution process because a physical link can only create entanglement over short distances. Therefore, the EDP is realized in a step-by-step manner via many physical links and by many short-distance entangled states. The end of the EDP is an end-to-end entangled state that spans over the intermediate nodes and physical links used in the distribution process between the sender and the receiver. In general, entanglement distribution is mainly referred to as the process of distributing entanglement of short links. Some important protocols for achieving this are the *meet-in-the-middle* or *sender-receiver* protocols.

In an unentangled quantum network, the achievable communication distances are limited because of the requirement of primarily point-by-point QKD between quantum nodes. However, several other uses are possible. Unentangled networks can also be used to transmit quantum information. To overcome the limitation of short distances in the transmission, one can encode a qubit into a quantum error correction code and place intermediate decode–encode stations after short distances. These stations simply decode the received logical qubit, thereby obtaining an error syndrome about which error occurred during transmission. Using the error syndrome, the station can hopefully correct for the error and encode the qubit again into a quantum error correction code. Note:

QKD does not ensure secure quantum communication, but it can be used to generate a secure classical key between two parties. QKD also does not provide stronger encryption, since it simply generates a secure classical key between two parties, which can be used for symmetric block ciphers, such as Advanced Encryption Standard (AES). If sufficient resources are available, such a key may even be used to perform one-time pad (OTP) encryption, which is perfectly secure given the key is perfectly random.

In an entangled quantum network, the entanglement distribution procedure eliminates the requirement of point-by-point quantum communications and extends it to a multi-hop quantum communication. Entangled quantum networks allow us to use all quantum protocols, such as QKD (see Ekert's entanglement-based QKD⁷) and other quantum cryptographic primitives similar to unentangled networks, but with the additional exploitation of the improved network structure, higher transmission reliability and rates, and significantly longer achievable

communication distances. As long-distance, end-to-end entangled states are available, the entangled quantum network can be used as a quantum local area network (QLAN), a quantum metropolitan area network (QMAN), a quantum wide area network (QWAN), or a global quantum Internet network.

In an entangled quantum network structure, one way to connect quantum networking devices is to use *bipartite entanglement* in the form of Bell pairs. Bell pairs are enough to generate any arbitrary state, either by merging them or by preparing the state locally and then teleporting qubits through the network. However, a lot of resources must be put into the network to generate arbitrary states in this way. Another variant of the entangled quantum network is the so-called *multipartite quantum network*. In these entangled network structures, the network device is connected using multipartite entangled quantum states,¹² cluster states, or multipartite entangled quantum states. Following such an approach for entangled quantum networks offers a very important

advantage over a network only using Bell pairs: If network clients want to share graph states or other multipartite entangled states, then the network devices or clients must apply much fewer merging operations at the end. This is a big advantage if the devices use a noisy apparatus, as a realistic setting implies, because every merging operation—for example, controlled phase gates, controlled NOT gates, and measurements—in which devices perform invariably introduces noise to the final state. Therefore, quantum networks using multipartite states to generate multipartite entangled states among clients (which are necessary for secret sharing, distributed sensing, and so on) introduce less noise to quantum systems in a realistic scenario—even though they are harder to implement experimentally, where the author certainly is right.

The entanglement level of an entangled connection determines the hop distance between a source node and the target node of the given entangled connection. The increment level is realized

Figure 2. Entangled network structure of a quantum Internet.

The quantum network consists of K source quantum nodes, $A_i, i = 1, \dots, K$, and K receiver quantum nodes (depicted by blue nodes); $B_i, i = 1, \dots, K$, and a set of intermediate quantum repeaters (depicted by gray nodes in the clouds); $R_i, i = 1, \dots, q$, between the sender and receiver quantum nodes; and satellites with free-space channels.

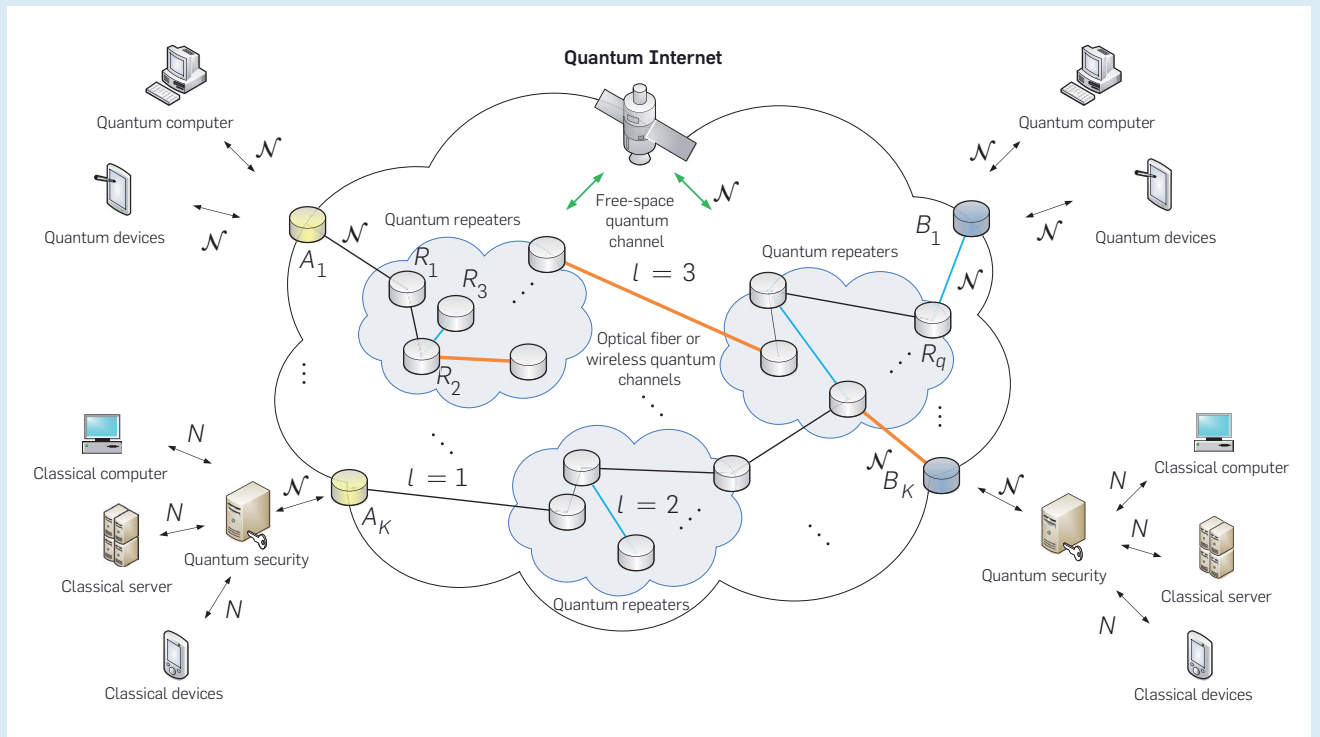


Table 5. Approaches to the quantum supremacy of the quantum Internet.

Network structure	Application	Benefits over classical networks	Fundamental concept of the quantum internet?
Entangled	Distributed cryptographic functions	Reduced computational complexity, decreased use of one-way functions and public key methods	Yes
	Distributed computation	Unconditional security	Yes
	High-precision sensor networks	Improved precision	Yes
	Advanced quantum protocols	Unconditional security, advanced communications (quantum teleportation, quantum encoding, and so on.)	Yes
	Multi-hop QKD	Unconditional security	Yes
	Multi-hop entanglement	Quantum Internet, long-distance quantum communications and QKD, and unconditional security over unlimited distances	Yes
	Extended secrecy for classical protocols	Unconditional security	Yes (Strong multi-hop settings)
Unentangled	Point-to-point QKD	Unconditional security	No (Limited distances, expandable by free-space quantum channels)
	Extended secrecy for classical protocols	Unconditional security	No (Weak multi-hop settings)

by the so-called entanglement swapping (entanglement extension) procedure applied in the intermediate quantum repeaters. Specifically, practical entanglement distribution is achieved within the framework of the doubling architecture (see Sidebar 7 and Figure 3), where each increment of the level of entanglement doubles the hop distance. At the end of the entanglement distribution procedure, the distant source node and the target node share a long-distance entangled connection.

At this point, we note that not all

quantum repeater schemes rely on the notion of increments. Particularly, only the early schemes for quantum repeaters with Bell pairs needed the nesting of purification and swapping of Bell pairs. Novel repeater schemes that use hashing entanglement purification do not need nesting at all, and therefore do not need a nesting of swapping and purification.

Apart from the use of the doubling architecture, third-generation quantum repeaters²⁹ can be implemented with highly entangled states and can be used

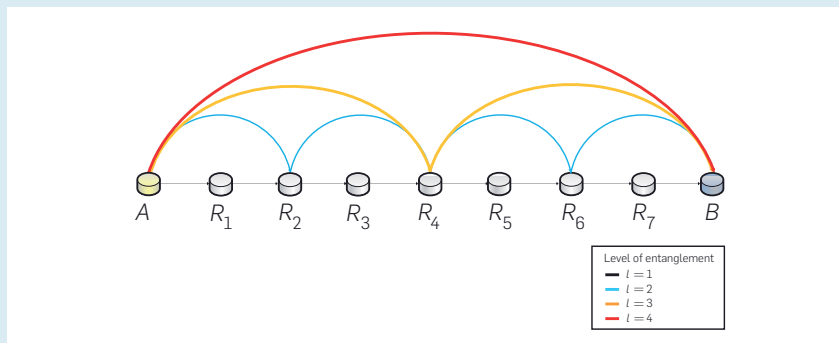
to distribute quantum information over long distances; thus, they can be used to distribute entanglement.

Table 5 summarizes the main approaches to the quantum supremacy of the quantum Internet. The main applications of the quantum Internet include the field of distributed computations, quantum secret sharing, blind quantum computation, client-server quantum communications, system area networks, distributed cryptographic functions (Byzantine agreement, leader election, QKD), and the field of sensor technology (interferometry, clocks, reference frames).⁴⁵

General architecture. Figure 2 depicts a general architecture of the quantum Internet. The network model consists of a set of legal users with quantum and classical devices as well as intermediate quantum repeaters with a set of entangled connections with different l entanglement levels. The quantum Internet integrates optical fiber and wireless optical channels between ground-to-ground quantum repeaters and free-space optical channels for ground-to-satellite communications. Quantum computers and quantum devices are communicating via an \mathcal{N} quantum channel (see Sidebar 4) with the abstract cloud of the quantum Internet, while classical devices use a secure quantum protocol, such as QKD, to access the quantum Internet. The communication channel between the classical devices

Figure 3. Entanglement distribution via the doubling architecture.

The aim is to generate long-distance entanglement between distant quantum nodes A and B through a chain of q intermediate R_i , $i = 1, \dots, q$, quantum repeaters. The architecture defines different l entanglement levels, $l = 1, 2, 3, 4$ in the current network situation with $q = 7$. First, the $l = 1$ -level entangled connections are established between the quantum nodes. To double the spanned distance, entanglement swapping is applied in the quantum repeaters. The result of the entanglement swapping procedure is a higher-level entangled connection. The $l = 2$ -level entangled connections are generated by quantum repeaters R_1, R_3, R_5 , and R_7 . The $l = 3$ -level entangled connections are generated by R_2 and R_6 , while the $l = 4$ -level entangled connection between A and B is generated by R_4 .



and the quantum protocol is an N classical channel, while the quantum protocol uses an \mathcal{N} quantum channel to access the quantum Internet.

In general quantum Internet architecture, the l entanglement levels between the quantum nodes of the cloud follow the structure of the doubling architecture. For a source quantum node A and receiver quantum node B , the construction of an $l = 4$ -level entanglement via the doubling architecture is depicted in Figure 3.

The quantum nodes are connected via l -level entangled connections, where $l = 1$ refers to a direct connection (black line), while $l > 1$ are multilevel connections. For $l = 2$ (thick blue line), the hop distance between the connected nodes is $d_l = 2$, while for $l = 3$ (thicker orange line), the hop distance between the connected nodes is $d_l = 4$. Quantum computers and quantum devices communicate with the cloud of quantum Internet via an \mathcal{N} quantum channel, while classical computers, servers, and other classical devices access the quantum

Internet through a secure quantum protocol (depicted by a Quantum security device: QKD, quantum cryptographic protocols, and so on). Communication between a classical device and a quantum security device is realized via an \mathcal{N} classical communication channel, while the quantum security device (quantum protocol) accesses the quantum Internet via a quantum channel \mathcal{N} .

Interoperability of quantum and classical Internet. In a near-term approach, the quantum Internet will function in parallel with the classical Internet. The quantum Internet adds several extensions and extra functions to the classical Internet, such as the use of quantum secure keys for secure communication between classical devices. In the interoperability model, devices of the classical Internet can access a quantum security protocol (such as QKD) and can also access the classical Internet. Using the quantum protocol, a quantum key can be shared via a quantum Internet path, which can be used for classical, encrypted, secure communication over

the classical Internet. In this approach, classical devices can use a different classical protocol with the quantum key for the encrypted communication through the classical Internet, such as IPSec (via IPSec Gateways and an IPSec Tunnel, which represent a classical Internet path secured with a quantum key) or via a Diffie-Hellman key exchange protocol, AES, or TLS. Figure 4 provides a model of interoperability of classical devices of the classical Internet and the quantum Internet. The quantum Internet is used to share quantum keys between distant quantum security devices, while the classical Internet serves for an encrypted classical communication between classical devices using quantum keys.

Proposals

Advanced information transmission and operations. In a quantum Internet setting, information transmission is realized through quantum communication links (quantum channels¹⁴). While a classical communication channel

Figure 4. Interoperability of classical devices of the classical Internet and the quantum Internet.

In Step 1, a quantum key is exchanged between the quantum security protocol (such as QKD) using a quantum Internet path via quantum channels \mathcal{N} . In Step 2, a classical Internet path is established between the classical devices using the quantum-secure key of Step 1 via classical channels N . The quantum security device communicates over a secure local connection with the classical devices for the key sharing. The classical path can use a different encryption protocol with the quantum-secure key (such as IPSec, Diffie-Hellman key exchange protocol, AES, and TLS).

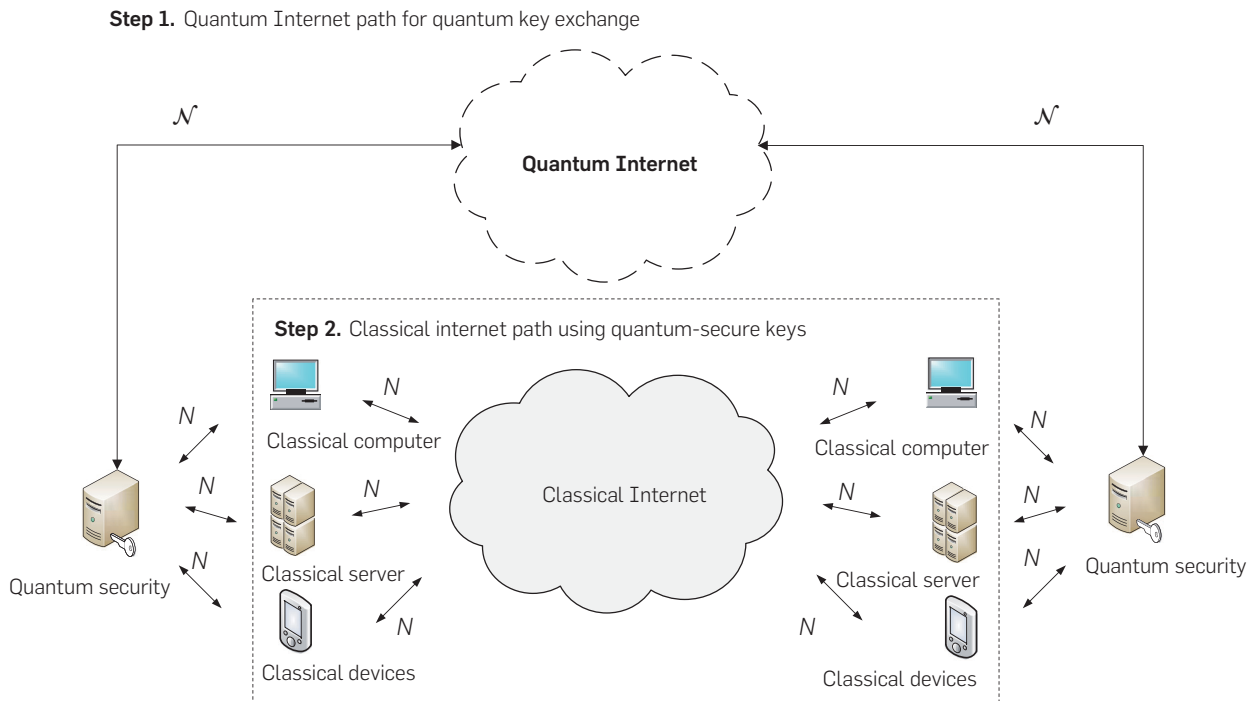
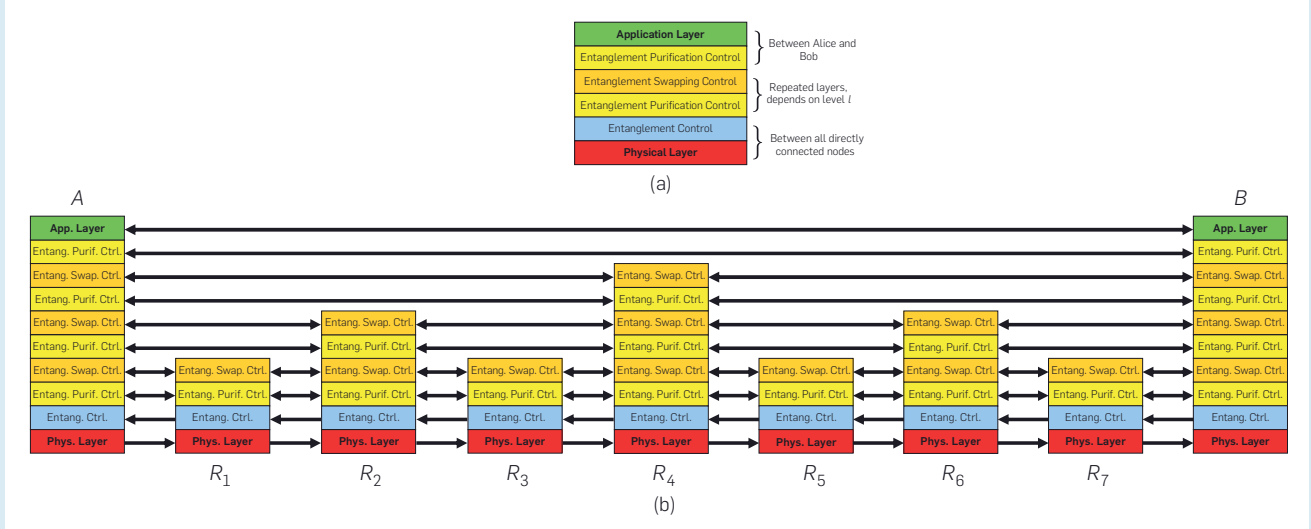


Figure 5. Protocol stack of quantum repeaters and protocol interactions.

(a) **Quantum repeater protocol stack.** The physical layer consists of only quantum communications, while the upper layers also use classical-side information for the control mechanisms. (b) **Protocol interactions of the $l = 4$ -level doubling architecture.** Layer interactions are depicted via the directed lines; the direction denotes the communication direction between the nodes in the particular layer. The physical layer and entanglement control layer are defined between all nodes connected by a physical communication channel, such as optical fiber or wireless optical channel. In the $l = 4$ -level doubling architecture, these node pairs are $[A, R_1]$, $[R_1, R_2]$, $[R_2, R_3]$, $[R_3, R_4]$, $[R_4, R_5]$, $[R_5, R_6]$, $[R_6, R_7]$, and $[R_7, B]$. The purification control and entanglement swapping control layers are defined between only those quantum nodes that are involved in the steps of entanglement swapping, therefore between nodes $[A, R_1]$, $[R_1, R_2]$, $[R_2, R_3]$, $[R_3, R_4]$, $[R_4, R_5]$, $[R_5, R_6]$, $[R_6, R_7]$, $[R_7, B]$, $[A, R_2]$, $[R_2, R_4]$, $[R_4, R_6]$, $[R_6, B]$, $[A, R_4]$, and $[R_4, B]$ in the $l = 4$ -level structure. End-to-end interactions are defined only between $[A, B]$ via the entanglement purification layer and the application layer.



allows us to transmit only classical information, a quantum channel extends the possibilities. It can be used to transmit classical information, functioning as a classical link; private classical information (QKD); and quantum information (quantum superposition or quantum entanglement). See Sidebars 1–4 for more information.

An important problem connected to entanglement distribution is the handling of the noise on the entangled states. Considering the noisy physical links and other effects of the environment, the received quantum states are noisy. Particularly, the fidelity of the actually created entangled system σ is far from the target fidelity F . To handle the situation, the noisy states should be purified—this process is called *entanglement purification*. Network optimization is essential in a quantum Internet setting to reduce the purification steps.

Some approaches use separable states to generate the entanglement.²³ In these schemes, the entanglement is not distributed directly, but only separable states are transmitted. The entanglement is then generated by the application of operations on the

separable subsystems. A drawback of these schemes is their resource-intensive needs, since their implementation requires correlated multipartite quantum systems, which are difficult to generate and use in practice.

Quantum repeater protocol stack. The quantum repeater protocol stack describes the networking interactions of entanglement distribution between quantum nodes.⁴⁵ The lowest layer of the stack is the physical layer, which describes only the purely quantum-level communications, such as the direct transmission of quantum entanglement over the physical optical channels between neighboring quantum nodes. The next layer, the entanglement control layer, defines control methods for the entanglement transmission procedure of the physical layer. These two layers are defined between all directly connected quantum nodes of the network, such as neighboring quantum nodes connected by an optical fiber or wireless optical channel. Communication is unidirectional only in these two layers, while it is bidirectional in all higher layers. The entanglement transmission process in the

physical layer starts from Alice toward Bob through the directly connected (that is, $l = 0$ -level connections) intermediate nodes. Interactions in the entanglement control layer are also unidirectional, with a reversed interaction direction between node pairs.

The next two layers—entanglement purification control and entanglement swapping control—are defined between only those quantum nodes involved in entanglement swapping and entanglement purification in the doubling architecture. Therefore, the repetition number of these layers depends on the level l of the entangled structure. Interactions are bidirectional in all these repeated layers.

The end-to-end layers between Alice and Bob are the entanglement purification control layer, to establish a high-fidelity entanglement between the sender and the receiver, and the application layer, to implement specific functions. Interactions are bidirectional in these layers.

The protocol stack of quantum repeaters is depicted in Figure 5. In Figure 5(a) depicts the general layer structure, while Figure 5(b) illustrates

Figure 3's protocol interactions of the $l = 4$ -level doubling architecture.

Advanced security. While classical networks do not allow unconditional security for legal parties with reasonable computational complexity, the quantum Internet offers this attribute as a default service. The quantum Internet's advanced security level is provided by QKD and distributed crypto-functions (Byzantine agreement, leader election, quantum secret sharing, blind quantum computation, and other quantum cryptofunctions). The main contribution of the entangled structure is multi-hop QKD over arbitrarily long distances realized by a chain of quantum repeaters. While the unentangled structure does not allow global QKD due to the point-to-point nature of the unentangled structure, the entangled structure of the quantum Internet allows legal parties to select this option. (Note: Satellite links can be used at some specific points of the network, and some current satellite-based methods use weak coherent states with decoy QKD protocols. Thus, there is a potential to use trusted node architectures that chain together certified QKD links.)

Another advantage of the advanced security provided by the quantum Internet is its extended interoperability with classical cryptofunctions, such as symmetric block ciphers (see AES), or with IPsec and TLS. The additional secrecy injected into classical cryptosystems via the use of the quantum Internet allows legal parties to decrease the dependency on classical one-way functions and public key methods. As a corollary, the computational complexity of classical cryptofunctions can be reduced via collaboration between the classical layer of the traditional network and the quantum layer of the quantum Internet.

The first QKD protocols that were introduced were based on discrete variables (DV), such as photon polarization. The first DVQKD protocol that was introduced was the so-called BB84³ protocol, which used single-photon polarization for encoding.

Since the polarization of single photons cannot be encoded and decoded efficiently due to the technological limitations of current physical devices, continuous variable (CV) QKD systems were proposed.³³ In a CVQKD system,

information is encoded in continuous variables (that is, photon packets) by a Gaussian modulation using the position or momentum quadrature of coherent quantum states. Compared with DVQKD, the modulation and decoding of continuous variables does not require specialized devices; it can be implemented using standard, currently available, and widely used telecommunication networks and devices.

Some details of recent QKD implementations are summarized in Table 6.

Advanced engineering possibilities.

From an engineering point of view, the quantum Internet requires the use of advanced network and service management. The main task in the physical layer of the quantum Internet is the reliable transmission of quantum states and the faithful internal storage of received quantum systems in the quantum memories of the quantum nodes. The quantum transmission and quantum storage processes in the physical layer require collaboration with network- and service-management services in a higher, logical layer. The logical layer uses classical-side information from the quantum network via traditional communication channels

to provide a feedback and adaption mechanism for the physical layer. The logical layer contains control and post-processing tasks, such as error correction, dynamic monitoring of quantum links and quantum memories, control of internal storage and error-correction mechanisms of quantum nodes, network optimization, and advanced service-management processes.

The field of the quantum Internet dynamically improves and challenges with several open questions. Since the structure and processes of the quantum Internet are fundamentally different from the mechanisms of the traditional Internet, it requires the development of novel and advanced services. The main challenge regarding these services is to provide an optimal solution for transmitting entangled systems, optimizing the network architecture, and developing networking services connected to the entanglement distribution. Networking procedures of the quantum Internet should consider the fundamentals of quantum mechanics (such as superposition, quantum entanglement, and no-cloning theorem) that require a significantly different network and service management compared

Table 6. Recent optical fiber and free-space optical QKD implementations.

QKD protocol	Quantum channel	Wavelength	Distance	Max. secret-key rate
DV (BB84) ²⁷	Optical fiber	1,310 nm	66 km	5.1 kbps
DV (BB84) ⁹	Optical fiber	1,548 nm	150 km	1 kbps
DV (BB84) ⁴⁶	Optical fiber	1,310 nm	80 km	1 kbps
DV (BB84) ⁶	Optical fiber	1,550 nm	50 km	1.26 Mbps
DV (BB84) ⁴	Optical fiber	1,550 nm	421 km	6.5 bps
DV (Satellite-to-ground BB84) ²⁴	Free-space optical	850 nm	1,200 km	1 kbps
DV (Entanglement-based free space QKD) ⁴⁹	Free-space optical	810 nm	1,120 km	0.12 bps
CV ¹⁷	Optical fiber	1,550 nm	150 km	50 bps
CV ⁵¹	Optical fiber	1,550 nm	202 km	6.214 bps
CV ²¹	Optical fiber	1,550 nm	20 km	90 kbps
CV ²⁰	Optical fiber	1,550 nm	80 km	0.1 kbps
Measurement device-independent QKD (MDIQKD) ⁴⁸	Optical fiber	1,550 nm	404 km	1.16 bit/h
Twin-field QKD ²⁶	Optical fiber	1,550 nm	550 km	0.1 kbps
Decoy-state QKD (Decoy-state BB84) ⁴⁰	Optical fiber	1,550 nm	107 km	12 kbps

DV: Discrete variable; CV: Continuous variable; BB84: Bennett-Brassard DVQKD protocol. See Sidebar 5 online for more information.

with the networking services of the traditional Internet.

Advanced distributed computing. The structure of the quantum Internet allows for the parties to realize distributed computations with advanced security and extended possibilities compared with traditional networking. The field of distributed quantum computations includes the application of the quantum effects in client-server communications, system-area network communications, and the fundamental distributed computations (information sharing, multiparty computations, multiparty security, quantum secret sharing, and blind quantum computation).

Measurement-based quantum computation is at the heart of distributed quantum computation using entanglement as a resource. The aim of quantum measurement is to extract valuable and usable information from the measured quantum system. While the input of the measurement can be a superposed or entangled quantum system, the output of the measurement is classical information—that is, bit strings. Quantum measurements can be performed in different ways, for example, via projective measurements or positive-operator-valued measure (POVM) measurements.

Routing quantum entanglement. In an entangled quantum network with heterogeneous entanglement levels, finding the shortest path³¹ between arbitrary quantum nodes for the level of entanglement is crucial to transmitting a message between

nodes in as few steps as possible. Since no global knowledge is available, in practical scenarios, about the nodes or properties of the entangled connections, routing must be performed in a decentralized way. A decentralized routing can use only local knowledge about the nodes, their neighbors, and their shared level of entanglement. Opportunistic entanglement distribution for the quantum Internet has been defined as a different method.¹³ The opportunistic model defines distribution sets that aim to select those quantum nodes for which the cost function picks up a local minimum. The cost function uses error patterns of the local quantum memories and the predictability of the evolution of the entanglement fidelities. This method provides efficient entanglement distributing with respect to the actual statuses of the local quantum memories of the node pairs. The model provides an easily applicable, moderately complex solution for high-fidelity entanglement distribution in experimental quantum Internet scenarios.

The decentralized routing approach is a promising way of routing bipartite entanglement. However, multipartite routing strategies on graph states, cluster states, and GHZ states as multipartite networks will use such states.

Implementation Basis

A practical implementation of the quantum Internet integrates standard

photonic devices, quantum memories, optical cavities, and fundamental physical devices required for practical quantum network communications. The quantum transmission and auxiliary classical communications between quantum nodes can be realized via standard links (for example, optical fibers, wireless channels, satellite communications) and using the fundamental quantum protocols of quantum networks.⁴⁵

The experimental quantum Internet is currently in the development phase and exists in physics laboratories and as theoretical approaches. Engineering problems associated with the construction of the quantum Internet need to be discussed and solutions must be found.

Important recent practical approaches to the quantum supremacy of the experimental quantum Internet are summarized in Table 7.

Conclusion and Outlook

The quantum Internet provides a large-scale application of advanced quantum communication technologies and protocols. The structure of the quantum Internet keeps user data safe for future networking. However, commercial quantum computers are currently not available to the public (users have only limited access via cloud^{10,11} services); the security issues represent tomorrow’s problems, while engineering high-performance and well-designed services and protocols for the quantum Internet represents the task at hand. A seamless transition from the traditional Internet to the quantum Internet must be enabled as quantum computers become available. Future research should define further services and protocols for the quantum Internet. One important problem that needs to be solved is how to organize and engineer quantum Internet standards. Like traditional networking, the standardization of quantum Internet protocols helps to define a uniform platform for building a global quantum network. The standardization will also serve as an evolving framework that can reflect the dynamically changing requirements of the quantum Internet.

One promising approach to address these important problems is the formation of the Quantum Internet Research


Result
General infrastructure for the quantum Internet ²⁵
Architecture for a quantum Internet ²²
Unite to build a quantum Internet ³²
Experimental structure of the quantum Internet ⁴⁷
Optimization of practical entanglement purification ⁴¹
Deterministic delivery of quantum entanglement on a quantum network ¹⁹
Entanglement-based secure quantum cryptography over 1,120 km ⁴⁹
Satellite-to-ground quantum key distribution over 1,200 km ²⁴
Satellite-based entanglement distribution over 1,200 km ⁵⁰
Twin-field quantum key distribution between distant nodes over 500 km ²⁶
Quantum teleportation of independent, single-photon qubits over 1,400 km ³⁹
Bell inequality violation using electron spins separated by 1.3 km ¹⁸
Modular entanglement of atomic qubits using photons and phonons ¹⁸
Quantum teleportation between remote, single-atom quantum memories ³⁰
Experimental realization of quantum repeaters based on atomic ensembles and linear optics ⁴²

Group (QIRG),³⁵ which already has international support and researcher collaboration. The QIRG also defined a technical roadmap with capability milestones for developing the experimental quantum Internet. The aim of the proposal is to find solutions to future engineering problems of the quantum Internet, such as defining a standardized architectural framework (interoperability, connection establishment, node roles, network coding, multiparty state transfer), designing an application programming interface (API), and defining the quantum Internet's application level.

In the near future, classical Internet and quantum Internet will co-exist and function in parallel. The quantum Internet will also use the classical Internet as an auxiliary network structure, since at several points, classical-side information and the use of classical public channels are required for quantum devices to function. Other important open questions for the short term revolve around identifying network boundaries in quantum networks, connecting quantum networks with different implementations basis, and constructing common communication languages and platforms to support the quantum devices of the quantum Internet. The main engineering issues cover the development of novel routing services for the heterogeneous network structure of the quantum Internet and the definition of connection establishment services, resource allocation services (such as services for entanglement distribution and entanglement allocation), and interoperability services (interoperability between different network layers and network components, and interoperability between classical and quantum network components).

Acknowledgments

This research has been supported by the Hungarian Academy of Sciences (MTA Premium Postdoctoral Research Program 2019); the National Research, Development and Innovation Fund (TUDFO/51757/2019-ITM, Thematic Excellence Program); the National Research Development and Innovation Office of Hungary (Project No. 2017-1.2.1-NKP-2017-00001); the Hungarian Scientific Research Fund—OTKA

K-112125 and in part by the BME Artificial Intelligence FIKP grant of EMMI (Budapest University of Technology, BME FIKP-MI/SC), and the Ministry of Innovation and Technology and the National Research, Development and Innovation Office within the Quantum Information National Laboratory of Hungary. 

References

- Aaronson, S. and Chen, L. Complexity-theoretic foundations of quantum supremacy experiments. In *Proceedings of the 32nd Computational Complexity Conf.* (2017), 22:1–22:67.
- Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* 574 (2019), 505–510, DOI: 10.1038/s41586-019-1666-5.
- Bennett, C.H. and Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of the IEEE Intern. Conf. on Computers, Systems and Signal Processing* (1984), 175–179.
- Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters* 121 (2018), 190502.
- Building the first reliable Quantum Internet on top of Europe's glass fiber network. QUAPITAL (2020), <https://quapital.eu/>.
- Comandar, L.C. et al. Room temperature single-photon detectors for high bit rate quantum key distribution. *Applied Physics Letters* 104 (2014), 021101.
- Ekert, A.K. Quantum cryptography based on Bell's theorem. *Physical Review Letters* 121 (1991), 661–663.
- Farhi, E., Goldstone, J., Gutmann, S., and Neven, H. Quantum algorithms for fixed qubit architectures. arXiv:1703.06199v1 (2017).
- Fröhlich, B. et al. Long-distance quantum key distribution secure against coherent attacks. *Optica* 4, 1 (2017), 16316.
- Gambetta, J. IBM's roadmap for scaling quantum technology. IBM Research Blog (September 2020).
- Gonzalez, C. Cloud-based QC with Amazon Braket. *Digitale Welt* 5 (March 2021), 14–17.
- Greenberger, D.M., Horne, M.A., and Zeilinger, A. Going beyond Bell's Theorem. In *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*. M. Kafatos ed. (1989) Kluwer Dordrecht, 69–72. arXiv:0712.0921.
- Gyongyosi, L. and Imre, S. Opportunistic entanglement distribution for the quantum Internet. *Nature Scientific Reports* 9 (2019), 2219. DOI: 10.1038/s41598-019-38495-w.
- Gyongyosi, L., Imre, S., and Nguyen, H.V. A survey on quantum channel capacities. *IEEE Communications and Surveys Tutor* 99, 1 (2018), 1149–1205, DOI: 10.1109/COMST.2017.2786748.
- Harrow, A.W. and Montanaro, A. Quantum computational supremacy. *Nature* 549 (2017), 203–209.
- Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* 526 (2015), 682–686.
- Huang, D. et al. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Nature Scientific Reports* 6 (2016), 19201. DOI: 10.1038/srep19201.
- Hucul, D. et al. Modular entanglement of atomic qubits using photons and phonons. *Nature Physics* 11, 1 (2015), 37–42.
- Humphreys, P. et al. Deterministic delivery of remote entanglement on a quantum network. *Nature* 558 (2018), 268–273.
- Jouget, P. et al. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics* 7 (2013), 378381.
- Karinou, F. et al. Toward the integration of CV quantum key distribution in deployed optical networks. *IEEE Photonics Technology Letters* 30, 7 (2018), 650653.
- Kimble, H.J. The quantum Internet. *Nature* 453 (2008), 1023–1030.
- Krisnanda, T. Distribution of quantum entanglement: Principles and applications. Ph.D. dissertation, Nanyang Technological University (2020). arXiv:2003.08657.
- Liao, S.K. et al. Satellite-to-ground quantum key distribution. *Nature* 549 (2017), 43–47.
- Lloyd, S. et al. Infrastructure for the quantum

Internet. *ACM SIGCOMM Computer Communication Review* 34, 5 (2004), 20.

- Lucamarini, M. et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* 557, 7705 (2018), 400–403.
- Mao, Y. et al. Integrating quantum key distribution with classical communications in backbone fiber network. *Optics Express* 26, 5 (2018), 60106020.
- Monroe, C. et al. The U.S. national quantum initiative: From act to action. *Science* 364, 6439 (2019), 440442.
- Muralidharan, S. et al. Ultrafast and fault-tolerant quantum communication across long distances. *Physical Review Letters* 112 (2014), 250501.
- Noelleke, C. et al. Efficient teleportation between remote single-atom quantum memories. *Physical Review Letters* 110 (2013), 140403.
- Pant, M. et al. Routing entanglement in the quantum Internet. *npj Quantum Inf* 5, 25 (2019), DOI: 10.1038/s41534-019-0139-x.
- Pirandola, S. and Braunstein, S.L. Unite to build a quantum internet. *Nature* 532 (2016), 169–171.
- Pirandola, S. et al. Advances in quantum cryptography. In *Advances in Optics and Photonics* (2020), DOI: 10.1364/AOP.361502.
- Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* 2 (2018), 79.
- Quantum Internet Research Group (2018), <https://datatracker.ietf.org/rq/qirg/about/>.
- Quantum manifesto: A new era of technology. *Quantum Flagship* (2016), https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf
- Quantum Technologies Flagship kicks off with first 20 projects. European Commission (2020), https://ec.europa.eu/commission/presscorner/detail/de/MEMO_18_6241.
- Quantum technologies in space. QTSPEC. <http://www.qtspace.eu/>.
- Ren, J.G. et al. Ground-to-satellite quantum teleportation. *Nature* 549 (2017), 70–73.
- Rosenberg, D. et al. Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters* 98 (2007), 010503.
- Rozpedek, F. et al. Optimizing practical entanglement distillation. *Physical Review A* 97 (2018), 062333.
- Sanguard, N. et al. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics* 83 (2011), 33.
- The future is quantum: EU countries plan ultra-secure communication network. European Commission (2020), <https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>.
- Truly secure quantum communication is here. OPENQKD (2020), <https://openqkd.eu/>.
- Van Meter, R. *Quantum Networking*. John Wiley and Sons Ltd., Hoboken, NJ, 2014, ISBN 1118648927, 9781118648926.
- Wang, L.J. et al. Long-distance co-propagation of quantum key distribution and terabit classical optical data channels. *Physical Review A* 95, 1 (2017), 012301.
- Wehner, S. et al. Quantum internet: A vision for the road ahead. *Science* 362 (2018), 6412.
- Yin, H.L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters* 117 (2016), 190501.
- Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* 582 (2020), 501.
- Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* 356 (2017), 1140.
- Zhang, Y. et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Physical Review Letters* 125 (2020), 010502.

more online

For additional information, access the supplementary material for this article at <https://dl.acm.org/doi/10.1145/3524455>.

Laszlo Gyongyosi (gyongyosi@hit.bme.hu) is a researcher at the Hungarian Academy of Sciences and Budapest University of Technology and Economics, Hungary.

Sandor Imre is a professor at Budapest University of Technology and Economics, Hungary.



This work is licensed under a <http://creativecommons.org/licenses/by/4.0/>