Quantum Networks

Table of contents

1. Quantum Key Distribution Networks (QKDNs)

Quantum mechanics offers new possibilities to securely transmit information, which provides for new methods of secure communication. Currently, point-to-point secure quantum communication has been achieved by means of Quantum Key Distribution (QKD) technology over optical fibre communication links and also over Free-Space Optical (FSO) communication links.

Limits are imposed on the optical transmission over point-to-point optical links because the propagation of photons (Box 1.1) through optical fibres or free space is subject to photon loss or dispersion, the extent of which increases with distance. For optical fibres, the effective operational distance of QKD products is limited to a few 100 km at the current state of optics technology.

The photon is an elementary subatomic particle. It is the quantum of the electromagnetic field, including electromagnetic radiation such as light and radio waves, and it is the force carrier for the electromagnetic force. Photons do not have electrical charge, they have zero mass and zero rest energy, and they only exist as moving particles. Photons move at 299,792,458 metres per second in a vacuum, the so-called "speed of light" denoted by *c* (from the Latin *celeritas*). The speed of photons in a medium depends upon the medium and is always slower than the speed in vacuum *c*.

Box 1.1: Photon

The QKD distance limitation can be overcome by deploying an intermediate node between the communicating parties. Examples of this approach are active optical switch technology (Box 1.2) or untrusted QKD intermediate station technology, either Measurement Device-Independent QKD (MDI-QKD, see Box 1.3), or Twin-Field QKD (TF-QKD, see Box 1.1.5), or a combination of these technologies. This approach is suitable for the implementation of Quantum Metropolitan Area Networks (QMANs) of limited geographical size.

An optical switch is a multi-port network bridge, which connects multiple optic fibres to each other and controls data packets routing between inputs and outputs. An active optical switch has optical gain elements.

Box 1.2: Active optical switch

In Measurement Device-Independent QKD (MDI-QKD) technology, neither endpoint (sender or receiver) is configured as an optical receiver (as is done in conventional QKD technology), but rather both endpoints are configured as optical transmitters. The two optical transmitters send photons to an intermediate node, called mid-station, which couples and measures the photons (using Bell inequality testing (Box 1.4) to ensure that the behaviour of the mid-station complies with the laws of quantum mechanics). The endpoints can then distil a shared secret key from the two-photon interference measurement results disclosed by the mid-station.

Box 1.3: Measurement Device-Independent QKD (MDI-QKD)

Bell's theorem is used to prove that quantum mechanics is incompatible with 'local hidden-variable' theories. It was introduced by physicist John Stewart Bell in a 1964 in response to the EPR paradox.

The EPR paradox refers to a thought experiment that Albert Einstein, Boris Podolsky and Nathan Rosen formulated in 1935, in order to argue that quantum mechanics was an incomplete theory. In their view (shared by many other leading physicists at the time), quantum particles carry physical attributes (later called ‘local hidden-variables’) not included in the quantum mechanics theory, and the uncertainties in quantum mechanics theory's predictions are due to ignorance of these attributes.

Bell carried out an analysis of quantum entanglement and deduced that if measurements are performed independently on the two separated halves of a pair of entangled particles, then the assumption that the outcomes depend upon ‘local hidden-variables’ within each half implies a constraint on how the outcomes on the two halves are correlated. This constraint would later be named the ‘Bell inequality’. Quantum mechanics predicts correlations that violate this inequality and multiple variations on Bell's theorem have been tested experimentally in physics laboratories many times. All these “Bell tests” have found that the hypothesis of ‘local hidden-variables’ is inconsistent with the way that quantum entanglement works. While the significance of Bell's theorem is not in doubt, its full implications for the interpretation of quantum mechanics remain unresolved.

Box 1.4: Bell inequality testing

Twin-Field QKD (TF-QKD) technology is similar to MDI-QKD technology, but is designed to generate secret key bits from single-photon interference in the intermediate node, thus removing the need to remedy photon losses via sophisticated techniques.

Box 1.5: Twin-Field QKD (TF-QKD)

A fully scalable QKD network architecture, which includes specialised trusted QKD relays to connect cascaded point-to-point QKD systems, extends the practical range of this technology and allows for secure key exchange over much longer distances in Quantum Wide Area Networks (QWANs). Trusted QKD relays are based on a simple concept: each relay executes the QKD protocol to securely exchange secret keys with its neighbouring relay(s), thus extending the key exchange capability over distances that are much larger than a single execution of the point-to-point QKD protocol could ever cope with. This is similar to the use of optical repeaters in classical optical fibre networks. To ensure the security of the secret keys that are exchanged in this manner, the QKD relays must be trusted devices (aka “trusted repeaters”), which are protected against intrusion and attacks by unauthorised parties. It goes without saying that this requirement precludes many use cases.

QKD trusted relay technology is expected to form the basis of global Quantum Key Distribution Networks (QKDNs), including both fibre-based and free space-based QKD links. The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) is currently developing a series standards (called Recommendations) for such QKDNs.

In particular, ITU-T Recommendation X.1710 defines a security framework for QKDNs. This Recommendation distinguishes three kinds of threats:

1. intentional: threats that involves malicious entities that may attack either communication itself or network resources;

2. administrative: threats that arises from security administration failures;

3. accidental: threats whose origin does not involve any malicious intent but results from technical failures.

The Recommendation focuses only on intentional threats:

- spoofing (masquerade): pretending to be a different entity in order to gain an illegitimate advantage;
- eavesdropping: breaching confidentiality by deciphering information assets (it is also possible for attackers to get information such as configuration data, user credentials, etc. for a future attack);
- deletion: compromising the integrity of information assets transferred or stored by unauthorised deletion;
- corruption: compromising the integrity of information assets transferred or stored by unauthorised insertion, modification, re-ordering, replaying or delaying;
- repudiation: denying having performed some actions, e.g. an administrator enforcing a malicious network policy (such as copying and forwarding specific traffic flows to a malicious node) may claim that he/she did not make such network policy enforcement;
- Denial-of-Service (DoS): performing activities to disrupt proper operations of a QKDN; this may include denial of access to the QKDN and denial of key generation and denial of other communication by flooding the QKDN.

ITU-T Recommendation X.1710 also prescribes security measures for QKDN operation:

- authentication: identifiers must be established and verified for the claimed identities of functional elements in the QKDN, as well as for those in the user network, and for any other entities if these are connected to the QKDN from outside;
- access control: functional elements in the QKDN must be prevented from gaining access to information or resources that these elements are not authorised to access;
- confidentiality: the confidentiality of stored and transferred key data must be ensured;
- integrity: the integrity of stored and transferred data (including key data) must be protected;
- availability:
    - the availability of key data must be ensured;
    - a QKDN must have capabilities for ensuring network resilience;
    - countermeasures for DoS attacks must be implemented;
- accountability:
    - activity logging: information about security relevant activities must be recorded, and there must be a capability to analyse the recorded information;
    - alarm notifications must be produced for relevant security events;
- a QKDN must implement security measures for deployment, support, maintenance and migration, in order to continuously provide security control of the QKDN network during and after these operations.

2. Quantum networks

There are two main approaches for exchanging quantum information (Box 2.1) in quantum networks:

Quantum information is concerned with studying the way in which the laws of quantum mechanics can be used to store and process information and to perform computations. In particular, the possibility of creating quantum superpositions (Box 2.2) of classical states, and to create correlations without a classical correspondence, such as entanglement (Box 2.3), give rise to a wide range of new phenomena in data processing and computation.

Box 2.1: Quantum Information

Quantum superposition is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct quantum states. The principle of quantum superposition states that if a physical system may be in one of many configurations (arrangements of particles or fields) then the most general state is a combination of all of these possibilities. The principle applies to the states that are theoretically possible without mutual interference or contradiction. It requires us to assume that between these states there exist peculiar relationships such that whenever the system is definitely in one state, we can consider it as being partly in each of two or more other states. The original state must be regarded as the result of a kind of superposition of the two or more new states, in a way that cannot be conceived on classical ideas. Any state may be considered as the result of a superposition of two or more other states, and indeed in an infinite number of ways.

Box 2.2: Quantum superposition

Quantum entanglement is a physical phenomenon that occurs when a group of particles are generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the group cannot be described independently of the quantum state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical physics and quantum mechanics.

Box 2.3: Quantum entanglement

1. Use quantum entanglement as a means for exchanging quantum information between quantum network nodes that are neither directly nor indirectly connected by physical communication links.

2. Forward quantum information by means of physical communication links between (intermediate) quantum network nodes.

The first approach has one significant characteristic compared to the second approach: the entanglement topology of such a network is completely independent of the underlying physical network configuration. Quantum entanglement redefines the concept of “neighbourhood” as two network nodes can be “neighbours” without being physically connected. However, entanglement generation and distribution still does require a physical connection; this process can be either proactive or reactive (aka on-demand or on-the-fly). Once two qubits are confirmed to be entangled, a qubit can be sent deterministically using quantum teleportation (Box 2.4). Long-distance entanglement can be built from shorter entanglement segments by using entanglement swapping (Box 2.5) or Quantum Error Correction (QEC) techniques (Box 2.6) in quantum repeaters.

Quantum (state) teleportation is a communication method that involves transmitting quantum information by exploiting the properties of quantum entanglement. It works by first creating pairs of entangled photons and then sending one photon of each pair to the sender and the other one to the receiver. The sender measures the quantum state of the photons that hold the quantum information and the state of the entangled photons at the same time. These interactions change the state of its photons, and because they are entangled with the receiver’s photons, the interactions instantaneously change the state of the receiver’s photons too. In effect, this “teleports” the quantum state in the sender’s photons to the receiver’s photons. However, the receiver cannot reconstruct the quantum information until the sender sends the result of its measurements in the form of classical bits (via optical fibre cables or other means).

Box 2.4: Quantum teleportation

Entanglement swapping involves the transfer (teleportation) of entanglement to two photons that were produced independently and never previously interacted. It is a process by which a quantum repeater consumes two halves of entangled pairs, producing a single longer-range entangled pair.

Box 2.5: Entanglement swapping

Quantum Error Correction (QEC) is used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise.

Box 2.6: Quantum Error Correction (QEC)

Imperfect entanglement states, arising from noise produced within the quantum entanglement generation and/or distribution process, can be countered by entanglement distillation (aka entanglement purification), which consists in generating a maximally entangled state from multiple imperfect entangled states.

The second approach is similar to the approach that is used for constructing classical networks. However, the quantum measurement postulate and the no-cloning theorem preclude the possibility of reading and copying quantum information without altering it, yet this very possibility fundamentally underlies classical network protocols throughout the whole network protocol stack. For example, classical bits can be stored for significantly longer times than needed for the execution of certain network functions, whereas qubits irreversibly degrade over time as a consequence of decoherence and this does not fit with the latency of classical computer networks. Quantum information forwarded over physical communication links must be protected against noise and decoherence using QEC and must be repeatedly refreshed at the intermediate quantum network nodes where QEC is being performed.

Quantum repeaters are quantum systems that act as quantum memories for temporary qubit storage, process quantum information and communicate with each other using quantum methods, to provide end-to-end transmission of qubits by means of quantum state teleportation mechanisms. Quantum repeaters are also known as “true quantum repeaters” or “untrusted quantum repeaters” (to distinguish them from the trusted QKD relays used in QKDNs which are sometimes called “trusted repeaters”).

The basic principles of quantum repeaters have been experimentally proved. However, quantum repeaters are very challenging to build in practice with current technology: they either require quantum memories (Box 2.7) or QEC (Box 2.6). Two promising quantum core technologies for building quantum repeaters are Rydberg atoms (Box 2.8) in high-quality microwave cavities (Box 2.9) and Nitrogen-Vacancy (NV) centres (Box 2.10).

Quantum memory is the quantum-mechanical version of classical computer memory. Whereas classical computer memory stores information as binary states, quantum memory stores quantum states for later retrieval. Unlike the classical computer memory states, the states stored in quantum memory can be in a quantum superposition.

A quantum state is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a quantum system. Knowledge of the quantum state together with the rules for the quantum system's evolution in time exhausts all that can be predicted about the quantum system's behaviour. A mixture of quantum states is again a quantum state. Quantum states that cannot be written as a mixture of other states are called pure quantum states, while all other states are called mixed quantum states.

Box 2.7: Quantum memory

A Rydberg atom is an excited atom with one or more electrons that have a very high principal quantum number. The principal quantum number is a non-zero integer value which indirectly describes the size of the electron orbital. The higher this number, on average the farther away the corresponding electron is from the nucleus. Rydberg atoms have a number of interesting properties, e.g. an exaggerated response to electric and magnetic fields, long decay periods and electron wavefunctions that approximate, under some conditions, classical orbits of electrons around the nuclei.

Box 2.8: Rydberg atom

A microwave cavity is a special type of resonator, consisting of a closed (or largely closed) metal structure that confines electromagnetic fields in the microwave region of the spectrum. The structure is either hollow or filled with dielectric material.

Box 2.9: Microwave cavity

The Nitrogen-Vacancy centre (NV centre) is one of numerous point defects in diamond. Its most explored and useful property is its photoluminescence, which allows observers to read out its electron spin-state. The NV centre's electron spin can be manipulated at room temperature by magnetic fields, electric fields, microwave radiation or light, resulting in sharp resonances in the intensity of the photoluminescence.

Box 2.10: Nitrogen-Vacancy centre (NV centre)

Deployment of quantum repeaters will enable constructing large-scale quantum networks, which could for example be used to connect clusters of quantum computers working together to perform quantum computations.

An interesting property of quantum networks is that there are likely to be many paths between a pair of endpoints that could be attempted in superposition fashion. This would increase not only the capacity of the quantum connection between these endpoints but would also contribute to its robustness.

Multiple proposals for repeater-based quantum networks have been put forward. One of the first quantum repeater protocols was the DLCZ protocol proposed by Duan, Lukin, Cirac, and Zoller. In the DLCZ protocol, quantum memories are entangled and the quantum states are transferred between the quantum memories and photons.

Quantum memory is a key requirement for quantum repeater protocols but, unfortunately, the limited coherence time of currently available quantum memories does not satisfy the requirements imposed by quantum repeaters. A quantum repeater protocol without quantum memory, using Repeater Graph States (RGS), has been proposed to address this problem. However, implementing RGS requires multiple entangled photon sources and photon interferometers (Box 2.11), which is technically very challenging for large RGS sizes. It is believed that a combination of an all-photonic protocol and a quantum memory-based protocol could enable development of a practical quantum repeater where use of RGS relaxes the requirement for the coherence time of the quantum memory, while a quantum memory reduces the size requirement for the RGS.

Interferometers work by merging two or more sources of light to create an interference pattern, which can be measured and analysed; hence “Interfere-o-meter”, or interferometer.

Box 2.11: Interferometer

Building large-scale quantum networks and building quantum networks with many nodes is still a very challenging proposition hence development of innovative techniques for constructing quantum networks is an active area of research. A major open issue is whether to follow the connection-oriented circuit-switching network design philosophy, which is based on central network management, or the connectionless packet-switching design philosophy, which is based on a best-effort strategy with no central management in place.

Qubits, entangled qubits in particular, are stateful resources. Qubit entanglement enables unicast dedicated communication channels between pairs of quantum network nodes that requires tight synchronisation and signalling. From this perspective, a quantum network which is based on qubit entanglement properties would probably be based on connection-oriented circuit-switching network design principles. Quantum network management and operation will however be particularly challenging due to the quantum nature embedded in the control plane and/or the data plane.

An important question regarding the feasibility of quantum networks is the extent to which they will be able to use the existing global optical communications infrastructure, i.e. the existing global fibre-optic backbone and international satellite links. Standardisation efforts by GSMA, ETSI, IEEE, IETF and ITU-T are ongoing, aiming at defining architectures, interfaces and protocols for ensuring interoperability between quantum networks and current telecommunication infrastructures.

Several quantum network testbeds are being used to test nascent quantum network technology under (near) real-world circumstances. An example is the Tucson Quantum Network System (QNS) testbed hosted at the University of Arizona in the US. The Tucson QNS testbed leverages an entangled photon distribution network connected by fibre between five buildings on campus. With room-temperature fault-tolerant quantum repeaters based on NV-centres and nuclear spin-photon interfaces (Box 2.12) developed by MIT and Lincoln Laboratories, it is the world's first quantum network testbed for multi-user 10+ million qubits/second fault-tolerant quantum entanglement distribution. It provides a means to thoroughly test silicon photonic chips with various integrated functionalities, to demonstrate quantum entanglement distribution with ever-increasing levels of performance, and to test out quantum resource allocation and quantum network management protocols.

It is common practice to call the total angular momentum of a nucleus "nuclear spin". For electrons in atoms a clear distinction is made between electron spin and electron orbital angular momentum, which is then combined to give the total angular momentum. But nuclei often act as if they are a single entity with intrinsic angular momentum. Associated with each nuclear spin is a nuclear magnetic moment which produces magnetic interactions with its environment.

Box 2.12: Nuclear spin

3. Quantum internet

The quantum internet is envisioned as the final stage of the quantum network evolution. The goal of the quantum internet is to interconnect quantum devices of all kinds in an open and worldwide quantum network infrastructure (the quantum equivalent of the classical internet). Quantum internet will enable sending and receiving information through this network infrastructure in the form of qubits, in full compliance with the laws of quantum mechanics. For this radically new networking technology, several major new and potentially game-changing use cases have already been identified. One such use case is to provide a fundamentally secure way of communication, in which privacy is guaranteed by the laws of quantum mechanics. Another use case consists of connecting quantum processors into a distributed quantum computing cluster. The latter is also called networked quantum computing (or distributed quantum computing) and offers a natural path towards quantum computing scalability. Still another use case consists of using the quantum internet for access to a networked quantum computer, thus allowing remote users/providers to perform secure quantum computing "in the cloud".

Communication between quantum devices (including quantum computers) requires conversion of the quantum states of "stationary qubits" into the quantum states of "flying qubits" and vice versa. This requirement has resulted in numerous efforts to design and engineer such conversions. Most of these efforts address conversion of qubit states into the states of transmissible photons using optical links (including conversion between photon technologies). Other efforts are based on conversion of superconducting qubit states to microwave transmission over special coax cables or microwave waveguides (Box 3.1). The equipment used for the conversion between "stationary qubits" and "flying qubits" is sometimes called a "quantum modem".

A microwave waveguide is a special form of transmission line, which consists of a hollow metal tube. Unlike a typical transmission line (such as a coax cable), a waveguide has no centre conductor.

Box 3.1: Microwave waveguide

The current internet cannot simply evolve into the quantum internet by merely replacing or extending some of its protocols by their quantum counterparts. The quantum internet will be governed by the laws of quantum mechanics hence quantum phenomena with no counterpart in the classical world impose major constraints on its design.

Quantum internet design challenges are however not limited to these constraints. Quantum entanglement properties revolutionise the very concept of communication protocols. For example, remote network nodes can be entangled even if there is no physical communication link between them; this will have tremendous impact on the quantum internet design. Also, correlations provided by quantum entanglement can be leveraged not only for transmitting classical and quantum information, but also for enabling use cases that have no counterpart in the classical internet, e.g. secure quantum communication, Blind Quantum Computation (BQC, see Box 3.2), distributed quantum computing and quantum sensing. The design of the quantum internet will therefore require a major paradigm shift of the internet protocol stack to harness the peculiarities of quantum entanglement. A one-to-one mapping between classical and quantum internet is most certainly not possible.

Homomorphic encryption is a technique that allows users to encrypt their data at their own site before sending it for processing to a cloud service. The cloud service executes a program while the data is still encrypted and then sends the encrypted results back to the users, which can then decrypt the results. The cloud service provider would not be able to determine the input data or the output data because the data is encrypted by the cloud service users. Access to the program that was executed by the cloud service could still be a potential security issue. Blind Quantum Computation (BQC) goes a step further in that it cannot only hide the input and output data, but also the program executed by the cloud-based quantum computer. It does require a quantum internet connection to the cloud service, but potentially this approach can provide the same level of security and privacy as having the quantum computer on-premise.

Box 3.2: Blind Quantum Computation (BQC)

The European Quantum Internet Alliance (QIA) is an interdisciplinary project in which partners from industry, research and development and academia are participating. Its mission is to develop a blueprint for a pan-European entanglement-based quantum internet by developing, integrating and demonstrating functional quantum hardware and software subsystems.

QIA will push the frontier of technology in both quantum end node computing subsystems, using trapped-ion qubits (Box 3.3), diamond NV centre qubits (Box 2.10), neutral-atom qubits (Box 3.4) and quantum repeater subsystems, based on rare-earth element-based quantum memories (Box 3.5), quantum-dot qubits (Box 3.6), etc.

An ion trap is a combination of electric and/or magnetic fields used to capture charged particles — known as ions — often in a system isolated from an external environment. In comparison to neutral atom traps, ion traps have deeper trapping potentials (up to several electronvolts) that do not depend on the internal electronic structure of a trapped ion. This makes ion traps more suitable for the study of light interactions with single atomic systems.

Box 3.3: Trapped-ion qubit

In neutral atom quantum computing, arrays of single neutral atoms are manipulated by light beams to encode and read out quantum states. In these types of quantum processors, a qubit is defined by one of two electronic states of an atom, and these single neutral atoms are arranged in configurable arrays.

Box 3.4: Neutral-atom qubit

Rare-earth elements, also called rare-earth metals, rare-earth oxides or lanthanides, are nearly-indistinguishable lustrous silvery-white soft heavy metals. Scandium and yttrium are also considered rare-earth elements because they tend to occur in the same ore deposits as the lanthanides and exhibit similar chemical properties (but they have different electronic and magnetic properties).

Box 3.5: Rare-earth element

Spin qubits in semiconductor quantum dots are formed when electrons or holes are confined in a static potential well in a semiconductor, giving them a quantised energy spectrum. The simplest spin qubit is a single electron spin located in a quantum dot.

Box 3.6: Quantum-dot qubit

QIA will demonstrate the integration of both types of subsystems. The project initially aims to achieve quantum entanglement and teleportation across a limited number of remote quantum network nodes, thereby making the leap from simple point-to-point quantum connections to multi-node quantum networks.

QIA will also implement a quantum software stack that will provide fast, reactive control and allow arbitrary high-level quantum applications to be realised in platform-independent software. Its industry partners will investigate real-world use cases of quantum applications and determine their hardware requirements.

Appendix A – References

Quantum Key Distribution Networks (QKDNs)

[Applied Sciences 2021] Quantum Key Distribution Networks: Challenges and Future Research Issues in Security

[ITU-T 2020] Recommendation X.1710: Security framework for quantum key distribution networks

[ITU-T 2021] Recommendation Y.3805: Quantum key distribution networks - Software-defined networking control

[JRC 2019] Quantum Key Distribution in-field implementations

Quantum networks

[ACM 2020] Concurrent Entanglement Routing for Quantum Networks: Model and Designs

[CUP 2021] The Quantum Internet – The Second Quantum Revolution

[TUD 2020] Designing a quantum network protocol

Quantum internet

Quantum Internet Alliance (QIA)

[arXiv 2022] Quantum Internet Protocol Stack: a Comprehensive Survey

[CUP 2021] The Quantum Internet – The Second Quantum Revolution

[UFPA-UMass 2020] Quantum Internet – The Future of Internetworking

Appendix B – Acronyms and abbreviations

ACM	Association for Computing Machinery
aka	also known as
bit	binary digit
BQC	Blind Quantum Computation
c	celeritas
coax	co-axial
CUP	Cambridge University Press
DLCZ	Duan, Lukin, Cirac, and Zoller
DoS	Denial-of-Service
e.g.	exempli gratia
EPR	Einstein – Podolsky – Rosen
etc.	et cetera
ETSI	European Telecommunications Standards Institute
FSO	Free-Space Optical
GSM	Global System for Mobile communications (Groupe Spéciale Mobile)
GSMA	GSM Association
i.e.	id est
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ion	ionised atom
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization Sector

JRC	Joint Research Centre
MDI-QKD	Measurement Device-Independent QKD
MIT	Massachusetts Institute of Technology
NV	Nitrogen-Vacancy
QEC	Quantum Error Correction
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QIA	Quantum Internet Alliance
QMAN	Quantum Metropolitan Area Network
QNS	Quantum Network System
qubit	quantum bit
QWAN	Quantum Wide Area Network
RGS	Repeater Graph States
TF-QKD	Twin-Field QKD
TUD	Technische Universiteit Delft
UFPA	Universidade Federal do Pará
UK	United Kingdom
UMass	University of Massachusetts
US	United States