ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Supplement

ITU-T Y Suppl. 75 (03/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

ITU-T Y.3000 series – Quantum key distribution networks – Quantum-enabled future networks

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Supplement 75 to ITU-T Y-series Recommendations

ITU-T Y.3000 series – Quantum key distribution networks – Quantum-enabled future networks

Summary

Supplement 75 to ITU-T Y-series Recommendations describes the approaches of ITU-T SG13 to the study of quantum-enabled future networks for network evolution towards the quantum era.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y Suppl. 75	2023-03-20	13	11.1002/1000/15522

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 75 to ITU-T Y-series Recommendations

ITU-T Y.3000 series – Quantum key distribution networks – Quantum-enabled future networks

1 Scope

This Supplement describes the approaches of ITU-T to the study of quantum-enabled future networks (QEFNs) for network evolution towards the quantum era.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 quantum key distribution [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.2 quantum key distribution module [b-ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

3.1.3 quantum information network (QIN) [b-ITU-T TR QIT4N D1.1]: A network that incorporates quantum communication technologies such as quantum teleportation and quantum repeating, for the purpose of transporting or storing of quantum states, which is to connect quantum information processing nodes, including QKD nodes, quantum computers and quantum sensors.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 quantum-enabled future network (QEFN): A network that connects devices using fundamental information technologies that are based on quantum concepts.

NOTE – Definitions for terms related to QEFN (e.g., quantum device, quantum network) could be further studied, but lie outside the scope of this Supplement.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

MPLS Multi-Protocol Label Switching

PQC Post-Quantum Cryptography

PRD Priority Research Direction

QEFN Quantum-Enabled Future Network

QIN Quantum Information Network

QIT Quantum Information Technology

QIT4N Quantum Information Technology for Networks

QKD Quantum Key Distribution

SDO Standards Development Organization

SFP Small Form-factor Pluggable

5 Conventions

None.

6 Introduction

A QEFN consists of connected devices using fundamental quantum information technologies (QITs) that are based on quantum theory such as superposition and entanglement. Well-known quantum devices include the quantum computer, quantum sensor and quantum key distribution (QKD) module.

The basic distinctions between QEFN and current digital networks derive from QITs. See Table 1.

Table 1 – Basic distinctions between digital and quantum information technologies

	Digital information technology	Quantum information technology
Theoretical background	Classical physics	Quantum physics
Delivered signal	Digital bits	Quantum states (e.g., qubits)
Amplification/repetition of the signal	Possible	Only repeating is possible (typically with quantum memory)

NOTE – It is known that some practical technologies to realize QEFN have been developed actively. QEFN-enabling technologies may have an impact on standardization progress.

7 Status of quantum-enabled future networks study

7.1 Standards development organizations

NOTE – For details of each standards development organization (SDO), see clause I.1.

7.1.1 ITU-T Focus Group on Quantum Information Technology for Networks

The ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N) was established to provide a collaborative platform for pre-standardization aspects of QITs for networks.

[b-ITU-T TR QIT4N D1.1] describes technologies necessary for QINs and explains terms related to QIN development. In [b-ITU-T TR QIT4N D1.2] introduces use cases of QIN and applied QIT. Finally, [b-ITU-T TR QIT4N D1.4] concerns the standardization outlook and technology maturity of QITs that either comprise or impact the requirements for QIN.

The term QIN is defined in clause 3.1.3.

7.1.2 Internet Engineering Task Force/Internet Research Task Force Quantum Information Research Group

The Internet Engineering Task Force/Internet Research Task Force (IETF/IRTF) Quantum Information Research Group (QIRG) will be beneficial in quantum network engineering because it has a lot of existing network engineering experience. With this background, two documents have been published.

[b-IETF RFC 9340] proposes a framework and vision to realize a quantum Internet and explains some basic architectural principles. [b-IETF RFC 9340] explains the basic principles of the quantum

internet, such as cubits and quantum entanglement, and describes the direction of development of quantum Internet-related technologies. In particular, [b-IETF RFC 9340] proposes a quantum network architecture inspired by classical network architectures.

[b-QIRG] provides an overview of some expected application categories for the quantum Internet, and then details selected application scenarios. Some general requirements for the quantum Internet are also provided.

[b-IETF RFC 9340] defines quantum networks as a collection of nodes that is able to exchange qubits and distribute entangled states amongst themselves. [b-QIRG] defines the quantum Internet as a network of quantum networks. The quantum Internet is expected to merge into the classical internet to form a new hybrid internet.

7.2 Research institutes and academia

NOTE – For details of research institutes and academia, see clause I.2.

7.2.1 United States Department of Energy and associated research institutes

[b-US DoE] is a strategic report that presents a blueprint for the implementation of the quantum Internet for which it identifies four priority research directions (PRDs) and outlines five blueprint roadmap milestones that must be achieved to facilitate an eventual national quantum Internet.

Also, in April 2019, scientists from the Brookhaven National Laboratory of the US Department of Energy (DoE), Stony Brook University (SBU), and the DoE's Energy Sciences Network (ESnet) achieved long-distance entanglement over 18 km using unique portable quantum entanglement sources and an existing DoE ESnet communications fibre network. Argonne National Laboratory has created an 84 km quantum loop entanglement distribution network that will be connected to Fermilab, establishing a three-node, 129 km testbed for quantum communication.

[b-ANL]: reviews materials, components and systems used for quantum interconnect; summarizes relevant scientific questions and issues; and addresses the most pressing research needs. [b-ANL] then distils these considerations into recommendations for strategic science and technology research imperatives for the next decade.

7.2.2 Quantum Internet Alliance and QuTech

The aim of the Quantum Internet Alliance (QIA) is a blueprint for a pan-European quantum Internet by ground-breaking technological advances, culminating in the first experimental demonstration of a fully integrated stack running on a multi-nodes quantum network.

[b-Wehner] is a comprehensive paper on implementation, which suggests six stages to complete the quantum Internet using qubits.

7.2.3 European Union Quantum Communication Infrastructure project

[b-EU QCI)] introduces a project plan aimed at commercializing a complete QIN from 2021 to 2035.

7.2.4 Quantum Internet Task Force

[b-QITF] takes into account the history of the current Internet, and while valuing the diversity and interconnectedness of technologies, aims to create a future information society based on the quantum Internet through its activities.

The QITF also aims to create a quantum Internet testbed that includes all layers, and through this the implementation of standardization and commitments to society.

7.2.5 Quantum Flagship

[b-EQF] introduces the objectives of the European Quantum Flagship for quantum communications for the periods 2023–2026 and 2027–2030.

8 Implications for quantum-enabled future networks

8.1 Implications from status of existing study

A QEFN is going to be implemented in testbed stage. At the time of publication, it is expected to be realized in near future, in spite of doubt about what it will be called: quantum Internet; quantum network; quantum information network; etc. Some studies propose "protocol stack", which is both a layered model and a primitive protocol. It implies that QEFN-related fundamental technology is developing well at the time of publication and should be standardized for real worldwide implementation. Considering IETF/IRTF is trying to develop requests for comment (RFCs) for the quantum Internet, the initiation of the QEFN study in ITU-T is now required in collaboration with other SDOs.

8.2 Implications for standardization activity on Study Group 13

The quantum Internet is expected to introduce classical Internet-like study items such as addressing, routing protocol, resource allocation and quality of service. The mandate of ITU-T SG13, *Future networks and emerging network technologies*, is to standardize networked quantum devices and the quantum network. The requirements, architectures and capabilities of the quantum network should also be specified and led by ITU-T SG13.

9 Conclusions

The quantum network is considered to be one of the future networks that should be studied in ITU-T SG13. It is required that ITU-T SG13 initiate quantum network-related studies.

Appendix I

Summary of status of quantum-enabled future networks studies

NOTE – This appendix was developed with information available as of March 2023.

I.1 Standards development organizations

I.1.1 ITU-T Focus Group on Quantum Information Technology for Networks

1) Quantum information technology for networks terminology: Network aspects of quantum information technologies [b-ITU-T TR QIT4N D1.1]

Summary

The scope of [b-ITU-T TR QIT4N D1.1] is as follows:

– building blocks for QINs: necessary technologies for QINs;

– application-driven network requirements: QITs that impose requirements on to a QIN to function within it;

– benefits to classical networks;

– supports the deliverables of FG QIT4N Working Group 1 on Network aspects of QIT.

[b-ITU-T TR QIT4N D1.1] gives explanations of terms related to QIN development.

2) Quantum information technology for networks use cases: Network aspects of quantum information technologies [b-ITU-T TR QIT4N D1.2]

Summary

The scope of [b-ITU-T TR QIT4N D1.2] covers use cases of network aspects of QIT.

For content related to QIN, see clause 7.4 of [b-ITU-T TR QIT4N D1.2].

The security function of quantum communication is much stronger than that existing. The development stage of the quantum communication network required to implement quantum communication is currently between QKD and the large-scale quantum Internet that connects quantum computers and quantum communication channels.

3) Standardization outlook and technology maturity: Network aspects of quantum information technologies [b-ITU-T TR QIT4N D1.4]

Summary

The scope of [b-ITU-T TR QIT4N D1.4] covers the standardization outlook and technology maturity of QITs that either comprise or impact the requirements for a QIN, at the period of performance of the ITU-T FG QIT4N.

In clause 1 of [b-ITU-T TR QIT4N D1.4], QIN standardization considerations are mentioned as follows:

– QITs that are building blocks for QINs: These are necessary technologies for QIN, which provide fundamentally enabling aspects of a quantum information network, from lower-level essential components up through higher-level systems. For example, these technologies may include quantum memories, quantum repeaters, quantum network end-nodes, and respective technologies that extend traditional network control technology to allow QIN functionality.

I.1.2 IETF QIRG, etc.

1) Architectural principles for a quantum Internet [b-IETF RFC 9340]

Summary

[b-IETF RFC 9340]: proposes a quantum Internet framework to realize a quantum Internet vision; explains some basic architectural principles, cubits and quantum entanglement; and describes the direction of development of quantum Internet-related technologies.

1 Introduction

Quantum networks are distributed systems of quantum devices that utilize fundamental quantum mechanical phenomena, such as superposition, entanglement and quantum measurement, to achieve capabilities beyond what is possible with non-quantum (classical) networks.

Fully quantum networks capable of transmitting and managing entangled quantum states in order to send, receive and manipulate distributed quantum information are imminent at the time of publication. There are no proposals worked out for how to run these networks. While physical mechanisms for transmitting quantum states also exist, there are no robust protocols for managing such transmissions.

2 Quantum information

In order to understand the framework of quantum networking, a basic understanding of quantum information is required, and the basic concepts mentioned are as follows:

– qubit;

– multiple qubits;

– entanglement as the fundamental resource;

– bell pair and teleportation.

3 Entanglement as the fundamental resource

Entanglement is created through local interactions between two qubits or as a product of the way the qubits were created (e.g., entangled photon pairs). To create a distributed entangled state, one of the qubits can then be physically sent to a remote node. Therefore, it is qubit transmission that draws the line between a genuine quantum network and a collection of quantum computers connected over a classical network.

A quantum network can be described as a collection of nodes that is able to exchange qubits and distribute entangled states among themselves. A quantum node that is able only to communicate classically with another quantum node is not a member of a quantum network.

4 Achieving quantum connectivity

A quantum network cannot be built by simply extrapolating all the classical models to their quantum analogues. Sending qubits over a wire in a similar fashion to sending classical bits is simply not as easy to do. There are several technological as well as fundamental challenges that make classical approaches unsuitable in a quantum context.

To achieve quantum connectivity, section 4 of [b-IETF RFC 9340] explains the meaning of quantum connectivity and the necessary physical processes.

5 Architecture of a quantum internet

Since the basic services provided by quantum networks are very different to existing networks, the architecture of the quantum Internet is very different from that of its classical predecessor. Section 5 of [b-IETF RFC 9340] describes the main basic challenges to building quantum networks.

6 Architectural principles

6.1 Goals of a quantum internet

Quantum network architectures are similar to those of the classical Internet, but the details are fundamentally different. To lead to the architecture of the quantum Internet, it is necessary to set the following goals:

– support distributed quantum applications;

– support tomorrow's distributed quantum applications;

– support heterogeneity;

– ensure security at the network level;

– make them easy to monitor;

– ensure availability and resilience.

6.2 The principles of a quantum internet

The following principles of the quantum Internet provide guidance on the direction to be achieved and should be considered when designing quantum networks:

– entanglement is the fundamental service;

– bell pairs are indistinguishable;

– fidelity is part of the service;

– time is an expensive resource;

– be flexible with regards to capabilities and limitations.

7 A thought experiment inspired by classical networks

In conclusion, the quantum network architecture conceived based on its classical predecessor is to provide an idea about the elements necessary for its construction. Based on the classical and well-known multi-protocol label switching (MPLS), it can be applied to the architecture of quantum networks.

Quantum networks can be thought of as quantum virtual circuits with multiple endpoints to create multilateral entanglement. Similarly, MPLS networks have the concept of a label-switched path for multicast. Based on these similar characteristics, the quality of service parameters of quantum networks can be expressed.

Quantum networks can employ the routing protocols and traffic engineering of classical communications to ensure optimal paths, speed or fidelity to quantum virtual circuits. However, there may be some differences between the classical and quantum Internet.

Hardware blocking is required to determine the delivery rules of quantum networks. In quantum networks, control traffic (routing and signal messages) is exchanged over classical channels, while data plane traffic (actual bell pair qubits) is exchanged over separate quantum channels. This is in contrast to most classical networks in which control and data unit traffic share the same channel and a single packet includes both user and header fields. However, there are classical similarities to the way quantum networks work. A generalized MPLS network uses a separate channel for control traffic and data unit traffic.

2) Application scenarios for the quantum Internet [b-QIRG]

Summary

[b-QIRG] provides an overview of some applications whose use on the quantum Internet is expected, and then categorizes them using various classification schemes. Some general

requirements for the quantum Internet are also discussed. [b-QIRG] describes a framework for applications and a few selected application scenarios for the quantum Internet.

1 Introduction

Research and experiments have picked up over the last few years for developing the quantum Internet [b-Wehner]. End-nodes will also be part of the quantum Internet, in that case called quantum end-nodes that may be connected by quantum repeaters or routers. These quantum end-nodes will also run value-added applications that are discussed in sections 3 and 4 of [b-QIRG].

The connections between the various nodes in the quantum Internet are expected to be primarily fibre optics and free-space optical lasers. Photonic connections are particularly useful because light (photons) is very suitable for physically realizing qubits. Transmission of qubits across the quantum Internet is expected.

The quantum Internet will operate according to quantum physical principles such as quantum superposition and entanglement [b-IETF RFC 9340]. The quantum Internet is not anticipated to replace, but rather to enhance its classical predecessor. The intent of [b-QIRG] is to provide a common understanding and framework of applications and application scenarios for the quantum Internet.

2 Terms and acronyms list

For clarity, several terms and concepts related to QIT are briefly defined and described: bell pair; entanglement swapping; quantum end-node; quantum teleportation; qubit; etc.

3 Quantum internet applications

3.1 Overview

Expected applications are still being developed, as at the time of publication the quantum Internet is in its formative stages. However, an initial (and non-exhaustive) list of the applications to be supported on the quantum Internet can be identified and classified using two different schemes. Note that [b-QIRG] does not include quantum-computing applications that are purely local to a given node (e.g., quantum random number generator).

3.2 Classification by application usage

Application usage is classified into three categories according to its amount, and the details are as follows.

– Quantum cryptography applications
  - Secure communication setup
  - Fast Byzantine negotiation
  - Quantum money
– Quantum sensors applications
  - Network clock synchronization
  - High sensitivity sensing
  - Quantum imaging
– Quantum computing applications
  - Distributed quantum computing
  - Secure quantum computing with privacy preservation
  - Quantum chemistry

3.3 Control versus data plane classification

Nodes in quantum Internet applications may also use the classification paradigm of control plane versus data plane functionality as follows (see Table I.1).

– Control plane – Network functions and processes that operate on: 1) control bits/packets or qubits (e.g., to setup up end-user encryption); or 2) management bits/packets or qubits (e.g., to configure nodes).

– Data plane – Network functions and processes that operate on end user application bits/packets or qubits (e.g., voice, video, data). Sometimes also referred to as the user plane.

Table I.1 – Examples of control vs data plane classification

	Classical Internet examples	**Quantum Internet examples**	**Hybrid internet examples**
Control plane	Internet control message protocol; domain name system	Quantum ping; Signalling for controlling entanglement distribution;	QKD-based secure communication setup
Data plane	Video conference	QKD; Entanglement distribution	Video conference using QKD-based secure communication setup

4 Selected quantum Internet application scenarios

[b-QIRG] also introduces several quantum Internet application scenarios.

4.1 Secure communication setup

One requirement for this secure communication setup process is that it should not be vulnerable to any classical or quantum computing attack. This can be realized using QKD, which has been mathematically proven to be information theoretically secure and unbreakable. QKD can securely establish a secret key between two quantum nodes, using one channel for classical authentication and another for insecure quantum communication without physically transmitting the key through the network and thus achieving the required security.

4.2 Secure quantum computing with privacy preservation

See Figure I.1 (Figure 2 of [b-QIRG]).

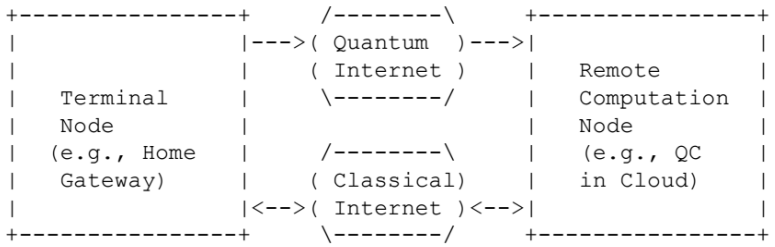

Figure I.1 – Secure quantum computing with privacy preservation

A terminal node such as a home gateway has collected lots of data on which it needs to perform computation. Although the terminal node can upload the data to leverage cloud computing without introducing local overhead, uploading to the cloud can cause privacy concerns. In this particular case, there is no privacy concern. since the source data will not be sent to the remote computation

node, which could be compromised. Delegated quantum computing or blind quantum computation can be leveraged to realize secure delegated computation and guarantee privacy preservation simultaneously.

4.3 Distributed quantum computing

There are two types of scenario in distributed quantum computers: utilizing quantum mechanics to improve classic distributed computing problems and distributing quantum computing capabilities to distributed quantum computers.

5 General requirements

5.1 Background

On the network level, six stages of quantum Internet development are described in [b-Wehner] as follows:

– trusted repeater networks (stage 1);
– prepare and measure networks (stage 2);
– entanglement distribution networks (stage 3);
– quantum memory networks (stage 4);
– fault-tolerant few qubit networks (stage 5);
– quantum computing networks (stage 6).

Table I.2 – Example application scenarios in different quantum internet stages

Quantum Internet stage	Example quantum Internet use cases	Characteristic
Stage 1	Secure communication setup using basic QKD	Trusted nodes
Stage 2	Secure communication setup using the QKD with end-to-end security	Prepare-and-measure capability
Stage 3	Secure communication setup using entanglement-enabled QKD	Entanglement distribution
Stage 4	Secure or blind quantum computing	Quantum memory
Stage 5	Higher-accuracy clock synchronization	Fault tolerance
Stage 6	Distributed quantum computing	More qubits

5.2 Requirements

Some general and functional requirements on the quantum Internet from the networking perspective, based on the application scenarios in section 4, are identified in [b-QIRG] as follows.

– Methods for facilitating quantum applications to interact efficiently with entangled qubits are necessary in order for them to trigger distribution of designated entangled qubits to potentially any other quantum node residing on the quantum Internet.
– Quantum repeaters and routers should support robust and efficient entanglement distribution in order to extend and establish high-fidelity entanglement connection between two quantum nodes.
– Quantum end-nodes must send additional information on classical channels to aid in transmission of qubits across quantum repeaters and receivers.

– Methods for managing and controlling the quantum Internet including quantum nodes and their quantum resources are necessary. Furthermore, a new management information model for the quantum Internet may need to be developed.

6 Conclusion

[b-QIRG] provides an overview of some expected application categories for the quantum Internet, and then details selected application scenarios. The applications are also classified as either control plane or data plane functionality as typical for the classical Internet. This set of applications may, of course, naturally expand over time as the quantum Internet matures. Finally, some general requirements for the quantum Internet are also provided. [b-QIRG] can also serve as an introductory text for readers interested in learning about the practical uses of the quantum Internet.

7 Security considerations

[b-QIRG] specifies neither an architecture nor a specific protocol for the quantum Internet. It focuses instead on detailing application scenarios, requirements and describing typical quantum Internet applications.

I.2 Research institutes and academia

I.2.1 United States Department of Energy and associated research institutes

1) Report of the DoE quantum Internet blueprint workshop [b-US DoE]

Summary

[b-US DoE] identifies four PRDs for the implementation of the quantum Internet and outlines five blueprint roadmap milestones that must be achieved to facilitate an eventual national quantum Internet.

The four PRDs are as follows:

– to provide the foundational building blocks for a quantum Internet;
– to integrate multiple quantum networking devices;
– to create repeating, switching and routing for quantum entanglement;
– eto nable error correction of quantum networking functions.

The five key milestones is as follows:

– verification of secure quantum protocols over fibre networks;
– inter-campus and intra-city entanglement distribution;
– intercity quantum communication using entanglement swapping;
– interstate quantum entanglement distribution using quantum repeaters;
– build a multi-institutional ecosystem between laboratories, academia and industry to transition from demonstration to operational infrastructure.

2) A roadmap for quantum interconnects report from Q-NEXT [b-ANL]

Summary

[b-ANL] identifies a number of applications of quantum communication systems (referred to as quantum networks) with likely technological impact over the next 10 to 15 years, including:

– QKD;
– quantum-enhanced classical communication;
– authentication and security beyond QKD;

– repeater-enabled fundamental science;
– quantum sensing aided by repeater-enabled quantum networks;
– networked quantum computing.

[b-ANL] also identifies seven science and technology imperatives over the next 10 years:

1 provide precise and near-term application of clear need for commerce, government or science;
2 develop critical quantum components that are compatible with photon-based qubits in the visible, near-infrared and telecommunication wavelengths;
3 demonstrate quantum repeater-enabled quantum communication, with success probabilities exceeding that possible via direct transmission;
4 demonstrate long-range (intercity) entanglement distribution using repeaters;
5 develop (optimize and standardize) a true multi-node quantum network architecture;
6 demonstrate a homogeneous multi-node quantum network at intercity scale;
7 demonstrate an inhomogeneous quantum internetwork at interstate scale.

I.2.2 Quantum Internet Alliance and QuTech

1) Quantum internet: A vision for the road ahead [b-Wehner]

Summary

[b-Wehner] is a comprehensive paper on implementation, which suggests six stages to complete the quantum Internet using qubits.

The six stages to the quantum network are as follows:

– trusted repeater networks (quantum repeater);
– prepare and measure networks;
– entanglement distribution networks;
– quantum memory networks;
– fault-tolerant few-qubit networks;
– quantum-computing networks.

I.2.3 European Union quantum communication infrastructure project

1) European industry white paper on the European quantum communication infrastructure [b-EU QCI]

Summary

[b-EU QCI] introduces a project plan aimed at commercializing a complete QIN from 2021 to 2035.

The goals of the implementation programme proposed in [b-EU QCI] are as follows.

– Specify stage 1 (2021–2028, quantum-secured networks) and stage 2 (2028–2035, quantum information networks).
– Specify structuring user requirements, deriving them from the terrestrial and space components of the overall architecture.
– Start the development of European terrestrial products to be progressively integrated in metropolis-scale networks.
– Start the space segment trade-off and architecture studies for a development and technology plan specification including necessary in-orbit demonstration.

– Complete the deployment of the terrestrial local networks and develop the operational elements of the space component and of the resulting hybrid network management and operation means by 2028.
– In parallel, launch the preparation of the technology transfer from laboratory to industry for the terrestrial and space equipment needed to reach the second objective of the QCI – building a complete quantum information network (2028–2034).
– In parallel, universities shall be incentivized to educate quantum engineers, a topic of utmost importance for a successful QCI ecosystem.
– In parallel, European lawmakers should draft the legislation needed to regulate aspects of QCI rights, use and competition, and support industry in the creation of appropriate international standards. Trusted repeater networks (Quantum repeater).

I.2.4 Quantum Internet Task Force

1) QITF – Quantum Internet white paper [b-QITF]

Summary

The QITF takes into account the history of the current Internet, and while valuing the diversity and interconnectedness of technologies, aims to create a future information society based on the quantum Internet through its activities.

In [b-QITF], the quantum Internet is a technology for exchanging quantum data, and in this respect, cannot be replaced by digital communication-based technology. The communication base of the quantum Internet is fundamentally different from that of digital data (hereinafter referred to as digital communication base).

For its implementation, a layered architecture for the quantum Internet is required with a communication management protocol, a communication resource reservation algorithm protocol and quantum entanglement purification. In other words, it is necessary to divide and organize functions and responsibilities necessary to realize the quantum Internet by layer, and specify interlayer interfaces. In the study from an architectural perspective, as previously described, "how many layers of functions are required to operate the quantum Internet" is an important research task.

Since research into layered architecture is essential technically and socially to extend the quantum Internet, the QITF describes the structure of the layered architecture of the quantum Internet by referring to the layered architecture of the classical Internet.

I.2.5 Quantum Flagship

1) Strategic Research and Industry Agenda (SRIA) report from European Quantum Flagship [b-EQF]

Summary

Quantum communication objectives in 2023 to 2026:

– improved performance, key rate and range, for QKD solutions;
– photonic integrated circuits, with efficient and cost-effective experimental devices for quantum communication;
– deployment of prototype payloads for space QKD;
– at least two industrialized QKD systems made in Europe and based mostly on a European supply chain;
– deployment of several metropolitan QKD networks;
– deployment of large-scale QKD networks with trusted nodes;

– operation and enhancement of MDI QKD, such as twin-field, with a range of 500 km or more, without repeaters or trusted nodes;
– advances in QKD: testing, certification, accreditation, and availability conditions (e.g., laboratories) to ensure robustness to side-channel attacks at the optical level;
– development of joint QKD and post-quantum cryptography (PQC) solutions;
– several telecommunications companies selling QKD services with a sustainable business model;
– demonstrating the use of quantum channels for other cryptographic applications, such as private data mining, secure multiparty computing, long-term secure storage, unforgeable cryptosystems;
– integration of reliable, small and cheap quantum noise random number generators into classical and quantum communication systems;
– large-scale communications and entanglement distribution systems outside the laboratory, including network management software;
– development of quantum internet sub-systems such as quantum memories, and processing nodes;
– demonstration of a functional elementary quantum repeater link over telecommunication wavelengths and fully independent nodes;
– design of new application protocols, pilot use cases, software and network stack for a quantum internet;
– coexistence of QKD with conventional communications solutions, including multiplexing, allowing one optical channel to be used for multiple services (quantum and classical).

Quantum communication objectives in 2027 to 2030:

– cost-effective development, maintenance, and power consumption for QKD systems;
– scaling of QKD solutions, due to increased market demand;
– small form-factor pluggable (SFP) QKD transmitter and receiver pair for key distribution;
– QKD systems robust to side-channel attacks, including power consumption and thermal noise, for standalone transmitters and receivers (without physical security);
– deployment of MDI QKD as an industrial product, over very long distances;
– deployment of a QKD network "backbone" connecting major European metropolitan networks;
– certification of quantum-safe security, including QKD possibly combined with PQC, by at least one national security agency;
– certification of SFP services and software for universal plug-in;
– mature quantum communications infrastructure for general usage by organizations and citizens;
– space-based quantum communications infrastructure;
– multi-node quantum networks supporting basic quantum internet applications;
– deployment of reliable interfaces between qubits at rest and in transit in the network;

- reliable industry-grade quantum memories to extend communication distances and the demonstration of quantum repeaters;
- long-distance fibre backbone using quantum repeaters capable of connecting metropolitan areas networks over hundreds of kilometres;
- integration of advanced quantum network applications into classical network infrastructure (i.e., orchestration platform) over a quantum network including quantum repeaters.

Bibliography

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

[b-ITU-T TR QIT4N D1.1] ITU-T Technical Report QIT4N D1.1 (2021), *Quantum information technology for networks terminology: Network aspects of quantum information technologies*.

[b-ITU-T TR QIT4N D1.2] ITU-T Technical Report QIT4N D1.2 (2021), *Quantum information technology for networks use cases: Network aspects of quantum information technologies*.

[b-ITU-T TR QIT4N D1.4] ITU-T Technical Report QIT4N D1.4 (2021), *Standardization outlook and technology maturity: Network aspects of quantum information technologies*.

[b-IETF RFC 9340] IETF RFC 9340 (2023). *Architectural principles for a quantum Internet.*

[b-EQF] European Quantum Flagship (2022). *Strategic research and industry agenda*. European Quantum Flagship. 50 pp. Available [viewed 2023-05-19] at: https://qt.eu/media/pdf/Quantum-Flagship_SRIA_2022.pdf?m=1674660050&

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*.

[b-EU QCI] Quantum Communication Infrastructure (2019). *European industry white paper on the European quantum communication infrastructure*. Brussels: European Union. 13 pp. Available [viewed 2023-05-19] at: http://www.qtspace.eu/sites/testqtspace.eu/files/other_files/IndustryWhitePaper_V3.pdf

[b-ANL] ANL (2022). *Next Generation Quantum Science and Engineering (Q-NEXT): A roadmap for quantum interconnects* (ANL-22/83). Lemont, IL: Argonne National Laboratory. 48 pp. Available [viewed 2023-05-18] at: https://publications.anl.gov/anlpubs/2022/12/179439.pdf

[b-QIRG] QIRG Workgroup (2023). *Application scenarios for the quantum Internet*. Fremont, CA: Internet Engineering Task Force. Available [viewed 2023-05-19] from: https://datatracker.ietf.org/doc/draft-irtf-qirg-quantum-internet-use-cases/

[b-QITF] QITF (2021). *"The" 量子インターネット* ["The" quantum Internet]. Fujisawa: Quantum Internet Task Force. 34 pp. Available [viewed 2023-05-19] at: https://qitf.org/files/20210222_qitf_whitepaper.pdf

[b-US DoE] US DoE (2020), *From long-distance entanglement to building a nationwide quantum Internet*, Report of the DoE Quantum Internet Blueprint Workshop, 2020-02-05/06. Washington, DC: United States Department of Energy. 36 pp. Available [viewed 2023-05-18] at: https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf

[b-Wehner] Wehner, S., Elkouss, D., Hanson, R. (2018), Quantum internet: A vision for the road ahead. *Science*, **362**, eaam9288, 9 pp. Available [viewed 2023-05-19] at: https://www.science.org/doi/10.1126/science.aam9288

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023