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

Quantum key distribution networks – Quantum-enabled future networks

CAUTION!
PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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

Quantum key distribution networks – Quantum-enabled future networks

Summary

The scope of this Supplement is to describe ITU-T's Views for Quantum-Enabled Future Networks (QEFN) for the future networks study to act as a document to help SG13 to study the future network evolution towards 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

Page

1. Scope 4

2. References 4

3. Definitions 4

4. Abbreviations and acronyms 4

5. Conventions 5

6. Introduction 5

7. Status of Quantum-Enabled Future Networks Study 5

8. Implications for Quantum-Enabled Future Networks 7

9. Conclusions 7

Appendix Summary of status of Quantum-Enabled Future Networks Studies 8

Bibliography 19

Supplement 75 to ITU-T Y-series Recommendations

Quantum key distribution networks – Quantum-enabled future networks

1. Scope

The scope of this Supplement is to describe ITU-T's Views for Quantum-Enabled Future Networks (QEFN) for the future networks study to act as a document to help SG13 to study the future network evolution towards Quantum era.

2. References

None.

3. Definitions

3.1. Terms defined elsewhere

3.1.1 quantum key distribution (QKD) [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 (QKD) module [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 networks [ITU-T FG QIT4N D1.1]: A network that incorporates quantum communication technology for the purpose of transmitting quantum states.

3.2. Terms defined in this Recommendation

3.2.1 quantum-enabled future network: A network that connects quantum devices using fundamental quantum information technologies which are based on quantum

Note – Some definitions for QEFN-related (e.g., quantum devices, quantum network, etc.) could be further studied, but those were out of scope of this document.

4. Abbreviations and acronyms

DoE	Department of Energy
ESnet	Energy Science Network
FG on QIT4N	Focus Group on Quantum Information Technology for Networks
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
QCI	Quantum Communication Infrastructure
QEFN	Quantum-Enabled Future Networks
QIA	Quantum Internet Alliance
QIN	Quantum Information Networks
QIRG	Quantum Information Research Group

QIT	Quantum Information Technology
QIT4N	Quantum Information Technology for Networks
Q-NEXT	Next Generation Quantum Science and Engineering
QKD	Quantum Key Distribution
SDO	Standard Development Organization

5. Conventions

None

6. Introduction

QEFN is connected quantum devices using fundamental quantum information technologies which are based on quantum theory such as superposition and entanglement. The well-known quantum devices are quantum computer, quantum sensor, and quantum key distribution (QKD) module.

The basic distinction of QEFN comparing to current digital network is derived from quantum information technologies. The below Table 1 introduces those distinctions.

Table 1. Basic distinction 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/Repeating 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 very actively. The QEFN enabling technologies may have an impact on standardization progress.

7. Status of Quantum-Enabled Future Networks Study

7.1. SDOs

Note – Details of each SDO are in Appendix.

7.1.1. ITU-T FG on QIT4N

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 QIT for networks.

Throughout ITU-T FG QIT4N D1.1, necessary technologies for QIN and explanations of related terms for QIN development are mentioned. In ITU-T FG QIT4N D1.2, the use case of QIN and applied QIT are introduced. Finally, ITU-T FG QIT4N D1.4 is about the standardization outlook and technology maturity of quantum information technologies which either comprise or impact the requirements for QIN.

The FG defines Quantum Information Networks (QIN) as any network that incorporates quantum communication technology for the purpose of transmitting quantum states.

7.1.2. IETF/IRTF QIRG

The IETF/IRTF will be beneficial in quantum network engineering because it has a lot of existing network engineering experience. With this background, two documents were published.

'Architectural Principles for a Quantum Internet' proposes a quantum Internet framework to realize a quantum Internet vision and explains some basic architectural principles. It explains the basic principles of quantum internet, such as cubits and quantum entanglement, and describes the direction of development of quantum Internet-related technologies. In particular, this document proposes a quantum network architecture inspired by classical network architectures.

'Application Scenarios for the Quantum Internet' 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.

The group defines Quantum Networks as a collection of nodes that is able to exchange qubits and distribute entangled states amongst themselves. Quantum Internet is defined as a network of Quantum Networks. The Quantum Internet is expected to be merged into the Classical Internet to form a new Hybrid Internet.

7.2. Research Institutes & Academia

Note – Details of each Research Institutes & Academia are in Appendix.

7.2.1. United States Department of Energy (DOE) and associated research institutes

In 2020, the U.S. Department of Energy published a strategic report that presents a blueprint for the implementation of the quantum Internet. This resulting report identifies four Priority Research Directions (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.

Also, in April 2019, scientists from the U.S. Department of Energy (DOE)'s Brookhaven National Laboratory, Stony Brook University (SBU), and 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 fiber network. Argonne National Laboratory has created a 52-mile quantum loop entanglement distribution network that will be connected to Fermi lab, establishing a three-node, 80-mile testbed for quantum communication.

In July 2022, Q-NEXT, a U.S. Department of Energy (DOE) National Quantum Information Science Research Centre, released A Roadmap for Quantum Interconnects report, in which reviewed the materials, components and systems used for quantum interconnect; summarized relevant scientific questions and issues; and addressed the most pressing research needs. The document then distilled these considerations into recommendations for strategic science and technology research imperatives for the next decade.

7.2.2. Quantum Internet Alliance (QIA) & QuTech

The Quantum Internet Alliance (QIA) targets 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.

In 2018, QuTech of the Netherlands published a comprehensive paper that could implement quantum Internet, and suggested six stages to complete quantum internet using qubit.

7.2.3. EU Quantum Communication Infrastructure (QCI) project

In 2019, the EU's QCI project introduced a project plan aimed at commercializing a complete quantum information network from 2021 to 2035.

7.2.4. Quantum Internet Task Force

The Quantum Internet Task Force take into account the history of the current Internet, and while valuing the diversity and interconnectedness of technologies, aim to create a future information society based on the Quantum Internet through its activities.

They also aim to create a Quantum Internet testbed that includes all layers, and through this they implement standardization and commitments to society.

7.2.5. Quantum Flagship

In November 2022, the European Quantum Flagship published the latest version of Strategic Research and Industry Agenda (SRIA) report, in which introduced objectives for quantum communications for the next years include 2023-2026 and 2027-2030.

8. Implications for Quantum-Enabled Future Networks

8.1. Implications from status of existing study

QEFN is going to be implemented in Testbed stage. It is expected to be realized in near future, in spite of how to be named; Quantum Internet, Quantum Network, Quantum Information Network, etc. Some studies proposed protocol stack which is a layered model and primitive protocol as well. It implies that QEFN-related fundamental technology is well developing nowadays and should be standardized for real world-wide implementation. Considering IETF/IRTF is trying to develop RFCs for 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

Quantum Internet is expected to introduce classical Internet-like study items such as addressing, routing protocol, resource allocation, quality of service, etc. Considering the mandate of ITU-T SG13, Future networks and emerging network technologies, standardizing networked quantum devices; quantum network, is the role of SG 13. The requirements, architectures and capabilities of quantum network should be specified and led by SG13.

9. Conclusions

Quantum Network is considering one of future networks should be studied in SG13. It is required that SG13 initiates quantum network-related studies.

Appendix

Summary of status of Quantum-Enabled Future Networks Studies

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

1. SDOs

1.1 ITU-T FG on QIT4N

1) Quantum information technology for networks terminology: Network aspects of quantum information technologies [b-QIT4N D1.1]
Summary The scope of this document FG QIT4N D1.1 is as follows： - Building blocks for QINs: Necessary technologies for QIN - Application-driven network requirements: Quantum information technologies that impose requirements onto a QIN to function within it. - Supports the deliverables of FG QIT4N Working Group 1 on Network aspects of QIT: Throughout this document, explanations of related terms for QIN development are mentioned.
2) Quantum information technology for networks use cases: Network aspects of quantum information technologies [b-QIT4N D1.2]
summary The scope of this document FG QIT4N D1.2 is the use cases of network aspects of quantum information technology (QIT). The contents related to QIN are mentioned in Quantum Communication in clause 7 of this document. The security function of quantum communication is much stronger than the existing security function. 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-QIT4N D1.4]
Summary The scope of this document FG QIT4N D1.4 is the standardization outlook and technology maturity of quantum information technologies which either comprise or impact the requirements for a quantum information network (QIN), at the period of performance of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). In this document, 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.

1.2. IETF QIRG, etc.

1) Architectural Principles for a Quantum Internet [b-I-D.qirg-principles-11]

Summary

This document proposes a quantum Internet framework to realize a quantum Internet vision and explains some basic architectural principles. It explains the basic principles of quantum Internet, such as 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 utilise 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 now imminent. There are no worked out proposals for how to run these networks. Also, whilst physical mechanisms for transmitting quantum states 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 & 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 can then physically send one of the qubits to a remote node. Therefore, it is the transmission of qubits that draws the line between a genuine quantum network and a collection of quantum computers connected over a classical network.

A quantum network is defined as a collection of nodes that is able to exchange qubits and distribute entangled states amongst 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 like we send 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, this section 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 from existing networks, the architecture of quantum Internet is very different from that of classical Internet. This section describes with the main basic challenges of building quantum networks.

6. Architectural principles

6.1. Goals of a quantum internet

Quantum network architectures are similar to classical Internet architectures, but the architectural details are fundamentally different. It is necessary to set goals that will lead the architecture of the quantum Internet, and the goals are as follows:

- 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 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 the classical network is to provide an idea about the elements necessary for its construction. Based on the classical and well-known MPLS (Multi-Protocol Label Switching), 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 LSP (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 Internet and the 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 (MPLS) network uses a separate channel for control traffic and data unit traffic.

2) Application Scenarios for the Quantum Internet [b-I-D.qirg-use-cases-14]

Summary

This document provides an overview of some applications expected to be used on the Quantum Internet, and then categorizes them using various classification schemes. Some general requirements for the Quantum Internet are also discussed. The intent of this document is to describe a framework for applications, and describe 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/routers. These quantum end-nodes will also run value-added applications which will be discussed later.

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

The Quantum Internet will operate according to quantum physical principles such as quantum superposition and entanglement [b-I-D.qirg-principles-11]. The Quantum Internet is not anticipated to replace, but rather to enhance the Classical Internet. The intent of this document 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 quantum information technology are briefly defined and described; Bell pair, Entanglement Swapping, Quantum End-node, Quantum Teleportation, Qubit, etc.

3. Quantum Internet Applications

3.1. Overview

The expected applications for the Quantum Internet are still being developed as we are in the formative stages of the Quantum Internet. 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, this document 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

It was classified into three categories according to the amount of application use, 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 vs Data Plane Classification

Nodes in the Quantum Internet applications may also use the classification paradigm of control plane functionality versus data plane functionality where:

- 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.

	Classical Internet Examples	Quantum Internet Examples	Hybrid Internet Examples
Control Plane	ICMP; DNS	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

Table A-1. Examples of Control vs Data Plane Classification

4. Selected Quantum Internet Application Scenarios

This document also introduced 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 a classical authentication channel and insecure quantum communication channel without physically transmitting the key through the network and thus achieving the required security

4.2. Secure Quantum Computing with Privacy Preservation

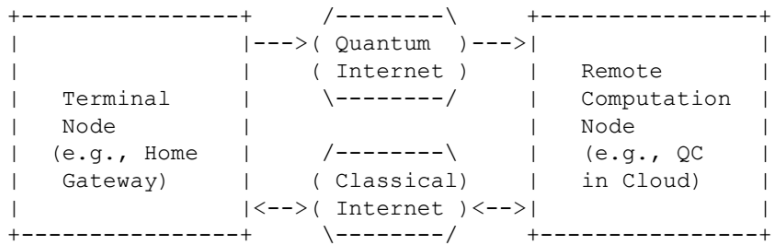

Figure A-1. Secure Quantum Computing with Privacy Preservation

A terminal node such as a home gateway has collected lots of data and needs to perform computation on the data. Although the terminal node can upload the data to the cloud to leverage cloud computing without introducing local computing overhead, to upload the data 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 (BQC) can be leveraged to realize secure delegated computation and guarantee privacy preservation simultaneously.

4.3. Distributed Quantum Computing

There are two types of scenarios 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)

Quantum Internet Stage	Example Quantum Internet Use Cases	Characteristic
Stage-1	Secure comm setup using basic QKD	Trusted nodes
Stage-2	Secure comm setup using the QKD with end-to-end security	Prepare-and-measure capability
Stage-3	Secure comm setup using entanglement-enabled QKD	Entanglement distribution
Stage-4	Secure/blind quantum computing	Quantum memory
Stage-5	Higher-Accuracy Clock synchronization	Fault tolerance
Stage-6	Distributed quantum computing	More qubits

Table A-2. Example Application Scenarios in Different Quantum Internet Stages

5.2. Requirements

Some general and functional requirements on the Quantum Internet from the networking perspective, based on the above application scenarios, are identified 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 in the Quantum Internet.
- Quantum repeaters/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/receivers.
- Methods for managing and controlling the Quantum Internet including quantum nodes and their quantum resources are necessary. Furthermore, new management information model for the Quantum Internet may need to be developed.

6. Conclusion

This document 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. This document can also serve as an introductory text to readers interested in learning about the practical uses of the Quantum Internet.

7. Security Considerations

This document does not define an architecture nor a specific protocol for the Quantum Internet. It focuses instead on detailing application scenarios, requirements, and describing typical Quantum Internet applications.

2. Research Institutes & Academia

2.1. United States Department of Energy (DOE) and the associated research institutes

1) Report of the DOE Quantum Internet Blueprint Workshop

Summary

This resulting report identifies four Priority Research Directions (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 Priority Research Directions (PRDs) is as follows :

- Provide the Foundational Building Blocks for a Quantum Internet
- Integrate Multiple Quantum Networking Devices
- Create Repeating, Switching, and Routing for Quantum Entanglement
- Enable Error Correction of Quantum Networking Functions

The five Key Milestones is as follows :

- Verification of Secure Quantum Protocols over Fiber 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

Summary

The report identified a number of applications of quantum communication systems (referred to in the document as quantum networks) with likely technological impact over the next 10–15 years, including:

- Quantum Key Distribution (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

The report also identified seven science and technology imperatives over the next 10 years:

1. Provide precise and near-term application of clear need for commerce, government, and/or science

2. Develop critical quantum components that are compatible with photon-based qubits in the visible, near-infrared (IR), and telecom 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 homogeneous multi-node quantum network at intercity scale

7. Demonstrate inhomogeneous quantum internetwork at interstate scale

2.2. Quantum Internet Alliance (QIA) & QuTech

1) Quantum internet: A vision for the road ahead

Summary

In 2018, QuTech of the Netherlands published a comprehensive paper that could implement quantum Internet, and suggested six stages to complete quantum Internet using Qubit.

The six stage of quantum network is 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

2.3. EU QCI project

1) European industry White paper on the European Quantum Communication Infrastructure

Summary

In 2019, the EU's QCI project introduced a project plan aimed at commercializing a complete quantum information network from 2021 to 2035.

The goals of the QCI implementation program proposed in this document is as follows :

- Define in the coming months the stage 1 (2021-2028, Quantum-Secured Networks) and stage 2 (2028-2035, Quantum Information Networks).
- Define the structuring user requirements and derive them on 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/architecture studies for a development and technology plan definition 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 law makers should generate the needed legislation in order to regulate the aspects of QCI rights, use and competition, and support industry in the creation of appropriate international standards. Trusted repeater networks (Quantum repeater)

2.4. Quantum Internet Task Force

1) QITF - Quantum Internet Whitepaper

Summary

The Quantum Internet Task Force take into account the history of the current Internet, and while valuing the diversity and interconnectedness of technologies, aim to create a future information society based on the Quantum Internet through its activities.

In this white paper, quantum Internet is a technology for exchanging quantum data, and in this respect, quantum Internet cannot be replaced by digital communication-based technology because it is fundamentally different from the communication base of digital data (hereinafter referred to as digital communication base).

In order to implement quantum Internet, a layered architecture for 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 quantum Internet by layer, and define interlayer interfaces. In the study from an architectural perspective, as described above, "how many layers of functions required to operate quantum Internet" is an important research task.

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

2.5. Quantum Flagship

1) Strategic Research and Industry Agenda (SRIA) report from European Quantum Flagship

Summary

Quantum Communication Objectives by 2023-2026.

- 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 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 QRNGs 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 telecom 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 by 2027-2030.

- 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/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 fiber backbone using quantum repeaters capable of connecting metropolitan areas networks over hundreds of kilometers.

- Integration of advanced quantum network applications into classical network infrastructure (i.e. orchestration platform) over a quantum network including quantum repeaters.

Bibliography

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

[b-I-D.qirg-principles-11] IRTF QIRG Internet Draft draft-irtf-qirg-principles-11 (2022), *Architectural Principles for a Quantum Internet*

[b-I-D.qirg-use-cases-14] IRTF QIRG Internet Draft draft-irtf-qirg-quantum-internet-use-cases-14 (2023), *Application Scenarios for Quantum Internet*

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

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

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

[b-Wehner] Wehner, S., Elkouss, D. and Hanson, R. (2018), *Quantum internet; A vision for the road ahead, Science, Vol. 362, No. 16412.*