International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(24 November 2021)

ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N)

FG QIT4N D1.1

Quantum information technology for networks terminology: Network aspects of quantum information technologies

ITU-T

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.

Quantum information technology (QIT) is a class of emerging technology that improves information processing capability by harnessing principles of quantum mechanics which is expected to have a profound impact to ICT networks.

The ITU Telecommunication Standardization Advisory Group established the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) in September 2019 to provide a collaborative platform to study the pre-standardization aspects of QITs for ICT networks.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

FG QIT4N concluded and adopted all its Deliverables as technical reports on 24 November 2021.

Number	**Title**
FG QIT4N D1.1	QIT4N terminology: Network aspects of QITs
FG QIT4N D1.2	QIT4N use cases: Network aspects of QITs
FG QIT4N D1.4	Standardization outlook and technology maturity: Network aspects of QITs
FG QIT4N D2.1	QIT4N terminology: QKDN
FG QIT4N D2.2	QIT4N use cases: QKDN
FG QIT4N D2.3	QKDN protocols: Quantum layer
FG QIT4N D2.3	QKDN protocols: Key management layer, QKDN control layer and QKDN management layer
FG QIT4N D2.4	QKDN transport technologies
FG QIT4N D2.5	QKDN standardization outlook and technology maturity

The FG QIT4N Deliverables are available on the ITU webpage, at https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx.

For more information about FG QIT4N and its deliverables, please contact tsbfgqit4n@itu.int.

Technical Report FG QIT4N D1.1

Quantum information technology for networks terminology: Network aspects of quantum information technologies

Summary

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).

Based on existing work of various Standards Development Organizations (SDOs) and academic literature, it surveys terminology on network aspects of quantum information technology, studies their overlap and divergence and provides a list of terms that are required but are yet to be standardized. Future efforts to standardize terminology on network aspects of quantum information technology could be informed by this technical report.

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.

Keywords

Network aspects of QIT; quantum information technology; terminology.

Chief Editor:	Minghan Li CAS Quantum Network Co., Ltd. China	Email: liminghan@qtict.com

Acknowledgments

The Chief Editor expresses his appreciation to all the contributors of this report and all participants of Working Group 1 of the Focus Group on Quantum Information Technology for Networks (FG QIT4N) for their invaluable inputs, thorough review and all comments provided during its development.

Table of Contents

Technical Report FG QIT4N D1.1

Quantum information technology for networks terminology: Network aspects of quantum information technologies

1 Scope

The main objective of this report is to collect, analyse and sort terminology on quantum information technology for networks. Related technical terms were collected from SDOs, academia and industry.

For the purpose of this technical report, a quantum information network (QIN) is defined as *any network that incorporates quantum communication technologies for the purpose of transporting quantum states*. The specific scope of this technical report is terminology that supports:

– **Building blocks for QINs:** *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.

– **Application-driven network requirements:** *Quantum information technologies that impose requirements onto a QIN to function within it.* This would include:

  i. QIT technologies that use a QIN in a piecewise manner, similar to but not including a quantum key distribution (QKD) network

  ii. QIT technologies that use a QIN end to end, for example, applications using entanglement whose distribution relies on the network.

– **Benefits to classical networks:** *Quantum information technologies overlaid on a classical network that substantially alter that network's quality, as for example but not exclusive to security and timing, beyond what is possible with classical technology*.

– **Supports the deliverables of FG QIT4N Working Group 1 on Network aspects of QIT:** *Quantum information technologies that support QIN use cases [b-QIT4N D1.2] and the QIN standardization outlook and technology maturity assessment [b-QIT4N D1.4].* Terms included make the applications involved in a use case understandable to a general audience, but not to provide the technical depth or breadth needed by QIT application developers.

QITs **not considered within this report** are those that do not satisfy the above requirements.

In particular, this technical report provides:

– Terminology landscape

– Terminology survey

– Terminology opinions

2 References

None.

3 Definitions

This clause is intentionally left blank.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

QIN Quantum Information Network

QIT Quantum Information Technology

QKD Quantum Key Distribution

QRNG Quantum Random Number Generator

5 Terminology landscape

Terminology on network aspects of quantum information technology (QIT) has been progressing in varying degrees at multiple institutions. With some related work already developed and under development in various SDOs, including ITU-T Study Groups 13 and 17 as well as in other deliverables of the Focus Group on Quantum Information Technology for Networks, it was necessary to study the potential gaps between these efforts. Terms that coincide with the scope of this technical report are collected and the aspects considered include:

– work by SDOs, academia and industry consortia engaged in standardization activities on terminology on network aspects of quantum information technology. Four work items from ETSI, ISO/IEC and ITU-T are cited in this report:
  - [b-ETSI GR QKD 007] which is the published Group Report on QKD vocabulary.
  - [b-Draft ETSI 007 V1.3.2] which is the draft version 1.3.2 (V1.3.2) of the revised [b-ETSI GR QKD 007] that was under development at the time of publication of this report.
  - [b-ISO/IEC JTC1 AG4] which is the process document of ISO/IEC AWI 4879, still under development, that aims to define the terminology and vocabulary of quantum computing.
  - [b-ITU-T X.1702] which is a published ITU-T Recommendation about quantum noise random number generator architecture.

  The descriptions of new QIT-related terms that are yet to be standardized are collected from a survey of public literature.

– links and references to relevant terminology lists.

NOTE – For the purposes of this technical report, the terminology considered is for QITs that provide fundamentally enabling components of a quantum network, such as single photon sources and detectors, or would have specific requirements of a quantum network, different from those required of a classical network, in order to be connected to that network.

In line with the scope of this technical report, the terminology is ordered alphabetically and categorized into four:

– terminology related to quantum synchronization for networks

– terminology related to quantum random number generators (QRNG)

– terminology related to quantum computing for networks

– general terminology related to network aspects of QIT

5.1 Terminology related to quantum synchronization for networks

5.1.1 Terms defined by Standards Development Organizations elsewhere

None.

5.1.2 Relevant terms not currently included in standards

This Technical Report lists the following terms found in a survey of public literature:

5.1.2.1 quantum clock [b-Ruiz]: a quantum system in a state of superposition of energy eigenstates can be used as a reference clock, according to which time evolution is defined

5.1.2.2 quantum clock device [b-Mignemi]: a device that measures time by counting the decays of a sample of radioactive matter

5.1.2.3 quantum clock network [b-Kómár]: a network can be operated near the fundamental precision limit set by quantum theory

5.1.2.4 quantum clock synchronization [b-Quan]: synchronizing two clocks based on second-order quantum interference between entangled photons generated by parametric down-conversion

5.1.2.5 quantum clock synchronization protocols [b-Krčo]: utilizes shared prior entanglement and broadcast of classical information to synchronize spatially separated clocks

5.1.2.6 quantum electron devices [b-Capasso]: when semiconductor devices become small enough, inescapable quantum effects open a whole new range of possibilities for electronic manipulation

5.1.2.7 quantum frequency conversion [b-Kumar]: the quantum states of two light beams of different frequencies can be interchanged

5.1.2.8 quantum logic clock [b-NIST]: an atomic clock that uses an aluminium atom to apply the logic of computers to the peculiarities of the quantum

5.1.2.9 quantum synchronization [b-Zhirov]: the synchronization is preserved in a quantum case

5.1.2.10 quantum synchronization over quantum network [b-Lohe]: network of quantum oscillators in which quantum states are distributed among connected nodes by means of unitary transformations

5.1.2.11 quantum time source [b-Time]: according to some theories that look to combine quantum mechanics and gravity into a single "theory of everything" (often referred to as quantum gravity), there is a possibility that time could in fact be quantized. A hypothetical chronon unit for a proposed discrete quantum of time has been proposed, although it is not clear just how long a chronon should be

5.1.2.12 remote quantum clock synchronization [b-Okeke]: closes the loophole for entanglement-based quantum clock synchronization protocols, which is a non-local approach to synchronize two clocks independent of the properties of the intervening medium

5.2 Terminology related to quantum random number generator

5.2.1 Terms defined by Standards Development Organizations elsewhere

5.2.1.1 bit error rate [b-Draft ETSI 007 V1.3.2]: number of bits with errors divided by the total number of bits that have been transmitted, received or processed over a given time period

NOTE – May be expressed as a rational number or a percentage.

5.2.1.2 clock rate [b-ETSI GR QKD 007]: number of repetition events per time unit, e.g., number of signals sent per time unit

5.2.1.3 dark count probability [b-ETSI GR QKD 007]: probability that a detector registers a detection event within a stated duration time, in the absence of optical illumination

5.2.1.4 dead time [b-Draft ETSI 007 V1.3.2]: time interval after a detection event when the detector is unable to provide an output

NOTE – The detection efficiency is exactly zero during the dead time.

5.2.1.5 detection efficiency [b-Draft ETSI 007 V1.3.2]: probability that a photon incident at the optical input of the photon detection system induces an output signal

NOTE 1 – In future documents ISG QKD intends to use this term exclusively to refer to the detection efficiency of detectors that are capable of giving a discernible output signal in response to a single photon.

NOTE 2 – Detection efficiency is likely to vary with parameters such as wavelength, polarization etc.

5.2.1.6 detector gate repetition rate [b-Draft ETSI 007 V1.3.2]: repetition rate of the time-intervals during which a detector has a non-zero single-photon detection efficiency

5.2.1.7 detector recovery time [b-ETSI GR QKD 007]: smallest time duration after which the detection efficiency is independent of previous photon detection history (i.e. its steady state value)

5.2.1.8 detector signal jitter [b-Draft ETSI 007 V1.3.2]: variation in the time delay, or latency, between when a photon arrives at the detector input port and when a signal is output from the detector

5.2.1.9 non-physical entropy sources [b-ITU-T X.1702]: an entropy source that does not use dedicated hardware but uses system resources (RAM content, thread number etc.) or the interaction of the user (time between keystrokes, etc.)

NOTE – This definition is identical to the definition of 'non-physical non-deterministic random bit generator' given in [b-NIST SP 800-90B].

5.2.1.10 physical entropy sources [b-ITU-T X.1702]: an entropy source that uses dedicated hardware or uses a physical experiment (noisy diode(s), oscillators, event sampling like radioactive decay, etc.)

NOTE – This definition is identical to the definition of 'physical non-deterministic random bit generator' given in [b-NIST SP 800-90B]

5.2.1.11 quantum entropy source [b-ITU-T X.1702]: an entropy source based on at least one quantum phenomenon

NOTE – Examples of quantum phenomena include quantum state superposition, quantum state entanglement, Heisenberg uncertainty, quantum tunnelling, spontaneous emission or radioactive decay.

5.2.1.12 random number generator [b-ETSI GR QKD 007]: physical device outputting unpredictable binary bit sequences

5.2.1.13 reset time [b-ETSI GR QKD 007]: time between the end of the dead time and the recovery time

5.2.1.14 single-photon detector [b-Draft ETSI 007 V1.3.2]: device that transforms a single-photon into a detectable signal with non-zero probability

5.2.1.15 source linewidth [b-Draft ETSI 007 V1.3.2]: **spectral** width of the distribution of emitted photons

NOTE 1 – One metric is the full-width at half-maximum (FWHM).

NOTE 2 – Another metric is to state the width corresponding to a specified number of standard deviations.

5.2.1.16 source spectral frequency [b-ETSI GR QKD 007]: spectral frequency of emitted photons

5.2.1.17 source timing jitter [b-ETSI GR QKD 007]: uncertainty in the emission time of an optical pulse at the optical output

5.2.1.18 source wavelength [b-ETSI GR QKD 007]: wavelength of emitted photons

5.2.1.19 stability of output power of emitted pulses [b-ETSI GR QKD 007]: variation in source power over the time period of a QKD session, or other stated time-interval

5.2.1.20 threshold detector [b-Draft ETSI 007 V1.3.2]: detector that can only distinguish between 'no detected photon' and 'one or more detected photons'

5.2.2 Relevant terms not currently included in standards

This Technical Report lists the following terms found in a survey of public literature:

5.2.2.1 backward security [b-Collantes]: knowledge of a part of the sequence shall not permit an attacker to compute the previous values of the generator with better accuracy than guessing

5.2.2.2 Bell inequality (or Bell-type inequality) [b-Bell]: a inequality to test if the system exists Bell nonlocality

5.2.2.3 Bell nonlocality [b-Bell]: a counter-intuitive property of quantum correlations discovered by John Bell in 1964

5.2.2.4 Bell test [b-Bell]: a test to test Bell inequality (or Bell-type inequality)

5.2.2.5 black box [b-Šupić]: it provides a minimalist level of abstraction that allows one to focus on what a device or system does without the need to model precisely how this is achieved

5.2.2.6 detection loophole [b-Pearle]: it states that the sample of detected events may not be an honest representative of what the entanglement source actually emits when the overall detection efficiency is lower than a certain threshold

5.2.2.7 device-independent [b-Colbeck]: a concept that does not rely on assumptions on the realization devices

5.2.2.8 device-independent quantum random number generator [b-Colbeck]: a quantum random number generator that can output certified quantum randomness even with uncharacterized and untrusted devices

5.2.2.9 entanglement distribution [b-Cirac]: a method for distributing quantum entanglement to different nodes

5.2.2.10 entanglement entropy source (EES) [b-Eisert]: a source that produces entropy based on at least one quantum entanglement phenomenon

5.2.2.11 entropy gathering [b-Collantes]: the process of collecting unpredictable data

5.2.2.12 entropy sources [b-Collantes]: the system with a physical system with some random physical quantity and the measurement equipment that reads these random variables

5.2.2.13 entropy source [b-NIST SP 800-90B]: the combination of a noise source, health tests, and an optional conditioning component that produces random bit strings to be used by a random bit generator

5.2.2.14 EPR steering [b-Cao-1]: two systems, one can affect the other's state through her choice of measurement basis

5.2.2.15 forward security [b-Collantes]: an attacker that knows the whole sequence cannot guess the next bit with a probability better than one half

5.2.2.16 locality loophole [b-Jarrett]: it states that the parties in the Bell test may be allowed to communicate about t heir measurement settings before outputting outcomes

5.2.2.17 measurement-device-independent [b-Cao-1]: a concept that does not rely on assumptions on the realization measurement devices

5.2.2.18 measurement-device-independent quantum random number generator [b-Cao-1]: a quantum random number generator that can output certified quantum randomness even with uncharacterized and untrusted measurement devices

5.2.2.19 physical random number generators [b-Collantes]: a process that produces a random output and seek to obtain random numbers from fundamentally random physical phenomena

5.2.2.20 polynomial-time unpredictability [b-Yao]: that no algorithm can take a subsequence from the generator and guess efficiently (in polynomial time) any previous or following subsequences with better results than total random guessing

5.2.2.21 pseudorandom number generator [b-Collantes]: produce random numbers from a deterministic algorithm

5.2.2.22 quantum random number [b-Collantes]: the random number based on inherent randomness at the core of quantum mechanics

5.2.2.23 quantum random number generator [b-Collantes]: devices that use quantum mechanical effects to produce random numbers

5.2.2.24 quantum randomness amplification [b-Collantes]: take a weak source, either classical or quantum, and use a quantum system to amplify the randomness in the weak source and give an arbitrarily close to uniform output

5.2.2.25 quantum randomness expansion [b-Collantes]: start from small random seed and, with the help of a quantum protocol, produce a longer bit sequence with strong guarantees of randomness

5.2.2.26 randomness beacon [b-Rabin]: a trusted third party offers public randomness service

5.2.2.27 random enough [b-Collantes]: the generated numbers simulating the statistics of the desired distribution, even if it produces a predictable sequence

5.2.2.28 randomness extractor [b-Collantes]: that transform the bits from the raw sequence into a uniform random sequence at the output with most or all of the randomness available in the input

5.2.2.29 secure lab [b-Colbeck]: it is an assumption that the information in the secure lab will not be leaked out

5.2.2.30 self-testing [b-Ma]: a method to infer the underlying physics of a quantum experiment in a black box scenario

5.2.2.31 self-testing quantum random number generator [b-Collantes]: a quantum random number generator that generate quantum randomness with self-testing of the realization devices or the system

5.2.2.32 semi-device-independent [b-Brask]: a concept that the output entropy can be lower bounded based on experimental data and a few general assumptions about the setup alone

5.2.2.33 semi-device-independent quantum random number generator [b-Brask]: a quantum random number generator in which output entropy can be lower bounded based on experimental data and a few general assumptions about the setup alone

5.2.2.34 semi-self-testing [b-Ma]: an intermediate category that provides a tradeoff between the trustworthiness on the device and the performance

5.2.2.35 semi-self-testing quantum random number generator [b-Ma]: a quantum random number generator that provides a tradeoff between practical QRNGs (high performance and low cost) and self-testing QRNGs (high security of certified randomness)

5.2.2.36 source independent [b-Cao-2]: a concept that does not rely on assumptions on the source

5.2.2.37 source independent quantum random number generator [b-Cao-2]: a quantum random number generator in which output randomness can be certified, even when the source is uncharacterized and untrusted

5.2.2.38 true random number generator [b-Collantes]: output random numbers that cannot be guessed

5.3 Terminology related to quantum computing for networks

5.3.1 Terms defined by Standards Development Organizations elsewhere

5.3.1.1 adiabatic quantum computer [b-ISO/IEC JTC1 AG4]: computation decomposed into a slow continuous transformation of an initial Hamiltonian into a final Hamiltonian, whose ground states contain the solution

5.3.1.2 one-way quantum computer [b-ISO/IEC JTC1 AG4]: computation decomposed into sequence of one-qubit measurements applied to a highly entangled initial state or cluster state

5.3.1.3 quantum [b-ISO/IEC JTC1 AG4]: the smallest unit that exhibits the properties of a substance or physical quantity

5.3.1.4 quantum chip [b-ISO/IEC JTC1 AG4]: quantum circuits integrated on substrates to carry the functions of quantum information processing

5.3.1.5 quantum coding [b-ISO/IEC JTC1 AG4]: the coding methods in quantum communication include quantum error correction code, quantum error averse code and quantum error correcting code

5.3.1.6 quantum communication [b-ISO/IEC JTC1 AG4]: a new communication method using quantum entanglement effect for information transmission

5.3.1.7 quantum computer [b-ISO/IEC JTC1 AG4]: physical devices for high-speed mathematical and logical operations, storage and processing of quantum information in accordance with the laws of quantum mechanics

5.3.1.8 quantum cryptography [b-ISO/IEC JTC1 AG4]: a cryptosystem based on the properties of quantum mechanics

5.3.1.9 quantum gate array [b-ISO/IEC JTC1 AG4]: computation decomposed into sequence of few-qubit quantum gates

5.3.1.10 quantum machine learning [b-ISO/IEC JTC1 AG4]: optimize traditional machine learning with the high parallelism of quantum computing

5.3.1.11 quantum superposition [b-ISO/IEC JTC1 AG4]: the smallest unit that exhibits the properties of a substance or physical quantity

5.3.1.12 topological quantum computer [b-ISO/IEC JTC1 AG4]: computation decomposed into the braiding of anyons in a 2D lattice

5.3.2 Relevant terms not currently included in standards

This Technical Report lists the following terms found in a survey of public literature:

5.3.2.1 blind quantum computing [b-Barz]: a secure cloud quantum computing protocol for delegating the quantum computing task to an untrusted quantum server without leaking any information

5.3.2.2 bold atomic quantum computer [b-Jaksch]: a quantum computing model based on the cold atoms, for example optical lattice, Rydberg atom

5.3.2.3 boson sampling [b-Aaronson]: a non-universal quantum computing model which sampling from the probability distribution of identical bosons scattered by a linear optical network

5.3.2.4 distributed quantum computing [b-Lim]: a research field focusing on quantum computing with distributed quantum systems

5.3.2.5 entangled photon source [b-Kwiat]: the light source of entangled photons

5.3.2.6 entanglement distribution [b-Yin]: a method for distributing quantum entanglement to different nodes

5.3.2.7 Grover's algorithm [b-Grover]: a quantum algorithm used for data searching, proposed by L. Grover in 1996

5.3.2.8 Hong-Ou-Mandel interference [b-He]: a two-photon quantum interference effect discovered by C. K. Hong, Z. Y. Ou and L. Mandel

5.3.2.9 hybrid quantum computing [b-Xiang]: a quantum computing architecture that composed of different physical components and different quantum computing models

5.3.2.10 indistinguishability [b-He]: the spectral overlap considering their all physical properties between two single photons

5.3.2.11 linear optical quantum computer [b-Kok]: a quantum computing model based on the linear optical elements, such as beam splitter, phase shifter, single-photon detector

5.3.2.12 modular quantum computing [b-Monroe]: a modular approach for constructing large quantum computer

5.3.2.13 quantum advantage [b-Bravyi]: a quantum computer can perform some particular computation significantly faster than a classical computer or that no classical computer can perform it at all

5.3.2.14 quantum algorithm [b-Harrow-1]: algorithm which runs on a realistic model of quantum computation. Several famous quantum algorithms are Shor's algorithm for large number factoring, Grover's algorithm for searching, HHL algorithm for solving linear equations

5.3.2.15 quantum annealer [b-Johnson]: find the solution of combinatorial optimization problems by an applying annealing method to quantum entangled system

5.3.2.16 quantum circuit [b-Nielsen]: a model for quantum computation, in which the computation is a sequence of quantum gates

5.3.2.17 quantum cloud computing platform [b-Devitt]: a cloud platform for all users reaching quantum computing

5.3.2.18 quantum computing [b-Nielsen]: a new computational model of quantum information unit is proposed, which follows the law of quantum mechanics based on quantum information unit

5.3.2.19 quantum connectivity [b-Kimble]: the connection between quantum nodes which has advantage comparing with classical connectivity

5.3.2.20 quantum electrodynamics [b-Tannoudji]: the relativistic quantum field theory of electrodynamics

5.3.2.21 quantum entanglement [b-Horodecki]: in quantum mechanics, because the properties of each particle have been integrated into a whole, it is impossible to describe the properties of each particle individually

5.3.2.22 quantum error correction [b-Nielsen]: the method used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise

5.3.2.23 quantum gate [b-Nielsen]: the basic quantum circuit operating on small number of qubits

5.3.2.24 quantum homomorphic encryption [b-Broadbent]: an encryption method that allows quantum computation to be performed over encrypted quantum data

5.3.2.25 quantum information [b-Nielsen]: the information identified by the state of micro particles or artificial particles is called quantum information

5.3.2.26 quantum network [b-Kimble]: the network linking multiple quantum processors by the transmission of information in the form of qubits

5.3.2.27 quantum node [b-Kimble]: the node can receive and emit quantum information

5.3.2.28 quantum processor [b-Arute]: a processor to handle quantum information, for example superconducting qubits chip for quantum computing, integrated photonic chip for multiphoton entanglement and boson sampling

5.3.2.29 quantum repeater [b-Yuan]: a quantum device that can extend the range of quantum communication between sender and receiver

5.3.2.30 quantum secret sharing [b-Hillery]: a protocol for sharing a secret among a number of participants such that only certain subsets of participants can collaboratively reconstruct it

5.3.2.31 quantum simulator [b-Barreiro]: a special quantum device to study quantum systems that are difficult or impossible to model even with a supercomputer

5.3.2.32 quantum software [b-Preskill]: the software with quantum programming languages and compilers for quantum information processing

5.3.2.33 quantum storage device [b-Bradley]: a device to store quantum information, for example atom ensembles

5.3.2.34 quantum supremacy [b-Harrow-2]: the goal of demonstrating that a quantum device can solve a problem that classical computers practically cannot (irrespective of the usefulness of the problem)

5.3.2.35 quantum tunneling [b-Grifoni]: the quantization behaviour of particles that can penetrate or cross a potential barrier

5.3.2.36 quantum Turing machine (or **universal quantum computer**) [b-Duan]: a quantum machine which captures all of the power of quantum computation

5.3.2.37 quantum verification [b-Gheorghiu]: a method to check whether quantum computers are indeed producing correct results

5.3.2.38 quantum wiring [b-Kimble]: an electrically conducting wire in which quantum effects influence the transport properties

5.3.2.29 random circuit sampling [b-Arute]: a non-universal quantum computing model which sampling from the probability distribution of random quantum circuit

5.3.2.40 semiconductor quantum computer [b-Ladd]: a quantum computing model based on the electric spin in semiconductors, including Silicon, InAs/GaAs quantum dots

5.3.2.41 Shor's algorithm [b-Shor]: a quantum algorithm used for large-number factoring, proposed by P. Shor in 1994

5.3.2.42 single-photon source [b-Wang]: the light source which emits one and only one photon at a specific time

5.3.2.43 spin-photon entanglement [b-De Greve]: the entanglement between an electric spin and a single photon

5.3.2.44 spin-spin interaction [b-Wilson]: the interaction between spins

5.3.2.45 superconducting quantum computer [b-Barends]: a quantum computer which based on the superconducting macroscopical quantum circuits

5.3.2.46 trapped-ion quantum computer [b-Kielpinski]: a quantum computing model based on the trapped-ion qubits

5.4 General terminology related to network aspect of quantum information technology

5.4.1 Terms defined by Standards Development Organizations elsewhere

5.4.1.1 entanglement [b-ETSI GR QKD 007]: property of quantum mechanical systems that shows correlations between two physical systems that cannot be explained by classical physics

5.4.1.2 entropy [b-ETSI GR QKD 007]: measure of uncertainty regarding information

5.4.1.3 mean photon number [b-ETSI GR QKD 007]: average number of photons per optical pulse

5.4.1.4 mean wavelength [b-Draft ETSI 007 V1.3.2]: average wavelength of spectral distribution of a physical quantity

5.4.1.5 multi-photon signal [b-ETSI GR QKD 007]: optical signal containing more than one photon

5.4.1.6 protocol [b-ETSI GR QKD 007]: list of steps to be performed by the participating entities to reach their goal

5.4.1.7 quantum [b-ISO/IEC JTC1 AG4]: the smallest unit that exhibits the properties of a substance or physical quantity

5.4.1.8 quantum bit (or qubit) [b-ISO/IEC JTC1 AG4]: quantum bits also called Qubit. In digital quantum computers, information units are called quantum bits, including "0" states, "1" states or superposition states

5.4.1.9 quantum channel [b-ETSI GR QKD 007]: communication channel for transmitting quantum signals

5.4.1.10 quantum entanglement [b-ISO/IEC JTC1 AG4]: in quantum mechanics, because the properties of each particle have been integrated into a whole, it is impossible to describe the properties of each particle individually, and the properties of the whole system

5.4.1.11 quantum mechanical state [b-ETSI GR QKD 007]: complete description of a physical system in quantum mechanics

5.4.1.12 quantum mechanics [b-ETSI GR QKD 007]: physical theory that describes natural phenomena

5.4.1.13 quantum mechanics [b-ISO/IEC JTC1 AG4]: the branch of physics that studies the motion of microscopic particles in the material world

5.4.1.14 quantum memories [b-ETSI GR QKD 007]: device that can store and retrieve quantum mechanical states

5.4.1.15 quantum photon source [b-ETSI GR QKD 007]: optical source for carrying quantum information

5.4.1.16 quantum signal [b-ETSI GR QKD 007]: signal described by a quantum mechanical state

5.4.1.17 quantum state [b-ISO/IEC JTC1 AG4]: a set of quantum representations is used to represent the motion state of a microscopic particle in quantum mechanics

5.4.1.18 quantum superposition [b-ISO/IEC JTC1 AG4]: the smallest unit that exhibits the properties of a substance or physical quantity

5.4.1.19 qubit [b-ETSI GR QKD 007]: unit of quantum information, described by a state vector in a two-level quantum mechanical system, which is formally equivalent to a two-dimensional vector space over the complex numbers

5.4.2 Relevant terms not currently included in standards

Four key terms related to quantum information technology for networks are proposed to be defined; the following are possible definitions which will require further research and discussion.

5.4.2.1 network aspects of QIT: the quantum information technologies which have impact on existing networks and the quantum information technologies which will forge the future quantum information network

5.4.2.2 quantum information network (QIN): refers to 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

5.4.2.3 quantum information technology (QIT): refers to the fusion of quantum physics and information technology

5.4.2.4 quantum internet [b-Kimble]: quantum information is locally generated, processed and stored in quantum nodes. These nodes are linked by quantum channels, which transmit quantum state from one site to another with high fidelity, and distribute entanglement throughout the network, forming a quantum internet

Bibliography

[b-ITU-T X.1702] Recommendation ITU-T X.1702 (2019), *Quantum noise random number generator architecture.*

[b-Aaronson] Aaronson, S. and Arkhipov, A. (2011), *The computational complexity of linear optics*. In Proceedings of the forty-third annual ACM symposium on Theory of computing, San Jose, California, USA.

[b-Arute] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett , B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., Fowler, A., Gidney, C., Giustina, M., Graff, R., Guerin, K., Habegger, S., Harrigan, M. P., Hartmann, M. J., Ho, A., Hoffmann, M., Huang, T., Humble, T. S., Isakov, S. V., Jeffrey, E., Jiang, Z., Kafri, D., Kechedzhi, K., Kelly, J., Klimov, P. V., Knysh, S., Korotkov, A., Kostritsa, F., Landhuis, D., Lindmark, M., Lucero, E., Lyakh, D., Mandrà, S., McClean, J. R., McEwen, M., Megrant, A., Mi, X., Michielsen, K., Mohseni, M., Mutus, J., Naaman, O., Neeley, M., Neill, C., Niu, M. Y., Ostby, E., Petukhov, A., Platt, J. C., Quintana, C., Rieffel, E. G., Roushan, P., Rubin, N. C., Sank, D., Satzinger, K. J., Smelyanskiy, V., Sung, K. J., Trevithick, M. D., Vainsencher, A., Villalonga, B., White, T., Yao, Z. J., Yeh, P., Zalcman, A., Neven, H. and Martinis, J. M. (2019). *Quantum supremacy using a programmable superconducting processor*. Nature Vol. 574, No. 7779, pp. 505-510.

[b-Barends] Barends, R., Kelly, J., Megrant, A., Veitia, A., Sank, D., Jeffrey, E., White, T. C., Mutus, J., Fowler, A. G., Campbell, B., Chen, Y., Chen, Z., Chiaro, B., Dunsworth, A., Neill, C., O'Malley, P., Roushan, P., Vainsencher, A., Wenner, J., Korotkov, A. N., Cleland, A. N. and Martinis, J. N. (2014). *Superconducting quantum circuits at the surface code threshold for fault tolerance*. Nature Vol. 508, No. 7497, pp. 500-503.

[b-Barreiro] Barreiro, J. T., Müller, M., Schindler, P., Nigg, D., Monz, T., Chwalla, Hennrich, M., Roos, C. F., Zoller, P. and Blatt, R. (2011), *An open-system quantum simulator with trapped ion*s. Nature Vol. 470, No. 7335, pp. 486-491.

[b-Barz] Barz, S., Kashefi, E., Broadbent, A., Fitzsimons, J. F., Zeilinger, A. and Walther, P. (2012), *Demonstration of blind quantum computing*. Science Vol. 335, No. 6066, pp. 303-308.

[b-Bell] Bell, J. S. (1964), *On the Einstein Podolsky Rosen paradox*. Physics Physique Fizika Vol. 1, No. 3, pp. 195–200

[b-Bradley] Bradley, C. E., Randall, J., Abobeih, M. H., Berrevoets, R. C., Degen, M. J., Bakker, M. A., Markham, M., Twitchen, D. J. and Taminiau, T. H. (2019), *A ten-qubit solid-state spin register with quantum memory up to one minute*. Physical Review X Vol. 9, No. 3, pp. 031045.

[b-Brask] Brask, J. B., Martin, A., Esposito, W., Houlmann, R., Bowles, J., Zbinden, H. and Brunner, N. (2017), M*egahertz-rate semi-device-independent quantum random number generators based on* *unambiguous state discrimination*. Physical Review Applied Vol. 7, No. 5.

[b-Bravyi] Bravyi, S., Gosset, D. and König, R. (2018), *Quantum advantage with shallow circuits*. Science Vol. 362, No. 6412, pp. 308-311.

[b-Broadbent] Broadbent, A. and Jeffery, S. (2015), *Quantum homomorphic encryption for circuits of low T-gate complexity*. In Gennaro R., Robshaw M. (eds) Advances in Cryptology -- CRYPTO 2015. CRYPTO 2015. Lecture Notes in Computer Science, vol 9216. Springer, Berlin, Heidelberg.

[b-Cao-1] Cao, Z., Zhou H. and Ma, X. (2015), *Loss-tolerant measurement-device-independent quantum random number generation*. New Journal of Physics Vol. 17, No. 125011.

[b-Cao-2] Cao, Z., Zhou, H., Yuan, X. and Ma, X. (2016), *Source-Independent Quantum Random Number Generation*. Physical Review X Vol. 6, No. 1.

[b-Capasso] Capasso, F. and Datta S. (1990), *Quantum electron devices*. Physics Today Vol. 43, No. 2, pp. 74.

[b-Cirac] Cirac, J. I., Zoller, P., Kimble, H. J. and Mabuchi, H. (1997), *Quantum State Transfer and Entanglement Distribution among Distant Nodes in a Quantum Network*. Physical Review Letters Vol. 78, No. 16, pp. 3221-3224.

[b-Colbeck] Colbeck, R. (2007), *Quantum and Relativistic Protocols For Secure Multi-Party Computation.* PhD Thesis, arXiv:0911.3814.

[b-Collantes] Herrero-Collantes, M. and Garcia-Escartin, J. C. (2017), *Quantum random number generators*. Reviews of Modern Physics Vol. 89, No. 1, pp. 015004.

[b-De Greve] De Greve, K., Yu, L., McMahon, P. L., Pelc, J. S., Natarajan, C. M., Kim, N. Y., Abe, E., Maier, S., Schneider, C., Kamp, M., Höfling, S., Hadfield, R. H., Forchel, A., Fejer, M. M. and Yamamoto, Y. (2012). *Quantum-dot spin–photon entanglement via frequency downconversion to telecom wavelength*. Nature Vol. 491, No. 7424, pp. 421-425.

[b-Devitt] Devitt, S. J. (2016). *Performing quantum computing experiments in the cloud*. Physical Review A Vol. 94, No. 3, pp. 032329.

[b-Draft ETSI 007 V1.3.2] Draft Group Report ETSI GR QKD 007 V1.3.2 (2021), *Quantum Key Distribution (QKD); Vocabulary.*

[b-Duan] Duan, L. M., Cirac, J. I. and Zoller, P. (2001), *Geometric manipulation of trapped ions for quantum computation*. Science Vol. 292, No. 5522, pp. 1695-1697.

[b-Eisert] Eisert, J., Cramer, M. and Plenio, M. B. (2010), *Colloquium: Area laws for the entanglement entropy*. Reviews of Modern Physics Vol. 82, No. 1, pp. 277-306.

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary* [b-Gheorghiu] Gheorghiu, A., Kapourniotis, T. and Kashefi, E. (2019). *Verification of quantum computation: An overview of existing approaches*. Theory of computing systems Vol. 63, No. 4, pp. 715-808.

[b-Grifoni] Grifoni, M. and Hänggi, P. (1998), *Driven quantum tunneling*. Physics Reports Vol. 304, No. 5-6, pp. 229-354.

[b-Grover] Grover, L. K. (1997), *Quantum mechanics helps in searching for a needle in a haystack*. Physical Review Letters, Vol. 79, No. 2, pp. 325-328.

[b-Harrow-1] Harrow, A. W. and Montanaro, A. (2017), *Quantum computational supremacy*. Nature Vol. 549, No. 7671, pp. 203-209.

[b-Harrow-2] Harrow, A. W., Hassidim, A., and Lloyd, S. (2009), *Quantum algorithm for linear systems of equations*. Physical Review Letters Vol. 103, No. 15, pp. 150502.

[b-He] He, Y. M., He, Y., Wei, Y. J., Wu, D., Atatüre, M., Schneider, C., Höfling, S., Kamp, M., Lu, C. Y. and Pan, J. W. (2013), *On-demand semiconductor single-photon source with near-unity indistinguishability*. Nature Nanotechnology Vol. 8, No. 3, pp. 213-217.

[b-Hillery] Hillery, M., Bužek, V. and Berthiaume, A. (1999). *Quantum secret sharing*. Physical Review A Vol. 59, No. 3, pp. 1829-1834.

[b-Horodecki] Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K. (2009), *Quantum entanglement*. Reviews of Modern Physics Vol. 81, No. 2, pp. 865-942.

[b-ISO/IEC JTC1 AG4] ISO/IEC JTC 1/AG 4 (2019), *Meeting report N50 – Quantum computing – Terminology and vocabulary.* https://isotc.iso.org/livelink/livelink?func=ll&objId=20626744&objAction=Open

[b-Jaksch] Jaksch, D., Bruder, C., Cirac, J. I., Gardiner, C. W. and Zoller, P. (1998). *Cold bosonic atoms in optical lattices*. Physical Review Letters Vol. 81, No. 15, pp. 3108-3111.

[b-Jarrett] Jarrett J. P. (1984), *On the physical significance of the locality conditions in the bell arguments*. Noûs Vol. 18, No.4, Special Issue on the Foundations of Quantum Mechanics, pp. 569-589.

[b-Johnson] Johnson, M. W., Amin, M. H. S., Gildert, S., Lanting, T., Hamze, F., Dickson, N., Harris, R., Berkley, A. J., Johansson, J., Bunyk, P., Chapple, E. M., Enderud, C., Hilton, J. P., Karimi, K., Ladizinsky, E., Ladizinsky, N., Oh, T., Perminov, I., Rich, C., Thom, M. C., Tolkacheva, E., Truncik, C. J. S., Uchaikin, S., Wang, J., Wilson, B. and Rose G. (2011), *Quantum annealing with manufactured spins*. Nature Vol. 473, No. 7346, pp. 194-198.

[b-Kielpinski] Kielpinski, D., Monroe, C. and Wineland, D. J. (2002), *Architecture for a large-scale ion-trap quantum computer*. Nature Vol. 417, No. 6890, pp. 709-711.

[b-Kimble] Kimble, H. J. (2008), *The quantum internet*. Nature Vol. 453, No. 7198, pp. 1023-1030.

[b-Kok]	Kok, P., Munro, W. J., Nemoto, K., Ralph, T. C., Dowling, J. P. and Milburn, G. J. (2007), *Linear optical quantum computing with photonic qubits*. Reviews of Modern Physics Vol. 79, No. 1, pp. 135-174.
[b-Kómár]	Kómár, P., Kessler, E. M., Bishof, M., Jiang, L., Sørensen, A. S., Ye, J. and Lukin M. D. (2014), *A quantum network of clocks*. Nature physics Vol. 10, pp. 582 – 587.
[b-Krčo]	Krčo, M. and Paul, P. (2008), *Quantum clock synchronization: a multi-party protocol*. Physical Review A Vol. 66, No. 2.
[b-Kumar]	Kumar, P. (1990), *Quantum frequency conversion*. Optics Letters Vol. 15, No. 24, pp. 1476-1478.
[b-Kwiat]	Kwiat, P. G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A. V. and Shih, Y. (1995), *New high-intensity source of polarization-entangled photon pairs*. Physical Review Letters Vol. 75, No. 24, pp. 4337-4341.
[b-Ladd]	Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C. and O'Brien, J. L. (2010). *Quantum computers*. Nature Vol. 464, No. 7285, pp. 45-53.
[b-Lim]	Lim, Y. L., Beige, A. and Kwek, L. C. (2005), *Repeat-until-success linear optics distributed quantum computing*. Physical Review Letters, Vol. 95, No. 3, pp. 030505.
[b-Lohe]	Lohe, M. A. (2010), *Quantum synchronization over quantum networks*. Journal of Physics A: Mathematical and Theoretical Vol. 43, No. 46, pp. 1-6.
[b-Ma]	Ma, X., Yuan, X., Cao, Z., Qi, B. and Zhang, Z. (2016), *Quantum random number generation*. npj Quantum Information Vol. 2, No. 16021.
[b-Mignemi]	Mignemi, S. and Uras, N. (2019), *Noncommutative geometry of the quantum clock*. Physics Letters A, Vol. 383, No. 7, pp. 585-588.
[b-Monroe]	Monroe, C., Raussendorf, R., Ruthven, A., Brown, K. R., Maunz, P., Duan, L. M. and Kim, J. (2014), *Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects*. Physical Review A Vol. 89, No. 2, pp. 022317.
[b-Nielsen]	Nielsen, M. A. and Chuang, I. (2002), *Quantum computation and quantum information*. American Journal of Physics Vol. 70, pp. 558-559.
[b-NIST]	National Institute of Standards and Technology (NIST) (2019), *Quantum logic clock returns to top performance*. ScienceDaily, 15 July. https://www.sciencedaily.com/releases/2019/07/190715114310.htm.
[b-NIST SP 800-90B]	National Institute of Standards and Technology (NIST) (2018), *Recommendation for the Entropy Sources Used for Random Bit Generation*. https://doi.org/10.6028/NIST.SP.800-90B
[b-Okeke]	Ilo-Okeke, E. O., Tessler, L., Dowling, J. P. and Byrnes T. (2018), *Remote quantum clock synchronization without synchronized clocks*. npj Quantum Information Vol. 4, No. 40, pp. 1-7.

[b-Pearle] Pearle P. M. (1970), *Hidden-variable example based upon data rejection*. Physical Review D Vol. 2, No. 8, pp. 1418-1425.

[b-Preskill] Preskill, J. (1999), *Plug-in quantum software*. Nature Vol. 402, No. 6760, pp. 357-358.

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

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

[b-Quan] Quan, R., Zhai, Y., Wang, M., Hou, F., Wang, S., Xiang, X., Liu, T., Zhang, S. and Dong, R. (2016), *Demonstration of quantum synchronization based on second-order quantum coherence of entangled photons*. Scientific Reports Vol. 6, No. 30453, pp.1-7.

[b-Rabin] Rabin, M. O. (1983), *Transaction protection by beacons*. Journal of Computer and System Sciences 27, No. 2, pp. 256-267.

[b-Ruiz] Ruiz, E. C., Giacomini, F. and Brukner, C. (2017), *Entanglement of quantum clocks through gravity*. In proceedings of the National Academy of Sciences of the United of America (PNAS), March 21. Vol. 114, No. 12, pp.2303-2309.

[b-Shor] Shor, P. W. (1994), *Algorithms for quantum computation: discrete logarithms and factoring*. In proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA (IEEE, 1994).

[b-Šupić] Šupić, I. and Bowles, J. (2020), *Self-testing of quantum systems: a review*. Quantum Vol. 4, pp. 337.

[b-Tannoudji] Cohen-Tannoudji, C., Dupont-Roc, J. and Grynberg, G. (1997), *Photons and Atoms: Introduction to Quantum Electrodynamics*. ISBN 0-471-18433-0. Wiley-VCH

[b-Time] Exactly What Is Time? *Quantum Time*. http://www.exactlywhatistime.com/physics-of-time/quantum-time/

[b-Wang] Wang, H., He, Y. M., Chung, T. H., Hu, H., Yu, Y., Chen, S., Ding, X., Chen, M. C., Qin, J., Yang, X., Liu, R. Z., Duan, Z. C., Li, J. P., Gerhardt, S., Winkler, K., Jurkat, J., Wang, L. J., Gregersen, N., Huo, Y. H., Dai, Q., Yu, S., Höfling, S., Lu, C. Y. and Pan, J. W. (2019). *Towards optimal single-photon sources from polarized microcavities*. Nature Photonics Vol. 13, No. 11, pp. 770-775.

[b-Wilson] Wilson, A. C., Colombe, Y., Brown, K. R., Knill, E., Leibfried, D. and Wineland, D. J. (2014). *Tunable spin–spin interactions and entanglement of ions in separate potential wells*. Nature, Vol. 512, No. 7512, pp. 57-60.

[b-Xiang] Xiang, Z. L., Ashhab, S., You, J. Q. and Nori, F. (2013), *Hybrid quantum circuits: Superconducting circuits interacting with other quantum systems*. Reviews of Modern Physics Vol. 85, No. 2, pp. 623-653.

[b-Yao] Yao, A.C. (1982), *Theory and application of trapdoor functions*. In 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982) (IEEE) pp. 80–91.

[b-Yin] Yin, J., Cao, Y., Li, Y. H., Liao, S. K., Zhang, L., Ren, J. G., Cai, W., Liu, W.-Y., Li, B., Dai, H., Li, G.-B., Lu, Q.-M., Gong, Y.-H., Xu, Y., Li, S.-L., Li, F.-Z., Yin, Y.-Y., Jiang, Z.-Q., Li, M., Jia, J.-J., Ren, G., He, D., Zhou, Y.-L., Zhang, X.-X., Wang, N., Chang, X., Zhu, Z.-C., Liu, N.-L., Chen, Y.-A., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y. and Pan, J.-W. (2017). *Satellite-based entanglement distribution over 1200 kilometers*. Science Vol. 356, No. 6343, pp. 1140-1144.

[b-Yuan] Yuan, Z. S., Chen, Y. A., Zhao, B., Chen, S., Schmiedmayer, J. and Pan, J. W. (2008). *Experimental demonstration of a BDCZ quantum repeater node*. Nature, Vol. 454, No. 7208, pp. 1098-1101.

[b-Zhirov] Zhirov, O. V. and Shepelyansky, D. L. (2006), *Quantum synchronization*. The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics Vol. 38, pp. 375-379.