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 D2.1

Quantum information technology for networks terminology: Quantum key distribution network

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 D2.1

Quantum information technology for networks terminology: Quantum key distribution network

Summary

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

This technical report provides a survey of terminology relevant to QKDN currently published or under development by SDOs including ETSI ISG QKD, ISO/IEC JTC1 SC27 WG3 and ITU-T SG13/17. Based on the survey, the terms are categorized according to the specific technical directions they fall under.

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

QKDN; quantum key distribution network; quantum information technology; terminology.

Chief Editor:	K. Karunaratne Qubitekk United States	Email: kkarunaratne@qubitekk.com
Co-editor:	Yan Jiang QuantumCTek Co. Ltd China	Email: yan.jiang@quantum-info.com

Acknowledgments

The editors express their appreciation to all the contributors of this report and all participants of Working Group 2 of the Focus Group on Quantum Information Technology for Networks (FG QIT4N) for their invaluable inputs, thorough review and all comments provided during the development of this report.

Table of Contents

Technical Report ITU-T FG QIT4N D2.1

Quantum information technology for networks terminology: Quantum key distribution network

1 Scope

This Technical Report contains a set of definitions of terms commonly used in quantum key distribution networks (QKDN). The terminologies have been obtained from work done by Standards Development Organizations (SDOs) and are categorized according to the specific technical directions they fall under.

2 References

None.

3 Definitions

This clause is intentionally left blank.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

API	Application Programming Interface
IT-secure	Information Theoretically secure
KM	Key Manager
KMA	Key Management Agent
KSA	Key Supply Agent
QKD	Quantum Key Distribution
QKDN	QKD Network
QRBG	Quantum Random Bit Generator

5 Introduction

In its simplest implementation, quantum key distribution (QKD) is a rapidly maturing technology whereby two parties actively share a secret cryptographic key whose fundamental security is bounded by the laws of quantum mechanics. As adoption of QKD becomes more prevalent throughout the current commercial marketplace, it is natural that this technology progresses in the direction of networking across a wide landscape of network topologies, ranging from private small-scale local area networks to the larger telecommunications infrastructure. Subsequently, standardization activities surrounding QKD networks (QKDN) are well underway around the globe. One important aspect of standardization is terminology, as terms and definitions provide the contextual basis upon which standards are both written and understood.

This report provides a non-normative survey of formal efforts related to the development of QKDN terminology by SDOs. As a survey of QKDN terminology, this report will emphasize terminology lists and associated definitions where relevant to QKDN that are either currently published or under development.

These lists come from ITU-T Study Groups on Next Generation Networks (SG13) and Security (SG17), respectively, as well as other groups in SDOs such as the ETSI ISG QKD and the ISO/IEC JTC1.

Based on the survey of QKDN terminology, the QKDN terms in this report are classified into eight terminology categories (TC) according to the respective technical directions they fall into. Figure 1 illustrates these technical directions and their relationship.

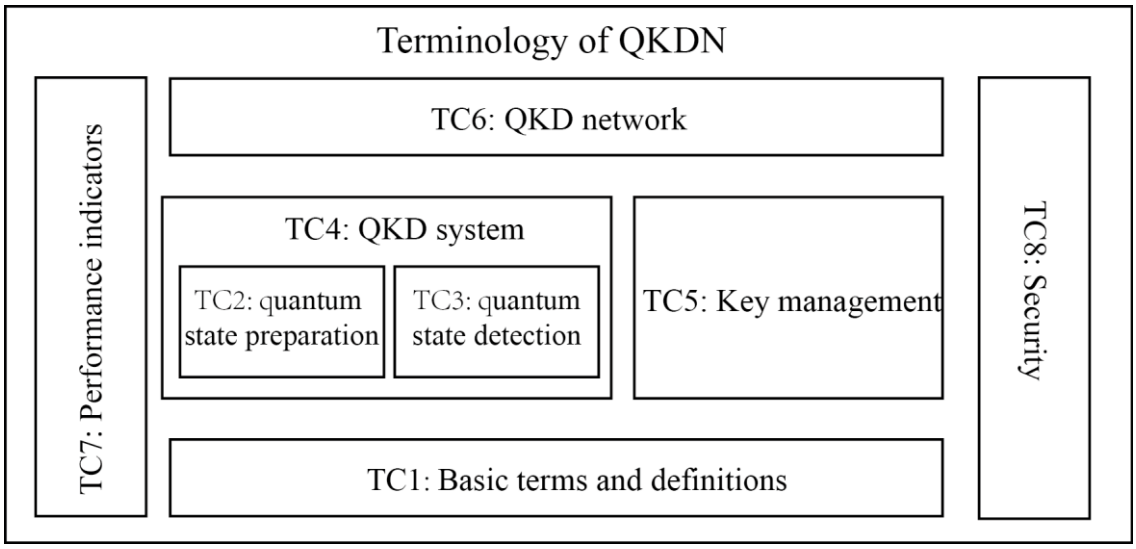

Figure 1 – Framework for QKDN terminology categorization

- **TC1: Basic terms and definitions** – general terminology on quantum technology used in QKDN
- **TC2: Quantum state preparation** – terminology related to the procedure of quantum state preparation at the transmitter of a QKD system
- **TC3: Quantum state measurement** – terminology related to the procedure of quantum state measurement at the receiver of a QKD system
- **TC4: QKD system** – terminology related to a QKD system (see clause 6.1.4.20) except for quantum state preparation (TC2) and quantum state measurement (TC3)
- **TC5: Key management** – terminology related to key management for QKDN
- **TC6: QKD network** – terminology related to QKD networking
- **TC7: Performance indicators** – terminology related to key performance parameters and indicators for QKD and QKDN
- **TC8: Security** – terminology related to the security of QKD and QKDN

6 Survey of QKDN relevant terms and definitions

6.1 TC1: Basic terms and definitions

6.1.1 classical channel [b-ETSI GR QKD 007]: communication channel that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced

6.1.2 classical channel [b-Draft ISO/IEC 23837 CD2]: communication channel that is used by two communicating parties for exchange of classical information

6.1.3 classical public channel [b-ETSI GR QKD 007]: insecure communication channel, for example broadcast radio or internet, where all messages sent over this channel become available to all parties, including adversaries

6.1.4 data path [b-ETSI GR QKD 007]: physical or logical route over which data passes (a physical data path may be shared by multiple logical data paths)

6.1.5 public announcement [b-ETSI GR QKD 007]: messages sent over the public channel during a protocol

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

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

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

6.1.9 quantum signal [b-Draft ISO/IEC 23837 CD2] and [b-ETSI GR QKD 007]: signal described by a quantum mechanical state

6.1.10 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

6.2 TC2: Quantum state preparation

6.2.1 attenuation [b-Draft ETSI 007 V1.3.2]: reduction in intensity of an optical signal

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

6.2.3 decoy state [b-ETSI GR QKD 007]: legitimate user intentionally and randomly replaces the usual protocol signals by different signals to test the channel action

6.2.4 encoding [b-Draft ISO/IEC 23837 CD2]: procedure of converting classical information into quantum signals

6.2.5 encoding [b-ETSI GR QKD 007]: process of mapping a secret message into a publicly accessible set of data from which the rightful user can decode the secret message again

6.2.6 intensity modulator [b-Draft ETSI 007 V1.3.2]: device that can actively modulate its transmittance

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

6.2.8 mean source power [b-Draft ETSI 007 V1.3.2]: average power emitted by the source (transmitter) over a stated time-interval

6.2.9 mean spectral frequency [b-ETSI GR QKD 007]: average frequency of spectral measurement

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

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

6.2.12 phase encoding [b-ETSI GR QKD 007]: method of encoding qubits using optical phase differences between optical pulses

6.2.13 phase modulator [b-ETSI GR QKD 007]: device that can actively modulate the phase of optical signals passing through it

6.2.14 photon number [b-ETSI GR QKD 007]: number of photons in a pulse

6.2.15 quantum error correction codes [b-ETSI GR QKD 007]: coding procedures for quantum states to protect them against errors during transmission or storage

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

6.2.17 single-photon source [b-ETSI GR QKD 007]: photon source that emits at most one photon at a time

6.2.18 source emission temporal profile [b-ETSI GR QKD 007]: temporal distribution of photons within a single emitted pulse

6.2.19 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.

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

6.2.21 source temporal profile [b-Draft ETSI 007 V1.3.2]: variation in the emission time of an optical pulse at the optical output with respect to a signal triggering the emission of the optical pulse

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

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

6.2.24 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

6.2.25 weak laser pulse [b-ETSI GR QKD 007]: optical pulse obtained through attenuating a laser emission

NOTE – A weak laser pulse typically contains less than one photon per pulse on average.

6.3 TC3: Quantum state detection

6.3.1 after-pulse [b-Draft ETSI 007 V1.3.2]: signal pulse in a single photon detector that is the result of a signal pulse in the same single photon detector at an earlier time

6.3.2 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

6.3.3 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.

6.3.4 decoding [b-Draft ISO/IEC 23837 CD2]: procedure of converting quantum signals into classical information

6.3.5 decoding [b-ETSI GR QKD 007]: process by which a receiver extracts the secret message from the publicly transmitted data

6.3.6 detection efficiency [b-Draft ETSI 007 V1.3.2]: probability that a photon incident at the optical input of the photon detection system includes 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.

6.3.7 detection efficiency linearity [b-ETSI GR QKD 007]: minimum detection efficiency divided by the maximum detection efficiency over the specified range of powers

6.3.8 detection efficiency range due to polarization of input pulses [b-ETSI GR QKD 007]: difference between the maximum DE for input polarized light, and the DE due to randomly polarized input light

6.3.9 detector gate efficiency profile [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

6.3.10 detector gate repetition rate [b-ETSI GR QKD 007]: repetition rate of the time-intervals during which a detector has single-photon sensitivity

6.3.11 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)

6.3.12 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

6.3.13 differential power analysis (**DPA**) [b-ETSI GR QKD 007]: analysis of the variations of the electrical power consumption of a QKD module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm or to any sensitive physical and logical internal state of the QKD module

6.3.14 homodyne detection [b-ETSI GR QKD 007]: method of detecting a weak frequency-modulated signal through mixing with a strong reference frequency-modulated signal (so-called local oscillator)

6.3.15 homodyne detection [b-Draft ISO/IEC 23837 CD2]: method to detect quadrature of a weak signal through interfering the weak signal and a strong phase reference

6.3.16 intrinsic 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, and excluding the probability of after-pulses generated from the intrinsic dark counts

6.3.17 partial detector recovery time (high) [b-ETSI GR QKD 007]: time duration after a photon detection event for the detection efficiency to return to 90% (or some other specified fraction) of its steady-state value

6.3.18 partial detector recovery time (low) [b-ETSI GR QKD 007]: time duration after a photon detection event for the detection efficiency to return to 10% (or some other specified fraction) of its steady-state value

6.3.19 photon number resolution [b-ETSI GR QKD 007]: ability of a photo-detection process to distinguish not only between 'no photon' and 'one or more photons', but being able to distinguish between 0, 1, 2, 3… photons

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

6.3.21 signature of a quantum process [b-ITU-T X.1702]: a set of measurable statistical properties that are characteristic of a given quantum process according to some assumptions provided in the description, and that permits quantification of this process' impact on the measurement outputs in a manner that enables a direct or indirect estimation of the minimum amount of entropy coming solely from the quantum process. For example, one signature of quantum entanglement is the violation of Bell inequalities

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

6.3.23 single-photon detector [b-Draft ISO/IEC 23837 CD2]: device that transforms a single-photon into a detectable signal with non-zero probability

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

6.4 TC4: QKD system

6.4.1 Alice [b-Draft ETSI 007 V1.3.2]: the first legitimate party operating a QKD module in a QKD system

6.4.2 Bob [b-Draft ETSI 007 V1.3.2]: the second legitimate party operating a QKD module in a QKD system

6.4.3 distillation [b-ETSI GR QKD 007]: distillation of a key which means the extraction of a secure key from some partially compromised data

6.4.4 encrypted key [b-ETSI GR QKD 007]: cryptographic key that has been encrypted using an approved security function with a key encrypting key

6.4.5 error corrected key [b-Draft ISO/IEC 23837 CD2]: keying material obtained after correcting the bit errors in the sifted key

6.4.6 error correction [b-ETSI GR QKD 007]: process of correcting errors in data that may have been corrupted due to errors during transmission or in storage

6.4.7 Eve or eavesdropper [b-ETSI GR QKD 007]: any adversary intending to intercept data in a quantum or classical channel

6.4.8 final key [b-Draft ISO/IEC 23837 CD2]: key generated by a complete run of a quantum key distribution procedure

6.4.9 link module [b-Draft ETSI 007 V1.3.2]: set of hardware, software, and/or firmware components with the capability to participate in QKD when located in a QKD link and where the security of symmetric keys established does not depend on the set of components under any of the QKD protocols in which it is capable of participating

NOTE – Examples of link modules include quantum repeater modules, entangled photon pair source modules in some entanglement-based QKD implementations and receiver modules in some MDI-QKD implementations, etc.

6.4.10 nonce [b-ITU-T X.1702]: a random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness, thus detecting and protecting against replay attacks

6.4.11 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.)

6.4.12 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.)

6.4.13 post-processing [b-Draft ISO/IEC 23837 CD2]: QKD protocol phase for converting a raw key into a final key

6.4.14 prepare-and-measure scheme [b-ETSI GR QKD 007]: scheme where the quantum optical signals used for QKD are prepared by Alice and sent to Bob for measurement

NOTE – Entanglement-based schemes where entangled states are prepared externally to Alice and Bob are not normally considered "prepare-and-measure". Schemes where entanglement is generated within Alice can still be considered "prepare-and-measure". Send-and-return schemes can still be "prepare-and-measure" if the information content from which keys will be derived is prepared within Alice before being sent to Bob for measurement.

6.4.15 pre-shared key [b-Draft ISO/IEC 23837 CD2]: key pre-established by some means between the legitimate parties before initiating a QKD session

NOTE – Pre-shared key is consumed to authenticate messages sent over the classical channel during the first QKD session.

6.4.16 privacy amplification [b-ETSI GR QKD 007]: process of distilling secret keys from partially compromised data

6.4.17 privacy amplification [b-Draft ISO/IEC 23837 CD2]: process of extracting keys from partially compromised data

6.4.18 QES1 [b-ITU-T X.1702]: a subclass of quantum entropy sources that will assess a given minimum entropy amount by measuring the implementation imperfections and verifying that they are within defined acceptable value ranges

6.4.19 QES2 [b-ITU-T X.1702]: a subclass of quantum entropy sources that will assess their generated entropy amount by measuring signatures of the quantum process

6.4.20 quantum entropy source (QES) [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.

6.4.21 QKD module [b-Draft ETSI 007 V1.3.2]: set of hardware, software and/or firmware components that implements part of one or more QKD protocol(s) to be capable of securely agreeing shared, confidential, random bit strings with at least one other QKD module

6.4.22 QKD module [b-Draft ISO/IEC 23837 CD2]: set of hardware and software components that implements the QKD transmitter party or receiver party

6.4.23 QKD protocol [b-Draft ISO/IEC 23837 CD2]: protocol that implements QKD

6.4.24 quantum key distribution protocol (QKD protocol) [b-ITU-T X.1710]: list of steps for establishing symmetric cryptographic keys with information-theoretical security based on quantum information theory

6.4.25 QKD receiver party [b-Draft ISO/IEC 23837 CD2]: quantum signal receiver in a QKD protocol

6.4.26 QKD session [b-Draft ETSI 007 V1.3.2]: set of actions and interactions performed by a pair of QKD modules to agree a shared, confidential, random bit string by QKD

NOTE 1 – Quantum state encoding, transmission and measurement as well as postprocessing and authentication, etc. can be part of a QKD session.

NOTE 2 – Actions in previous QKD sessions or those required to place a QKD module into a normal operating state (such as the provision of pre-shared key) are not part of the QKD session.

6.4.27 QKD session [b-ISO/IEC 23837 CD2]: session comprising a series of operations defined in a QKD protocol to generate a final key, which generally includes the phases of raw key exchange and post-processing

6.4.28 QKD system [b-Draft ISO/IEC 23837 CD2]: system that is composed of functional modules that implement QKD protocols, including at a minimum a QKD transmitter module, a QKD receiver module as well as the interconnecting quantum and classical channels

6.4.29 QKD transmitter party [b-Draft ISO/IEC 23837 CD2]: quantum signal sender in a QKD protocol

6.4.30 quantum key distribution (QKD) [b-ISO/IEC 23837 CD2]: procedure or method for two legitimate parties to agree on symmetric keys using a pre-shared key, whose security is based on quantum information theory

Note 1 to entry: in some QKD protocols establishment of keys occurs jointly involving both legitimate parties, while in others one party generates keys that are eventually transported to the other party.

6.4.31 quantum key distribution [b-Draft ETSI 007 V1.3.2]: procedure involving the transport of quantum states to agree shared secret bit strings between remote parties using a protocol with security

based on quantum entanglement or the impossibility of perfectly cloning or measuring the unknown transported quantum states

6.4.32 quantum key distribution link [b-ITU-T Y.3800]: a communication link between two quantum key distribution (QKD) modules to operate the QKD

NOTE – A QKD link consists of a quantum channel to transmit quantum signals and a classical channel to exchange information for synchronization and key distillation.

6.4.33 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

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, that is, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

6.4.34 quantum random bit generator (QRBG) [b-ISO/IEC 23837 CD2]: RBG that generates random bits based on principles of quantum mechanics

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

6.4.36 raw key [b-Draft ISO/IEC 23837 CD2]: keying material generated by measuring quantum states of the signal pulse

6.4.37 raw key exchange [b-ISO/IEC 23837 CD2]: QKD protocol phase of generating raw key by transmitting and detecting quantum signals

6.4.38 send-and-return protocol [b-Draft ETSI 007 V1.3.2]: protocol in which quantum optical signals are derived from optical signals previously sent in the reverse direction along the quantum channel

NOTE – Such schemes are also referred to elsewhere as "plug-and-play". Many systems running other protocols are auto-aligning and also able to deliver plug-and-play functionality so "send-and-return" will be used in ETSI ISG QKD documents.

6.4.39 X-type error [b-ETSI GR QKD 007]: bit-flip error

6.4.40 Y-type error [b-ETSI GR QKD 007]: phase error

6.4.41 Z-type error [b-ETSI GR QKD 007]: combination of bit-flip and phase error

6.5 TC5: Key management

6.5.1 key data [b-ITU-T Y.3803]: random bit strings that are used as a cryptographic key

6.5.2 key life cycle [b-ITU-T Y.3800]: a sequence of steps that a key undergoes from its reception by a key manager (KM) through its use in a cryptographic application and until deletion or preservation depending on the key management policy

6.5.3 key management [b-ITU-T Y.3800]: all activities performed on keys during their life cycle starting from their reception from the quantum layer, the storage, formatting, relay, synchronization, authentication, to supply to cryptographic application and delete or preserve depending on the key management policy

6.5.4 key management agent (KMA) [b-ITU-T Y.3802]: a functional element to manage keys generated by one or multiple quantum key distribution (QKD) modules in a QKD node (trusted node)

NOTE – KMA acquires keys from one or multiple QKD modules, synchronizes, resizes, formats, and stores them. It also relays keys through key management agent (KMA) links.

6.5.5 key management agent link [b-ITU-T Y.3802]: a communication link connecting key management agents (KMAs) to perform key relay and communications for key management

6.5.6 key management agent-key [b-ITU-T Y.3803]: key data stored and processed in a key management agent (KMA), and securely shared between a KMA and a matching KMA

6.5.7 key manager (KM) [b-ITU-T Y.3800]: a functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer

6.5.8 key manager link [b-ITU-T Y.3800]: a communication link connecting key managers (KMs) to perform key management

6.5.9 key supply [b-ITU-T Y.3800]: a function providing keys to cryptographic applications

6.5.10 key supply agent (KSA) [b-ITU-T Y.3802]: a functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application

NOTE – Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys and verifies their integrity via a KSA link before supplying them to the cryptographic application.

6.5.11 key supply agent-key [b-ITU-T Y.3803]: key data stored and processed in a key supply agent (KSA), and securely shared between a KSA and a matching KSA

6.5.12 quantum key distribution key [b-ITU-T Y.3802]: a pair of symmetric random bit strings generated by a pair of quantum key distribution (QKD) modules, particularly referring to random bit strings before being resized and formatted in a key manager

6.6 TC6: QKD network

6.6.1 application link [b-ITU-T Y.3800]: a communication link used to provide cryptographic applications in the user network

6.6.2 application programming interface (API) [b-ETSI GR QKD 007]: interface implemented by a software program to be able to interact with other software programs

6.6.3 key relay [b-ITU-T Y.3800]: a method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s)

6.6.4 pre-operational test [b-ETSI GR QKD 007]: test performed by a QKD module between the time a QKD module is powered on and the time that the QKD module uses a function or provides a service using the function being tested

6.6.5 QKD entity [b-ETSI GR QKD 007]: entity providing key distribution functionality including acting as an endpoint for the distribution of keys to at least one other QKD Entity using QKD protocols

6.6.6 QKD link [b-Draft ETSI 007 V1.3.2]: set of active and/or passive components that connect a pair of QKD modules to enable them to perform QKD

NOTE 1 – The security of symmetric keys established does not depend on the link components under any of the one or more QKD protocols executed.

NOTE 2 – QKD links may be persistent or dynamically created and destroyed.

NOTE 3 – A QKD link may be simple optical path, e.g., an optical fibre.

NOTE 4 – A QKD link may include one or more link module.

6.6.7 QKD network [b-ETSI GR QKD 007]: network comprised of two or more Trusted Nodes

6.6.8 quantum key distribution network (QKDN) [b-ITU-T Y.3800]: a network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

6.6.9 quantum key distribution network controller [b-ITU-T Y.3800]: a functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network

6.6.10 quantum key distribution network manager [b-ITU-T Y.3800]: a functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network

6.6.11 quantum key distribution node [b-ITU-T Y.3800]: node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties

NOTE – A QKD node can contain a key manager (KM).

6.6.12 security demarcation boundary [b-ITU-T Y.3800]: a boundary to one layer's responsibility on keys to be supplied from another layer's responsibility on the use of keys

6.6.13 software module [b-ETSI GR QKD 007]: module that is composed solely of software

6.6.14 user network [b-ITU-T Y.3800]: a network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network

NOTE – "Key" in [b-ITU-T Y.3800] means "symmetric random bit strings2 produced by QKDN.

6.6.15 web API [b-ETSI GR QKD 007]: application programming interface that can be accessed using HTTP or HTTPS protocols

6.7 TC7: Performance indicators

6.7.1 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.

6.7.2 key rate [b-ETSI GR QKD 007]: rate of shared secret key generation resulting from a quantum key distribution process

6.7.3 KSA-key delivery error ratio (KKDER) [b-ITU-T Y.3806]: the ratio of the number of KSA keys corrupted in transit between a KSA and a cryptographic application to the total number of KSA keys successfully transferred

6.7.4 KSA-key delivery loss ratio (KKDLR) [b-ITU-T Y.3806]: the ratio of the number of KSA keys not received by a cryptographic application to the total number of KSA keys sent to it by a KSA

6.7.5 KSA key response delay [b-ITU-T Y.3806]: the time measured at KSA, (t2 – t1) between the occurrence of two corresponding events, key request message at time1 and replied KSA key at time2 over a reference point between a cryptographic application and KML in QKDNs, where (t2 > t1)

6.7.6 key request session recovery ratio [b-ITU-T Y.3806]: the ratio of the numbers of recovered key request sessions to the total number of failed key request sessions

6.7.7 wavelength reservation ratio [b-ITU-T Y.3806]: the ratio of the reserved wavelength resources for recovery to the total of the allocated wavelength resources

6.8 TC8: Security

6.8.1 authentication [b-ETSI GR QKD 007]: act of establishing or confirming that some message indeed originated from the entity it is claimed to come from and was not modified during transmission

NOTE – Used as short term for message authentication.

6.8.2 collective attack [b-Draft ETSI 007 V1.3.2]: attack where an adversary optionally interacts independent ancilla(s), each with no more than one quantum state emitted under the QKD protocol,

and can then perform an unrestricted joint measurement on all the ancilla(s) and / or quantum state(s) emitted under the QKD protocol to extract information

NOTE 1 – Attacks involving the joint measurement of correlated quantum states emitted under the QKD protocol (e.g., attacks on entanglement protocols) without ancillas are considered collective attacks.

NOTE 2 – This definition places no other limits to the computing power or resources of the adversary beyond that of independent ancilla(s) described. However, in some cases it can be meaningful to consider collective attacks with further limitations on the capabilities of the adversary, e.g., the fidelity or storage time of available quantum memory, etc.

NOTE 3 – This definition does not prevent the adversary from using any information obtained about the system other than from quantum states transmitted under the QKD protocol.

6.8.3 cryptographic boundary [b-ETSI GR QKD 007]: explicitly defined continuous perimeter that establishes the physical bounds of a QKD module and contains all the hardware and software components of a QKD module

6.8.4 cryptographic hash function [b-ETSI GR QKD 007]: computationally efficient function that maps binary strings of arbitrary length to binary strings of fixed length, such that it is computationally infeasible to invert it, or to find two distinct values that hash into a common value

6.8.5 eavesdropping [b-ETSI GR QKD 007]: act of attempting to listen to the private conversation of others without their consent

6.8.6 individual attack [b-Draft ETSI 007 V1.3.2]: attack where an adversary optionally interacts independent ancilla(s), each with no more than one quantum state emitted under the QKD protocol, and performs measurements that are each limited to being performed on a set of states including one such quantum state and any ancilla(s) it interacted with

NOTE 1 – This definition places no other limits to the computing power or resources of the adversary beyond that of individual ancilla(s) / measurements described. However, in some cases it can be meaningful to consider individual attacks with further limitations on the capabilities of the adversary, e.g., the fidelity or storage time of available quantum memory, etc.

NOTE 2 – This definition does not prevent the adversary from using any information obtained about the system other than from quantum states transmitted under the QKD protocol.

6.8.7 information theoretically secure (IT-secure) [b-ITU-T Y.3800]: secure against any deciphering attack with unbounded computational resources

6.8.8 physical protection [b-ETSI GR QKD 007]: safeguarding of a QKD module, cryptographic keys, or critical security parameters using physical means

6.8.9 resilience [b-ITU-T X.1710]: ability to adapt to and recover from adverse conditions and attacks

6.8.10 security analysis [b-ETSI GR QKD 007]: analysis of a cryptographic protocol to relate the security parameters with the exact security claim of the protocol

6.8.11 security claim [b-ETSI GR QKD 007]: precise formulation in which sense a cryptographic protocol is secure

6.8.12 security infrastructure [b-ETSI GR QKD 007]: hierarchy of devices and protocols that manage key, user privileges and controls the cryptographic protocols

6.8.13 security model [b-Draft ETSI 007 V1.3.2]: model of devices, protocols, and channels that affect the security level of a cryptosystem under a given security proof in the presence of a given adversary

NOTE – A "channel" in this definition is any physical quantity related to the information protected by the cryptosystem.

6.8.14 security parameters [b-ETSI GR QKD 007]: parameters in a protocol that regulate the level of protection against adversaries

6.8.15 trojan horse attack [b-ETSI GR QKD 007]: attack on a QKD system where optical radiation is inserted by an adversary into apparatus under the control of a sender and / or receiver in order to measure information about the state of active optical components within quantum channel inside the apparatus

EXAMPLE: Optical pulses might be inserted into the quantum port of phase-modulated QKD transmitter module and photons introduced by the adversary that are reflected from an optical interface beyond the phase-modulator may be measured by the adversary to gain information about the basis used to encode bit values enabling the adversary to know how to measure the bit values from the signal photons or in some systems the phase of reflected photons might directly contain information about the bit values sent.

NOTE 1 – The optical radiation enters said apparatus via the normal quantum channel for the entry / exit of photons used for key exchange. Information is leaked back to the adversary via a portion of the previously inserted optical radiation exiting the apparatus via the normal quantum channel.

NOTE 2 – The adversary may combine the information leaked in this manner with information obtained from that intentionally encoded on either the quantum or classical channels by said apparatus. Any attempt by the adversary to combine information from Trojan horse attack with an attempt to exploit any other side-band or vulnerability or to attempt to interfere with the QKD module apparatus in any other manner would be considered a joint attack and not a pure Trojan horse attack.

7 Findings on QKDN terminology

In this clause, a simple comparison of similar terminology defined by different SDOs is made. Through this comparison, it has been found that since QKDN technologies have been in development for a long time, different SDOs have adopted either identical or similar definitions (with more details) for certain terminology.

7.1 Identical definitions

7.1.1 quantum signal [b-Draft ISO/IEC 23837 CD2] and [b-ETSI GR QKD 007]: signal described by a quantum mechanical state

7.2 Similar definitions

7.2.1 classical channel

- [b-Draft ISO/IEC 23837 CD2]: communication channel that is used by two communicating parties for exchange of classical information
- [b-ETSI GR QKD 007]: communication channel that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced

7.2.2 encoding

- [b-Draft ISO/IEC 23837 CD2]: procedure of converting classical information into quantum signals
- [b-ETSI GR QKD 007]: process of mapping a secret message into a publicly accessible set of data from which the rightful user can decode the secret message again

7.2.3 decoding

- [b-Draft ISO/IEC 23837 CD2]: procedure of converting quantum signals into classical information
- [b-ETSI GR QKD 007]: process by which a receiver extracts the secret message from the publicly transmitted data

7.2.4 homodyne detection

- [b-Draft ISO/IEC 23837 CD2]: method to detect quadrature of a weak signal through interfering the weak signal and a strong phase reference
- [b-ETSI GR QKD 007]: method of detecting a weak frequency-modulated signal through mixing with a strong reference frequency-modulated signal (so-called local oscillator)

7.2.5 quantum key distribution module

- [b-Draft ETSI 007 V1.3.2]: set of hardware, software and/or firmware components that implements part of one or more QKD protocol(s) to be capable of securely agreeing shared, confidential, random bit strings with at least one other QKD module
- [b-Draft ISO/IEC 23837 CD2]: set of hardware and software components that implements the QKD transmitter party or receiver party
- [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

  NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, that is, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

7.2.6 quantum key distribution protocol

- [b-Draft ISO/IEC 23837 CD2]: protocol that implements QKD
- [b-ITU-T X.1710]: list of steps for establishing symmetric cryptographic keys with information-theoretical security based on quantum information theory

7.2.7 quantum random bit generator

- [b-ETSI GR QKD 007]: physical device outputting unpredictable binary bit sequences
- [b-Draft ISO/IEC 23837 CD2]: RBG that generates random bits based on principles of quantum mechanics

7.2.8 QKD session

- [b-Draft ETSI 007 V1.3.2]: set of actions and interactions performed by a pair of QKD modules to agree a shared, confidential, random bit string by QKD

  NOTE 1 – Quantum state encoding, transmission and measurement as well as postprocessing and authentication, etc. can be part of a QKD session.

  NOTE 2 – Actions in previous QKD sessions or those required to place a QKD module into a normal operating state (such as the provision of pre-shared key) are not part of the QKD session.
- [b-Draft ISO/IEC 23837 CD2]: session comprising a series of operations defined in 185 a QKD protocol to generate a final key, which generally includes the phases of raw key exchange and post-processing

7.2.9 QKD network:

- [b-ETSI GR QKD 007]: network comprised of two or more Trusted Nodes
- [b-ITU-T Y.3800]: a network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links

  NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

Bibliography

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

[b-ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.

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

[b-ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture*.

[b-ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

[b-ITU-T Y.3806] Recommendation ITU-T Y.3806 (2021), *Quantum Key Distribution Network – Requirements for quality of service assurance*.

[b-Draft ETSI 007 V1.3.2] Draft Group Report ETSI GR QKD 007 V1.3.2 (2021-11), *Quantum Key Distribution (QKD); Vocabulary*.

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.

[b-Draft ISO/IEC 23837 CD2] Draft ISO/IEC 23837 CD2, *Security requirements, test and evaluation methods for quantum key distribution*.