ETSI GR QKD 007 V1.2.1 (2026-01)

GROUP REPORT

Quantum Key Distribution (QKD); Vocabulary

Disclaimer

The present document has been produced and approved by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGR/QKD-007ed2_Vocab

Keywords
quantum key distribution, vocabulary

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Quantum Key Distribution (QKD).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document collects together definitions and abbreviations used in relation to Quantum Key Distribution (QKD) and ETSI ISG QKD documents. QKD introduces new concepts and technologies to the field of telecommunications and considerable related vocabulary. Many terms derive from the wider fields of quantum physics and classical cryptography, and in some cases terms assume a modified or more specific meaning when applied to QKD.

The main objectives of the present document are:

- To improve the consistency with which terminology and abbreviations are used within ISG QKD documents.
- To provide a reference document to reduce confusion by readers who may not be familiar with QKD.

Most definitions and abbreviations come from ISG QKD Group Specifications and Group Reports or are expected to be used in published documents. The terms included have been selected to focus the present document on those that are expected to be of widespread use or where consistency is felt to be particularly important, e.g. due to a specific risk of confusion. Terms introduced in a single ISG QKD published document for a specific purpose that is local to that document are excluded unless of particular importance.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 101 909-11 (V1.2.1): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

[i.2] ISO/IEC 2382:2015: "Information technology — Vocabulary", (2015).

[i.3] R. Canetti: "Universally Composable Security: A New Paradigm for Cryptographic Protocols", FOCS'01: Proc. of the 42nd IEEE Symposium on Foundations of Computer Science (October 2001).

[i.4] J. Müller-Quade and R. Renner: "Composability in quantum cryptography", New J. Phys. 11, 085006 (2009).

[i.5] ISO 7498-2:1989: "Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture", (1989).

[i.6] ISO/IEC 19790:2025: "Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules".

[i.7] ISO/IEC 17825:2024: "Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules", (2024).

[i.8] ISO/IEC 18031:2025: "Information technology — Security techniques — Random bit generation", (2025).

[i.9] ISO/TR 22100-4:2018: "Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects", (2018).

[i.10] ISO/IEC 23837-1:2023: "Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements", (2023).

[i.11] M. Peter and W. Schindler: "A Proposal for Functionality Classes for Random Number Generators", Version 3.0, AIS 31, Bundesamt für Sicherheit in der Informationstechnik (BSI) (2014).

[i.12] ISO/IEC 27034-7:2018: "Information technology — Application security — Part 7: Assurance prediction framework", (2018).

[i.13] C. H. Bennett and G. Brassard: "Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing", Bangalore India, pp. 175–179 (1984).

[i.14] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt: "Proposed Experiment to Test Local Hidden-Variable Theories", Phys. Rev. Lett. 23, 880 (1969).

[i.15] A. Einstein, B. Podolsky and N. Rosen: "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" Phys. Rev. 47, 777 (1935).

[i.16] F. Grosshans and P. Grangier: "Continuous Variable Quantum Cryptography Using Coherent States", Phys. Rev. Lett., 88(5), 057902 (2002).

3 Definition of terms, symbols and abbreviations

3.1 Terms

A

adversary: party seeking to compromise the confidentiality or authenticity of symmetric keys agreed by QKD or to compromise the operation of a QKD system or associated infrastructure

after-pulse: 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

Alice: legitimate party operating a QKD module in a QKD system/protocol

NOTE 1: In a prepare-and-measure quantum key distribution system, Alice is the user preparing and sending the quantum information carriers.

NOTE 2: In an entanglement-based quantum key distribution system, Alice is one of the users measuring the quantum information carriers.

NOTE 3: In a measurement-device independent quantum key distribution system, Alice is one of the users preparing and sending the quantum information carriers.

ancilla: auxiliary (quantum mechanical) system

Application Programming Interface: interface implemented by a software program to be able to interact with other software programs

attack: any malicious action by an adversary

attenuation: reduction in intensity of an optical signal

authenticated classical channel: communication channel for the exchange of digital data where the data transferred possesses the security property of authenticity to enable the recipient to verify the identity of the transmitter and to ensure the data has not been modified in transit

NOTE: An authenticated channel does not necessarily employ encryption, but it can optionally encrypt data in transit.

authenticity: ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information

NOTE: See ETSI TS 101 909-11 [i.1].

B

bit error rate: number of erroneous bits divided by the total number of bits transmitted, received, or processed over some stipulated period of time

NOTE 1: Can be expressed as a rational number or a percentage.

NOTE 2: See clause 2124483 in ISO/IEC 2382 :2015 [i.2] in which the preferred term is "bit error ratio".

Bob: legitimate party operating a QKD module in a QKD system/protocol

NOTE 1: In a prepare-and-measure quantum key distribution system, Bob is the user receiving and measuring the quantum information carriers.

NOTE 2: In an entanglement-based quantum key distribution system, Bob is one of the users receiving and measuring the quantum information carriers.

NOTE 3: In a measurement-device independent quantum key distribution system, Bob is one of the users preparing and sending the quantum information carriers.

C

classical channel: 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

coherent attack: attack where an adversary interacts ancilla(s) coherently with quantum state(s) emitted under the QKD protocol and can then perform a joint measurement on the ancilla(s) and / or quantum state(s) emitted under the QKD protocol to extract information

NOTE 1: This definition places no limits to the computing power or resources of the adversary and can therefore include the most general and powerful types of attack. However, in some cases it can be meaningful to consider coherent attacks with limitations, e.g. on the fidelity or storage time of quantum memory available to the adversary, 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.

collective attack: 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.

composability: security statements that hold for individual protocols can be used to prove security statements for more complex cryptographic schemes built from combinations of those protocols

NOTE 1: This means that the security of a composite protocol can be automatically determined from the security of its sub-protocols as long as they are all satisfy this property.

NOTE 2: "composability" is shorthand for "Universal Composability" [i.3] and [i.4].

cryptography: discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

NOTE 1: Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

NOTE 2: See clause 3.3.20 in ISO 7498-2 :1989 [i.5].

cryptographic algorithm: well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output

cryptographic boundary: explicitly defined perimeter that establishes the boundary of all components (i.e. set of hardware, software or firmware components) of the cryptographic module

NOTE: See clause 3.32 in ISO/IEC 19790 :2025 [i.6].

cryptographic hash function: 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

cryptographic key: sequence of symbols that controls the operation of a cryptographic transformation

NOTE 1: A cryptographic transformation can include but is not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.

NOTE 2: Cryptographic keys can be produced from one or more QKD key.

NOTE 3: See clause 3.34 in ISO/IEC 19790:2025 [i.6].

cryptographic primitives: fundamental protocols from which cryptographic applications can be composed

D

dark count probability: probability that a detector registers a detector event within a stated time duration, in the absence of optical illumination

dead time: time duration after a detector event during which the detector will not output subsequent detector events

NOTE: The detection efficiency is exactly zero during the dead time. After the dead time there will a reset time during which the detection efficiency is transitioning from zero back to its steady-state value.

decoy state: state legitimately introduced to a channel to help monitor disturbance in the channel

NOTE: In QKD protocols decoy states are generally introduced randomly into the quantum channel.

detection efficiency: probability that a photon incident on the optical input surface of the photon detection system induces an output signal

NOTE 1: This definition is appropriate where it is clear from the context that it refers to a single-photon detector. Where this is not clear, use of more specific term "single-photon detection efficiency" can be more appropriate.

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

detector gate efficiency profile: detection efficiency as a function of incident pulse arrival time

detector signal jitter: variation in the delay between the time a photon arrives at the input port of a detector and when the detector outputs a signal

device model: mathematical model of a physical device that captures its essential characteristics and behaviour

differential power analysis: analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation

NOTE: See clause 3.5 in ISO/IEC 17825 :2024 [i.7].

E

eavesdropper: entity performing eavesdropping

eavesdropping: unauthorized interception of data in quantum and/or classical channel(s)

electrostatic discharge: sudden and momentary electric current that flows when an excess of electric charge, stored on an electrically insulated object, finds a path to an object at a different electrical potential (such as ground)

entanglement: property of quantum mechanical systems that shows correlations between two physical systems that cannot be explained by classical physics

entity: person, a group, a device, or a process

error correction: process of correcting errors in data that may have been corrupted due to errors during transmission or in storage

entropy: measure of the disorder, randomness or variability in a closed system

NOTE 1: The entropy of a random variable X is a mathematical measure of the amount of information provided by an observation of X.

NOTE 2: See clause 3.13 in ISO/IEC 18031 :2025 [i.8].

Eve: See eavesdropper.

F to G

Void.

H

homodyne detection: method of detecting a weak frequency-modulated signal through mixing with a strong reference frequency-modulated signal (so-called local oscillator)

I

independent ancilla: quantum state created by Eve and interacted with the signal(s) from a single QKD round that is uncorrelated with any ancilla(s) or other information relating to any other rounds

individual attack: 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.

intensity modulator: device that can actively modulate its transmittance

intrinsic dark count probability: probability that a detector registers a detector 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

IQ modulator: device that can actively modulate both the in-phase component (denoted by 'I') and the quadrature component (denoted by 'Q') of optical signals passing through it

J to K

Void.

L

link module: 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.

M

mean photon number: average number of photons per optical pulse or specified time period

mean source power: average power emitted by a source over a specified time interval

mean spectral frequency: average frequency of the spectral distribution of a physical quantity

mean wavelength: average wavelength of the spectral distribution of a physical quantity

minimum entropy: lower bound of entropy that is useful in determining a worst-case estimate of sample entropy

NOTE: See ISO/IEC 19790:2025 [i.6], clause 3.84.

multi-photon signal: optical signal containing more than one photon

N to O

Void.

P

partial recovery time: time duration after a detector event for the detection efficiency to return to a specified fraction of its steady-state value

NOTE: The partial recovery time is the sum of a detector's dead time and partial reset time.

partial reset time: time duration during which the detection efficiency is transitioning from zero back to a specified fraction of its steady-state value after the dead time following a detector event

NOTE: The detection efficiency can transition back to its steady-state value in a non-monotonic fashion.

password: string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization

NOTE: See clause 3.13 in ISO/TR 22100-4:2018 [i.9].

permutation: change in the order of elements of a sequence of data

Personal Identification Number: numeric code, used to authenticate an identity

phase encoding: method of encoding qubits using optical phase differences between optical pulses

phase modulator: device that can actively modulate the phase of optical signals passing through it

photon number resolution: 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

physical protection: safeguarding of a QKD module, cryptographic keys, or Critical Security Parameters using physical means

plaintext key: unencrypted cryptographic key

polarization: property of electromagnetic waves that describes the orientation of the oscillating electric field vector

post-processing: classical procedures in a QKD protocol for converting raw data into a QKD key

NOTE: Post-processing can include sifting, error correction and privacy amplification, etc. The resulting string is not necessarily the same as any string in the prior possession of any party.

power meter: device which measures incident optical power

pre-operational test: 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

prepare and measure QKD protocol: protocol for a QKD system to establish QKD keys in which one QKD module prepares quantum states and the other measures quantum states

prepare and measure scheme: 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.

privacy amplification: process of distilling secret keys from potentially compromised data

NOTE: QKD protocols use "privacy amplification" to distil ε-secure composable secret keys.

protocol: list of steps to be performed by the participating entities to reach their goal

public announcement: messages sent over the public channel during a protocol

Q

QKD Authentication Key: shared secret used for authentication mechanisms between two QKD modules

NOTE: The authentication is required to ensure the proper functionality of the prepare and measure QKD protocol. The QKD authentication keys have to be available to the QKD modules before any communication using the QKD link can be established.

QKD key: pair of secret random bit strings established by a QKD system jointly in both QKD modules after successfully running a QKD protocol and considered to be identical

QKD key agreement rate: average rate at which keys are generated from a quantum key distribution process

QKD link: set of active and/or passive components that connect QKD modules to enable them to perform QKD

NOTE 1: The security of symmetric keys agreed across a QKD link using a QKD protocol does not depend on the components of the QKD link under the QKD protocol executed.

NOTE 2: QKD links can be persistent or dynamically created and destroyed.

NOTE 3: A QKD link can be simple optical path, e.g. an optical fibre.

NOTE 4: A QKD link can include one or more link module, e.g. for entanglement-based or measurement-device independent QKD protocols.

NOTE 5: A QKD link can include all channels used in a QKD protocol, such as the authenticated classical channel, quantum channel and synchronization channel.

QKD module: set of hardware, software, and/or firmware components that implements part of a QKD protocol as well as cryptographic functions to be capable of securely agreeing shared, confidential, random bit strings with at least one other QKD module

QKD receiver: QKD module that is capable of receiving quantum states in the quantum channel

QKD round: an attempted transmission of a quantum state as part of a quantum key distribution protocol

QKD session: set of operations performed according to a QKD protocol that either aborts or agrees a shared, random, confidential bit string in the QKD modules

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.

QKD transceiver: QKD module that is capable of transmitting and receiving quantum states in the quantum channel

NOTE: A QKD transceiver is also a QKD transmitter and a QKD receiver.

QKD transmitter: QKD module that is capable of transmitting quantum states in the quantum channel

QKD system: system that implements QKD protocols, including at least two QKD modules as well as the interconnecting QKD link(s)

NOTE: See clause 3.28 in ISO/IEC 23837-1 [i.10] (with adaptations).

quantum bit error rate: number of erroneous raw bits divided by the total number of bits transmitted, received, or processed using/from quantum states over some stipulated period of time

NOTE 1: This does not represent errors in QKD keys but errors in raw data before error correction, privacy amplification, etc.

NOTE 2: In QKD the denominator will typically be the number of relevant measured bit values retained in the raw data after sifting.

NOTE 3: Common units can be erroneous raw bits per second or erroneous raw bits per bit received. In both cases a mean is typically used. The latter case can be expressed as a rational number or a percentage.

NOTE 4: See clause 2124483 in ISO/IEC 2382:2015 [i.2], in which the preferred more general term is "bit error ratio" (with adaptations).

quantum channel: communication channel for transmitting quantum signals

quantum error correction codes: coding procedures for quantum states to protect them against errors during transmission or storage

quantum key distribution: 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

quantum key distribution protocol: list of steps that implements QKD and is supported by a security proof

qubit: 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

R

radiation hardening: improving the ability of a device or piece of equipment to withstand nuclear or other radiation; applies mainly to dielectric and semiconductor materials

random number generator: group of components or an algorithm that outputs sequences of discrete values (usually represented as bit strings) that appears to be statistically independent and unbiased

NOTE: See glossary in AIS 31 [i.11] and clause 3.40 in ISO/IEC 18031:2025 [i.8] (combined with adaptations).

raw data: digital data (including but not limited to partially correlated data in more than one QKD module relating to the generation, encoding or measurement of quantum states) from which QKD modules can attempt to agree a QKD key via post-processing

NOTE 1: Data generated by implementations of a QKD protocol are not considered "keys" unless and until a QKD protocol completes successfully without aborting, to agree a QKD key. The term "raw key" is widely used in academic literature on QKD but risks mis-interpretation in wider cryptographic contexts.

NOTE 2: In many QKD protocols a subset of raw data is retained as "sifted data".

recovery time: time duration after a detector event for the detection efficiency to return to its steady-state value

NOTE: The recovery time is the sum of the dead time and reset time.

reset time: time duration during which the detection efficiency is transitioning from zero back to its steady-state value after the dead time following a detector event

NOTE: The detection efficiency can transition back to its steady-state value in a non-monotonic fashion.

S

security analysis: analysis of a cryptographic protocol to relate the security parameters with the exact security claim of the protocol

security claim: specific claim that security properties are present in an application

NOTE: See clause 3.6 in ISO/IEC 27034-7:2018 [i.12].

security model: model including devices, protocols and physical systems used to establish the security of a cryptosystem against adversaries under a given security proof

send-and-return protocol: 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 "plug-and-play" is not a favoured term.

sifted data: digital data obtained by the legitimate users from sifting the raw data according to an agreed strategy

single-photon detection efficiency: probability that a photon incident on the optical input surface of the photon detection system induces an output signal

NOTE 1: Where it is clear from the context that it refers to a single-photon detector the shorter term "detection efficiency" can be used.

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

single-photon detector: device that is able to produce a discernible output signal with non-zero probability due to a single photon incident on the detector's optical input surface

NOTE: Other discernible output signals can be due to dark counts, after-pulses, or electronic noise, etc.

software module: module that is composed solely of software

source linewidth: width of the spectral distribution of photons emitted by a source

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.

source wavelength: wavelength of emitted photons

spectral responsivity: detection efficiency as a function of the wavelength of the incident photons

spectrometer: device for measuring the spectrum of optical radiation

T

threshold detector: detector that can only distinguish between 'no detected photon' and 'one or more detected photons'

Trojan horse attack: attack on a QKD module in which optical radiation is inserted by an adversary to attempt to measure information about the state of active optical components inside the security boundary of the QKD module by measuring reflections of the light inserted

EXAMPLE: An adversary injects bright optical pulses into the quantum port of a QKD transmitter module that is encoding bit values on the phase of quantum states. The adversary attempts to measure the phases of reflections of the inserted pulses from an interface behind the encoding phase modulator to determine the bit values encoded without altering the quantum states transmitted.

NOTE 1: The optical radiation measured in a Trojan horse attack was previously inserted by the adversary through the quantum port. Information is leaked to the adversary by reflections of the previously inserted optical radiation.

NOTE 2: An adversary can combine the reflected signals with information intentionally encoded on either the quantum or classical channels by the QKD module. Attempts by the adversary to control the operation of the QKD module by inserting bright optical signals, or to combine information from a Trojan horse attack with information from an independent passive side-channel are beyond the scope of an isolated Trojan horse attack.

U to V

Void.

W

weak laser pulse: optical pulse obtained through attenuating a laser pulse

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

Web API: Application Programming Interface that can be accessed using HTTP protocols

X

X-type error: bit-flip error

Y

Y-type error: phase error

Z

zeroization: method of erasing electronically stored data to prevent the recovery of the data

Z-type error: combination of bit-flip and phase error

3.2 Symbols

Void.

3.3 Abbreviations

A

AC	Alternating Current
AMZI	Asymmetric Mach-Zehnder Interferometer
APC	Angled Physical Contact
APD	Avalanche PhotoDiode
API	Application Programming Interface
APPA	Application A
APPB	Application B

B

BB84	Bennett and Brassard 1984

NOTE: See [i.13].

BNC	Bayonet Neill-Concelman connector
BS	British Standard
BW	BandWidth

C

CHSH	Clauser-Horne-Shimony-Holt

NOTE: See [i.14].

CIE	International Commission on Illumination (Commission Internationale de l'Eclairage)
CML	Current Mode Logic
CMS	Configuration Management System
COW	Coherent One-Way
CSP	Critical Security Parameter
CV	Continuous Variable
CV-QKD	Continuous Variable QKD
CW	Continuous Wave

D

DAC	Digital-to-Analogue Converter
DC	Direct Current
DE	Detection Efficiency
DPA	Differential Power Analysis
DPS	Differential Phase Shift
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
DUT	Device Under Test
DV	Discrete Variable
DVM	Digital VoltMeter

E

ECDSA	Elliptic Curve Digital Signature Algorithm
ECL	Emitter Coupled Logic
EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EME	ElectroMagnetic Emanation

EPR Einstein-Podolsky-Rosen

NOTE: See [i.15].

ESD Electrostatic Discharge

F

FC Ferrule Connector or Fibre Channel
FC/PC Ferrule Connector/Physical Contact
FIPS Federal Information Processing Standard
FPGA Field Programmable Gate Array
FSM Finite State Model
FSR Free Spectral Range
FW Full-Width
FWHM Full-Width at Half Maximum

G

GG02 Grosshans and Grangier 2002

NOTE: See [i.16].

GM Gaussian Modulation
GMCS Gaussian Modulated Coherent State
GSPD Gated Single Photon Detector

H

HBT Hanbury Brown and Twiss
HDL Hardware Description Language
HMAC keyed-Hash Message Authentication Code
HTTP Hypertext Transfer Protocol

I

I/O Inputs and Outputs
IR Infrared

J

JSON JavaScript Object Notation

K

KAT Known Answer Test
KME Key Management Entity
KMIP Key Management Interoperability Protocol

L

LDPC Low-Density Parity-Check
LED Light-Emitting Diode
LLO Local Local Oscillator
LO Local Oscillator

M

MAC Message Authentication Code

MCA	Multi-Channel Analyser
MDI	Measurement-Device Independent
MM	Multi-Mode
MRI	Magnetic Resonance Imaging
MSI	Module Software Interface

N

NA	Numerical Aperture
NFAD	Negative Feedback Avalanche Photodiode
NIM	Nuclear Instrumentation Module
NIST	National Institute of Standards and Technology

O

OASIS	Organization for the Advancement of Structured Information Standards
OTDR	Optical Time Domain Reflectometry
OS	Operative System

P

PBS	Polarizing Beamsplitter
PC	Physical Contact
PDE	Photon Detection Efficiency
PIN	Personal Identification Number
PM	Polarization-Maintaining
PNS	Photon Number Splitting
PSP	Public Security Parameter
PSK	Phase Shift Keying

Q

QAK	QKD Authentication Key
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDE	QKD Entity
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying

R

REST	REpresentational State Transfer
RBG	Random Bit Generator
RP-SMA	Reverse Polarity Sub-Miniature version A connector
RRDPS	Round Robin DPS
RX	Receiver

S

SAE	Secure Application Entity
SDE	System Detection Efficiency
SI	International System of Units (Système International d'Unités)
SM	Single-Mode
SMA	Sub-Miniature version A connector
SMB	Sub-Miniature version B connector
SMK	Sub-Miniature version K connector
SNR	Signal-to-Noise Ratio
SNSPD	Superconducting Nanowire Single-Photon Detector
SPA	Simple Power Analysis

SPAD	Single-Photon Avalanche Photodiode
SPDC	Spontaneous Parametric Down-Conversion
SSP	Sensitive Security Parameter

T

TA	Timing Analysis
TAC	Time-to-Amplitude Converter
TAT	Trap-Assisted Tunnelling
TCSPC	Time-Correlated Single-Photon Counting
TLO	Transmitted Local Oscillator
TLS	Transport Layer Security
TN	Trusted Node
TTL	Transistor-Transistor Logic
TX	Transmitter

U

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

V

VHDL	VHSIC Hardware Description Language
VHSIC	Very-High-Speed Integrated Circuits
VOA	Variable Optical Attenuator

W

WDM	Wavelength Division Multiplexing

X to Z

Void.

Annex A:
Usage of terms

A.1 General comments

A1.1 Key agreement / establishment / distribution

QKD protocols do not distribute keys that are known in advance by either of the parties involved. For this reason the term "key agreement" is generally favoured over "key establishment" to describe QKD. In some contexts, such as documents relating to security evaluation under the Common Criteria, "key establishment" is used to match existing security functional requirements, etc.

The term "quantum key distribution" is widely used and "distribution" is used in this one term without any implication that keys are transported unmodified in QKD.

A1.2 Unconditional security

The term "unconditional security" predates quantum cryptography and means there are no computational assumptions. Technical usage within cryptography does not imply the absence of side-channels, implementation weaknesses, etc. However, due to the potential for confusion between technical usage and interpretation in non-technical contexts its use is to be avoided, except where existing usage is being explained.

A1.3 Information theoretically secure

The term "information theoretically secure" is a property of a cryptographic protocol in which the security of the protocol does not depend on assumptions about limitations on the computing power of any adversary. However, there is no universally accepted definition of this term so its use can give rise to confusion is to be avoided, except where existing usage is being explained.

The term "ε-secure composable security" is preferred.

A1.4 "plug-and-play" protocols

Many QKD systems are able to function automatically after connection. A particular type of protocol in which quantum optical signals are derived from optical signals previously sent in the reverse direction along the quantum channel became known as "plug-and-play" protocols. The use of the term "send-and-return" avoids potential confusion.

A.2 Entities within a QKD system

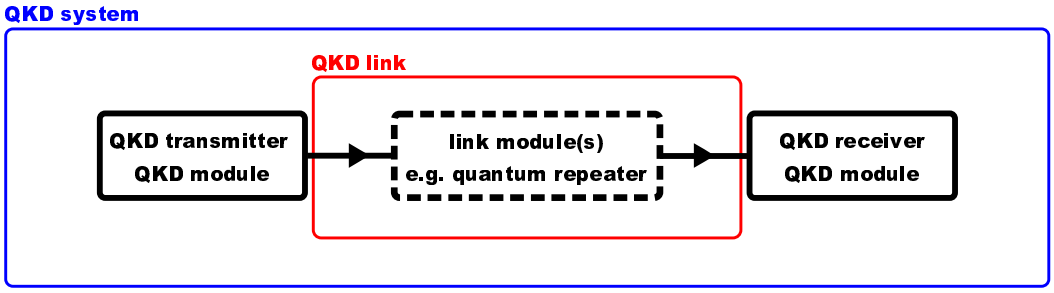

Figure A.2-1: Entities in an example QKD system that could represent many QKD systems operating prepare and measure QKD protocols

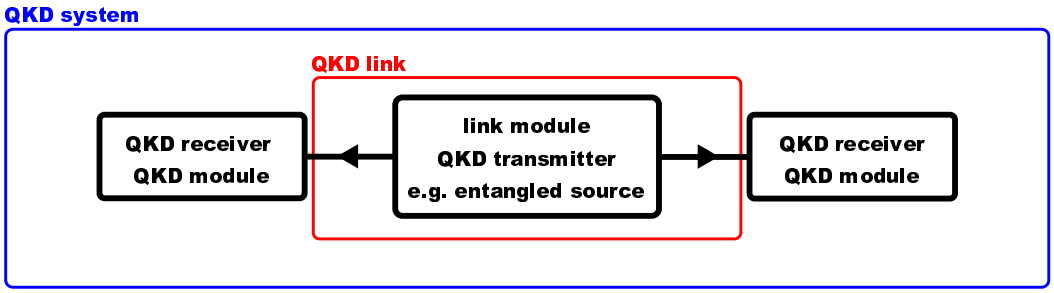

Figure A.2-2: Entities in an example QKD system that could represent many QKD systems operating QKD protocols involving the distribution of entangled photon pairs from a link module

Figures A.2-1 and A.2-2 show examples of QKD systems, and the entities they are comprised of. For clarity the classical and optional synchronization channels are omitted from the QKD link and only the quantum channel is indicated.

Figure A.2-1 could represent many QKD systems that operate prepare and measure protocols. Link modules(s) within the QKD link are optional but could include, for example, modules implementing quantum repeater functionality. QKD transmitters and QKD receivers are examples of QKD modules, depending on whether they transmit or receive the quantum states referred to in the definition of QKD. QKD modules can also be QKD transceivers where they are capable of both sending and receiving the quantum states referred to in the definition of QKD.

Figure A.2-2 could represent many QKD systems that operate QKD protocols involving the distribution of entangled photon pairs from a link module.

Where the security of QKD keys agreed using a particular QKD protocol does not depend on the set of components that comprise a module in a QKD link, such a module is not regarded a QKD module and can be called a link module. In dynamic networks, a module can at times be in a QKD link and considered a link module and at other times it can be acting as a QKD module delivering keys to local applications.

A.3 Communication channels in a QKD link

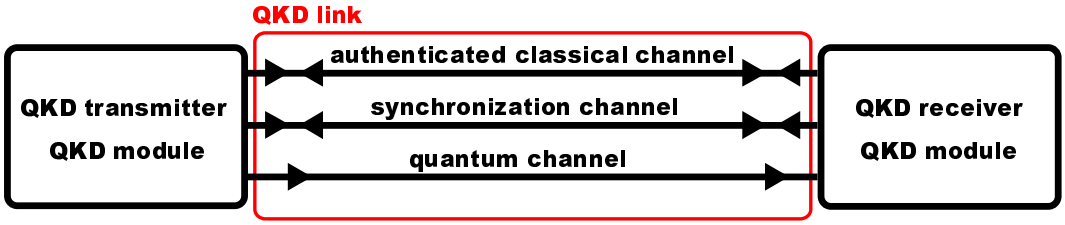

Figure A.3-1: Communication channels in a QKD link

Figure A.3-1 shows an example of communication channels that may be present within a QKD link. The quantum channel is used to pass the quantum states upon which the security of the QKD protocol is based. The classical channel is used to communicate digital data between the QKD modules to perform the post-processing required to agree a QKD key. Many QKD protocols assume that the classical channel is an authenticated channel, or more specifically that the QKD modules ensure that messages received on the classical channel are authentic and that the origin of the message is confirmed to be the other QKD module. The synchronization channel is an optional channel that may be used to synchronize events in time between the two QKD modules, or to share a phase reference, other analogue information, or quantum states other than those upon which the security of the QKD protocol is based.

The communications channels may be implemented over a common optical path between the QKD modules. For example, as wavelength multiplexed channels on an optical fibre or free space optical link. The classical channel may take a separate path from the quantum channel. Some implementations require the synchronization channel to follow the same optical path as the quantum channel but in other implementations they can be separated to different optical paths, e.g. different optical fibres.

History

Version	Date	Status
V1.1.1	December 2018	Publication
V1.2.1	January 2026	Publication