ETSI GR QKD 007 V1.1.1 (2018-12)

Quantum Key Distribution (QKD); Vocabulary

Disclaimer

The present document has been produced and approved by the Group 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
DGR/QKD-0007_Ontology

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Group 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 but 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 future 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 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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] 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, December (1984).

[i.2] F. Grosshans and P. Grangier: "Continuous Variable Quantum Cryptography Using Coherent States", Phys. Rev. Lett., 88(5), 057902 (2002).

[i.3] 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.4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev: "The security of practical quantum key distribution", Reviews of Modern Physics, Vol. 81, July-September 2009, pp. 1301-1350 and references therein.

[i.5] Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? A. Einstein, B. Podolsky, and N. Rosen Phys. Rev. 47, 777 – Published 15 May 1935 by American Physical Society.

NOTE: Available at https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777.

3 Definition of terms and abbreviations

3.1 Terms

A

adversary: malicious entity in cryptography whose aim is to prevent the users of the cryptosystem from achieving their goals

after-pulse probability: probability that a detector registers a false detection event in the absence of illumination, conditional on a detection event, due to incident photons of stated mean photon number, in a preceding detection gate

Alice: quantum information sender/transmitter in a QKD system

ancilla: auxiliary (quantum mechanical) system

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

attenuation: reduction in intensity of the light beam (or signal)

authentication: 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.

B

bit error rate: percentage of bits with errors divided by the total number of bits that have been transmitted, received or processed over a given time period

Bob: quantum information receiver in a QKD system

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

classical public channel: insecure communication channel, for example broadcast radio or internet, where all messages sent over this channel become available to all parties, including adversaries

clock rate: number of repetition events per time unit, e.g. number of signals sent per time unit

collective attack: attack where an adversary lets each individual signal interact with an ancilla each, but can perform joint operation on all the ancillas to extract information

composability: property that the output of one cryptographic protocol can be used by another cryptographic protocol in such a way that the security proof can be done for each protocol independently

compromise: unauthorized disclosure, modification, substitution, or use of sensitive data or an unauthorized breach of physical security

cryptography: art and science of keeping data or messages secure

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

cryptographic boundary: 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

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 (**key**)**:** parameter used in conjunction with a cryptographic algorithm that determines such operations as:

- the transformation of plaintext data into ciphertext data;
- the transformation of ciphertext data into plaintext data;
- a digital signature computed from data;
- the verification of a digital signature computed from data;
- an authentication code computed from data; or
- an exchange agreement of a shared secret.

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

D

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

data path: physical or logical route over which data passes (a physical data path may be shared by multiple logical data paths)

dead time: time interval after a detection event when the detector as a whole is unable to provide an output in response to incoming photons at the single photon level

decoding: process by which a receiver extracts the secret message from the publicly transmitted data

decoy state: legitimate user intentionally and randomly replaces the usual protocol signals by different signals to test the channel action

detection efficiency: probability that a photon, of a specific energy (spectral frequency) or wavelength, incident at the optical input will be detected within a detection gate, and produce an output signal

detection efficiency linearity: minimum detection efficiency divided by the maximum detection efficiency over the specified range of powers

detection efficiency range due to polarization of input pulses: difference between the maximum DE for input polarized light, and the DE due to randomly polarized input light

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

detector gate repetition rate: repetition rate of the time-intervals during which a detector has single-photon sensitivity

detector recovery time: smallest time duration after which the detection efficiency is independent of previous photon detection history (i.e. its steady state value)

detector signal jitter: detection efficiency variation with respect to the arrival of a single photon at the input port of the DUT

device model: physical model of a device to capture the essential behaviour

Differential Power Analysis (**DPA**)**:** 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

distillation: distillation of a key which means the extraction of a secure key from some partially compromised data

E

eavesdropping: act of attempting to listen to the private conversation of others without their consent

ElectroStatic Discharge (**ESD**)**:** 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)

encoding: process of mapping a secret message into a publicly accessible set of data from which the rightful user can decode the secret message again

encrypted key: cryptographic key that has been encrypted using an approved security function with a key encrypting key

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 uncertainty regarding information

Eve or eavesdropper: any adversary intending to intercept data in a quantum or classical channel

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

individual attack: attack where Eve lets each signal interact separately with its own ancilla, and keeps the ancillas apart at later times

NOTE: A slightly different definition is used in Scarani et al [i.4].

intensity modulator: device that can actively modulate its transmittance of optical signals passing through it

intrinsic dark count probability: 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

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

Void.

K

key rate: rate of shared secret key generation resulting from a Quantum Key Distribution process

L

Void.

M

mean spectral frequency: average frequency of spectral measurement

mean photon number: average number of photons per optical pulse

mean source power: absolute average power emitted by the source (transmitter) over the time period of a QKD session, or other stated time-interval

mean wavelength: average wavelength of spectral measurement

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

N to O

Void.

P

partial detector recovery time (high): 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

partial detector recovery time (low): 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

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

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

Personal Identification Number (PIN): 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: number of photons in a pulse

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

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 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 partially compromised data

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 Entity: 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

QKD link: link connecting a pair of QKD Entities

QKD Module: set of hardware and software components that implements cryptographic functions and quantum optical processes, including cryptographic algorithms and protocols and key generation, and is contained within a defined cryptographic boundary

QKD network: network comprised of two or more Trusted Nodes

QKD session: set of all raw bits which are subject to one particular round of sifting, error correction, and privacy amplification, to generate a particular secret key

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 or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory

quantum mechanics: physical theory that describes natural phenomena

quantum mechanical state: complete description of a physical system in quantum mechanics

quantum memories: device that can store and retrieve quantum mechanical states

quantum photon source: optical source for carrying quantum information

quantum signal: signal described by a quantum mechanical state

quantum storage: See quantum memories.

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: physical device outputting unpredictable binary bit sequences

reconciliation: process of generating a set of data on which sender and receiver agree from a set of data which contains differences

NOTE: The result of reconciliation is not necessarily either the sender's or receiver's version of the data.

reset time: time between the end of the dead time and the recovery time

S

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

security claim: precise formulation in which sense a cryptographic protocol is secure

security infrastructure: hierarchy of devices and protocols that manage key, user privileges and controls the cryptographic protocols

security model: modelling of devices and protocols, and also of adversarial power

security parameters: parameters in a protocol that regulate the level of protection against adversaries

send-and-return scheme: scheme where 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.

single-photon detector: device that transforms a single-photon into a detectable signal with finite probability

single-photon source: photon source that emits at most one photon at a time

software module: module that is composed solely of software

source emission temporal profile: temporal distribution of photons within a single emitted pulse

source spectral frequency: spectral frequency of emitted photons

source linewidth: full width at half maximum of measured spectrum

source temporal profile: temporal intensity variation within a single optical pulse

source timing jitter: uncertainty in the emission time of an optical pulse at the optical output

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

stability of output power of emitted pulses: variation in source power over the time period of a QKD session, or other stated time-interval

T

threshold detector: photon detector that can tell the difference between i) having no photon and ii) having one or more photons, but cannot tell the number of photons

Trojan horse attack: 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.

U to V

Void.

W

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

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 or HTTPS 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 Abbreviations

A

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

B

BB84	QKD protocol published by Bennett and Brassard in 1984

NOTE: This reference is available at [i.1].

BNC	Bayonet Neill-Concelman connector
BS	British Standard
BW	Band Width

C

CHSH	Clauser-Horne-Shimony-Holt

NOTE: This reference is available at [i.3].

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 [after Einstein et al. Phys. Rev. 47(10), 777 (1935)]

NOTE: This reference is available at [i.5].

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	QKD protocol published by Grosshans and Grangier in 2002

NOTE: This reference is available at [i.2].

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

H

HBT	Hanbury Brown-Twiss
HDL	Hardware Description Language
HMAC	Hash-Based Message Authentication Code

I

I/O	Inputs and Outputs
IR	Infrared
IV	Initial Value
IV	Initialization Vector

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
PIN	Positive Intrinsic Negative
PM	Polarization-Maintaining
PNS	Photon Number Splitting
PSP	Public Security Parameter
PSK	Phase Shift Keying

Q

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:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Martin Ward, Toshiba Research Europe Limited (TREL), United Kingdom

Other contributors:
Christopher J. Chunnilall, Department for Digital, Culture, Media and Sport (DCMS) & National Physical Laboratory (NPL), United Kingdom

Gaby Lenhart, ETSI, France (until March 2017)

Thomas Länger, Austrian Institute of Technology GmbH (AIT), Austria (until September 2014)

Vicente Martín Ayuso, University Politécnica de Madrid, Spain

Yoshimichi Tanizawa, Toshiba Corporation, Japan

History

Document history		
V1.1.1	December 2018	Publication