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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms and abbreviations 7
3.1 Terms 7
A 7
B 7
C 7
D 8
E 9
F to G 9
H 9
I 9
J 9
K 9
L 9
M 10
N to O 10
P 10
Q 11
R 11
S 11
T 12
U to V 12
W 13
X 13
Y 13
Z 13
3.2 Abbreviations 13
A 13
B 13
C 13
D 14
E 14
F 14
G 14
H 14
I 14
J 15
K 15
L 15
M 15
N 15
O 15
P 15
Q 15
R 16
S 16
T 16
U 16
V 16

W 16
X to Z 16

Annex A: Authors & contributors 17

History 18

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.