ETSI GR QKD 003 V2.1.1 (2018-03)

Quantum Key Distribution (QKD); Components and Internal Interfaces

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
RGR/QKD-003ed2

Keywords
interface, quantum key distribution

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

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 is a preparatory action for the definition of properties of components and internal interfaces of QKD Systems. Irrespective of the underlying technologies, there are certain devices that appear in most QKD Systems. These are e.g. quantum physical devices such as photon sources and detectors, or classical equipment such as protocol processing computer hardware and operating systems. For these components, relevant properties should be identified that will subsequently be subject to standardization. Furthermore, a catalogue of relevant requirements for interfaces between components should be established, to support the upcoming definition of internal interfaces.

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] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields: "Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security", Opt. Express 15, 8465 (2007).

[i.2] G. Ribordy, J-D. Gautier, N. Gisin, O. Guinnard and H. Zbinden: "Fast and user-friendly quantum key distribution", J. Mod Opt. 47, 513-531 (2000).

[i.3] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum Cryptography, Rev. Mod. Phys. 74, 145-195 (2002).

[i.4] Y. Zhao, B. Qi, H.-K. Lo, L. Qian: "Security analysis of an untrusted source for quantum key distribution: passive approach", New Journal of Physics, 12, 023024 (2010).

[i.5] L. Duraffourg, J.-M. Merolla, J.-P. Goedgebuer, Y. Mazurenko, W. T. Rhodes: "Compact transmission system using single-sideband modulation of light for quantum cryptography", Opt. Lett 26(18) 1427-1429 (2001).

[i.6] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden: "Fast and simple one-way quantum key distribution" Applied Physics Letters 87(19); 194108, (2005).

[i.7] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, S. Ten: "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres", New J. Phys. 11(7), 75003 (2009).

[i.8] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger: "Practical quantum key distribution with polarization entangled photons", Opt. Express 12(16), 3865-3871 (2004).

[i.9] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel and A. Zeilinger: "A fully automated entanglement-based quantum cryptography system for telecom fiber networks", New Journal of Physics 11, 045013 (2009).

[i.10] Juan Yin, Yuan Cao, Yu-Huai Li, Ji-Gang Ren, Sheng-Kai Liao, Liang Zhang, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Ming Li, Yong-Mei Huang, Lei Deng, Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan: "Satellite-to-ground entanglement-based quantum key distribution", Phys. Rev. Lett. 119, 200501 (2017).

[i.11] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, P. Grangier: "Field test of a continuous-variable quantum key distribution prototype", New J. Phys. 11(4), 045023 (2009).

[i.12] A. Leverrier & P. Grangier: "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation", Phys. Rev. Lett. 102, 180504 (2009).

[i.13] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, A. J. Shields: "High speed single photon detection in the near infrared", Appl. Phys. Lett. 91(4), 041114 (2007).

[i.14] M. A. Itzler, X. Jiang, B. Nyman, and K. Slomkowski: "InP-based negative feedback avalanche photodiodes", Proceedings of SPIE 7222, 72221K (2009).

[i.15] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden: "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency", Appl. Phys. Lett. 104, 081108 (2014).

[i.16] G. Boso, H. Zbinden, B. Korzh, and E. Amri: "Temporal jitter in free-running InGaAs/InP single-photon avalanche detectors", Opt. Lett. 41(24), 5728-5731 (2016).

[i.17] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield: "Superconducting nanowire single-photon detectors - physics and applications", Supercond. Sci.Technol. 25, 063001 (2012).

[i.18] E. A. Dauler, M. E. Grein, A. J. Kerman, F. Marsili, S. Miki, S. W. Nam, M. D. Shaw, H. Terai, V. B. Verma, and T. Yamashita: "Review of superconducting nanowire single-photon detector system design options and demonstrated performance", Optical Engineering 53(8), 081907 (August 2014).

[i.19] S. Dorenbos, E. Reiger, N. Akopian, U. Perinetti, V. Zwiller, T. Zijlstra, and T. Klapwijk: "Superconducting single photon detectors with minimised polarisation dependence". Appl. Phys. Lett. 93, 161102 (2008).

[i.20] V. B. Verma, F. Marsili, S. Harrington, A. E. Lita, R. P. Mirin, and S. W. Nam: "A three-dimensional polarization-insensitive superconducting nanowire avalanche photodetector". Appl. Phys. Lett. 101, 251114 (2012).

[i.21] V. Burenkov, H. Xu, B. Qi, R. H. Hadfield, and H.-K. Lo: "Investigations of afterpulsing and detection efficiency recovery in superconducting nanowire single-photon detectors", J. Appl. Phys. 113, 213102 (2013).

[i.22] D. Rosenberg, A. J. Kerman, R. J. Molnar, and E. A. Dauler: "High-speed and high-efficiency superconducting nanowire single photon detector array", Opt. Exp. 21, 1440-1447 (2013).

[i.23] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam: "Detecting single infrared photons with 93% system efficiency", Nature Photon. 7, 210-214 (2013).

[i.24] S. Miki, T. Yamashita, H. Terai, and Z. Wang: "High performance fiber-coupled NbTiN superconducting nanowire single photon detectors with Gifford-McMahon cryocooler", Opt. Exp. 21, 10208-10214 (2013).

[i.25] J. Lodewyck & P. Grangier: "Tight bound on the coherent-state quantum key distribution with heterodyne detection", Phys. Rev. A 76, 022332 (2007).

[i.26] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, P. Grangier: "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers", J. Phys.: Atomic, Molecular and Optical Physics 42, 114014 (2009).

[i.27] P. M. Intallura, M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, P. Atkinson, D. A. Ritchie, A. J. Shields: "Quantum communication using single photons from a semiconductor quantum dot emitting at a telecommunication wavelength", J. Opt. A: Pure Appl. Opt., 11(5), 054005 (2000).

[i.28] A. R. Dixon, J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. J. Bennett, A. J. Shields: "Ultrashort dead time of photon-counting InGaAs avalanche photodiodes", Applied Physics Letters 94, 231113 (2009).

[i.29] W.-Y. Hwang: "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett. 91, 057901 (2003).

[i.30] X.-B. Wang: "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography", Phys. Rev. Lett. 94, 230503 (2005).

[i.31] H.-K. Lo, X. Ma, K. Chen: "Decoy state quantum key distribution", Phys. Rev. Lett. 94, 230504 (2005).

[i.32] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih: "New High-Intensity Source of Polarization-Entangled Photon Pairs", Phys. Rev. Lett. 75(24), 4337-4341 (1995).

[i.33] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, A. Zeilinger: "A wavelength-tunable fiber-coupled source of narrowband entangled photons", Opt. Express 15, 15377-15386 (2007).

[i.34] B. Blauensteiner, I. Herbauts, S. Bettelli, A. Poppe, H. Hübel: "Photon bunching in parametric down-conversion with continuous wave excitation", Phys. Rev. A 79, 063846 (2009).

[i.35] 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.36] 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.37] P. W. Shor and J. Preskill: "Simple proof of security of the BB84 quantum key distribution protocol", Phys. Rev. Lett., 85, 441 (2000).

[i.38] D. Mayers: "Unconditional security in Quantum Cryptography", JACM, 48(3), 351-406 (2001).

[i.39] D. Bruß: "Optimal Eavesdropping in Quantum Cryptography with Six States", Phys. Rev. Lett. 81, 3018 (1998).

[i.40] H-K. Lo: "Proof of Unconditional Security of Six-State Quantum Key Distribution Scheme", Quantum Information and Computation, 1(2), 81 (2001).

[i.41] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, K. Azuma: "Loss-tolerant quantum cryptography with imperfect sources", Phys. Rev. A 90, 052314 (2014).

[i.42] S. M. Barnett, B. Huttner, S.J.D. Phoenix: "Eavesdropping Strategies and Rejected-data Protocols in Quantum Cryptography", J. Mod. Opt. 40, 2501-2513 (1993).

[i.43] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders: "Limitations on practical quantum cryptography", Phys. Rev. Lett., 85, 1330 (2000).

[i.44] V. Scarani, A. Acin, G. Ribordy, N. Gisin: "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations", Phys. Rev. Lett. 92(5), 057901 (2004).

[i.45] A. Ekert: "Quantum Cryptography based on Bell's theorem", Phys. Rev. Lett. 67(6), 661-663 (1991).

[i.46] C. H. Bennett, G. Brassard and N. D. Mermin: "Quantum Cryptography without Bell's theorem", Phys. Rev. Lett. 68(5), 557-559 (1992).

[i.47] K. Inoue, E. Waks, Y. Yamamoto: "Differential Phase Shift Quantum Key Distribution", Phys. Rev. Lett. 89(3), 037902 (2002).

[i.48] K. Inoue, E. Waks, Y. Yamamoto: "Differential-phase-shift quantum key distribution using coherent light", Phys. Rev. A 68(2) , 022317 (2003).

[i.49] T. Sasaki, Y. Yamamoto, M. Kaoshi: "Practical quantum key distribution protocol without monitoring signal disturbance", Nature 509, 475-478 (2014).

[i.50] N. Walenta: "Concepts, components and implementations for quantum key distribution over optical fibers", PhD thesis, available at: http://archive-ouverte.unige.ch/unige:26776.

[i.51] H-K. Lo, M. Curty, B. Qi: "Measurement-Device-Independent Quantum Key Distribution", Phys. Rev. Lett. 108(13), 130503(5) (2012).

[i.52] F. Grosshans, P. Grangier: "Continuous Variable Quantum Cryptography Using Coherent States", Phys. Rev. Lett., 88(5), 057902 (2002).

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Alice: quantum information sender/transmitter in a QKD system

Bob: quantum information receiver in a QKD system

classical channel: communication channel that is used by two communicating parties for exchanging data encoded in a form which may be non-destructively read and fully reproduced

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

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

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

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

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.

quantum channel: communication channel for transmitting quantum signals

quantum photon source: optical source for carrying quantum information

random number generator: physical device outputting unpredictable binary bit sequences

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

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.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

C_{max}	Maximum count rate
Δ_{el}	electrical noise measurement variance accuracy
Δ_{ξ}	total excess noise measurement variance accuracy
Δ_{sn}	shot-noise measurement variance accuracy
η	photon detection probability, photon detection efficiency
$\eta(\lambda)$	detection efficiency (nm)
$\eta(\nu)$	detection efficiency (Hz)
$\eta(t)$	photon detection probability profile
$\eta(t,T)$	detector signal jitter
$f_{\Delta el}$	electrical noise measurement variance stability
$f_{\Delta\xi}$	total excess noise measurement variance stability
$f_{\Delta sn}$	shot-noise measurement variance stability
f_{gate}	gate repetition rate
f_{source}	optical pulse repetition rate
$g^{(2)}$	second-order correlation coefficient
J_{source}	timing jitter
L_{RX}	total receiver loss
λ	wavelength
$\Delta\lambda$	spectral bandwidth
λr	wavelength range
Mdf	modulated degree of freedom
MaxDev	maximal deviation values
μ	mean photon number
N	photon-number resolving depth
$N_{emitters}$	number of photon-emitters in a multiple-source QKD transmitter
N_0	vacuum noise variance
ν	spectral frequency
$\Delta\nu$	spectral bandwidth
Opr	optical robustness
ξ	total excess noise measurement variance
p_{after}	after-pulse probability
p_{dark}	dark count probability
$p(n)$	photon number probability distribution]
$P_{emission}(t)$	emission temporal profile
P_{mean}	mean optical power
$P_{pulse}(t)$	temporal profile
s_{el}	electrical noise measurement variance
s_{ind}	spectral indistinguishability
SNR_{min}	supported signal-to-noise ratio
SNU	shot-noise unit (1 SNU = vacuum noise variance, N_0)
t_{ind}	temporal indistinguishability
t_{dead}	dead time
$t_{partial\_f}$	partial recovery time
$t_{recovery}$	recovery time
$t_{r/f}$	rise and fall time
T	temperature

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Alternating Current
AMZI	Asymmetric Mach-Zehnder Interferometer
APD	Avalanche PhotoDiode
BB84	QKD protocol published by Bennett and Brassard in 1984 [i.36]
BNC	Bayonet Neill-Concelman connector

BW	Band Width
CHSH	Clauser-Horne-Shimony-Holt [i.35]
COW	Coherent One-Way
CV	Continuous Variable
CV-QKD	Continuous Variable QKD
CW	Continuous Wave
DAC	Digital-to-Analogue Converter
DC	Direct Current
DPS	Differential Phase Shift
DSP	Digital Signal Processor
DUT	Device Under Test
DV	Discrete Variable
ECL	Emitter Coupled Logic
EPR	Einstein-Podolsky-Rosen [after Einstein et al. Phys. Rev. 47(10), 777 (1935)]
FC/PC	Ferrule Connector/Physical Contact
FPGA	Field Programmable Gate Array
FW	Full-width
FWHM	Full-width at Half-maximum
GG02	QKD protocol published by Grosshans and Grangier in 2002 [i.52]
GM	Gaussian Modulation
GMCS	Gaussian Modulated Coherent State
LDPC	Low Density Parity Check codes
LLO	Local Local Oscillator
LO	Local Oscillator
MDI	Measurement-Device Independent
MM	Multi-Mode
NFAD	Negative Feedback Avalanche Photodiode
NIM	Nuclear Instrumentation Module
PBS	Polarising Beamsplitter
PDE	Photon Detection Efficiency
PNS	Photon Number Splitting
PSK	Phase Shift Keying
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QPSK	Quadrature Phase Shift Keying
RRDPS	Round Robin DPS
RX	Receiver
SDE	System Detection Efficiency
SM	Single-Mode
SMA	Sub-Miniature version A connector
SNR	Signal-to-Noise Ratio
SNSPD	Superconducting Nanowire Single-Photon Detector
SPAD	Single-Photon Avalanche Photodiode
SPDC	Spontaneous Parametric Down-Conversion
TAT	Trap-Assisted Tunnelling
TLO	Transmitted Local Oscillator
TTL	Transistor-Transistor Logic
TX	Transmitter
VOA	Variable Optical Attenuator
WDM	Wavelength Division Multiplexing

4 QKD systems

4.1 Generic description

A QKD system comprises a number of internal components. The purpose of the present document is to identify the components which are common to many systems and their properties which may require calibration. The present document also defines the interfaces between these common components.

A survey of the literature reveals that many different types of QKD system have been proposed. Many of these have been implemented physically with different levels of sophistication. At the most basic level, these systems utilize the laws of quantum theory to make claims about the security levels of the shared key. Most commonly, they use signal encoding upon quantum light states using several different bases which are non-orthogonal to one another. Quantum theory dictates that it is impossible to gain full information of this encoding through measurement without prior information about the encoding basis or post-selection of the basis used. This property is used to ensure that the legitimate users of the system share more information than an eavesdropper can determine.

One convenient method of categorizing different types of QKD system is according to the photon source that they use. Examples include true single-photon sources, entangled-photon pair sources and weak laser pulses. Common methods for encoding the qubit information include controlling the phase or the polarization state of the transmitted photon. A QKD system consists of two units which are physically separated at opposite ends of a pair of communication channels, as illustrated by figure 4.1. The sending and receiving unit contain a source of randomness for use in the key generation protocol. The source of randomness can be intrinsic, as in the case of sending entangled photons, or it can be an active random number generator or a passive random selection component, such as a non-polarizing beamsplitter. Here, the sending unit consists of a signal source and an encoder for the source, the receiving unit contains a component for signal demodulation, i.e. for selecting the measurement basis, as well as one or more signal detectors. Control electronics, with access to an independent random number generator, are necessary to generate the drive signals for these devices. The detected signals are used by the control electronics to form the initial (or raw) shared key, which is then post-processed (sifted, reconciled and privacy amplified) to achieve the final secure shared key.

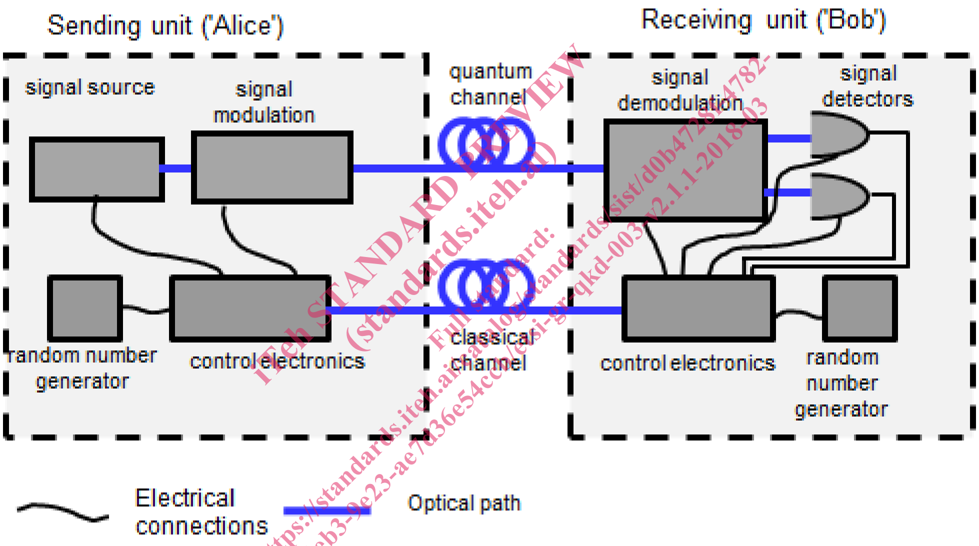

Figure 4.1: Schematic of a generic QKD system showing internal interfaces and connections

Alice and Bob may exchange classical optical signals for clock synchronization/recovery and sifting and data processing. These signals are transmitted through classical channels which may be on a separate fibre, or combined with the quantum signal through the same fibre using wavelength- or time-division multiplexing. (In pure classical communications, the channel used to perform management functions is called the signalling channel. It is the classical communications equivalent of QKD synchronization and distillation channels).

4.2 Weak Laser Pulse QKD Implementations

4.2.1 Generic Description

In weak laser pulse QKD systems, the qubit values are encoded upon laser pulses attenuated to the single-photon level. The sender (Alice) in a weak laser pulse QKD contains at least one weak laser source that is used as a quantum information carrier. In implementations involving more than one weak laser source, the sources should be indistinguishable from one another in every measurable attribute except the degree of freedom the quantum information is encoded upon.