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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.
All rights reserved.

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

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.

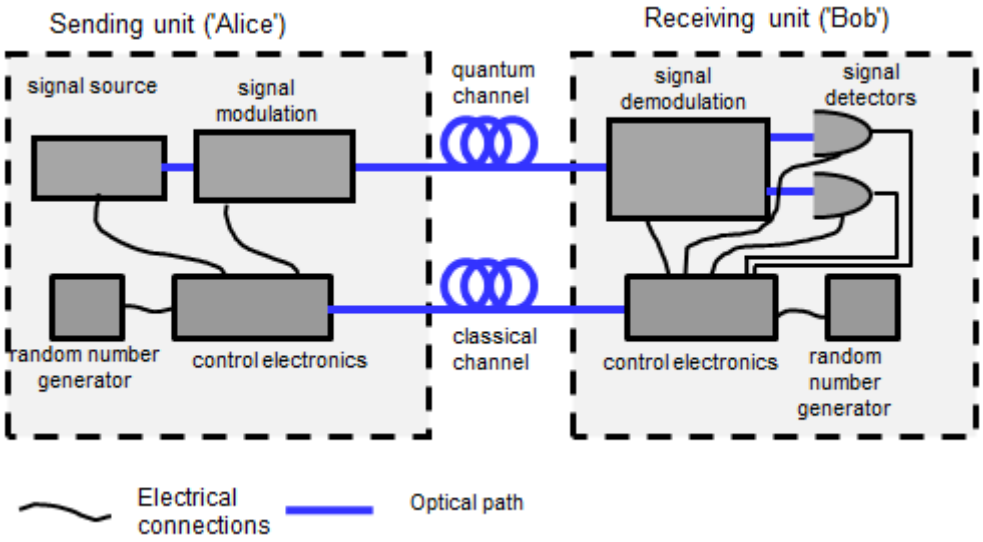


Figure 4.1: Schematic of a generic QKD system showing internal interfaces and connections

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.

The sender should contain a quantum encoder that encodes qubit information on each weak laser pulse. This encoder should have a source of randomness that determines an encoding basis and an encoding bit value for each weak pulse. The source of randomness should come from a random number generator.

The photon number splitting attack, and other such attacks, should be accounted for in the privacy amplification process in a QKD session. To achieve this, the intensity and photon number statistics of each weak laser source should be calibrated. The source stability should also be calibrated. In the case that the source is unstable, the worst case scenario should be considered in the privacy amplification process.

In the following, a few example realisations of weak laser pulse QKD systems are presented.

4.2.2 One-Way Mach-Zehnder

Figure 4.2 shows an example of a QKD system using weak laser pulses as the signal carriers and Asymmetric Mach-Zehnder Interferometers (AMZIs) to encode the quantum states, based on the paper by Dynes et al. [i.1]. The system uses the decoy pulse protocol to obtain higher secure bit rates than are otherwise possible using weak laser pulses with constant intensity. Intensity modulation is used to produce signal, decoy and vacuum pulses of differing intensities, as well as strong reference pulses to enable active stabilization. The vacuum pulses could also be produced by omitting trigger pulses to the signal laser. The signal, decoy and vacuum pulses are produced in a non-deterministic sequence and have pre-determined relative occurrence probabilities assigned to them. The signal and decoy pulses are attenuated to the single-photon level before entering the quantum channel implemented in standard single mode fibre.

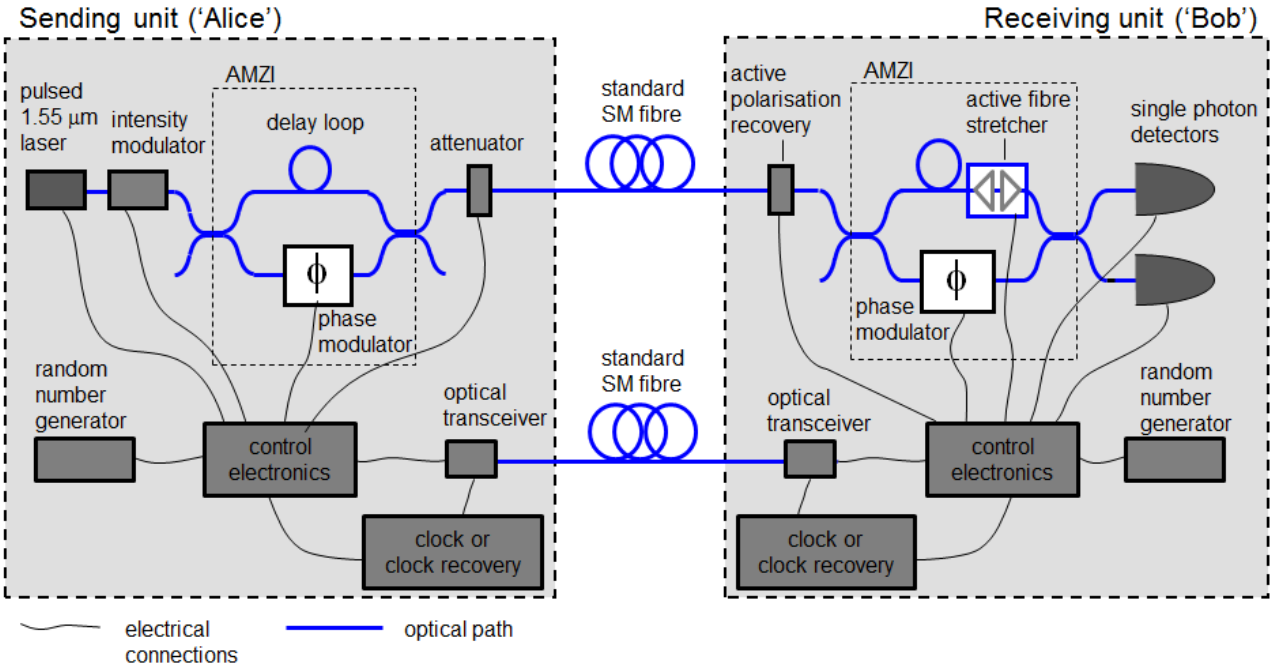


Figure 4.2: Schematic of a one-way, weak-laser-pulse QKD system

The receiver's single-photon detectors are two InGaAs avalanche photodiodes (APDs), operated in gated Geiger mode.

This system uses active stabilization to lock the path phase difference in the sending and receiving AMZI. The strong reference pulses are produced by the intensity modulator(s) at pre-determined times. These strong reference pulses are either unmodulated, or modulated with pre-determined phase values by the phase modulator in the sending AMZI. Detection rates of these reference pulses are used as a feedback to actively adjust a phase compensation component in Bob, here a fibre stretcher, to compensate for the path phase difference. A similar active stabilization technique is used to control the polarization state of photons entering Bob's AMZI.

In this implementation, the combination of the 1 550 nm laser diode, the intensity modulator and the attenuator forms the photon source. Because only one laser diode is used for encoding all qubits, the indistinguishability of the source is guaranteed. An intensity modulator is required to implement the decoy QKD protocol. Alice's AMZI is the encoder. Standard single mode fibre is used as the quantum channel. In the receiving unit, the combination of the active polarization recovery, active fibre stretcher and AMZI forms the decoder.

Each control electronics unit can contain optoelectronics components, such as optoelectronics-based random-number generators used as the sources of randomness.

Optical transceivers at Alice and Bob are used to provide signals for clock synchronization/recovery and classical communications for sifting and data processing.

4.2.3 Send-and-return scheme (Mach-Zehnder)

Figure 4.3 depicts a typical send-and-return scheme (also called "plug-and-play") with a Mach-Zehnder architecture, described in detail in [i.2] and [i.3]. Pulses emitted from the source S in Bob are directed by the circulator C to the coupler BS1, where they split into two pulses. The pulse propagating along the short arm, P_{short} has its polarisation conditioned so that it is fully launched into the quantum channel by the polarisation splitter PS. The pulse propagating along the long arm, P_{long}, also has its polarisation conditioned such that it is fully launched into the quantum channel at PS (i.e. P_{long} and P_{short} are 90° out-of-phase with respect to each other at PS). The phase shifter Φ_2 is inactive during the transit of P_{long}. At Alice, a beamsplitter BS2 reflects part of the incoming pulses to a detector D3:

i) providing a timing signal; and

ii) to monitor for so-called Trojan-horse attacks.

The transmitted pulses are reflected by a Faraday mirror (FM) which compensates for any birefringence in the quantum channel, and returns the pulses to Bob orthogonally polarised with respect to their emitted states. An attenuator (AT) reduces the intensity of the pulses to a suitably weak intensity (depending on the protocol used). Φ1 applies a phase shift to P_{long} (but not to P_{short}) to encode a bit value. At the receiving unit, P_{long} takes the short path and P_{short} takes the long path where Φ2 applies a phase shift to it to implement the measurement basis choice. Both pulses reach BS1 simultaneously with identical polarisation, leading to interference. Single-photon detectors D1 and D2 indicate which output port is taken by the photon. The circulator C ensures isolation between the laser source and D1. With this scheme, the security of a protocol has to be carefully investigated. In particular, without any knowledge of the state Alice sends to Bob, the security is difficult to guarantee. Therefore, some monitoring has to be performed on the outgoing pulses from Alice [i.4].

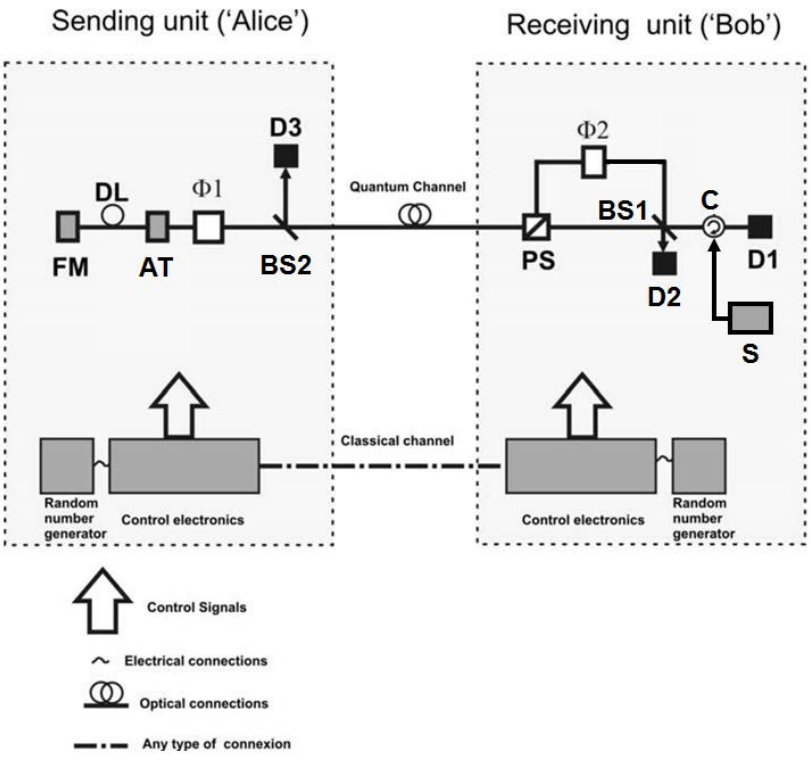


Figure 4.3: Schematic of a send-and-return scheme in a Mach-Zehnder system

4.2.4 Phase-Intensity Modulator Implementation

Figure 4.4 depicts a simplified Single Sideband (SSB) system, according to L. Duraffourg et al.,[i.5]. The source S1 is an attenuated pulsed laser diode operating at optical frequency ω_0 (quantum signal). An unbalanced integrated Mach-Zehnder modulator MZ1 modulates the intensity of the reference beam at $\Omega \ll \omega_0$ with a modulation depth $m < 1$. The modulating signal is produced by a local oscillator (OS) that drives simultaneously a second integrated Mach-Zehnder MZ2. The light emitted by the source S2 (synchronization signal), operating at optical frequency ω_s, is then modulated at the same frequency Ω. Both optical signals are launched in a standard fibre. Their optical spectra are composed by a central peak and two sidebands $\omega_0 \pm \Omega$ ($\omega_s \pm \Omega$) with phase $\Phi_1(0)$ relative to the central peak. At the receiver, a WDM demultiplexer allows to separate the transmitted signals. The synchronization signal is converted by a detector (DS) that generates an electrical signal at frequency Ω. The amplitude of the electrical signal is matched to the modulation depth m and drives a phase modulator MZ2 with a $3\lambda / 4$-optical path difference bias. When a phase shift Φ_2 is added to the electrical signal, it can be shown that the probability P_1 and P_2 of detecting one photon in the lower-sideband and the upper-sideband of the quantum signal is governed respectively by a sine-squared and a cosine-squared function of the phase difference ($\Phi_1 - \Phi_2$). One of the sidebands and the reference beam are separated by optical filter F. Any protocol can in principle be implemented with this system, which features two outputs with complementary probabilities of photon detection. The advantage of transmitting the synchronization signal in the same fibre link is to reduce drastically the sensitivity of the system to optical path fluctuations and thus allow long distance key distribution.

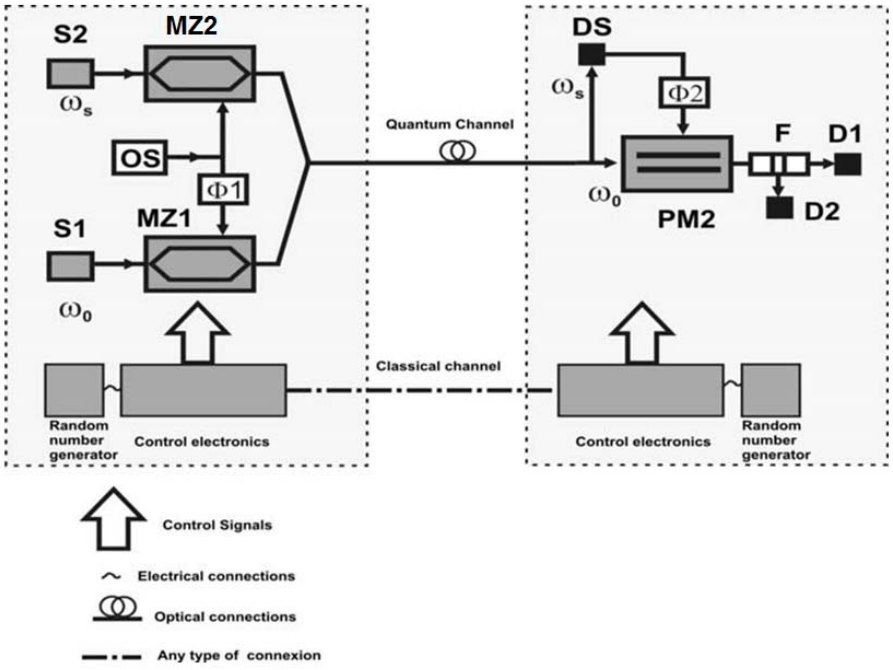


Figure 4.4: Schematic of a one-way, weak-laser-pulse frequency-domain QKD system

4.2.5 Coherent One-Way (COW)

In the COW protocol [i.6] and [i.7], the encoding is provided by a high-visibility intensity modulator, which generates weak pulses in specific time-bins. Each bit is encoded by sending a weak coherent pulse in one out of two possible time-bins, while the other time-bin contains ideally the vacuum. These states can be discriminated by a simple time-of-arrival measurement on each state. In addition, a third state called a decoy sequence, with both time-bins containing weak coherent pulses is randomly prepared.

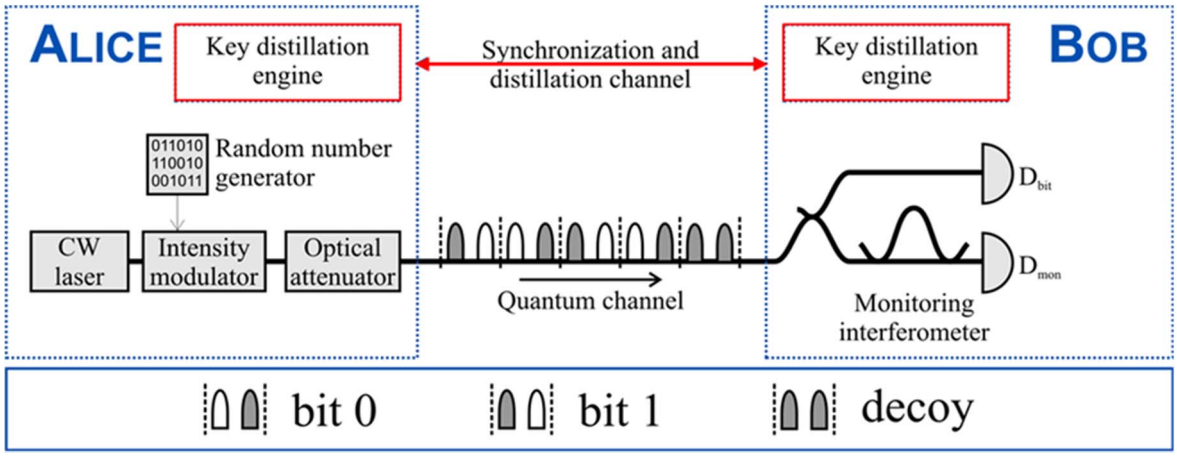


Figure 4.5: Schematic of the Coherent One-Way (COW) QKD protocol

Quantum states are prepared by Alice by intensity modulation of the output of a continuous-wave (CW) laser and subsequent attenuation to the single-photon level. On the receiver side (Bob), two single-photon detectors are used to decode the bit value (D_{bit}) and to monitor the coherence (D_{mon}) of the received states. Importantly, the receiver is completely passive, without the need for active elements or random numbers to choose the measurement basis.

4.3 Entanglement-based QKD Implementations

A schematic of a polarisation-entanglement-based QKD implementation from [i.9] is depicted in figure 4.6 (the initial fibre deployment was reported in [i.8]). The source at Alice emits an entangled photon pair, with one photon at 810 nm and the other at 1 550 nm. The 810 nm photon is measured in four possible polarisation states (0°, 45°, 90° and 135°) at Alice, using Si APDs. The 1 550 nm photon is sent over the quantum channel (standard telecom fibre) to Bob, where its polarisation is also analysed along the four directions using InGaAs APDs.

Several automated control loops enable continuous operation and movable mirrors ensure that optimal coupling into fibres is maintained. Synchronization pulses multiplexed over the same fibre gate the single-photon detectors at Bob whenever one of Alice's detectors registers an event, and also provide a polarisation reference. By analysing the received polarisation state, dynamical compensation for unwanted polarisation rotation in the optical fibre can be performed.

The ultimate technological test came in 2016, when the satellite *Micius* was launched into space carrying an entanglement-based QKD system. A secure key exchange between the satellite and a ground station could be achieved with a measured state fidelity of 0,86 [i.10]. This demonstration clearly shows that entanglement-based QKD can be implemented even in very challenging environments, such as space.

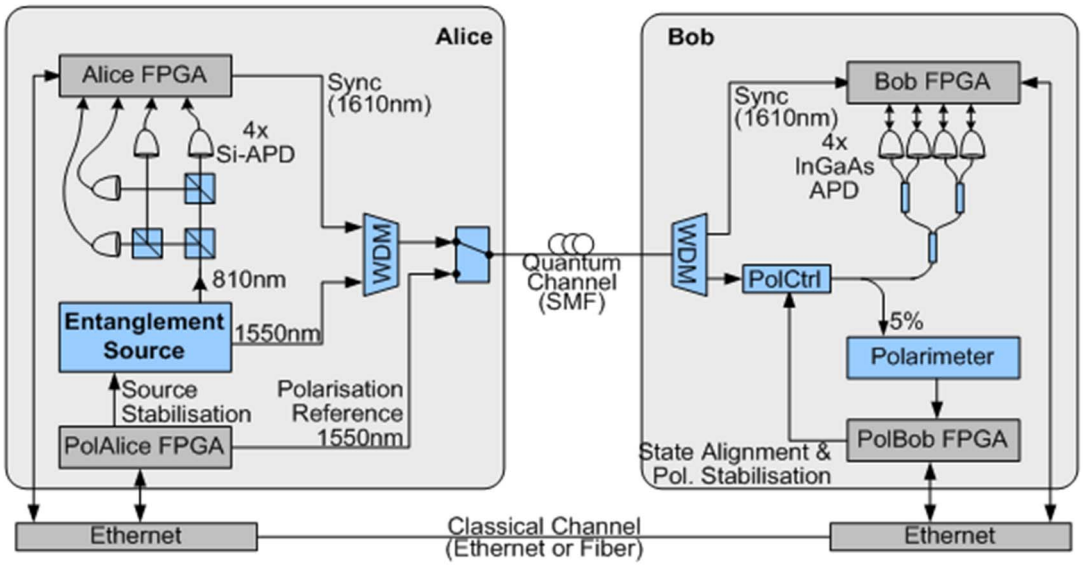


Figure 4.6: Schematic of an entanglement-based QKD system

4.4 Continuous-Variable QKD Implementations

4.4.1 Generic Description

In CV-QKD the two conjugate variables used to guarantee security are the real and imaginary part of the electromagnetic field corresponding to the two quadratures of a coherent state (coherent state based prepare-and-measure schemes). At the transmitter (Alice, sender, emitter), the phase and amplitude of weak coherent signals (typically with intensity corresponding to less than 5 photons per symbol) are modulated using either continuous modulation e.g. a Gaussian probability distribution (Gaussian Modulation - GM) or a discrete modulation e.g. QPSK (quadrature-PSK), which is extensively used in telecom transmission.

At the receiver (Bob), the electromagnetic wave surviving after attenuation in the optical channel is optically mixed with a strong electromagnetic wave, the local oscillator. The two outputs of the optical mixing are detected with photodiodes. The subtraction of the photo diode currents is proportional to the square root of the multiplication of the two optical input powers and the phase difference between the two electromagnetic waves. The choice of phase difference allows either the real or the imaginary part of the attenuated electromagnetic wave to be measured, which is further amplified by the power of the strong electromagnetic wave. The inherent uncertainty in phase and amplitude of a coherent state will be measured as shot noise on the photo diodes. Evaluation of the additional noise exceeding the minimal shot noise allows the detection of possible attacks, and fulfils a similar function to that of QBER in discrete variable QKD.

At the sender, the real and imaginary part of the field are defined with respect to a phase reference. This reference is synchronized between the transmitter and the receiver either by sending a strong optical signal "Transmitted Local Oscillator" (TLO) or a weak signal used to synchronize a local laser source "Local oscillator" (LLO) over the same transmission channel as the quantum signal. In the TLO case the strong signal is directly used in the balanced receiver as Local Oscillator (LO) whereby at the LLO scheme, the synchronized local laser is used as an LO.

4.4.2 Transmitted Local Oscillator: TLO-CV-QKD scheme

In one design option, called "Transmitted Local Oscillator" (TLO), the transmitter produces a local oscillator state and a signal state having a well-defined phase reference. Therefore, both pulses should originate from the same laser source. The source can be a diode laser. In the pulsed regime, it can be externally modulated with amplitude modulators. It can also directly produce optical pulses if driven by a pulsed current. In a practical implementation, the laser pulse may be split by a highly unbalanced optical coupler with the two output ports corresponding to a high-intensity and a low intensity for the local oscillator channel and to the quantum signal channel, respectively. The quantum signal is modulated and multiplexed to the local oscillator before being sent into the transmission channel.

A pioneering realization of Gaussian modulated CV-QKD scheme is presented in Fossier *et al.*, [i.11], Alice uses a pulsed 1 550 nm telecom laser diode to generate coherent light pulses with a duration of 100 ns and a repetition rate of 500 kHz (see figure 4.7). The pulses are separated into a weak signal and a strong local oscillator (LO) using a 99/1 asymmetric coupler. The signal is then randomly modulated, using amplitude and phase modulators in both quadratures x and p independently, according to a Gaussian distribution with mean zero and variance $V_A N_0$ where N_0 is the vacuum noise variance. It should be noted that CV QKD is not limited to Gaussian modulation. Other modulation schemes can be considered including discrete modulation protocols. In that case one should be very careful with the security proofs – see Leverrier & Grangier [i.12].

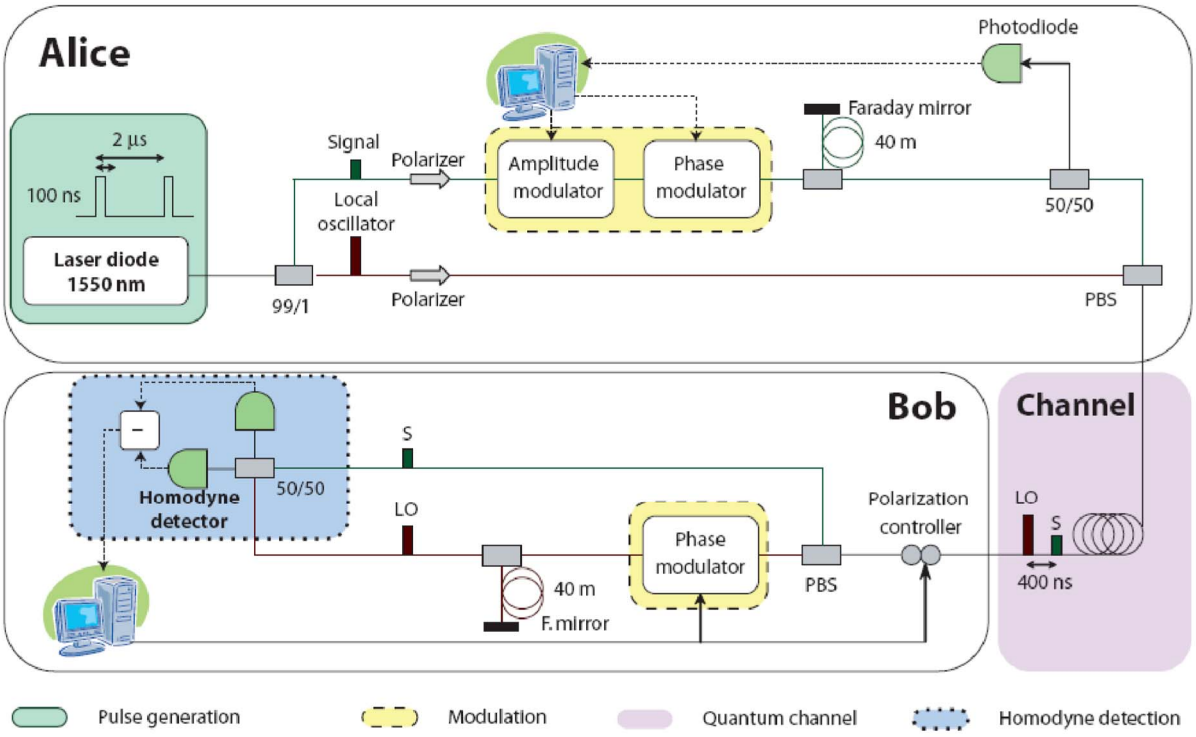


Figure 4.7: Schematic depicting the implementation of a coherent state CV QKD set-up

Different methods are used to multiplex the quantum signal and the LO signal for transmission: In case of time multiplexing, a delay line is inserted into one of the two channels. The delay should be much longer than the pulse duration. The receiver set-up should be able to demultiplex both pulses introducing minimal additional noise to the signal pulse. Demultiplexing means that the signal and oscillator pulses are coupled to physically separated channels. For time multiplexing only, this can be obtained with an unbalanced optical coupler. For example, 90 % of the incoming light can be coupled to the signal channel and 10 % to the local oscillator channel. Although, this introduces 10 % added noise to the signal pulse, the TLO suffers from 90 % loss.

To separate both channels without high losses, polarisation multiplexing can be used. At the sender, the signal and local oscillator is coupled to the two input ports of a polarising beamsplitter (PBS). In the output port, one polarisation corresponds to the signal and the other one to the local oscillator. Thus the two pulses propagate with orthogonal polarisation state in the transmission channel. At the receiver, the initial polarisation states of the pulses is recovered. This can be done using an active polarisation controller system. The two pulses can then be separated with another PBS. As a result the local oscillator and signal pulses can be sent to two separated channels.

In figure 4.7, both time and polarisation multiplexing are used so that the signal and LO are transmitted to Bob in the same optical fibre without any cross-talk. First, the signal is delayed by 400 ns using a 2 × 40 m delay line, in which the pulse is reflected by a Faraday mirror, as shown in the figure. This system imposes a $\pi/2$ polarization rotation to the pulse when it is reflected, and thus compensates all the polarization drifts that the signal has undergone. The LO is then coupled with the signal in the transmission fibre, using a PBS. Thanks to this double multiplexing, the two pulses can be separated at Bob's site very efficiently and with minimal losses, by using a simple PBS and delaying the LO after the separation.

The local oscillator and signal pulse can be sent to the receiver using two different optical channels. Such a set-up is not immune from the phase drifts between the two channels, which can disturb the phase reference between those pulses. In addition, this requires two optical channels that are not necessarily available. In a practical implementation, the signal and local oscillator pulses should be multiplexed in the same propagation channel. When propagating into the same fibre, the signal and local oscillator pulses experience the same disturbances, which do not affect their phase difference.

The phase noise requirements on the emitter laser are not stringent in this design, but interferometric stability of the de-multiplexing stage, at reception, is necessary in order to have signal and LO interfere. Once the local oscillator pulse and signal pulse are de-multiplexed, they should be synchronized in order to arrive at the coherent detection system simultaneously. This should be done with a passive fibre delay line inserted on the channel of the first arriving pulse. The delay is to be matched to the time separation between the signal and local oscillator pulse.

Finally, in Bob's system, the signal and LO interfere in a pulsed, shot-noise limited homodyne detector. This detection system outputs an electric signal, whose intensity is proportional to the quadrature x_φ of the signal, where φ is the phase difference between the signal and the LO. Following the implemented protocol, Bob measures randomly either x_0 or $x_{\pi/2}$ to select one of the two quadratures. For this purpose, he imposes randomly a $\pi/2$ phase shift to the local oscillator using a phase modulator placed in the LO path.

4.4.3 Local Local Oscillator: LLO-CV-QKD scheme

In another design option, called "Local Local oscillator" (LLO), a laser at the transmitter is used to generate the signal, while another laser, located at the receiver, is used to generate (completely locally) the Local Oscillator. A simplified scheme of such a design option is presented in figure 4.8. In this case, the phase drift between both lasers should be actively monitored or controlled, imposing stringent requirements on their phase noise.

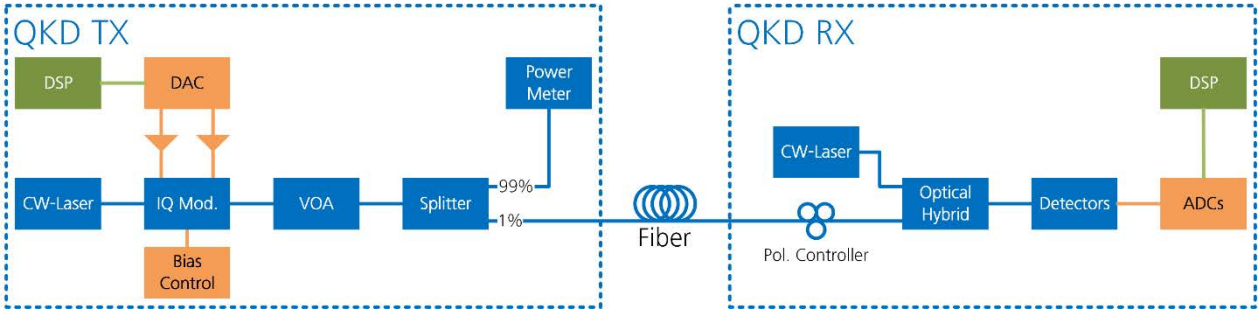


Figure 4.8: Schematic depicting the implementation of a coherent state CV QKD set-up

In figure 4.8 the optical path is indicated with blue colour. The transmitter (QKD TX) generates the quantum signals by modulating a CW-Laser employing an IQ modulator (IQ Mod.) and, subsequently, attenuates the signals to the required level. Thereby a splitter to monitor the average photon flux and a variable optical attenuator (VOA) are used. At the receiver (QKD RX), the polarization corrected quantum signal is mixed in the optical hybrid with the CW-laser utilizing the LLO scheme. The detectors are balanced detectors.

The digital signal processing (DSP, shown in green) is used to handle the flow of signals. At the QKD TX, the DSP module the signals are prepared to modulate the quantum information to the optical domain. This is carried out using the supporting electronics (shown in orange), which includes the digital-analogue-convertors (DAC) that transforms the original digital values to analogue ones that are then used to steer the modulator. At the QKD RX the detectors deliver an analogue value of the amplified voltage of the quantum measurement to the analogue-digital-convertors (ADC) and the digital value is again processed in the DSP, the main objective being the phase synchronization of the two lasers.

Different options to lock the frequencies of the CW-lasers can be used that are not shown in figure 4.8. Typically, specific synchronization pulses are employed, which do not carry quantum information but have higher amplitudes, and thus allow the phase to be determined with higher precision. Also sequences of these stronger pulses are used. Alternatively, to enable feedback loops to control the wavelength and phase of the receiving CW-laser, a pilot tone can be modulated with a polarization orthogonal to the quantum signal. Then the IQ modulator (IQ Mod) and an Optical Hybrid need to support dual polarizations and the number of detectors should be increased to allow the measurement of the pilot tone. Another future possibility motivated by telecom research is to allow a certain drift of both lasers and correct the phase directly using DSP methods.

5 Photon Detector

5.1 Single-Photon Detector

5.1.1 Generic Description and Parametrization

A single-photon detector is an optically-sensitive device that probabilistically transforms a single-photon into a macroscopically detectable signal. Figure 5.1 shows a generic single-photon detector with optical input, electrical input and output.

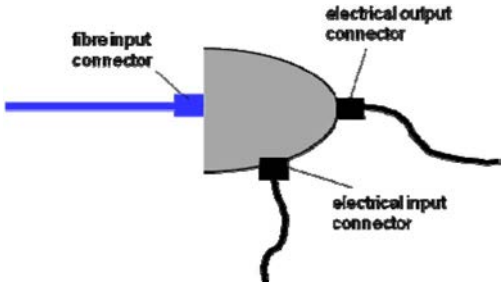


Figure 5.1: Schematic of a generic single-photon detector showing electrical and optical connections

In operation the detector output is monitored to determine the times at which the output voltage rises above the discrimination level (detection times) and/or the number of detection events within certain time duration, from which the detection count rate can be determined.

The performance of a single-photon detector can be characterized by a number of parameters, listed and described in table 5.1 and the text immediately below it.

The parameters should be specified for a defined set of operating conditions, given in table 5.2. Table 5.3 lists additional attributes to be specified for the detector.

In QKD systems that require multiple single-photon detectors for qubit detections, the detectors should be set so as to have balanced photon detection efficiencies. Ideally, the detection rates should be maintained exactly the same for all the qubit detectors. The parameters in tables 5.1, 5.2 and 5.3 should be defined for each single-photon detector in the system.

Table 5.1: Parameters that can be used to specify a single-photon detector

Parameter	Symbol	Units	Definition
Detector gate repetition rate [Gated detectors only]	f_{gate}	Hz	Repetition rate of the time-intervals during which the detector has single-photon sensitivity.
Photon detection probability (Photon detection efficiency)	η η, PDE	**Gated:** Unitless (probability/gate) **Free-running:** Unitless (probability)	**Gated detector:** The probability that a photon incident at the optical input will be detected (within a detection gate). **Free-running detector:** The probability that a photon incident at the optical input will be detected.
Spectral Responsivity	$\eta(\lambda)$ $\eta(\nu)$	Unitless	The photon detection probability as a function of the energy (i.e. wavelength, λ or spectral frequency, ν) of the incident photons.
Dark count probability	p_{dark}	**Gated:** Unitless (probability/gate) **Free Running:** s^{-1} (probability/s)	**Gated detector:** The probability that a detector registers a detection event per gate, in the absence of optical illumination. Free running detector: The probability that a detector registers a detection event in a stated time-interval, in the absence of optical illumination.
After-pulse probability	 $p_{after\_first}(\Delta T)$ $p_{after\_all}(\Delta T)$ p_{after_total}	Unitless (probability/event)	The probability that a detector registers a false detection event in the absence of illumination, conditional on a detector event at a time ΔT earlier. The probability of first after-pulses. The sum of the probabilities of first and secondary after-pulses. The sum of $p_{after\_all}(\Delta T)$ terms for all ΔT.
Dead time	t_{dead}	s	The 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.
Recovery Time	$t_{recovery}$	s	The smallest time duration after which the detection efficiency is independent of previous photon detection history.
Partial recovery time	$t_{partial\_f}$	s	The time duration after a photon detection event for the detection efficiency to return to a specified percentage, f%, of its steady-state value.
Maximum count rate	C_{max}	Hz	The maximum rate of photon detection events in the single/few-photon/gate regime when exposed to strong illumination.
Detector signal jitter	$\eta(t,T)$ where T denotes photon arrival time	Unitless (probability/gate or probability)	Photon detection probability variation with respect to the arrival of a single photon at the input port of the DUT.
Photon detection probability profile	$\eta(t)$	Unitless	Photon detection probability as a function of incident pulse arrival time.
Photon number resolution depth	N	Unitless	For detectors than can resolve the number of photons in the incident pulse, this is the maximum number of photons that can be distinguished.

The photon detection efficiency should be defined for the external input to the device and should not be adjusted for any losses occurring after the optical input. The photon detection efficiency is not to be confused with the quantum efficiency of the detection element, which describes the probability that a photon is absorbed in the active region of the detection element.

NOTE: The photon detection efficiency is referred to as the system detection efficiency (SDE) in some publications.

More generally, the photon detection efficiency should be defined as a function of the wavelength (or spectral frequency) of the incident photon.

The detector may sometimes record an event when there is no photon incident on the device. This is commonly referred to as a dark count. The dark count probability should be defined as the probability that a detector registers a detection event per gate or per unit time, when the detector is not illuminated.

After-pulses are false counts which are secondary detection events triggered by previous events (photon detections or dark counts). The after-pulse probability should be defined as the probability that a detector registers a false detection event in the absence of illumination, conditional on a preceding detection event due to incident photons of stated mean photon number, or a dark count.

The recovery time should be defined as the smallest time duration after which the detection efficiency is independent of the previous photon detection history.

The maximum count rate should be defined as the maximum rate of photon detection events under strong illumination.

The variation in the photon detection time should be referred to as the detector signal jitter. The profile of the mean detection time over a range of photon arrival times should be referred to as the photon detection probability profile.

Table 5.2: Operating conditions that should be specified for a single-photon detector

Operating Condition	Symbol	Units	Definition
Detector Temperature	T	°C or K	Physical temperature of the detection element during operation.
Environmental Requirement	N/A	N/A	The environment conditions under which a detector module operates. These conditions include environmental temperature, humidity, pressure, and requirement for surrounding electromagnetic radiation.
Mode of Operation	N/A	N/A	Describes how the electrical bias is applied to the detector. Three modes of operation are common: DC current mode, DC voltage mode, and gated mode.
Operating Wavelength	λ	nm	Wavelength of the photons to be detected.
Gating Frequency	F	Hz	The frequency of the gating signal applied to the detector, if operating in gated mode.
Gate Width	W	s	For detectors operating in gated mode, this is the nominal duration of the electrical signal applied to turn the detector on.
DC Bias	V_{dc}	Volts	The dc voltage level applied to the detector.
AC Bias	V_{ac}	Volts	The peak-to-peak ac voltage level applied to the detector. The ac voltage is defined to vary between 0 and Vac. The total bias applied to the device therefore varies between Vdc and (V_{dc} + V_{ac}).
Discrimination level	V_{disc}	Volts	Voltage threshold above (or below) which the amplitude of an output pulse is exceeded to be registered as a detection event.

Table 5.3: Additional attributes that should be specified for a single-photon detector

Parameter	Definition
Electrical input	Defines electrical input signals to the device along with the type of connector used. Input signals may be used for biasing the detector, providing a trigger signal or as a power supply.
Optical input	Defines the format of the optical input to the device. Often this is through SM or MM optical fibre. The fibre connector should also be specified, e.g. FC/PC. The device may also be coupled through free space, in which case the active area and location within the unit should be specified.
Electrical output	Defines the format of electrical output signal from the device upon photon detection, such as ECL, TTL, NIM, etc., as well as the type of connector, e.g. BNC, SMA.
Optical robustness	The maximum illumination power that a detector can endure without altering its detection parameters.
Physical dimensions	The physical size of a detector module that is independently operational.
Power consumption	Power consumption is the total power that is needed to continuously operate a detector.
Handling instructions	Instructions for the safe handling of the detector, such as information regarding toxicity and the presence of high voltages.

5.1.2 InGaAs Single-Photon Avalanche Photodiodes

5.1.2.1 Generic Description

InGaAs single-photon avalanche photodiodes (SPADs) are compact semiconductor devices that provide single-photon sensitivity over the wavelength range from 900 nm to 1 700 nm, suitable for use in fibre-optic based QKD. They can be operated in gated or free-running mode.

The bandgap of InGaAs at room temperature is 0,75 eV. Therefore, when a photon with wavelength $\lambda_{photon} < 1{,}67$ µm is absorbed, it has sufficient energy to create an electron-hole pair. Applying an electric field that exceeds the breakdown voltage (Geiger mode) accelerates the photo-induced charge-carriers, creating an avalanche of secondary charge-carriers by impact ionization. These avalanches can in turn be detected by suitable electronics. The probability of generating an avalanche increases with the excess of the bias over the breakdown voltage.

The avalanche process is self-sustaining, and has to be quenched to reset the SPAD. Therefore, these detectors are usually biased with a voltage above breakdown for only a short interval referred to as a 'gate', leading to gated-mode operation. An alternative is to passively or actively quench the avalanche, leading to free-running operation.

Charge may be thermally generated or created by trap-assisted tunnelling (TAT) in the avalanche region. Both of these processes can cause avalanches in the absence of any photodetection, leading to 'dark counts'. Typically, the TAT processes dominate for $T < 220$ K, hence cooling these devices below this temperature does not reduce the total dark count probability further.

Some of the avalanche charge-carriers can be trapped at defects within the avalanche region. If a trapped carrier is released during a subsequent gate it can trigger a spurious avalanche, even when there is no photodetection. This is known as an after-pulse. To reduce the after-pulse rate, it is necessary to reduce the gating frequency so that the trapped carriers have sufficient time to relax. Typical relaxation times are of order a few microseconds. Even operating at a gating frequency of around 10 MHz, a dead time of up to 10 µs is often required to suppress the total after-pulse probability. The after-pulse probability can be reduced by using shorter gates and lower bias voltages (while still exceeding the breakdown voltage).

The variation in the time at which the electrical output signal presents itself, compared to the time of photon incidence, is termed the jitter. This variation is due to the statistical nature of the impact ionization process that creates an avalanche. Typically, the jitter is reduced at higher bias voltage and lower temperature.

An applied electric field exceeding the breakdown voltage leads to a high dark count probability in InGaAs. Therefore telecom wavelength SPADS typically combine an InGaAs region for photodetection, and an InP region for avalanche generation.

5.1.2.2 Gated-mode operation

One of the main limitations of the InGaAs SPAD is the low maximum gating frequency of 10 MHz, which has a detrimental effect upon the bit rate of a QKD system. This restriction upon the gating frequency is necessary to limit the probability of recording an after-pulse to an acceptable level of a few percent.

Higher gate frequencies may be achieved using techniques to detect weaker avalanches. This allows the avalanche charge through the device to be reduced and thereby lowers the probability of an avalanche carrier to be trapped in the device. Weaker avalanches may be detected using a self-differencing circuit to remove the capacitive response of the diode to the applied gating signal, leaving the weak single-photon induced avalanche. The lower avalanche charge reduces the after-pulse probability at high gating frequencies dramatically and to a level that is tolerable for QKD.

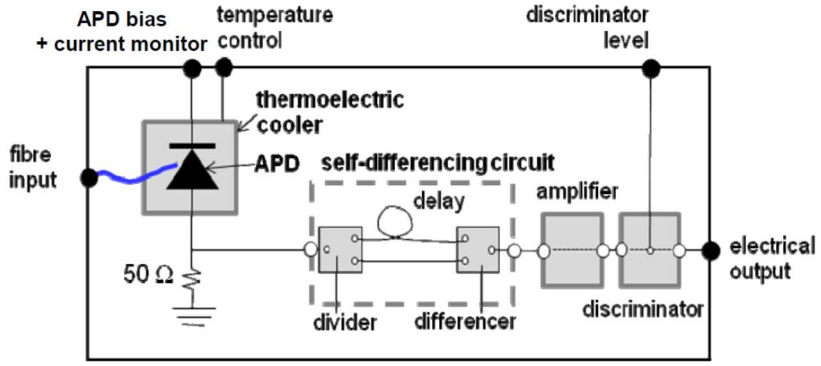


Figure 5.2: Schematic of a single-photon detector based on a self-differencing avalanche photodiode

Figure 5.2 shows a schematic for a self-differencing SPAD setup. The SPAD is housed within a thermoelectric cooler and cooled typically to -30 °C. An electrical source is applied to power and control the thermoelectric cooler. The SPAD is biased by with a square wave voltage of GHz frequency in combination with a DC voltage bias. The DC bias is typically set 1 V to 4 V below the SPAD's breakdown voltage, while the amplitude of the square wave varies from 3 V to 12 V. The SPAD output is sensed on a 50 Ω serial resistor as a voltage signal.

The high gating frequency and finite capacitance of the SPAD results in a strong capacitive component in the output signal from the SPAD. This capacitive response would dominate over the much weaker signal due to a photon-induced avalanche. To detect the weak avalanches, the self-differencing circuit compares the SPAD output signal with an identical copy that is shifted by an integer number of gating cycles. The capacitive signal is thus cancelled due to its periodic nature, leaving only the photon-induced signal.

This signal then passes through an amplifier and a discriminating circuit in order to generate an emitter-coupled-logic (ECL) output pulse compatible with the control electronics of the QKD system. The pulse discrimination voltage can be adjusted according to the background noise level.

Table 5.4 lists typical parameters reported for self-differencing InGaAs SPADs; devices with parameters similar to those in table 5.4 have been used in several QKD experiments [i.1].

Table 5.4: Typical parameters measured for conventional Geiger-mode and self-differencing InGaAs avalanche photodiodes

Parameter	Geiger Mode InGaAs SPAD	InGaAs SD-SPAD
Gating frequency	7,1 MHz	1,25 GHz
Device Temperature	-30 °C	-30 ºC
Gate width	3,5 ns	612 ps
Photon detection probability	10 %	10,9 %
After-pulse probability	2 %	6,2 %
Dark count probability	7×10^{-5} per gate	$2{,}34 \times 10^{-6}$ per gate
Dead Time	5 µs	< 2 ns
Recovery time	5 µs	< 2 ns
Jitter	500 ps	55 ps
Maximum Count Rate	200 kHz	497 MHz (1 GHz gating frequency)
Photon Number Resolution	1	4
Maximum clock frequency	10 MHz	2 GHz
Wavelength response	900 nm to 1 700 nm	900 nm to 1 700 nm
Optical robustness	1 mW	1 mW
Reference	Dynes et al., (2007) [i.1]	Yuan et al., (2007) [i.13]

5.1.2.3 Free-running operation

Free-running SPADS require a mechanism to quench an avalanche. A recent development is the so-called negative feedback avalanche photodiode (NFAD), which has a monolithic thin-film resistor integrated directly on its surface, linking the SPAD and ground [i.14]. When the avalanche current flows through this resistor, a voltage is created which lowers the bias voltage below threshold, shutting off the avalanching process. The integrated resistor leads to a very fast quench, as opposed to using external circuitry.

Improved fabrication processes have also reduced the temperature at which trap-assisted tunnelling dominates thermally created charge, enabling dark counts to be further reduced by using temperatures as low as 140 K [i.15]. Controlled variation of the bias voltage, temperature, and hold-off time subsequent to an avalanche allows the optimum combination of detection efficiency, dark count probability, after-pulse probability, and jitter to be achieved for a particular application, as described for using these devices in a 625 MHz clocked QKD system [i.15]. Jitter as low as 50 ps has recently been reported for these devices [i.16].

Table 5.5: Parameters reported for free-running InGaAs single-photon avalanche photodiodes

Reference	App. Phys. Lett. 104, 081108 (2014) [i.15]	App. Phys. Lett. 104, 081108 (2014) [i.15]	App. Phys. Lett. 104, 081108 (2014) [i.15]
Gating frequency	N/A	N/A	N/A
Avalanche duration	1 ns	1 ns	1 ns
Device temperature	-110 °C	-90 °C	-50 °C
Photon detection probability	11,5 %; 27,7 %	11,5 %; 27,7 %	11,5 %; 27,7 %
After-pulse probability	2,2 % ; 20 %	0,8 % ; 6 %	0,1 % ; 1 %
Dark count probability	1,2 Hz ; 15,2 Hz	5 Hz ; 40 Hz	200 Hz ; 1 000 Hz
Hold-off time	20 µs	20 µs	20 µs
Recovery time			
Jitter (FWHM)		400 ps ; 129 ps	
Jitter (FW @ 1%)		900 ps ; 400 ps	
Maximum Count Rate	50 kHz	50 kHz	50 kHz
Photon Number Resolution	1	1	1
Maximum clock frequency	N/A	N/A	N/A
Wavelength response	900 nm to 1 700 nm	900 nm to 1 700 nm	900 nm to 1 700 nm

5.1.3 Superconducting nanowire single-photon detectors (SNSPDs)

Superconducting nanowire single-photon detectors (SNSPDs) [i.17], [i.18] and references therein operate at a few kelvin, requiring the use of liquid helium or a closed-cycle refrigerator. This is in contrast to SPADs that operate at room temperature, or temperatures achievable using thermoelectric cooling.

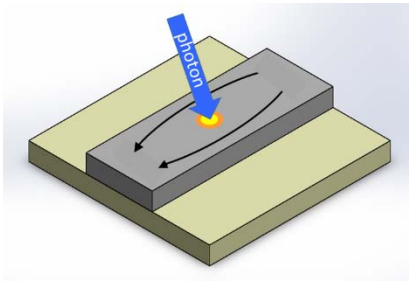


Figure 5.3: Illustration of the SNSPD photon detection mechanism

The SNSPD photon detection mechanism is illustrated in figure 5.3. The nanowire is cooled below its superconducting transition temperature, and a bias current that is just below the nanowire's critical current is applied. The local heating caused by photon absorption creates a resistive 'hot spot' on the wire, which the current diverts around. If the diverted current exceeds the critical current density, an entire cross section of the wire becomes resistive until the energy is dissipated. This process is used to generate a measurable voltage pulse. As the mechanism is not based on the superconducting transition temperature, the nanowires are typically maintained a few degrees below their critical temperature.

SNSPDs are noted for their excellent timing properties. Their fast switching and natural recovery mechanism result in low timing jitter (< 30 ps FWHM) and short reset times (< 10 ns), while the small energy gap between superconducting and resistive ground states means that their single-photon sensitivity extends to wavelengths of several microns. Their low dark count rate (< 1 kHz, bias dependent) facilitates free-running operation. The first devices used NbN nanowires, but exploiting optical cavities, alternative device geometries and other superconducting materials have led to significant improvements in performance.

The 'wire grid' structure of a nanowire meander causes polarisation-dependent photon absorption. This effect becomes stronger with increasing wavelength and decreasing fill factor, where fill factor is the fraction of the active area covered by the nanowire. Polarisation dependence can be reduced by using spiral meanders or orthogonally-oriented panels of nanowires at the cost of a lower, averaged efficiency across all input polarisations [i.19]. More recently, stacking orthogonal nanowire meanders was demonstrated to reduce polarisation dependence to the 2 % level without compromising efficiency [i.20].

Table 5.6: Parameters reported for SNSPDs

Reference	Rosenberg et al., Jan 2013 [i.22]	Marsili et al., Mar 2013 [i.23]	Miki et al., Apr 2013 [i.24]
Nanowire material	NbN on Si	α-WSi	NbTiN
Sensor temperature		0,12 - 2 K	2,3 K
Sensor critical temperature	2,5 K	3,7 K	7,5 K
Cavitised	Yes	Yes	Yes
System detection probability	76 % 40 %	93 %	74 % 55 %
After-pulse probability See [i.21]			
Polarization response (max/min)		1,22	
Dark count probability	10^4 Hz 10^2 Hz	~1 Hz (intrinsic) 10^3 Hz (unfiltered)	100 Hz 10 Hz
Dead Time			
Reset time	5 - 10 ns	40 ns	
Jitter (FWHM)	68 ps 100 ps	150 ps	68 ps
Wavelength response	centred at 1 550 nm	1 520 nm - 1 610 nm	1 300 nm - 2 000 nm; peaking at 1 550 nm

5.2 Photon Detector for a CV-QKD Set-up

5.2.1 Coherent Detection

Coherent detection is central to any CV-QKD optical set-up. It enables the measurement of one, or both of the two quadratures of incoming states. A coherent detection is said to be shot-noise limited when its main source of noise is the intrinsic quantum noise of the incoming state, and not other noise sources such as optical imbalance or electronic noise of subsequent amplifiers. In quantum communication with continuous variables, the coherent detection should be close to shot-noise limited.

A coherent detection coherently combines an intense reference signal, the LO, and a weak signal. The phase relation between both of them should be stable at the timescale of several subsequent signals, in order to allow possible phase drift to be efficiently tracked and corrected.

Signal and LO should be mixed with a balanced optical coupler. An optical coupler combines two optical inputs to produce two optical outputs in a given proportion of the inputs. In a balanced optical coupler, the outputs should contain, as much as possible, equal parts of the inputs (50/50 coupling factor). The signal and local oscillator should be coupled to each of the two inputs of the 50/50 coupler. Each of the two output ports of the coupler should be coupled to one of the balanced photodiodes. The photodiodes should produce an electric signal proportional to the intensity of the incoming light. The resulting photocurrents should be electrically subtracted from one another. With ideal components, the resulting electrical signal is proportional to the product of the signal amplitude with the local oscillator amplitude. Therefore, very weak signals can be efficiently amplified by a strong LO. The phase of the local oscillator is being considered as a phase reference. This gives access to the values of the phase and amplitude of the signal field, or equivalently to both quadratures of incoming quantum states.

In practice, the electrical subtraction should be a balanced match as much as possible. The two photodiodes should be paired. Their photon detection efficiencies and temporal response should be as similar as possible. The photon detection efficiency is the probability that an incoming photon is detected. Therefore, the common mode rejection ratio should be made as high as possible by appropriate balancing and a mitigation of all noise sources. As an example, if the LO is 10^8 more intense than the signal, then the overall balancing of the coherent detection should be better than 10^{-4} in amplitude.

A properly balanced coherent detection is able to retrieve an electrical signal proportional to the phase and amplitude of the incoming signal. An electronic amplifying chain should be used to amplify the signal from the photodiodes. It should be able to detect the total intensity present in a signal. The electronic bandwidth should be chosen accordingly. In order to be usable in a quantum optics set-up, the detection should be limited by the intrinsic noise of the incoming light (shot-noise in the case of a coherent state) and all other noise sources should be made negligible. A low noise electrical preamplifier should be used. As an example, a charge amplifier can be used; this gives an electronic noise level 10 times smaller than that of usual impedance preamplifiers. The electrical signal to be measured is proportional to the amplitude of the local oscillator. Increasing the intensity of the local oscillator makes the electrical signal arbitrarily higher than the electronics noise, provided saturation is not reached. In practice, taking into account the available power of optical sources and the attenuation of optical channels for typical distances, it is possible to obtain a local oscillator power at the reception stage that allows useful signal levels of 20 dB above the electronics noise, for clock rates in the MHz range. This is enough to ensure that the electronics noise is negligible and to guarantee a set-up working in the quantum regime.

The different versions of the TLO-CV-QKD scheme include only one balanced receiver, because further splitting of the LO that is anyway attenuated would degrade the SNR by (at least) 3 dB. In the LLO-CV-QKD scheme, the LLO will be powerful enough to allow measuring of both quadratures simultaneously. Additionally there exists the possibility to lock the wavelength of both lasers to a certain intermediate frequency (in the MHz range) to allow for less complex feedback loops. Here, three possible schemes are discussed: single- and dual-quadrature homodyne detection as well as heterodyne detection.

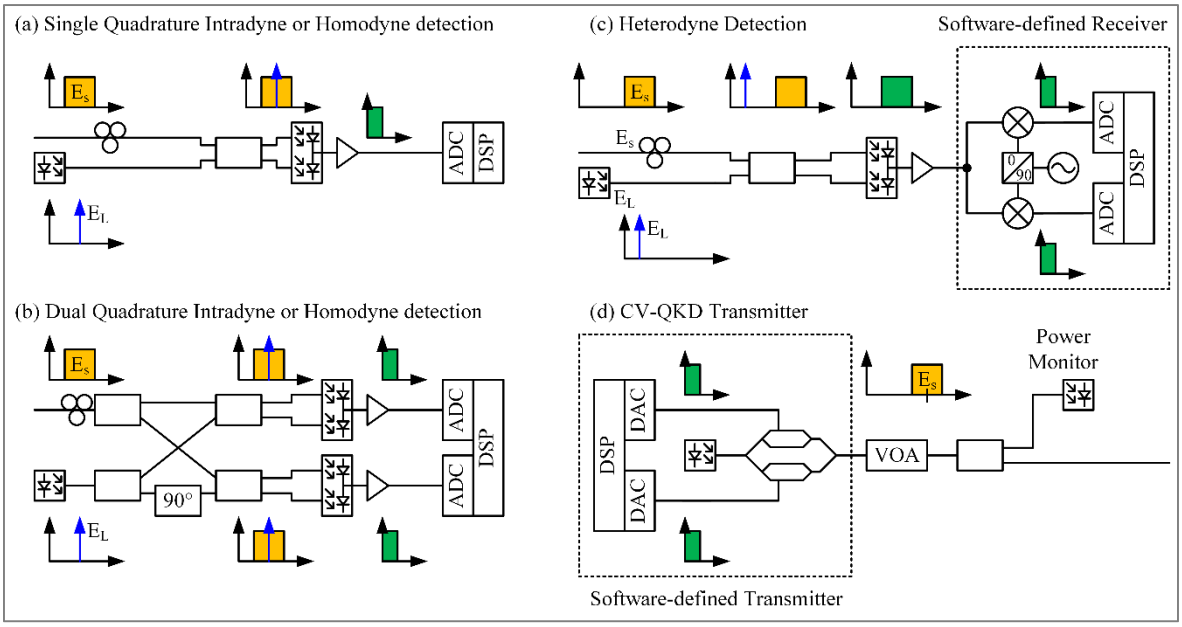


Figure 5.4: Software-defined transmitter and different detector implementation possibilities

5.2.2 Single-quadrature homodyne detection

In a single-quadrature homodyne detection setup (sometimes called intradyne in telecom or homodyne in quantum communication) only one coherent detection is used to measure incoming quantum states. This is shown in figure 5.4(a). Frequency and phase reference of the LO have to be locked optically to the quantum signal, which is an inherent property of the TLO scheme, but a challenging task for LLO schemes. Only one quadrature of an incoming state can be measured at a time. Depending on the phase of the LO, the quantum signal is projected and measured in the respective quadrature by the balanced detectors. Changing the phase of the LO allows access to both quadratures to attain security against e.g. squeezed state attacks and to measure on demand in one of the bases (following very much the idea of BB84).

This kind of homodyne detection should be able to change the phase reference in order to select any quadrature of the quantum state. This can be obtained by inserting a phase modulator either on the signal or alternatively on the local oscillator path. Therefore homodyne detection is mainly the combination of a coherent detection as described above with phase control of the local oscillator. Alice and Bob retain symbols obtained when they use a common basis, and discard those obtained with different bases, during a sifting procedure.

5.2.3 Dual-quadrature homodyne detection

For dual-quadrature intradyne or homodyne detection (figure 5.4(b)) (sometimes called heterodyne by the QKD community) both quadratures are measured simultaneously. For that both the signal and the LO are split, one branch of the LO is phase-shifted by 90°, then the two branches are brought to interference with the LOs and detected in two balanced detectors. In this setup, the phase of the received signal can be corrected in the digital domain. The homodyne detection does not require an additional phase modulator on the local oscillator channel. Only the frequency of the LO has to be locked optically to the quantum signal. The phase can be fixed in a digital processing step. However, the gain in diversity comes at the cost of splitting the signal power between the two phase-space components resulting in an additional shot-noise unit introduced by the beamsplitter. The setup now requires two detectors and four couplers (instead of one detector and one coupler) which, in addition to increasing insertion loss, more than doubles the optical complexity, and complicates the calibration procedure. For some configurations, dual-quadrature homodyne detection can be advantageous over single-quadrature homodyne detection [i.25] and [i.26].

5.2.4 Heterodyne Detection

The heterodyne detection scheme as defined in the telecom community and mapped to QKD is shown in figure 5.4(c). The central wavelengths of both CW-lasers are locked to differ by an intermediate frequency outside of the quantum signal band. Heterodyne detection then down-converts the signal to the intermediate frequency. Both signal quadratures are preserved and can be recovered through subsequent electrical down conversion. The cost for this reduced complexity is that the signal is superimposed with the image band, so the noise bandwidth is effectively doubled. From a communication point of view, both setups (b) and (c) reach the same performance and the same SNR. They have however different implementation issues: While dual quadrature homodyne or intradyne has a larger optical complexity, it directly recovers the baseband signal after the balanced detectors, which offers the largest signal-detection bandwidth for a given balanced-detector bandwidth. For heterodyne detection instead, the main complexity lies in the electrical domain, which is less sensitive to noise sources.

5.2.5 CV-QKD Detector Parameters

Table 5.7: Noise sources and QKD signal at an LLO CV-QKD receiver, and measurement modes that can be used to estimate them

Mean variance of measured signal	Input signal	Local oscillator	Measurement mode
electronic noise + quantization noise (s_{el})	Vacuum (not connected)	OFF	1
s_{el} + shot noise (s_{shot})	Vacuum (not connected)	ON	2a
s_{el} + s_{shot} + test noise (s_{test_out})	s_{test_in} (input directly into receiver)	ON	2b
s_{el} + s_{shot} + service noise ($s_{service}$);	Service signals (trusted dark fibre or back-to-back)	ON	3a
s_{el} + s_{shot} + $s_{service}$ + s_{test_out}	s_{test_in} + service signals (trusted dark fibre or back-to-back)	ON	3b
s_{shot} + s_{sys} + QKD signal (s_{QKD}); system noise, s_{sys} = s_{el} + $s_{service}$ + operational noise ($s_{operation}$)	QKD signal + service signals (transmitter and receiver connected via trusted dark fibre or back-to-back)	ON	4a
s_{shot} + s_{sys} + s_{QKD} + s_{test_out}	QKD signal + service signals + s_{test_in} (transmitter and receiver connected via trusted dark fibre or back-to-back)	ON	4b
s_{shot} + s_{sys} + channel noise ($s_{channel}$) + eavesdropper noise (s_{Eve}) + s_{QKD}	QKD signal + service signals + classical traffic + Eve (operational mode)	ON	5

The mean variance of the measured signal is the mean of measured variances, where each variance is calculated from a volley of measured data. When stating a variance, the number of measurements within each volley, as well as the number of volleys, should be stated.

Electronic noise is generated by, e.g. the dark current of the photodiodes and electronic amplification of their output signals

Service noise is generated by the signals required to manage the CV-QKD link, e.g. synchronization and equalization signals, which might spill into the CV-QKD channel.

Operational noise is due to imperfections in the modulation and equalization of the CV-QKD signal, e.g. imperfections in the phase and phase noise compensation, amplification variation or clock skew.

Channel noise is used to describe the effect of non-QKD-related traffic in the optical channel generating signals in the optical passband of the receiver (e.g. by scattering processes such as Raman scattering). Channel noise is a property of the channel between Alice and Bob. It is the noise which is not present in a dark fibre.

The excess noise, ξ, is the estimated variance of all the noise signals at the receiver, minus the shot noise. For a strict security assumption, the total excess noise has to be assumed to be in the hands of Eve, although the actual eavesdropper noise, $s_{Eve,}$ might be smaller. Looser security assumptions, which assume that parts of the system noise cannot be attributed to Eve, have to be clearly stated. The calibrated and trusted part of the excess noise may be called calibrated excess noise, while the remainder may be called uncalibrated excess noise. For such a loose security assumption only the uncalibrated excess noise is assumed to be in the hands of Eve. The calibrated noise may be measured using modes 1, 2a, 3a and 4a of table 5.7.

The lower measurable bound for these noises is defined by the resolution and uncertainty of the measured values.

S_{test_in} is a calibrated noise source. The magnitude of this noise can be varied, and s_{test_out} is the measurement value at the receiver. This can be used (modes 2b, 3b, and 4b) to estimate the resolution and uncertainty of measurements (modes 2a, 3a, and 4a respectively) at the receiver.

A similar scheme can be used to analyse TLO CV-QKD systems. The main difference is that in the LLO scheme, the shot noise can be estimated directly.

Table 5.8: Parameters that can be used to specify a CV-QKD receiver and receiver channel

Parameter	Symbol	Units	Definition
Photon detection probability (Photon detection efficiency)	η η, PDE	Unitless (probability)	The probability that a photon incident at the optical input will be detected.
Temporal response indistinguishability	t_{ind}	Unitless	Indistinguishability of the temporal response of the two detectors used in a homodyne detection unit.
Supported modulation formats			
Bandwidth	BW	MHz	Employed detector bandwidth for QKD.
Detection scheme			See, for example, clause 5.2.
Supported signal-to-noise ratio	SNR_{min}	dB	Lowest supported signal-to-noise ratio of the quantum signal at the input of the receiver, not only for detecting a signal but also for generating a key. This should be supported by a sufficient error correction ability.
Total receiver loss	L_{RX}	dB	Combined losses of optics, photon detection efficiency, electrical and digital processing, etc. in the receiver.
Excess noise	ξ	SNU mSNU	Expressed in shot noise units or milli shot noise units. For single-quadrature homodyne detection this is normalized to the shot noise measurement variance [receiver]. For dual-quadrature homodyne detection and heterodyne detection this value has to be multiplied by 2 to express the excess noise in shot noise units [receiver channel].
Excess noise uncertainty	Δ_{ξ}	%	Measurement uncertainty of excess noise normalized to the measured excess noise. This should be supported by the number of samples used.
Excess noise stability	$f_{\Delta\xi}$	Hz	Maximum frequency of measured excess noise fluctuations. This should be supported by the estimated measurement uncertainty.
Shot noise	s_{shot}	W	Measured mean shot noise variance.
Shot noise uncertainty	Δ_{sn}	%	Measurement uncertainty of the shot noise normalized to the measured shot noise. This should be supported by the number of samples used.
Shot noise stability	$f_{\Delta sn}$	Hz	Maximum frequency of measured shot noise fluctuations. This should be supported by the estimated measurement uncertainty.
Electronic noise	s_{el}	SNU mSNU	The measurement procedure should follow the same steps as for the shot noise. Normalized to the measured shot noise, and expressed in shot noise units or milli shot noise units.
Electronic noise uncertainty	Δ_{el}	%	Measurement uncertainty of the electronic noise normalized to the measured electronic noise. This should be supported by the number of samples used.
Electronic noise stability	$f_{\Delta el}$	Hz	Maximum frequency of measured electronic noise fluctuations. This should be supported by the estimated measurement uncertainty.

6 QKD Source

6.1 Single-photon source

6.1.1 Generic Description and Parametrization

A QKD source emits light pulses upon which quantum information is encoded. A source suitable for QKD should possess a property such that the encoded quantum information can be recovered faithfully through quantum measurement only when the measurement and encoding basis are compatible. Quantum information can be encoded upon polarisation, phase and angular momentum.

An ideal QKD system would have a perfect single-photon sources that always emits exactly one photon in response to an applied trigger. In practice, however, single-photon sources have a single-photon efficiency less than unity and a finite probability of generating two or more photons. Experimental systems that have demonstrated single-photon emission include single atoms, single ions, and single defect sites in diamond and single quantum dots. Sources based on quantum dots are the best candidate to generate on-demand single photons at fibre wavelengths.

Figure 6.1 summarizes several different methods for generating polarisation-encoded single-photons in QKD. In an ideal system, a perfect single-photon source is used. In the weak pulse scheme, the photon source is an attenuated laser that obeys Poissonian photon number statistics. A heralded photon pair source is based on photon pair creation by spontaneous parametric down-conversion process (SPDC). Detection of one photon in the pair is used to indicate (herald) the existence of the second photon. Closely related to the heralded photon system, correlated or entangled photon QKD also uses pairs of photons for key distribution. Here the correlation between the polarisations of the two photons may be used to passively encode/determine the signal state.

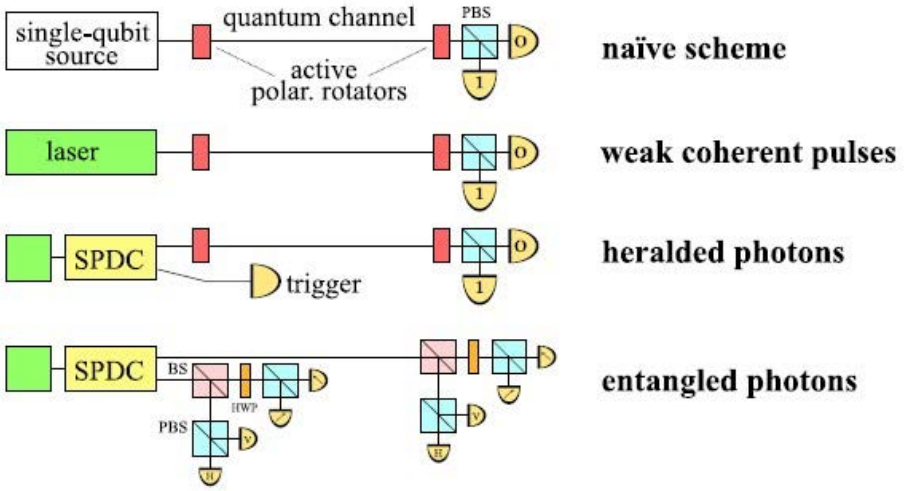


Figure 6.1: Several methods to generate photons for QKD

In figure 6.1, all the QKD sources just have a single light emitting element and are categorized as discrete. A QKD source can also consist of a number of light emitting elements. For example, in polarisation-encoded BB84, qubits of different polarisation can be prepared by different emitters, thus removing the need for further polarisation encoding. These types of sources are categorized as composite. Each composite source is made of a number of discrete light emitting elements.

A QKD light source should maintain indistinguishability for qubits in all degrees of freedom except that of the encoding. In other words, it should not be possible to discriminate between qubits through measurement of parameters other than the encoded freedom. For example, in the polarisation-encoding BB84 protocol, qubits in all four states should have exactly the same wavelength, temporal profile and arrival time, etc. Discrimination of these polarisation-encoded qubits can be made possible only through polarisation measurement. Indistinguishability is a necessary requirement to prevent information leakage through auxiliary measurements by an eavesdropper.

A QKD source should be specified by the source intensity (μ), defined as the average number of photons per clock cycle. For phase encoding BB84, this corresponds to twice the intensity of the phase encoded pulse. For polarisation-encoded BB84, this just corresponds to the intensity of the polarisation-encoded pulse.

A QKD source should be further specified by its photon number probability distribution, $p(n)$, defined as the probability distribution of having n photons per signal pulse. A conveniently measured parameter is the second order correlation function at $t_1 = t_2$, $g^{(2)}(0)$, defined as the rate of photon pairs compared to a Poissonian source of the same average intensity.

Table 6.1 lists the parameters that define the performance of a single-photon emitter. These parameters should be specified for a defined set of operating conditions, given in table 6.2. Table 6.3 lists additional attributes to be specified for the emitter.

Table 6.1: Parameters that can be used to specify a QKD photon source

Parameter	Symbol	Units	Definition
Optical pulse repetition rate	f_{source}	Hz	The frequency at which light pulses are emitted.
Photon number probability distribution	p(n)	Unitless	Probability distribution of having n photons in an optical pulse.
Mean photon number	μ	Photons/pulse	Average number of photons per signal pulse.
Mean source optical power	P_{mean}	W	Average optical power emitted during time of a QKD session.
Long-term power stability		dB/hr	Variation in source intensity over the duration of a QKD session, or some other stated time-interval.
Short-term power stability		dB	The variation in pulse intensity over a set period, e.g. 1 minute.
Number of emitters	$N_{emitters}$	Unitless	Number of light emitters that constitute a QKD source. $N_{emitters} = 1$ for a discrete source, while $N_{emitters} > 1$ for a composite source.
Second order correlation function	$g^{(2)}(0)$	Unitless	The second order correlation function at zero time delay $g^{(2)}(0)$ quantifies the photon number statistics. $g^{(2)}(0) = 1$ for a perfect coherent source, while $g^{(2)}(0) = 0$ for a perfect single-photon source.
Wavelength Spectral frequency	λ_{source} ν_{source}	nm Hz	Wavelength (or spectral frequency) of emitted photons.
Spectral linewidth	$\Delta\lambda$ $\Delta\nu$	nm Hz	Bandwidth of the emitted photons.
Emission temporal profile	$P_{emission}(t)$		The distribution of photons within emitted pulses as a function of temporal position. $P_{emission}(t) = J_{source} * P_{pulse}(t)$
Timing jitter	J_{source}	s	The uncertainty in the emission time of a single pulse at the optical output.
Temporal profile	$P_{pulse}(t)$		The intensity variation within a single pulse as a function of temporal position within the pulse.
Spectral indistinguishability	s^{ind}	Unitless	A quantity to quantify the extent to which two qubits can be distinguished through spectral measurement. $0 \leq s^{ind} \leq 1$. $s^{ind} = 0$ means a complete distinguishability between qubits, while $s^{ind} = 0$ means a complete indistinguishabilty.
Temporal indistinguishability	t^{ind}	Unitless	A quantity to quantify the extent to which two qubits can be distinguished through temporal measurement. $0 \leq t^{ind} \leq 1$. $t^{ind} = 0$ means a complete distinguishability between qubits, while $t^{ind} = 1$ means a complete indistinguishabilty.

Table 6.2: Operating conditions that should be specified for a QKD source

Operating Condition	Symbol	Units	Definition
Emitter Temperature	T	°C or K	Physical temperature of the emitting element during operation.
Environmental Requirement	N/A	N/A	The environmental conditions under which a detector module operates. These conditions include environmental temperature, humidity, pressure, and requirement for surrounding electromagnetic radiation.
Mode of Operation	N/A	N/A	Describes the condition upon which a QKD source emits an optical pulse. Two modes of operation are common: triggered and heralded.

Table 6.3: Additional attributes to be specified for a single-photon source

Parameter	Definition
Electrical input	Defines electrical input signals to the device along with the type of connector used. Input signals may be used for providing a trigger signal or as a power supply.
Optical output	Defines the format of the optical output from the device. Often this is through SM or MM optical fibre. The fibre connector should also be specified, e.g. FC/PC.
Electrical output	Defines the format of electrical output signal from the device upon photon emission, such as ECL, TTL, NIM, etc., as well as the type of connector, e.g. BNC, SMA. This output is compulsory for a heralded QKD source.
Physical dimensions	The physical size of a QKD source module that is independently operational.
Power consumption	Power consumption is the total power that is needed to continuously operate a QKD source.
Handling instructions	Instructions for the safe handling of the source, such as information regarding toxicity and the presence of high voltages.

6.1.2 True Single-Photon Sources

A true single-photon source is a quantum emitter which emits one and only photon upon an optical or electrical trigger as schematically shown in figure 6.2. To characterize such sources, source intensity, temporal profile, maximum operation frequency and wavelength should be specified. The value of the second order correlation function at zero time delay should be measured to specify the probability of a pulse containing more than one photon.

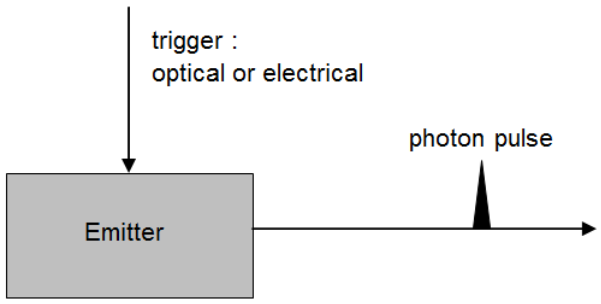
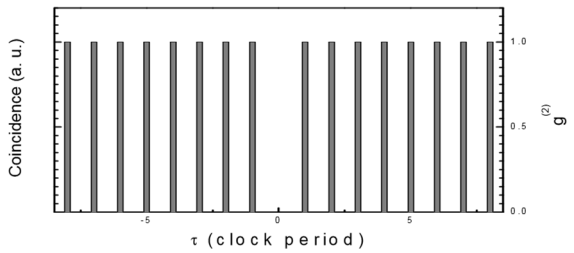


Figure 6.2: Schematic of a generic single-photon source

A perfect single-photon source has the property of $\mu = 1$ and $g^{(2)}(0) = 0$. For such source, a photon is emitted upon each trigger, and its correlation measurement will give a histogram shown in figure 6.3 where the coincidence at zero time intervals is absent.

Currently available single-photon sources are sub-Poissonian sources which have $\mu < 1$ and $g^{(2)}(0) < 1$. One example is the semiconductor quantum-dot-based single-photon source [i.27]. Figure 6.4 shows a correlation histogram for a quantum dot source that has suppressed correlation coincidence at zero time delay. A reduced rate of photon pairs can enhance the secure key generation rate of QKD.



NOTE: The coincidences at zero time delay should be strictly absent when the detector dark counts are excluded.

Figure 6.3: A correlation histogram expected from a perfect single-photon source

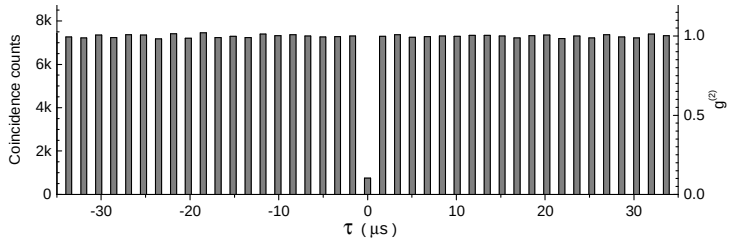


Figure 6.4: Correlation measurement for a quantum dot single-photon source

6.1.3 Weak Pulses

6.1.3.1 Weak Laser

Figure 6.5 depicts the simplest weak pulse source, which consists of a triggered laser, an attenuator, and a fixed ratio beamsplitter. In a QKD system, the encoding optics should be placed between the laser and the attenuator so that the attenuator can act as a defence against the so-called large pulse attack. This type of source is called a weak laser source. An intensity monitor which integrates the 'single-photon' signals over time, possessing the necessary sensitivity to determine the average optical power, can be incorporated after the attenuator.

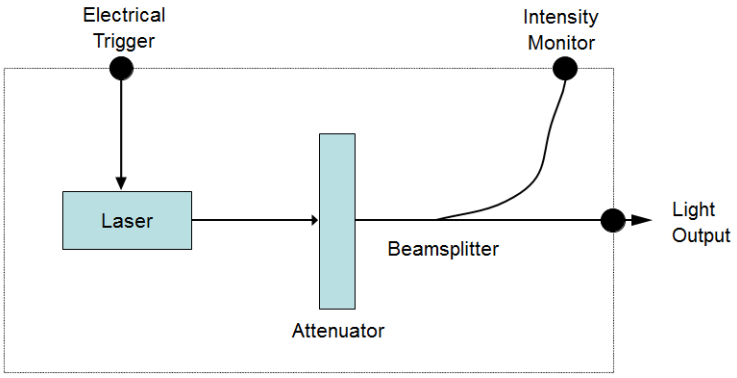


Figure 6.5: Schematic of an attenuated laser source

Indistinguishability is automatically fulfilled by an attenuated laser source, since all qubits are prepared by the same emitter and attenuator.

A Poissonian number distribution is generally assumed for a weak laser source. These Poissonian statistics have been applied in the QKD security analysis, particularly in practical decoy-state protocols. However, photon number statistics should be examined experimentally before application into security analysis. For example, semiconductor lasers can severely deviate from the Poissonian statistics when the diode is biased close to its lasing threshold [i.28].

6.1.3.2 Intensity-Modulated Weak Laser

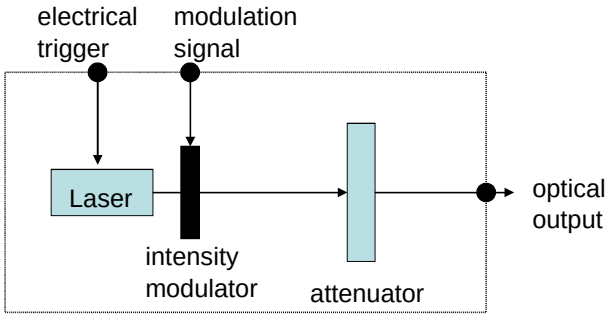


Figure 6.6: Schematic of a decoy source

Figure 6.6 shows an attenuated laser source which is intensity-modulated. An intensity-modulated source consists of a laser, intensity modulator and optical attenuator. Upon a trigger, this source emits a pulse with a distinctive intensity that is dependent on the modulation signal.

An intensity-modulated weak laser source is required in QKD protocols that require several groups of pulses that have distinct intensities. Decoy QKD protocols [i.29], [i.30] and [i.31] require Alice to randomly emit weak and vacuum pulses in order to detect and quantify the photon number splitting attack.

Like weak laser sources, indistinguishability is automatically maintained in both temporal and spectral domains for intensity-modulated weak sources. It is important that the intensity modulation does not distinguish the pulses in any way other than their intensity.

6.1.3.3 Phase-Coherent Weak Laser

In distributed-phase reference protocols, the laser source emits phase-coherent pulses.

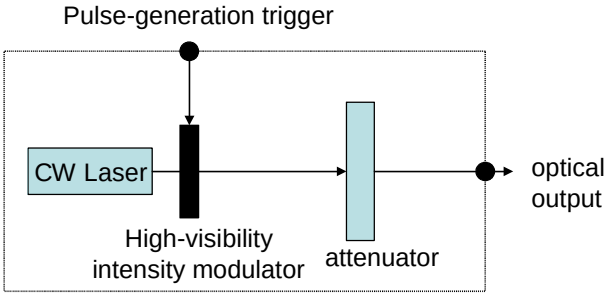


Figure 6.7: Schematic of a phase-coherent source

Figure 6.7 shows the principle of a phase-coherent source. The continuous-wave (CW) laser is modulated by the high-visibility optical modulator to generate the optical pulses. The long coherence time of the CW laser generates phase-coherent pulses. This source is required for distributed-phase reference protocols, such as the Differential Phase Shift (DPS) and the Coherent One-Way (COW) protocols.

6.1.3.4 Composite Weak Laser

A composite source is often used whenever there is difficulty in achieving fast encoding of qubit information. Instead, each qubit state is emitted by an individual light emitter. Use of a composite source can lead to a simpler encoder for the QKD transmitter.

Figure 6.8 depicts a composite source. In this source, an individual laser is used to set each state for the qubits. For example, for the polarisation encoded BB84 protocol, four lasers, emitting photons with -45º, 0, 45º and 90º polarisations respectively, can be used. The outputs of these individual lasers are then combined using a beam combiner and attenuated by an optical attenuator to the desired intensity levels. Upon an external trigger, only one laser fires; which one fires depends on the input switching signal.

To maintain indistinguishability, each emitter should be carefully tested to have identical wavelength, spectral profile, temporal profile, and photon number statistics. Wavelength and spectral profile can be made identical using a spectral filter. Temporal profiles should be measured.

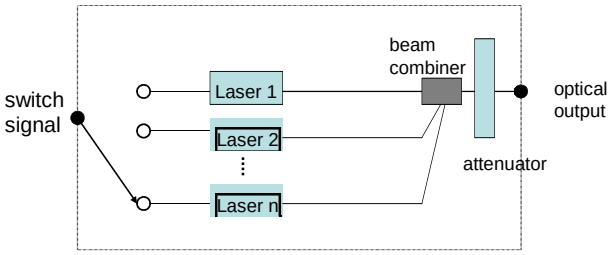


Figure 6.8: Schematic of a composite source

6.1.4 Entangled-photon sources

An entanglement-based QKD system requires the generation and distribution of entangled photon pairs. In this source, photon pair production is achieved by optically pumping a nonlinear media, as shown in Figure 6.9(a). This method is technologically mature, offers large conversion efficiencies and can be tailored to match wavelength requirements and spatial emission profiles. The optical excitation can be provided by a pulsed or continuous-wave laser. The two most widely-employed processes for generation are SPDC, a $\chi^{(2)}$ nonlinear process, where *one* pump photon decays into two photons called signal and idler and the four-wave-mixing process, requiring a $\chi^{(3)}$ nonlinearity, where *two* pump photons give rise to the generation of signal and idler photons.

Single pairs of polarisation entangled photons can also be emitted from a quantum emitter such as a quantum dot, optionally electrically excited within a light emitting diode.

Different schemes exist in order to entangle the photons of a generated photon pair. The most popular schemes are based on birefringent effects [i.32] or interferometric designs [i.33]. In those sources, one of the four maximally entangled bi-partite states, also called Bell states [i.32], is generated.

Apart from the actual generation mechanism of the entangled pairs, one should also distinguish between two possible locations of the source. The first configuration is the typical entanglement distribution case, where a source *between* Alice and Bob generates entangled pairs and transmits one photon to Alice and the other to Bob using two quantum channels, as depicted in figure 6.9(b). The communication parties collect, analyse and measure the photons and perform either the BBM92 or the E91 protocol with their detection events. In the other configuration, see figure 6.9(c), the source producing the entangled photons is located *within* Alice and only a single external channel connects the source to Bob. Alice is analysing and measuring her photons directly using single-photon detectors and since the state is entangled, Alice projects the other photon state depending on her measurement outcome. This scheme is very similar to a *prepare-and-measure* scheme, since Alice becomes a source of single photons, and the BBM92 protocol should be employed.

Many entangled sources are not true single entangled photon pair sources. For example in SPDC sources the emission of entangled pairs is probabilistic with the generation of multiple pairs of entangled states becoming increasingly likely if the probability of obtaining at least one entangled pair is increased. Correlations are however typically only found over the (short) coherence time of the photons [i.34].

Distinguishability in other degrees of freedom can be directly measured by either evaluating the interference visibility or by measuring the so-called S-parameter which indicates the degree of violation of a Bell inequality [i.35]. But even for the BBM92 protocol, it is normally sufficient to simply take the QBER as a measure since all distinguishabilities will lead to a loss of entanglement and hence a higher QBER. The potential information gain by Eve will be erased during the privacy amplification, the degree of which depends on the value of the QBER.

Many entanglement sources are fully passive apart from a pumping source. Modulators or quantum random number generators are not necessarily needed in either Bob or Alice, to select the bit and basis values. Therefore some entanglement schemes avoid elements that might require protection against Trojan horse attacks in some other schemes. Consideration of other attacks against an implementation, such as those against detectors, remains important.

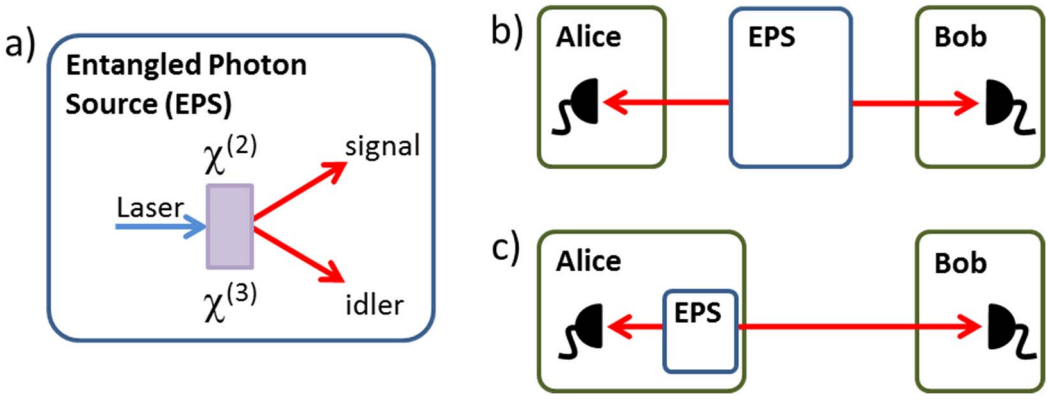


Figure 6.9: Schematic of an entanglement source (a) and possible distribution scenarios (b, c)

6.2 Continuous-Variable QKD Source

The setup of the source (transmitter) in the original CV-QKD TLO designs, i.e. multiplexing and transmitting the LO together with the quantum signal on the same fibre, is more complex compared to the design in which the LO is generated locally (LLO). The text below focusses solely on the modulation scheme.

The modulation of the quantum signal is very similar in both schemes. To generate coherent states an attenuated laser can be used for coherent state based, prepare-and-measure schemes. Earlier implementations of CV-QKD, preceding the GG02 protocol [i.52], have required a source of squeezed states utilizing CV-entanglement to introduce EPR type of correlations. The discussion here is limited to the transmission of coherent states, whereby the signal is modulated by inserting an amplitude modulator and a phase modulator into the signal channel and be attenuated accordingly (e.g. see figure 5.4(d)). Depending on the modulation scheme (Gaussian Modulation or Discrete Modulation, i.e. selection of discrete phase space points as coherent state's "centres" for PSK) the modulators should be steered correspondingly. The supporting electronics and the optical modulators should be chosen so that the excess noise is reduced as much as possible (e.g. to avoid modulation imperfections), as the excess noise can be exploited by an eavesdropper to retrieve information on the secret key. Then, in order to reach a quantum signal level, corresponding typically to amplitudes compatible with less than 5 photons per signal, the signals should be strongly attenuated, using an optical attenuator.

Table 6.4: Parameters that can be used to specify a CV-QKD transmitter

Parameter	Units	Definition
Bandwidth	Hz (MHz, GHz)	Range of frequencies in which the transmitted signal is sent
Modulation format		Type of modulation (QPSK, Gaussian…)
Synchronization/phase recovery signal type		Type of signal sent to synchronize the LO at the receiver (TLO, pilot tone…)
Multiplexing type of synchronization/phase recovery signal		E.g. polarization, frequency
Synchronization/phase recovery signal strength	dBm	The power of this signal
Synchronization/phase recovery signal strength range	dBm	The power range of this signal
Accuracy of the transmission power of synchronization/ phase recovery signal	%	The accuracy of this power
Accuracy of the transmission power of the quantum signal	%	The accuracy of this power

7 Modulators

Modulators are devices that can manipulate certain degrees of freedom of light by using a controlling signal. Figure 7.1 represents a generic description of an optical modulator.

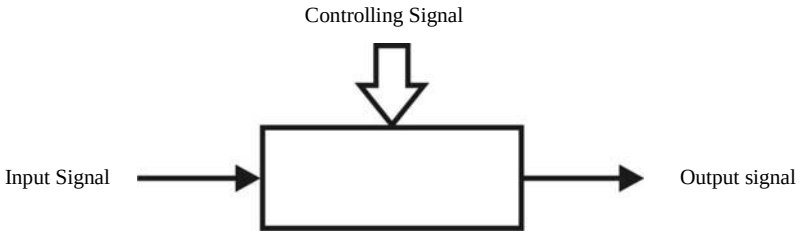
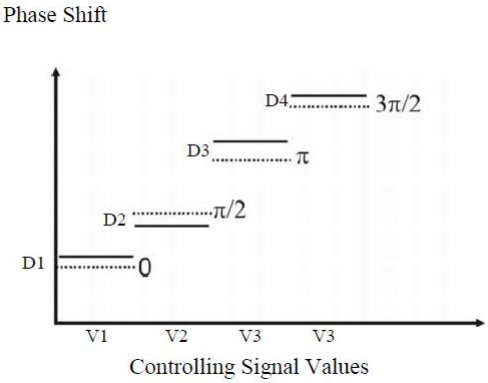


Figure 7.1: Schematic of a modulator

Usually in quantum cryptography, modulators are used to encode (transmit) or decode (receive) information but they can also be used as attenuating elements. Mainly, the degrees of freedom used as carriers of the quantum information when light is used as an input signal are polarization, relative phase, frequency or time-bin. The controlling signal employed to modify a particular degree of freedom of the Input Signal can vary continuously or discretely depending on the protocol used. For an idealized modulator only the selected degree of freedom of light is modified by the Controlling Signal. In real modulators, the controlling signal can modify other degrees of freedom of the light simultaneously. At the transmitter, correlations between different degrees of freedom have to be considered as potential threats (side channels). They should be either quantified in order to take them into account at the privacy amplification step, or cancelled to ensure the different states sent to the receiving unit can be distinguishable only through the selected degree of freedom. As an example, if the relative phase between pulses is used to encode information, for any chosen relative phase, output signals should have identical wavelength, spectral profile, temporal profile, polarisation and photon number statistics.

Additionally, deviations between targeted values and actual values of the controlled degree of freedom have to be determined and taken into account during the privacy amplification process. Figure 7.2 represents a typical deviation of a selected degree of freedom (phase) versus the values of the Controlling Signal.



NOTE: The dashed lines represent the ideal phase shifts 0, π/2, π, 3π/2 corresponding to the controlling signal values V1, V2, V3 and V4. The lines represent the actual phase shifts introduced. D1, D2, D3 and D4 represent the deviations between the ideal values and actual values of the phase shifts.

Figure 7.2: Simplified diagram of phase deviations

Table 7.1 lists the mandatory parameters defining the performance of a modulator for QKD. These parameters should be specified for a defined set of operating conditions, given in table 7.2.

Table 7.1: Parameters that can be used to specify a modulator

Parameter	Symbol	Units	Definition
Modulated degree of freedom	Mdf	N/A	The degree of freedom of light that is modulated. It could be the intensity, the phase, the polarisation or the wavelength.
Deviations	MaxDev	Depends on modulated degree of freedom	Maximal deviation values of the selected degree of freedom given targeted values.
Rise and Fall time	$t_{r/f}$	ns/μs	Rise (fall) time refers to the time required for the selected degree of freedom to change from a specified low (high) value to a specified high (low) value.
Optical robustness	Opr	dBm/W	The maximum illumination power that a modulator can accept without altering its parameters.

Table 7.2: Operating conditions that should be specified for a modulator

Operating Condition	Symbol	Units	Definition
Environmental Requirements	N/A	N/A	The environmental conditions under which a modulator operates. These include environmental temperature, humidity, pressure, and requirement for surrounding electromagnetic radiation.
Wavelength Range	λr	nm	Wavelength range in which specifications are valid.
Lifetime	N/A	N/A	Duration for which specifications are verified.

Annex A:
Discrete Variable Protocols

A.1 BB84

A.1.1 Basic protocol

In 1984, Bennett and Brassard showed that secure key distribution could be possible via quantum states [i.36]. This possibility was subsequently rigorously proved, for instance in [i.37] and [i.38]. In the original protocol, referred to as BB84, the use of a single-photon source is assumed. Bit information is encoded in four states in two non-orthogonal bases, where the two states in a basis have to be orthogonal, e.g. $|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Typical physical degrees of freedom used to encode the information are polarization or relative phase of a pair of pulses containing a single-photon in total. The sender has to choose a bit value and a basis at random for a transmitted single-photon pulse, requiring two random bits for each pulse. The modulated state is transmitted to the receiver through a quantum channel, where it is detected by a single-photon detector. To decode the bit information from a received pulse, the receiver selects a measurement basis at random from two bases, and takes note of the resulting bit value if it is obtained; if no photon is observed, the event is recorded as a non-detection event. After repeating this quantum communication many times, the sender and the receiver proceed to a sifting phase where they broadcast through an authenticated public channel all the bases ($Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+\rangle, |-\rangle\}$) employed in the quantum communication phase. The receiver also announces in which time slot the detection of a photon was observed. They keep only those bit values where a detection occurred and where the sender and the receiver chose the same basis. These bit values form a sifted key. After the sifting phase, they announce some information via an authenticated public channel about part of the sifted key to enable parameter estimation for selecting an appropriate error correcting code and a hash function for privacy amplification. Then, they use the code and the hash function to covert the remaining sifted key to the secret key. This key is information-theoretically secure, provided that the estimated QBER is lower than a threshold [i.37].

The BB84 protocol has also been extended to use six states in three bases to enhance the key generation rate, especially in the longer distance regime [i.39] and [i.40].

A.1.2 Refinements

A.1.2.1 State preparation - imperfections

For the sending device, the protocol assumes that the four states have to be perfectly prepared. For instance, two states in a basis have to be perfectly orthogonal, but in practice such a perfect state preparation is impossible due to inevitable noise in practical devices. The actually prepared states could deviate from the ideal states only slightly, but it turns out that even slight deviation results in significant decrease in the key generation rate. This problem was overcome by the loss-tolerant protocol [i.41] where basis mismatched events are also employed [i.42] for the parameter estimation, and the degradation of the key generation rate can be avoided.

A.1.2.2 Multi-photon emission

A.1.2.2.1 Security loophole

In practice, there is some probability for a source to emit multiple photons; this can be a security loophole from an eavesdropper who employs the photon number splitting (PNS) attack [i.43]. With this attack the eavesdropper can obtain perfect information from one of the multi-photons, which decreases the secure key generation rate drastically.

Since a perfect single-photon source is currently unavailable, a weak coherent laser source is commonly used to implement discrete variable (DV) QKD protocols. Such a source generates a pulse having a finite probability of multiple photons, and Eve can utilize this as follows: Eve intercepts one photon out of a weak coherent pulse in a multiple-photon state and stores it in her quantum memory so that she measures it with a publicly announced basis after sifting. Then, Eve can obtain identical bit information of Alice and Bob without causing errors.

The decoy state method [i.29], [i.30], [i.31] and the modified BB84 protocol, the SARG04 protocol [i.44], are candidates to solve this issue.

A.1.2.2.2 Decoy state method

The decoy state protocol, proposed by Hwang in 2003 and further studied by Wang and Lo-Ma-Chen [i.29], [i.30] and [i.31] overcomes the PNS attack by adding decoy states to the BB84 protocol. Decoy states have, in general, mean photon numbers different from original BB84 signal states. Alice and Bob monitor statistics of the decoy and signal states, and use the statistics to tightly estimate the fraction of the detection events caused by the single-photon emissions. This tighter estimation improves the performance of the original BB84 protocol in terms of transmission distance of secure keys. This is so because with this method, Alice and Bob do not have to assume the worst-case scenario that all the multi photons emitted by a source cause the detection events, and instead they can use the tightly estimated fraction.

A.1.2.2.3 SARG04

To mitigate a PNS attack, the SARG04 protocol [i.44] modifies the sifting process. Instead of directly revealing bases, Alice and Bob publicly announce one of the four pairs of non-orthogonal states consisting of $\{|0\rangle, |+\rangle\}$, $\{|0\rangle, |-\rangle\}$, $\{|1\rangle, |+\rangle\}$, and $\{|1\rangle, |-\rangle\}$.

The protocol works as follows: First, Alice chooses one of the four pairs and one of the two states in the pair and transmits it to Bob. Then, Bob performs a measurement with two bases $\{|0\rangle, |1\rangle\}$ or$\{|+\rangle, |-\rangle\}$. After that, sifting is performed for unambiguous discrimination between states in an announced pair. For example, assume Alice transmits $|0\rangle$ state in a set $\{|0\rangle, |+\rangle\}$ and Bob measures it with a basis$\{|+\rangle, |-\rangle\}$. If Bob measures $|+\rangle$ state, then it is discarded since it can be from $|0\rangle$ or$|+\rangle$. If Bob measures $|-\rangle$ state, then it is stored for post processing because it can be only from the $|0\rangle$ state.

Since two states in a set are non-orthogonal, the PNS attack cannot provide Eve with perfect information on the encoded bit.

A.2 Entanglement-based

A.2.1 Overview

Whereas many other QKD principles introduced here are asymmetric in the sense that one entity (station A, Alice) prepares a quantum state and the second entity (station B, Bob) performs measurements to yield quantum correlations, it is also possible to use entanglement to build up a QKD system. Thereby pairs of photons are generated in contrast to single-photons in the other schemes. Each entangled photon-pair is distributed between Alice and Bob, who independently measure the photon distributed and jointly form a secret key based on a series of measurements.

Two important families of entanglement-based protocols are described in clauses A.2.2 and A.2.3.

A.2.2 E91

The first protocol was given in [i.45]. The security could be guaranteed by an ongoing test of Bell's inequality to root out Eve's attack. The commonly-used version in experiments as well as proposed here are the CHSH-inequalities [i.35].

A.2.3 BBM92

The second protocol [i.46], adopts the conventional BB84 protocol. Instead of Alice preparing photons and Bob measuring, a third party generates entangled photon pairs. For each pair, one photon is sent to Alice while the other is sent to Bob. Alice and Bob perform their measurements, independent of each other, randomly using one of at least two non-compatible bases. By comparing the measurement bases, Alice and Bob can obtain correlated measurement results when using a common basis, from which a secret key can be distilled.

A.3 Distributed-phase reference protocols

A.3.1 Overview

In some QKD protocols, phase randomization of sending pulses is not required, as in distributed-phase-reference QKD protocols. One example is the differential phase shift (DPS) protocols. A second example is the Coherent One-Way (COW) protocol.

A.3.2 Differential phase shift (DPS)

Differential phase shift (DPS) QKD is the first example of the distributed-phase-reference QKD protocols. The original protocol [i.47] assumed the use of single-photon source. Later, a DPS protocol that exploits trains of coherent light pulses was proposed [i.48], enabling one to use a laser light source.

There are variant protocols for DPS QKD, and in any of such protocols, information is encoded in the relative phase between two pulses. To realize this encoding, Alice generates trains of pulses and applies phase modulations selected randomly to each pulse. To decode the information, Bob performs a measurement that can read out the relative phase and keeps the measurement outcome as the sifted bit. When Bob obtains a detection event of the incoming pulses, he announces the measurement setting he employed, i.e. he announces in which pair of the pulses he succeeded in reading out the relative phase, and Alice keeps the corresponding information as the sifted bit. Alice and Bob proceed to error correction of the sifted bits, and then they perform privacy amplification to generate a secret key.

In the original DPS QKD protocols, information is encoded in the relative phase between two adjacent pulses, and Bob employs a one-bit delay Mach-Zehnder interferometer. Note that the encoding and decoding method is not limited only to the one based on two adjacent pulses, but it can be the one based on any two pluses. For instance, as was proposed in [i.49], the information is encoded in the relative phase of a randomly selected pair of pulses. This protocol is called Round Robin DPS (RRDPS) protocol.

A.3.3 Coherent One-Way (COW)

Another example of a distributed-phase-reference QKD protocol is the Coherent One-Way (COW) QKD protocol, first introduced in [i.6]. An implementation is presented in [i.7], and a complete description of the protocol in [i.50].

In the COW protocol, presented in figure 4.5, each bit is encoded by sending a weak coherent pulse in one out of two possible time-bins, while the other time-bin contains ideally the vacuum. These states can be discriminated by a simple time-of-arrival measurement on each state. In addition, a third state called decoy sequence, with both time-bins containing weak coherent pulses is randomly prepared. As in distributed-phase reference QKD, the channel is monitored by measuring the coherence between pulses in two successive, non-empty time-bins, either within a bit when a decoy sequence was prepared, or across bit separation whenever corresponding sequences are prepared. The coherence measurement is performed by means of a fibre interferometer, where the imbalance between the two arms matches precisely the distance between the two pulses. The visibility of the interferometer provides the test parameter for eavesdropping. This additional measurement across bit separation largely reduces the advantages an eavesdropper could have due to PNS attacks. As a consequence, the optimal average number of photons which can be sent per qubit becomes independent of the fibre transmission, but dependent on the Quantum Bit Error Rate (QBER) of the time-bin detection, and of the visibility of the interferometer. The advantages of the COW protocol are that it allows implementation of a completely passive receiver without any active element for base choice, that there is no need for polarisation control, and that it requires only two detectors. In combination with low noise detectors, the COW protocol is especially advantageous for long or lossy fibres.

A.4 Measurement-Device Independent (MDI)

A.4.1 Overview

The security issue in detecting devices can be more serious than that of the sending device because the device for photon detection has to accept a signal sent down the optical channel, and Eve can exploit this to hack the system. A protocol called measurement device independent QKD [i.51] was proposed to overcome this issue, and remarkably, any imperfection and side-channel in the detectors can be overcome with this protocol.

Annex B:
Continuous Variable Protocols

B.1 Basic Protocols

B.1.1 Basic protocols

Several CV protocols make use of light pulses to encode the key, and this condition will be assumed in the remainder of this clause. Their specificity is to use light pulses with a few photons per pulse instead of single-photon pulses as well as coherent optical detection instead of photon counters. The states of light used in CV QKD are in general squeezed states or coherent states.

Discussion will be restricted to coherent state CV protocols that make use of a sequence of light pulses described by coherent states $|\, x + ip \,\rangle$. In the so-called GMCS (Gaussian modulated coherent state) CV-QKD protocol [i.52], the two quadratures of the signal pulse, x and p, are modulated independently according to a Gaussian distribution with mean zero and variance $V_A N_0$ where N_0 is the vacuum noise variance. Those coherent states are sent from the emitter, Alice, to the receiver, Bob, through a quantum channel. In most implementations of CV-QKD, the laser source used by Alice to generate signal states is also used to produce, at Alice, an intense phase reference pulse, called local oscillator (LO). At the receiver, signal and local oscillator interfere on a balanced shot noise limited coherent detection system. The simplest configuration makes use of homodyne detection. Choosing the phase of the local oscillator, Bob can choose at random to measure the x or p quadrature.

In CV QKD, even with a perfect detection and with no eavesdropper, Bob's measurements are always affected by the intrinsic quantum noise that adds to each quadrature measurement. Consequently, after the quantum transmission, Alice and Bob do not share identical quadrature measurements, but only correlated continuous variable data. Thus, CV QKD requires specific data processing to extract the secret keys from those correlated data. This makes an important difference in comparison with discrete variable QKD protocols for which Alice and Bob share identical data after sifting in the ideal case. Part of Alice and Bob's data, chosen at random, is revealed publicly in order to evaluate the parameters of the transmission channel. The remaining data is used to establish the secret key between Alice and Bob. Alice and Bob first perform a classical error correction. For example, they can use a multilevel decoding based on efficient, one-way low density parity check codes (LDPC). Then they proceed with privacy amplification to produce a secret key common to Alice and Bob on which Eve has no information.

Annex C:
Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Christopher J Chunnilall, National Physical Laboratory (NPL), United Kingdom

Other contributors:
Romain Alléaume, Institut Mines Telecom - Télécom ParisTech, France

Hans Brunner, Huawei Technologies Duesseldorf GmbH, Germany

Ivo Pietro Degiovanni, Istituto Nazionale di Ricerca Metrologica (INRIM), Italy

Chi-Hang Fred Fung, Huawei Technologies Duesseldorf GmbH, Germany

Marco Gramegna, Istituto Nazionale di Ricerca Metrologica (INRIM), Italy

Hannes Hübel, Austrian Institute of Technology (AIT), Austria

Bruno Huttner, ID Quantique SA (IDQ), Switzerland

Marco Lucamarini, Toshiba Research Europe Limited (TREL), United Kingdom

Momtchil Peev, Huawei Technologies Duesseldorf GmbH, Germany

Andreas Poppe, Huawei Technologies Duesseldorf GmbH, Germany

June-Koo Kevin Rhee, Qunion, South Korea

Alastair G Sinclair, National Physical Laboratory (NPL), United Kingdom

Kiyoshi Tamaki, Nippon Telegraph and Telephone Corporation (NTT), Japan

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

Yongseok Yoo, Qunion and SK Telecom, South Korea

Zhiliang L Yuan, Toshiba Research Europe Limited (TREL), United Kingdom

Annex D:
Change History

date	Version	Information about changes
October 2016	V0.0.1	Early Draft. First revision of ETSI GS QKD 003 V1.1.1 which was published in December 2012 Sections to be inserted are identified Sections to be deleted are identified Sections to be revised are identified Minor corrections
December 2016	V0.0.2	Updates to clauses 5.1 and 6.2 Updating of protocol clauses Restructuring of document to place protocols clauses in Appendices
May/June 2017	V0.0.3	Stable Draft Significant updates to clauses: 2.2 4.1, 4.2, 4.2.1, 4.2.1, 4.2.5, 4.4, 4.4.1, 4.4.2, 4.4.3 5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.4 6.1.3.3, 6.1.4, 6.2 B 1.1, B 1.2.1, B 1.2.2 and sub-clauses B.5.3 B 6.1 Other minor changes throughout document
November 2017	V0.0.4	Update to stable draft Significant changes to following clauses (and their sub-clauses): 2.2 3.1, 3.2, 3.3 4.3, 4.4 5.2 Appendices re-lettered Other minor changes throughout the document

History

Document history		
V1.1.1	December 2010	Publication as GS QKD 003
V2.1.1	March 2018	Publication