ETSI GS QKD 003 V1.1.1 (2010-12)

Group Specification

Quantum Key Distribution (QKD); Components and Internal Interfaces

Disclaimer

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

Reference

DGS/QKD-0003_CompInternInterf

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

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

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

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 must be identified that will subsequently be subject to standardisation. Furthermore, a catalogue of relevant requirements for interfaces between components must be established, to support the upcoming definition of internal interfaces.

2 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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

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 et al, Opt. Express 15, 8465 (2007).

[i.2] N Gisin et al, Rev.Mod. Phys. 74, 145 (2002).

[i.3] L.Duraffourg et al, Opt. Lett 26, 18 (2001).

[i.4] A. Ekert, Phys. Rev. Lett. 67, 661 (1991).

[i.5] J. Clauser et al., Phys. Rev. Lett. 23, 880-884 (1969).

[i.6] C. H. Bennett, G. Brassard and N. D. Mermin Phys. Rev. Lett. 68, 557 (1992).

[i.7] Fossier et al., New J. Phys. 11 045023 (2009.

[i.8] Leverrier & Grangier, Phys. Rev. Lett. 102, 180504 (2009).

[i.9] Dixon et al, Applied Physics Letters 94, 231113 (2009).

[i.10] Appl. Phys. Lett. 91, 041114 (2007).

[i.11] Lodewyck & Grangier, Phys. Rev. A 76, 022332 (2007).

[i.12] Fossier et al., J. Phys.: Atomic, Molecular and Optical Physics 42, 114014 (2009).

[i.13] Intallura et al., J. Opt. : Pure Appl. Opt. 11, 054005 (2009).

3 Definitions 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 exchange of classical information

Eve or eavesdropper: any adversary intending to intercept communication between Alice and Bob

intensity modulator: device that can actively set the intensity of an optical pulse that is passing through the modulator

phase modulator: device that can actively set the phase of a photon that is passing through the modulator

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

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 Abbreviations

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

AMZI	Asymmetric Mach-Zehnder Interferometer
APD	Avalanche PhotoDiode
BB84	QKD protocol published by Bennett and Brassard in 1984
BNC	Bayonet Neill-Concelman connector
CV	Continuous Variable
DC	direct current
ECL	Emitter Coupled Logic
LDPC	Low Density Parity Check codes
LO	Local Oscillator
NIM	Nuclear Instrumentation Module
PNS	Photon Number Splitting attack
QKD	Quantum Key Distribution
QND	Quantum Non Demolition
SM	Single Mode
SMA	Sub-Miniature version A connector
SPC	Single-Photon Counting
SPDC	Spontaneous Parametric Down-Conversion process
TTL	Transistor-Transistor Logic

4 QKD System Components

4.1 Generic Description

A QKD system is comprised of a number of internal components. The purpose of the present document is to identify the components which are common to many systems, to define the interfaces between these common components, to define how these components shall be characterised in a relevant and controlled manner and to define the component performance required for QKD.

A survey of the academic literature reveals that there have been many different types of QKD system proposed. Many of these have been implemented physically with different levels of sophistication. At the most basic level these systems utilise 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 bases or post-selection of the bases used. In QKD 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 categorising different types of QKD systems is according to the photon source that they use. Examples include single-photon sources, entangled photon pair sources and weak laser pulses. Common methods for encoding the qubit information include controlling the phase or the polarisation state of the transmitted photon.

A QKD system consists of two units which are physically separated at opposite ends of a communication channel as illustrated by figure 4.1. The sending unit consists of a signal source and an encoder for the source. The sending and receiving unit consist a source of randomness for use in the key generation protocol. The source of randomness can be either an active random number generator or a passive random selection component, such as a non-polarising beam splitter. The receiving unit consists of a component for signal demodulation, or in other words for selecting the measurement basis, as well as one or more signal detectors. Control electronics, with access to an independent random number generator, is necessary to generate the drive signals for these devices. The detected signals are used by the control electronics to form the shared key.

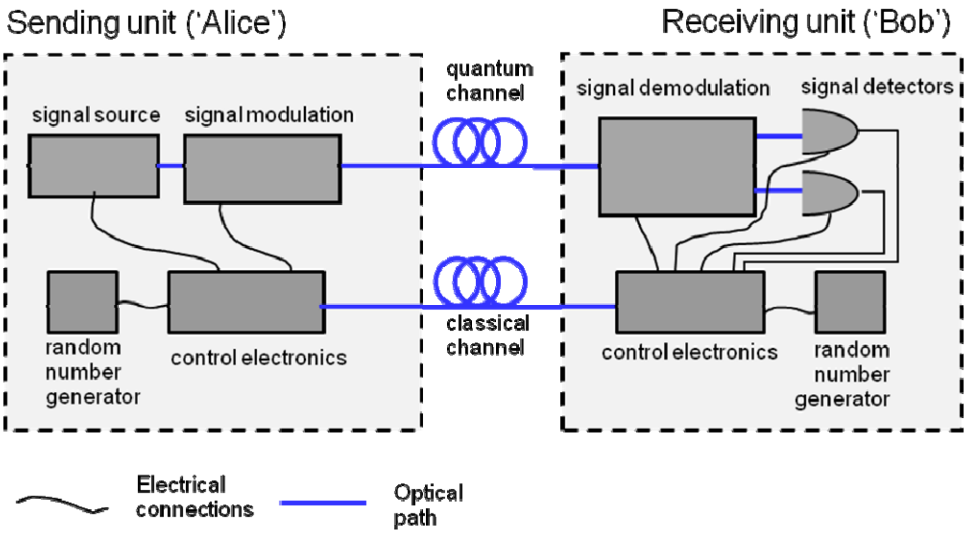


Figure 4.1: Schematic of a generic QKD system showing internal interfaces and connections

4.2 Weak Laser Pulse QKD

In weak laser pulse QKD, the bit values are encoded upon attenuated laser pulses. The sender (Alice) in a weak laser pulse QKD contains at least one weak laser pulse source that is used as quantum information carrier. In implementations involving more than one weak laser source, the sources must be indistinguishable from one another in every measurable attribute.

Alice shall consist also a quantum encoder that encodes qubit information on each weak laser pulse. This encoder shall have a source of randomness that determines an encoding basis and an encoding bit value for each weak pulse. The source of randomness shall come from either a random number generator or a passive optical component that acts as a source of randomness.

The photon number splitting attack must be appropriately included in the privacy amplification process in a QKD session. To achieve this, the intensity and photon number statistics of each weak laser source shall be carefully calibrated. The source stability shall also be calibrated. In the case that the source is instable, the worst case scenario shall be considered in the privacy amplification process.

In the following, we give a few example realizations of weak laser pulse QKD systems.

4.2.1 One-Way Mach-Zehnder Implementation

Figure 4.2 shows an example of a QKD system using weak laser pulses as the signal carriers and Asymmetric Mach-Zehnder Interferometers (AMZI) to encode the quantum states, based on the paper by J. F. Dynes et al, Opt. Express 15, 8465 (2007) [i.1]. The system shown uses the decoy pulse protocol to obtain higher secure bit rates than are otherwise possible using weak laser pulses. In one implementation, the transmitter source is a distributed feedback laser and emits a fixed intensity train of pulses at a repetition rate of 7,143 MHz. An intensity modulator is used to produce signal and decoy pulses of differing intensities. The vacuum decoy pulse is produced by omitting trigger pulses to the signal laser. All signal, decoy and vacuum pulses are produced at random times and have pre-determined relative occurrence probabilities assigned to them. The signal and decoy pulses are attenuated strongly to the single-photon level after which a much stronger clock pulse is wavelength division multiplexed with them to provide synchronization between Alice and Bob's electronics (not shown in figure 4.2).

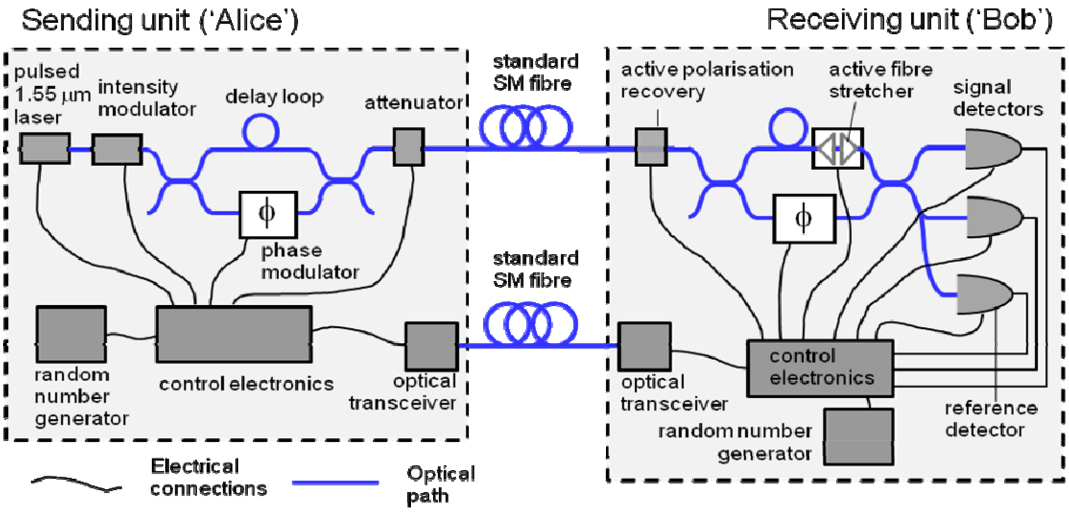


Figure 4.2: Schematic of a one-way, weak-laser-pulse QKD system

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

This system uses active stabilisation to lock the path difference in the sending and receiving AMZI. The pulsed 1 550 nm laser generates both weak signal pulses and a later, stronger reference pulses with a delay in one arm. Care must be taken to ensure that the reference pulses are not modulated by the phase modulator in the sending AMZI. Detection of the reference pulses in the reference detector is used to provide a feedback signal to vary the setting of the fibre stretcher in the receiving AMZI. A similar active stabilisation technique is used to control the polarisation state entering Bob's AMZI.

In this implementation, 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 naturally guaranteed. Use of an intensity modulator is required to implement the decoy QKD protocol. Alice's AMZI is the encoder. The standard Single Mode (SM) fibre is used as the quantum channel. In Bob, Combination of the active polarisation recovery, active fibre stretcher and AMZI forms the decoder.

The source of randomness arises from a random number generator in each control electronics.

4.2.2 Send and Return Mach Zehnder Implementation

Figure 4.3 depicts a typical send-and-return Mach-Zender architecture, described in detail in N Gisin et al, Rev.Mod. Phys. 74, 145 (2002) [i.2]. Pulses emitted from the source S are split in two pulses. The first pulse propagates along the short arm and launches in the quantum channel through a polarization splitter PS. The second pulse is delayed and its polarization is rotated using the polarisation rotator (PR) by 90 degrees and launched into the quantum channel via the same polarisation beam splitter. The phase shifter present in this long arm is left inactive. The polarization splitter PS allows launching the second pulse into the quantum channel. At the emitting unit, a beam splitter BS2 reflects a weak part of the incoming signals to a detector D3:

i) providing a timing signal; and

ii) preventing so-called Trojan horse attacks.

The transmitted pulses are then reflected by a Farady mirror (FM) to compensate any birefringence effects of the quantum channel. An attenuator (AT) allows reducing the intensity of the pulses to a suitably weak intensity (depending on the protocol used). A phase difference Φ1 is then introduced between the delayed pulses in order to encode a bit value. At the receiving unit, the pulses are separated by the polarization splitter PS and a phase Φ2 is applied to one of the two pulses to implement the measurement basis choice. Single-photon detectors D1 and D2 are then used to indicate which output port was chosen by the photon. A circulator C ensures the isolation between the laser source and the photon detectors.

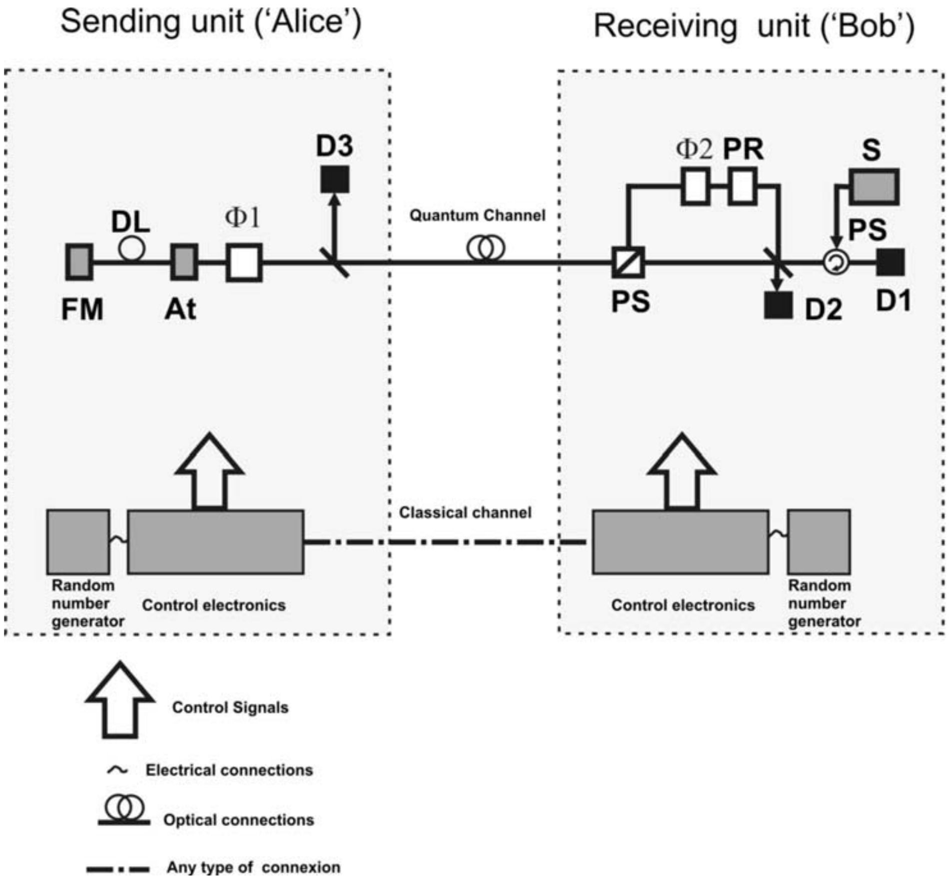


Figure 4.3: Plug and Play phase-intensity modulator system

4.2.3 Phase-Intensity Modulator Implementation

Figure 4.4 depicted a simplified Single Sideband (SSB) system, according to L.Duraffourg et al, Opt. Lett **26**, 18 (2001) [i.3]. 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 $\Omega << \omega_0$ 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 (synchronisation signal), operating at optical frequency ω_S, is then modulated at the same frequencyΩ. 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 Φ_1 *(0)* relative to the central peak. At the receiver, a WDM demultiplexer allows to separate the transmitted signals. The synchronisation 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 3λ / 4-optical path difference bias. When a phase shift Φ_2 is added to the electrical signal we can show 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 sideband 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 synchronisation 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.

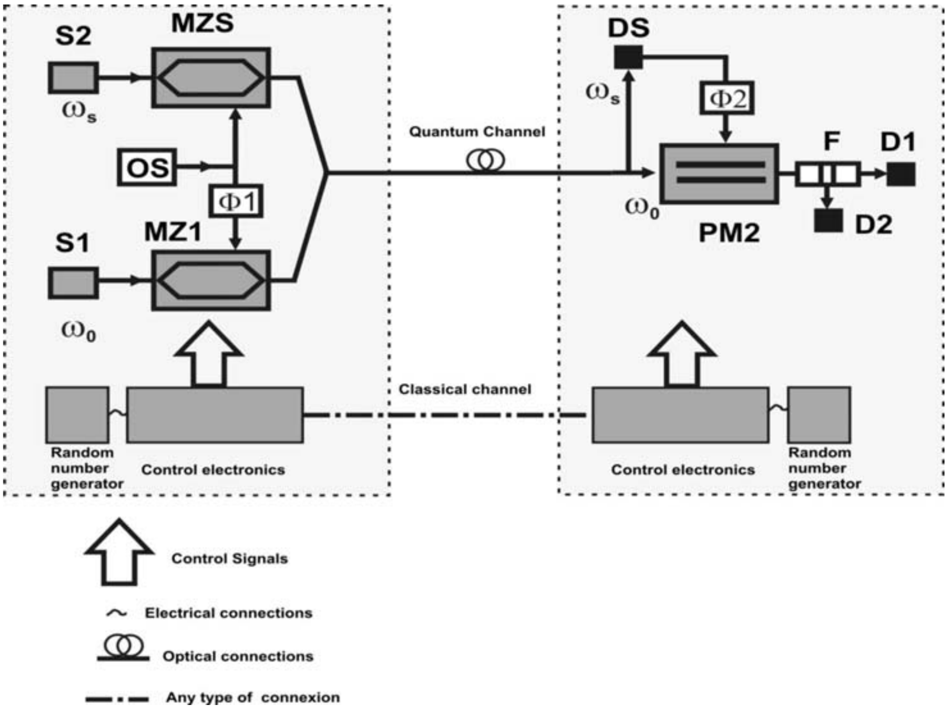


Figure 4.4: Schematic of a one-way, weak-laser-pulse Frequency domain QKD system

4.3 Entanglement-based QKD

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 exist:

1) The first protocol was given in A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991) [i.4]. 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 by J. Clauser *et al., Phys. Rev. Lett.* **23**, 880–884 (1969) [i.5].

2) The second protocol, suggested by C. H. Bennett, G. Brassard and N. D. Mermin *Phys. Rev. Lett.* **68,** 557 (1992) [i.6], adopts the conventional BB84 protocol. Instead of Alice preparing photons and Bob measuring, a third party generated 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 basis Alice and Bob can obtain correlated measurement results, from which a secret key can be distilled.

4.4 Continuous-Variable QKD

Most of QKD implementations are based on single photons or weak pulses for encoding qubits on the degree of polarization or phase. Alternativley, alternative protocols based on continuous variable (CV) can also be used for encoding qubits. For example, the two quadratures of a coherent state can be used as conjugate variables.

4.4.1 Principle of Continuous-Variable QKD Protocols

Several CV protocols make use of light pulses to encode the key, and we will assume this condition in the following. 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. Coherent state CV protocols make use of a sequence of light pulses described by coherent states $\left|x+ip\right\rangle$. The two quadratures x and p are modulated according to a two dimensions Gaussian distribution centred at ($x=0$, $p=0$) and with variance $V_A N_0$. N_0 is the quantum noise variance that occurs in the Heisenberg relation $\Delta x \Delta p \geq N_0$. Those coherent states are sent from the emitter, Alice, to the receiver, Bob, through a quantum channel at the same time as an intense phase reference called local oscillator (LO). At the receiver, signal and local oscillator interfere in a shot noise limited coherent detection. The simplest configuration makes use of homodyne detection. Choosing the phase of the local oscillator, Bob can choose at random x or p quadrature. It is particularly important to keep the symmetry between those to quadratures in order to prevent QND attacks (Quantum Non Demolition) where the eavesdropper, Eve, would not introduce any noise on the quadrature to be measured and would transfer all the noise on the quadrature that is not measured by Alice and Bob.

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 data. Thus, CV QKD requires an intensive data treatment 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 reconciliation 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 process a secret key common to Alice and Bob on which Eve has no information.

4.4.2 Implementation Example of the CV QKD protocol.

As presented in detail in Fossier *et al.*, *New J. Phys.* **11** 045023 (2009) [i.7], 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 4.5). 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, following a centred Gaussian distribution in both quadratures x and p, so that the variance of the Gaussian distribution reaches a target value of $V_A N_0$. It must 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 must be very careful with the security proofs Leverrier & Grangier, *Phys. Rev. Lett.* **102**, 180504 (2009) [i.8].

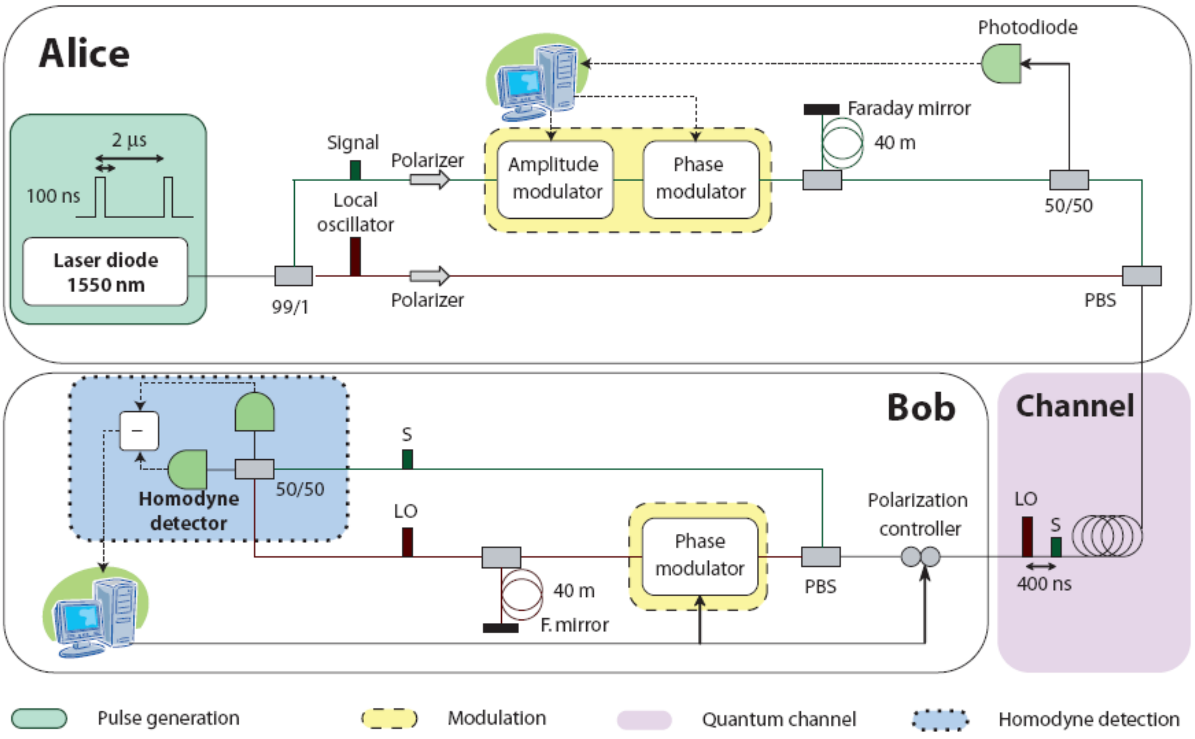


Figure 4.5: Scheme depicting the implementation of a coherent state CV QKD set-up

Time and polarization 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 undergone by the signal. The LO is then coupled with the signal in the transmission fibre, using a polarization beamsplitter (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.

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.

5 Photon Detector

5.1 Single-Photon Detector

5.1.1 Generic Description and Parameterisation

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.

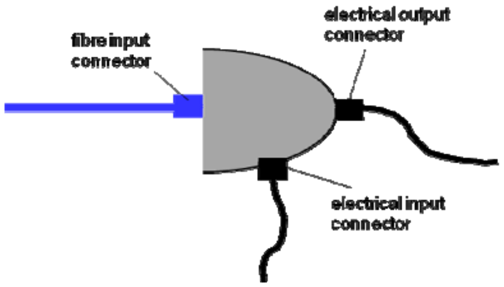


Figure 5.1: Schematic of a generic single-photon detector showing electrical and optical connections

In operation the detector is used 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 shall be characterised by a number of parameters, as described below.

The photon detection efficiency shall be defined as the probability that a photon incident at the input to the device will be detected. This parameter shall be defined for the external input to the device and shall not be adjusted for any losses occurring after the optical input. The photon detection efficiency shall not 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.

More generally the photon detection efficiency shall be defined as a function of the wavelength of the incident photon.

The uncertainty in deteremining the photon detection time shall be referred to as the timing jitter. The timing jitter shall be characterised as the full width half maximum (FWHM) in the distribution of detection times when the detector is incident with a pulsed laser, the pulse duration of which is shorter than the jitter determined.

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

Afterpulse are false counts which are secondary detection events triggered by previous photon detection events. The afterpulse probability shall be defined as the probability that a detector registers an afterpulse event, conditional on a true photon detection event.

Detection times of single photons shall be determined in QKD. The precision in the detection times shall be finer than the clock period of the QKD.

The dead time of the detector shall be defined as the smallest time duration after which the detection efficiency is independent of the previous photon detection history.

The recovery time shall be defined as the time duration after a photon detection event for the detection efficiency to return to 90 % of its steady-state value.

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

The maximum clock frequency shall be defined as the maximum clock frequency at or below which the detector can be operated in a QKD system.

Table 5.1 lists the parameters that define the performance of a single-photon detector. These parameters shall be specified for a defined set of operating conditions, given in table 5.2. Table 5.3 list additional attributed to be specified for the detector.

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

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

Parameter	Symbol	Units	Definition
Photon detection probability	η	Unitless (probability/gate)	The probability that a photon incident at the optical input will be detected within a detection gate.
Dark count probability	P_{dark}	Gated: Unitless (probability/gate) Free Running: ns^{-1} (probability/ns)	The probability that a detector registers a detection event per gate, despite the absence of optical illumination. For a free running detector this may be defined as the probability that a detector registers a detection event per ns, despite the absence of optical illumination.
Afterpulse probability	$P_{afterpulse}$	Gated : Unitless (probability/gate) Free Running: ns^{-1} (probability/ns)	The probability that a detector registers a false detection event in the absence of illumination, conditional on a true photon detection event in the preceding detection gate.
Dead time	T_{dead}	ns/μs	The smallest time duration after which the detection efficiency is independent of previous photon detection history.
Recovery Time	T_{rec}	ns/μs	The time duration after a photon detection event for the detection efficiency to return to 99 % of its steady-state value.
Maximum count rate	C_{max}	MHz/GHz	The maximum rate of photon detection events under strong illumination condition in the single/few photon/gate regime.
Timing jitter	t_{jitter}	ps/ns	The uncertainty in determining the arrival time of a photon at the optical input.
Photon number resolution	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.
Maximum clock frequency	F_{max}	MHz/GHz	The maximum clock frequency at or below which a detector can be operated in a QKD system without giving rise to an intolerable bit error rate.
Spectral Responsivity	R_s	unitless	The photon detection efficiency as a function of wavelength of the incident photons.

Table 5.2: Operating conditions that shall 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	MHz/GHz	The frequency of the gating signal applied to the detector, if operating in gated mode.
Gate Width	W	Volts	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 must overcome to be registered as a detection event.

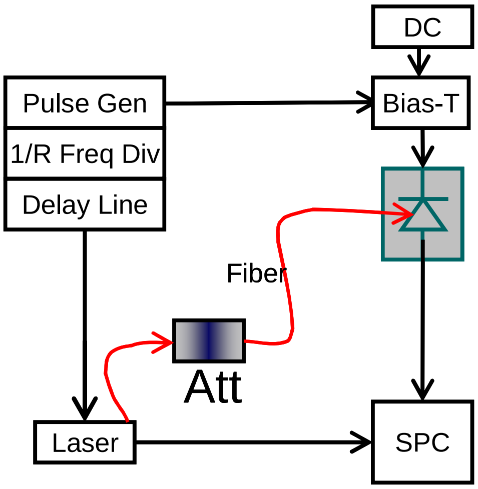
Table 5.3: Additional attributes to be specified for a single-photon detector

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 Test Measurements

This clause describes some of the measurements that shall be carried out in order to quantify the parameters defined above. Some of the parameters are straightforward to determine or do not need to be known to high accuracy, for example maximum count rate. Other parameters require specific measurement techniques. The most important parameters to specify for operation in a QKD system are the photon detection probability, dark count probability, afterpulse probability and the timing jitter. These parameters shall be determined using the test set up illustrated in figure 5.2 for a gated detector.

A pulse generator (Pulse Gen) shall be used to generate the ac gating bias. This shall be combined with a dc bias from a voltage source (DC) using a bias-T and is applied to the device under test. The pulse generator shall be used to trigger a laser diode that produces light pulses with ps duration that are used to illuminate the device. The frequency of the laser trigger shall be stepped down by a factor R ($R \geq 10$) compared to the detector gating bias using a frequency divider (Freq Div). An electrical delay line shall be used to ensure that the gate bias and optical pulse overlap temporally. The laser input to the device under test shall be attenuated with a programmable attenuator (Att) to the single-photon level. Time correlated single-photon counting (SPC) shall be used to record a histogram of time delays between the laser pulse and output pulses from the device under test. The attenuated laser intensity shall be described as n photons per illumination pulse on average.



NOTE: Pulse Gen: pulse generator that triggers the laser and gates the detector; Freq Div: frequency divider; Att: optical attenuator; and SPC: time-correlated photon counters.

Figure 5.2: A measurement setup that shall be used to measure photon detection probability, afterpulse probability, dark count probability and timing jitter

Under pulsed optical excitation, the time-correlated photon counter produces the histogram shown in the top panel of figure 5.3, in which the dominant peak at the zero-delay is due to detection of the optical excitation. The FWHM of this peak shall be taken as a measure of the timing jitter of the detector, provided that the measured value is considerably larger than the pulse duration of the exciting laser. The other peaks are due to dark and afterpulse counts in non-illuminated gates. A histogram recorded without illumination shall also be measured, as shown in the bottom panel of figure 5.3. In both cases the detected count rate shall be normalised to the total number of applied gates to form a detection probability, and the following parameters shall be extracted:

- P_i: probability of a detection event for each illuminated gate.
- $P_{n\text{-}i}$: probability of a detection event for each non-illuminated gate under optical excitation.
- P_d: probability of a detection event for each gate under no optical excitation.

Based on these parameters, the calibrated photon flux (n), the frequency ratio (R) of the gating to the illumination or the frequency division ratio, the following parameters can be calculated:

- $P_{afterpulse} = \dfrac{P_{n-i} - P_d}{P_i - P_{n-i}} \cdot R$: the afterpulse probability.
- $\eta = \dfrac{P_i - P_d}{n} \cdot \dfrac{1}{1 + P_{afterpulse}}$: the photon detection probability.
- $P_{dark} = P_d$: the dark count probability.

These parameters will depend upon the clock frequency and the photon wavelength. They shall be measured for each clock frequency and wavelength at which the detector will be used.

The precision of the measurements depends on the calibration of the intensity of the optical source. The intensity of the optical source shall be calibrated using a trustworthy and traceable standard. However, as single-photon level calibration standard is not available commercially at this time, an acceptable solution shall be to calibrate the source and attenuator at high laser power. It is then possible to attenuate the high power source down to single-photon level.

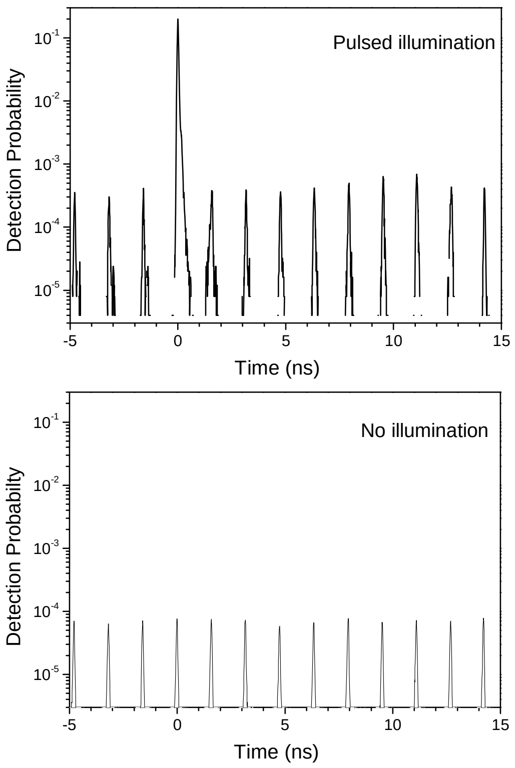


Figure 5.3: Count arrival histograms measured using pulsed illumination (top panel) and without illumination (bottom panel)

The detector dead time is another important parameter for a single-photon detector. This parameter shall be characterised using the set up shown schematically in figure 5.4. Two optical pulses with equal intensities and a tuneable temporal separation Δt shall be used to illuminate a detector under test. The dead time shall be determined as the smallest Δt, with which the detection probability of pulse 2 is independent of the detection outcome of pulse 1. A detailed description of this method can be found in Dixon et al, *Applied Physics Letters* **94**, 231113 (2009) [i.9].

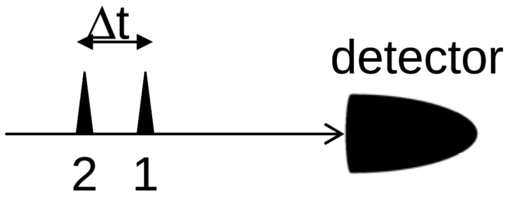


Figure 5.4: Schematic of a set up to characterise the detector dead time

5.1.3 InGaAs Avalanche Photodiodes

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

Table 5.4 displays the typical performance of an InGaAs APD operated in gated Geiger mode with a gating frequency of 7 MHz and a device temperature of -30 ^{o}C. InGaAs APDs with parameters similar to those in table 5.4 have been used in several QKD experiments and prototypes J F Dynes *et al.*, Optics Express **15**, 8465 (2007) [i.1].

One of the main limitations of the InGaAs APD 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 afterpulse to an acceptable level of a few percent.

Afterpulses occur because some of the avalanche carriers can be trapped on defects within the semiconductor. If a trapped carrier is released during a subsequent gate it can trigger a second spurious avalanche (an afterpulse). To reduce the afterpulse 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 to around 10 MHz, a dead time of up to 10 µs is often required to suppress the total afterpulse probability.

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 afterpulse probability at high gating frequencies dramatically and to a level that is tolerable for QKD.

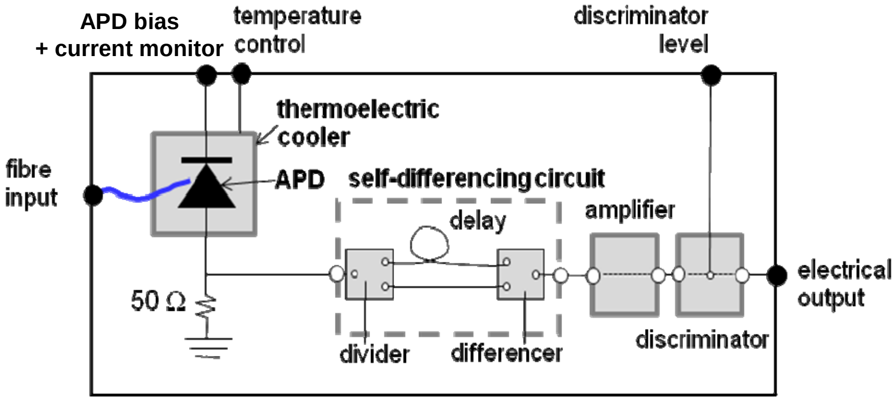


Figure 5.5: Schematic of a single-photon detector based on a self-differencing avalanche photodiode

Figure 5.5 shows a schematic for a self-differencing APD setup. The APD 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 APD 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 APD's breakdown voltage, while the amplitude of the square wave varies from 3 V to 12 V. The APD output is sensed on a 50 Ω serial resistor as a voltage signal.

The high gating frequency and finite capacitance of the APD results in a strong capacitive component in the output signal from the APD. 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 APD 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.

To detect blinding attacks using bright light illumination, the photocurrent flowing through the APD shall be monitored constantly. Photocurrent shall be monitored in the DC path of the APD bias, as shown in figure 5.5. The photocurrent shall be monitored to ensure that the APD operates under single-photon counting regime. In the single photon counting regime, the photocurrent is equal to the product of the photon count rate and the avalanche gain. A photocurrent with an anomalously high values shall be treated as an indication of a possible detector blinding attack and the system must not be used to acquire secure key until the photocurrent returns to the expected value. Table 5.4 lists typical parameters determined for self-differencing InGaAs APDs.

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

Parameter	Geiger Mode InGaAs APD	InGaAs SD-APD
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 %
Afterpulse probability	2 %	6,2 %
Dark count probability	7 x 10^{-5} per gate	2,34 x 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	Optics Express **15**, 8465 (2007)	Appl. Phys. Lett. **91**, 041114 (2007) [i.10]

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 allows to retrieve the two quadratures of an incoming light pulse. The detection shall be limited by the intrinsic quantum noise of the incoming light pulse and not by any other noise source such as electronic noise of the subsequent amplifiers. In case of an incoming coherent state (including vacuum), the detection shall be shot-noise limited. The coherent detection shall coherently combine an intense reference pulse called local oscillator and a weak signal pulse called signal. The phase relation between both of them shall be preserved.

The two pulses shall be mixed with a balanced optical coupler. An optical coupler combines two input optical pulses to produce two output optical pulses in a given proportion of the input pulses. In a balanced optical coupler, the output pulses should contain, as much as possible, equal parts of the input pulses (50/50 coupling factor). The signal and local oscillator shall be coupled to each of the two inputs of the 50/50 coupler. Each of the two output ports of the coupler shall be coupled to a photodiode. The photodiodes shall produce an electric signal proportional to the intensity of the incoming light pulse. The resulting photocurrents shall 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. The phase of the local oscillator 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 the incoming signal quantum state.

In practice, the electrical subtraction shall be balanced match as much as possible. The two photodiodes shall be paired. Their quantum efficiencies and time-response should as close as possible. The quantum efficiency is the probability that an incoming photon is detected. Therefore, the common mode rejection ratio shall be made as high as possible. This makes other electrical signals resulting from the local oscillator negligible. As an example, if the local oscillator is 10^8 more intense than the signal, then the overall balancing of the coherent detection should be better then 10^{-4}.

A properly balanced coherent detection shall be able to retrieve an electrical signal proportional to the phase and amplitude of the incoming signal pulse. An electronic amplifying chain shall be used to amplify the signal from the photodiodes. It shall be able to integrate the total intensity present in a pulse, and to resolve consecutive pulses. The electronic bandwidth shall be chosen accordingly. In order to be usable in a quantum optics set-up, the detection shall be limited by the intrinsic noise of the incoming light pulse (shot-noise in the case of a coherent state) and all other noise sources shall 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 pulse. Increasing the intensity of the local oscillator makes the electrical signal arbitrarily higher than the electronics noise. 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 allow useful signal levels of 20 dB above the electronics noise. This is enough to state that the electronics noise is negligible and to guarantee a set-up working in the quantum regime.

5.2.2 Multiplexing

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. This multiplexing can be made in time and in polarisation, for example. In this case, the receiver set-up shall be able to demultiplex both pulses introducing minimal additional noise to the signal pulse. Demultiplexing means that the signal and oscillator pulses shall be 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, this does not prevent the operation of the set-up (figure 4.5).

In case of polarisation multiplexing, the local oscillator and signal pulse shall have orthogonal polarisation states when travelling into the transmission channel. At the receiver, the initial polarisation states of the pulses shall be recovered. This can be done using an active polarisation controller system. The two pulses shall then be separated with a polarisation beamsplitter. As a result the local oscillator and signal pulses can be sent to two separated channels.

Once the local oscillator pulse and signal pulse are de-multiplexed, they shall be synchronized in order to arrive at 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 shall be matched to the time separation between the signal and local oscillator pulse.

5.2.3 Homodyne Detection

In a homodyne detection set-up, only one coherent detection is used to measure both quadratures of an incoming quantum state. The coherent detection projects the incoming signal on the quadrature corresponding to the phase of the local oscillator reference. Therefore, homodyne detection shall be able to change that phase reference in order select any quadrature of the signal quantum state. This can be obtained inserting a phase modulator on the optical fibre carrying the local oscillator pulse after demultiplexing. Therefore homodyne detection is mainly the combination of a coherent detection as described above with phase control of the local oscillator.

5.2.4 Heterodyne Detection

In a heterodyne detection, the incoming signal pulse is divided into two parts of equal intensity thanks to a 50/50 beamplitter inserted on the signal channel after demultiplexing. The resulting pulses are used to measure two orthogonal quadratures of the incoming quantum state. This is performed with two coherent detections where the two local oscillators have a $\pi/2$ phase difference. The heterodyne detection does not require an additional phase modulator on the local oscillator channel. It allows a simultaneous measurement of both quadratures of the incoming state at the price of an additional one shot-noise unit introduced by the beamsplitter. For some configurations, heterodyne detection can be advantageous over heterodyne detection Lodewyck & Grangier, *Phys. Rev. A* **76**, 022332 (2007) [i.11]; Fossier *et al.*, *J. Phys.: Atomic, Molecular and Optical Physics* **42,** 114014 (2009) [i.12].

6 QKD Source

6.1 Generic Description and Parameterisation

A QKD source emits light pulses upon which quantum information is encoded. A source suitable for QKD shall 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 source 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, 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 summarises 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 polarisation of the two photons may be used to passively encode/determine the signal state.

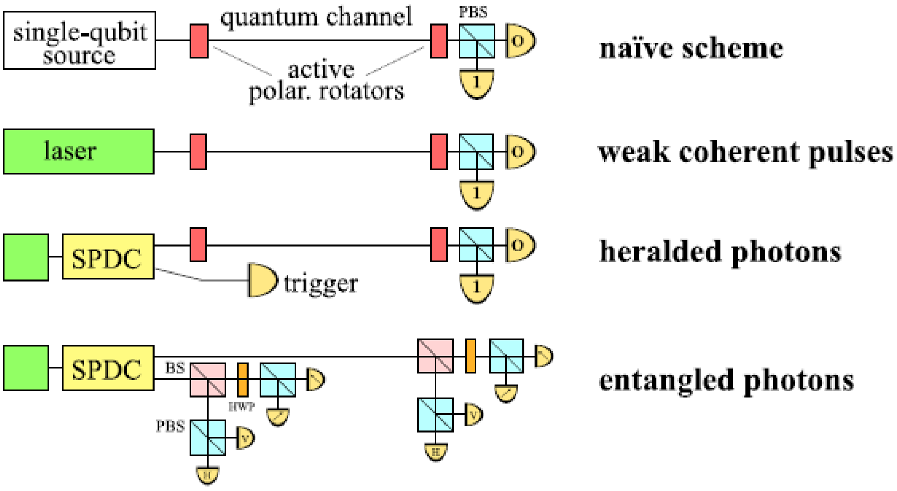


Figure 6.1: Several principles to generate photons for QKD

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 consists 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 shall maintain indistinguishability for qubits in all degrees of freedom except that of the encoding. In other words, it shall 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 shall 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 shall 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 shall be further specified by its photon number distribution, P(n), defined as occurrence probability of having n photons per signal pulse. A conveniently measured parameter is the second order correlation function $g^{(2)}(0)$, 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 shall be specified for a defined set of operating conditions, given in table 6.2. Table 6.3 list additional attributed to be specified for the emitter.

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

Parameter	Symbol	Units	Definition
Clock frequency	f	Hz	The frequency at which light pulses are emitted.
Source intensity	μ	Photons/pulse	Average number of photons per signal pulse
Number of emitters	N	Unitless	Number of light emitters that constitute a QKD source. N = 1 for a discrete source, while N>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	λ	nm	Wavelength of photons that are emitted.
Spectral linewidth	δ	Nm	Bandwidth of the emitted photons by a QKD source. δ is quantifiable using the full width at the half maximum in the emission spectrum.
Timing jitter	t_{jitter}	ps/ns	The uncertainty in the emission time of a photon at the optical output.
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 shall 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 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 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 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 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.

6.2 Test Measurements

As discussed above, the most important parameters to specify a light source for operation in a QKD system are the indistinguishability and photon number distribution. In this clause we describe how these shall be determined.

In QKD, an optical pulse is used to represent a qubit. Apart from the encoding degree of freedom, these optical qubits must be indistinguishable in all other degrees of freedom, such as wavelength, spectral width and temporal profile etc. Distinguishability in the non-encoding degree of freedom can therefore act as a side-channel, through which an eavesdropper can gain information. In particular, for QKD systems that use a composite source, each light emitting element shall be tested to quantify distinguishability among elements.

Indistinguishabilty tests shall include spectral, temporal, and other possible physical properties associated with the encoding process. Parameters, such as spectral indistinguishability s^{ind} or temporal indinguishability t^{ind}, shall be used for quantification.

Spectral indistinguishability s^{ind} quantifies the extent to which two qubits can be distinguished through spectral measurements. Figure 6.2 shows probability distributions in wavelength of a photon for two different qubits A, B. $\int_\lambda p^A(\lambda)d\lambda = \int_\lambda p^B(\lambda)d\lambda = 1$. Mathematically, s^{ind} shall be defined as:

$$s^{ind} = 1 - \frac{1}{2}\int_\lambda \left| p^A(\lambda) - p^B(\lambda) \right| d\lambda .$$

For indistinguishable qubits, $p^A \equiv p^B$ and therefore $s^{ind} = 1$. For the opposite case, *i.e.*, spectrally distinguishable qubits, $s^{ind} = 0$, because $\left| p^A - p^B \right| = p^A + p^B$. A QKD source shall be specify with s^{ind} values for all combination of a pair of different qubits.

Similar to the spectral indistinguishability, temporal indistinguishability t^{ind} shall be defined. Let p^A(t), and p^B(t) be the probability distributions of the time for qubits A and B respectively. $\int_t p^A(t)dt = \int_t p^B(t)dt = 1$. Temporal indistinguishability t^{ind} shall be defined as

$$t^{ind} = 1 - \frac{1}{2}\int_t \left| p^A(t) - p^B(t) \right| dt .$$

Again, $t^{ind} = 1$ represents temporal indistinguishabilty while $t^{ind} = 0$ means temporal distinguishability.

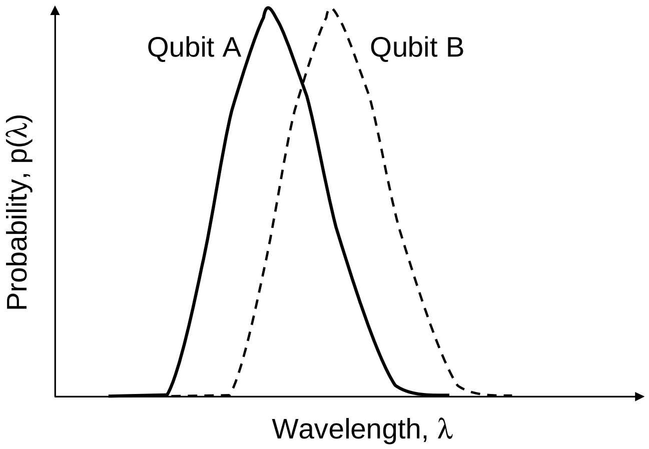


Figure 6.2: Probability distributions in wavelength for photons encoded with qubit A or B

Photon number distribution tests shall include (1) source intensity, (2) source stability and (3) the photon number statistics.

Source intensity, defined as the average number of photons per signal pulse (μ) when leaving Alice's apparatus, shall be measured over a duration that is comparable to a QKD session. Calibrated photon detectors shall be used. In case of single-photon sources, single-photon detectors shall be used. For attenuated laser sources, source intensity shall be determined by measurement of the unattenuated laser and calibration of the attenuation.

Source stability shall be tested continuously at least for a 24-hour period under ambient conditions that are specified by the QKD system. Source intensity bounds shall be given through this test, and the worst-case scenario shall be considered in the QKD security analysis.

Photon number statistics shall be measured using a Hanbury-Brown and Twiss setup as shown in figure 6.3. In this setup, a source under test is fed into a beam splitter with each output monitored by a single-photon detector. The photon arrival times are analyzed using a time-interval analyser.

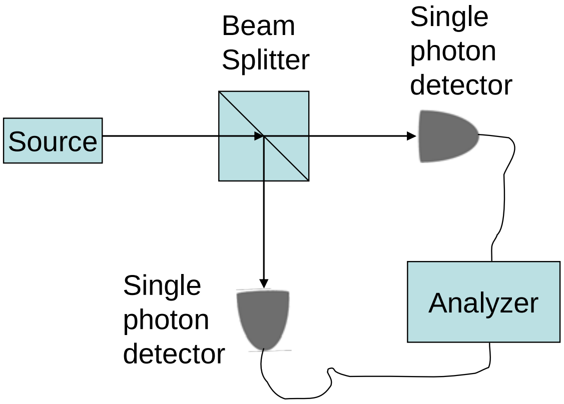


Figure 6.3: A Hanbury-Brown and Twiss setup for measurement of the second order correlation function

Figure 6.4 shows a correlation spectrum that can be obtained by the setup of figure 6.3 for a pulsed optical source. In this correlation spectrum, coincidence count rate is plotted as a function of the time interval τ between detection events by two single-photon detectors. For a Poissonian source, coincidence peaks at each interval should have identical height, within experimental uncertainties. By normalising the coincidence rates to the average rate at non-zero time intervals, the value for the second order correlation function is readily obtainable. As shown by the example in figure 6.6, $g^{(2)}(0)$, the value of the second order correlation function at zero time interval, is 1.0. This is characteristic of all sources obeying Poissonian statistics. For a true single-photon source, $g^{(2)}(0) = 0$. In simple terms, $g^{(2)}(0)$ indicates the probability of finding two photons within an optical pulse as compared to a Poissonian source of the same average intensity.

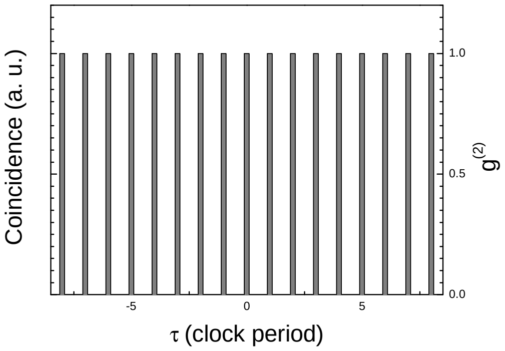


Figure 6.4: An example correlation spectrum that can be measured using the setup shown in figure 6.3

The experimental setup is suitable for sources that have an intensity μ<<1. For strong sources, an attenuator shall be used to reduce the intensity for calibration.

The measurement shall be sufficiently long so that uncertainty in the coincidence count rates shall be less than 10^{-3} for non-zero time intervals.

6.3 Single-Photon Sources

A single-photon source is a quantum emitter which emits one and only photon upon an optical or electrical trigger as schematically shown in figure 6.5. To characterise such sources, source intensity, temporal profile, maximum operation frequency and wavelength must be specified. The value of the second order correlation function at zero time delay shall be measured to specify the probability of a pulse containing more than one photon.

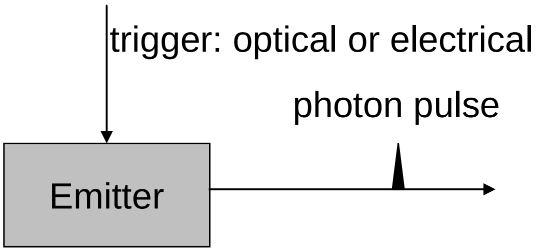
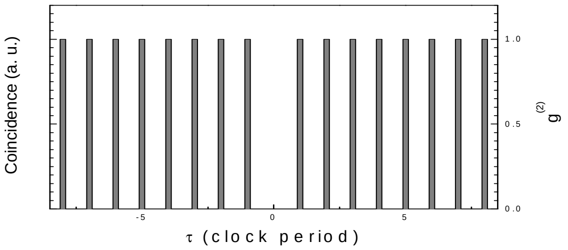


Figure 6.5: Schematic of a generic single-photon source

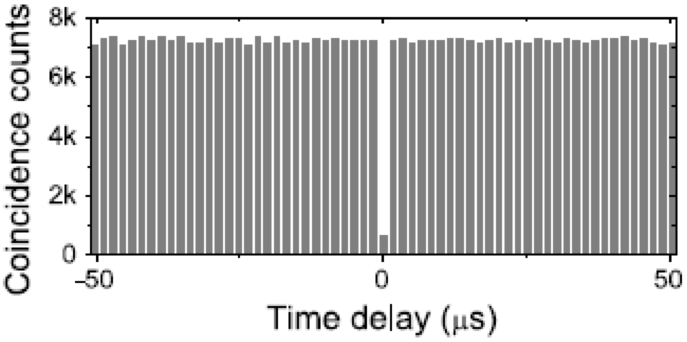
A perfect single-photon source shall have the property of $\mu = 1$ and $g^{(2)}(0) = 0$. For such source, a photon is emitted upon each trigger, and its correlation measurement shall give a spectrum shown in figure 6.6 where the coincidence at zero time intervals is absent.

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 quantum photon source. Figure 6.7 shows a quantum dot source that has suppressed correlation coincidence at zero time delay. A reduced rate of photon pairs can enhance the security of QKD.



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

Figure 6.6: A correlation spectrum that a perfect single-photon source shall look like



NOTE: See Intallura *et al*., J. Opt. : Pure Appl. Opt. 11, 054005 (2009) [i.13].

Figure 6.7: Correlation measurement for a quantum dot photon source

6.4 Weak Pulses

6.4.1 Weak Laser

Figure 6.8 depicts the simplest weak pulse source, which consists of a triggered laser, a fixed ratio beam splitter, and optical attenuator. In a QKD system, the encoding optics shall 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 weak laser.

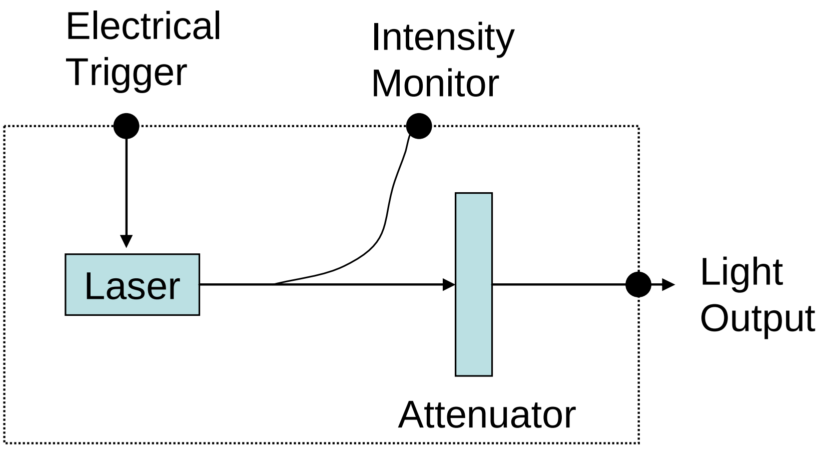


Figure 6.8: Schematic of an attenuated laser source

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

For determining the source intensity, the laser output power and the optical attenuator shall be calibrated separately using a calibrated optical powermeter. In particular, the laser output power shall be measured at Alice's exit port with the attenuator set to its minimum attenuation (0 dB). The source intensity shall be calculated using

$$\mu = \frac{P}{f \cdot hc/\lambda} \cdot 10^{-A/10},$$

Where P is the optical output power of the laser (Watt), f clock frequency (Hz), hc/λ the photon energy (J), and A is the optical attenuation (dB) set by the optical attenuator.

The laser output power shall be constantly monitored through the intensity monitor port using an optical power meter, and the attenuator or the electrical signal applied to the laser shall be adjustable to maintain a constant output power.

A Poissonian number distribution is generally assumed for a weak laser source. This Poissonian statistics have been applied in the QKD security analysis, particularly in practical decoy-state protocols. However, photon number statistics shall 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 [Dixon et al, Appl. Phys. Lett. **94**, 231113 (2009)].

6.4.2 Intensity-Modulated Weak Laser

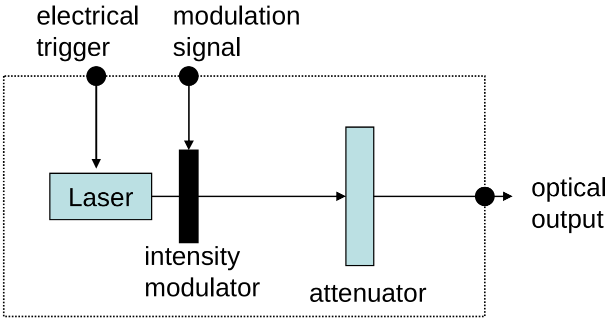


Figure 6.9: Schematic of a decoy source

Figure 6.9 shows an attenuated laser source which is intensity-modulated. This source is called intensity-modulated weak laser. 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 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.

The source intensity calibration shall be done in three steps. First, the intensity shall be calibrated when the intensity modulator is set for maximum transmission. Second, the modulation signal of the intensity modulator shall be calibrated to produce desirable relative intensity ratio among the signal and decoy pulses. Thirdly, the attenuator shall be calibrated and set to produce desired absolute intensities (μ) for signal and decoy pulses.

The photon number statistics shall be evaluated using a setup as shown in figure 6.2. During this evaluation, the intensity modulator shall be set to minimum attenuation for all pulses. The obtained photon number statistics shall be assumed to apply to both the signal and decoy pulses.

The laser output shall be splitted using a beam splitter and shall be constantly monitored using an optical power meter. The attenuator or the electrical signal applied to the laser shall be continuously adjusted to maintain a constant output power at the optical output after the attenuator.

6.4.3 Composite Weak Laser

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

Figure 6.10 shows 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, shall be used. The outputs of these individual lasers are then combined using a beam combiner and then attenuated by an optical attenuator to desired intensity levels. Upon an external trigger, only one laser fires at a time and which one fires depending on the input switching signal.

To maintain indistinguishability, each emitter shall be carefully tested to have identical wavelength, spectral profile, temporal profile, and photon number statistics. Wavelength and spectral profile may be made identical using a spectral filter. Temporal profiles shall be measured using a time-correlated single-photon counting setup.

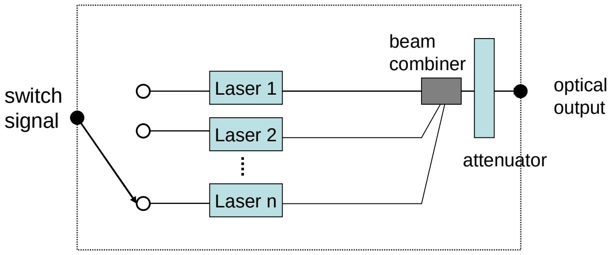


Figure 6.10: Schematic of a composite source

Calibration of source intensity and photon number statistics for each laser shall follow the procedure for weak laser described in clause 6.4.1.

Each laser output shall be splitted using a beam splitter and shall be constantly monitored using an optical power meter. The attenuator shall be continuously adjusted to maintain a constant output power at the optical output after the attenuator for each laser.

6.5 Continuous-Variable QKD Source

The emitter shall produce 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 case of pulsed regime, it can be externally modulated with amplitude modulators. It can also directly produce optical pulses if driven by a pulsed current.

The signal pulse shall be limited by quantum noise and its properties shall not be modified by the propagation in the channel, in particular optical losses. Therefore the signal state should be a coherent state. This can be obtained when strongly attenuating an initial laser pulse, which removes its possible excess noise (e.g. phase noise of diode laser pulses). Thus, in a practical implementation, the laser pulse shall be coupled into an unbalanced optical coupler (typically 99/1) with two output ports corresponding to the local oscillator channel and to the signal channel. The most intense pulse shall be used as the local oscillator. The less intense pulse shall be used as a signal pulse.

The signal pulse shall be modulated inserting an amplitude modulator and a phase modulator into the signal channel. Therefore, it is possible for the emitter to choose any amplitude and phase for the produced coherent state. The modulators should be chosen to reduce as much as possible the excess noise that can result from modulation imperfections. Such excess noise can be exploited by the eavesdropper to retrieve some information on the secret key. Then, the signal pulse shall be strongly attenuated, using an optical attenuator, in order to reach a level of typically 10 photons per pulse. In addition, the strong attenuation removes the residual excess noise that could be present. As result, the attenuated pulse is a coherent state that can be used in the CV-QKD protocol. The fine-tuning of the signal level can be obtained with an amplitude modulator inserted at the output of the signal channel.

The signal and local oscillators are then multiplexed before being sent into the transmission channel. In case of a time multiplexing, a delay line is inserted into one of the two channels. The delay shall be much longer than the pulse duration. In case of polarisation multiplexing, the signal and local oscillator shall be coupled to the two input ports of a polarising beamsplitter. 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.

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.

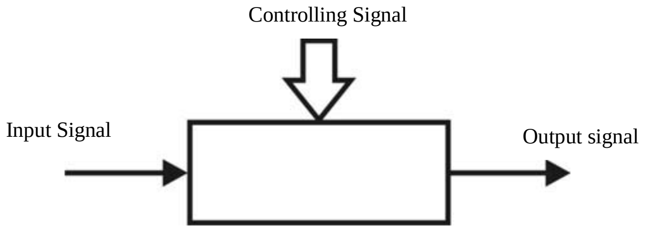
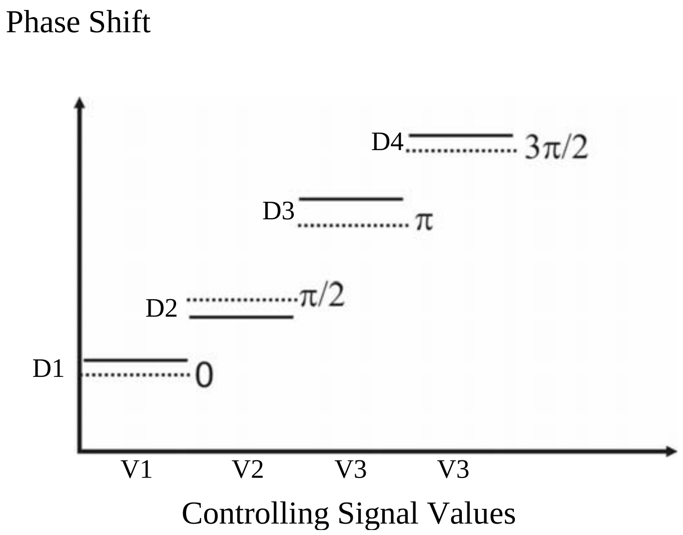


Figure 7.1: Schematic of a modulator

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 intensity. 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 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 dash lines represent the ideal phase shifts - 0, π, $\pi/2$, π 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 shall be specified for a defined set of operating conditions, given in table 7.2.

Table 7.1: Parameters that shall 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	D	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 shall 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.

History

Document history		
V1.1.1	December 2010	Publication