FINAL PUBLISHABLE JRP REPORT

JRP-Contract number	IND06
JRP short name	MIQC
JRP full title	Metrology for Industrial Quantum Communication Technologies
Version numbers of latest contracted Annex Ia and Annex Ib against which the assessment will be made	Annex Ia: V1.3 Annex Ib: V1.2
Period covered (dates)	From 1st September 2011 to 31st August 2014
JRP-Coordinator	
Name, title, organisation	Dr Maria Luisa Rastello, INRIM
Tel:	+39 011 39 19 219
Email:	m.rastello@inrim.it
JRP website address	www.miqc.org
Other JRP-Partners	JRP-Partner 1: INRIM, Italy JRP-Partner 2: Aalto, Finland JRP-Partner 3: CMI, Czech Republic JRP-Partner 4: Metrosert, Estonia JRP-Partner 5: NPL, United Kingdom JRP-Partner 6: PTB, Germany JRP-Partner 7 AIT, Austria JRP-Partner 8: IDQ, Switzerland JRP-Partner 9: KRISS, Republic of Korea JRP-Partner 10: MIKES, Finland

REG1- Researcher	Damien Stucki	Start date:1st Sep 2011
(associated Home Organisation)	IDQ, Switzerland	Duration: 36 months
REG2- Researcher	Alberto Tosi	Start date:1st Sep 2012
(associated Home Organisation)	PoliMi, Italy	Duration: 12 months
REG3- Researcher	Anas Al Natsheh	Start date:1st Jan 2013
(associated Home Organisation)	UOULU, Finland	Duration: 20 months

EMRP
European Metrology Research Programme
Programme of EURAMET

The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union

TABLE OF CONTENTS

1 Executive Summary

Introduction

This project provided a significant contribution to the process of standardisation of quantum key distribution (QKD) commercial systems lead by the European Telecommunications Standards Institute (ETSI). The scope was the development of characterisation techniques of quantum optical components of QKD systems, i.e. emitters, channels and receivers, as their characterisation is crucial for security analysis of QKD systems at the quantum optical level, and so for the standardisation of these systems.

The Problem

Implementation of QKD requires that its systems are trusted by its users (e.g. financial institutions, military establishments). QKD offers to guarantee security of a channel only after carrying out measurements to ensure the channel has not been compromised. Therefore, the security of QKD systems requires the ability to accurately determine the properties of optical components such as photon sources, quantum channels and detectors. A framework is also required for the underlying theoretical security proof which again requires accurate knowledge of all the critical components of the system.

The successful market uptake of QKD technologies and products requires the solution to a number of metrological challenges which had not yet been sufficiently addressed. Prior to this project, QKD relied on quantum physical devices that were not traceable to any national standards. In fact, standards, when existing, operated in the regime of microwatts or above and were not suitable to be used for measurements at single photon level.

Without the development of this metrological infrastructure, the effectiveness and reliability of QKD products cannot be monitored. Lack of independent measurement capabilities impairs the control and check of QKD products which in turn can lead to a breakdown of trust and disputes among parties.

The Solution

In response to the problem, the project set out to develop technically challenging measurement facilities and standards operating at single-photon level at the telecom wavelength (1.5 micrometre), i.e., in the spectral and power regime of interest for QKD application. In this project, we developed, refined and applied new metrology to qualify and quantify properties of photon emitters, quantum channels and photon receivers. New methodologies were also developed to optimise QKD products for reliable and stable operation.

Impact

The outputs from this project contributed to the necessary metrological foundations for the standardisation of the QKD. The wider impact of this project is the assurance to end users of the conformance of QKD components to standards thereby promoting market uptake of the technology and ultimately revolutionising data security in ICT. Successful deployment of QKD will also kick start the quantum industry – there are already related areas of research which are being pursued by academia to take QKD to the next phase – such as quantum repeaters and quantum memories.

The impact was ensured by the presence in the consortium of influential manufacturers, standardisation bodies and researchers from all over and outside Europe. The key European QKD manufacturers, namely ID Quantique, and Toshiba Research Europe Laboratories, were actively involved in this project through the ETSI industry-specification group (ISG) on QKD. In particular, members of the consortium contributed to reviewing the published ETSI document “GS QKD 003: Quantum Key Distribution (QKD); Components and Internal Interfaces” (before the project start), and to the drafting of current ETSI documents “DGS/QKD-0011_OptCompChar: Quantum Key Distribution (QKD) Component characterisation: characterising optical components for QKD systems” and “DGS/QKD-0010_ISTrojan: Quantum Key Distribution (QKD) Implementation security: protection against Trojan horse attacks in one-way QKD systems”).

2 Project context, rationale and objectives

Cryptography is the art of rendering a message unintelligible to any unauthorized party. To achieve this goal, an algorithm (also called a cryptosystem or cipher) is used to combine a message with some additional information - known as the key - to produce a cryptogram. This technique is known as encryption. For a cryptosystem to be secure, it should be impossible to unlock the cryptogram without the key. Although confidentiality of information is the traditional application of cryptography, it is used nowadays to achieve

broader objectives, such as authentication, digital signatures, and nonrepudiation. Security on classical communications relies on making cryptographic keys longer and longer to stay ahead of ever-increasing computing speeds that make it possible to identify keys and decode encrypted information. However, the successful development of extremely powerful computers, such as quantum computers will render this tactic useless. The security of QKD instead does not depend on the limitation of an attacker's computing power. Provided side channels are well controlled, QKD is secure against attackers with arbitrary classical or quantum computing power. QKD Quantum cryptography, in particular QKD, is therefore considered the only truly secure key-distribution technology (except for secret courier). It has great potential to become the key technology for securing confidentiality and privacy of communication in the future ICT world and thus to become the driver for the success of a series of services in the field of e-government, e-commerce, e-health, transmission of biometric data, intelligent transport systems and many others. Its power stems from the fact that quantum mechanics allows for a new primitive, that permits two parties to establish a secret key from a short pre-shared secret and a public exchange, i.e. something which was never possible with classical, non-quantum means.

QKD is essentially the generation of truly random cryptographic keys between two parties that are connected by a quantum channel. Cryptographic keys are the key element to realise secure communication between two legitimate parties. QKD was not invented as solution to an urgent demand; rather it originated from theoretical speculations on the power that is added to information theory through the use of quantum mechanical systems. Over time, QKD has given strength to the development of quantum information and is likely to be a disruptive technology in information management industry. With its strong long-term security perspective, QKD will be an important building block for dependably secure communication networks and it is likely that in the short term it will be used to complement current security protocols. It has the potential to increase usability and acceptance for typical services of today's information society and in the near and long term future QKD has great potential to become a key technology for securing communication confidentiality and privacy in the future information society and thus become a driver for the success of a series of services. It has also been a driver for the development of new detectors and sources as well as generating new areas of research such as quantum entanglement based QKD, used to develop next generation QKD.

Implementation of QKD requires that QKD systems are trusted by its users (e.g. financial institutions, military establishments). In other fields this is usually achieved by a complex assurance procedure including security specification, evaluation and certification according to a standardised methodology. QKD offers to guarantee security of a channel only after carrying out measurements to ensure the channel has not been compromised. Therefore, the security of QKD systems requires the ability to accurately determine the properties of optical components such as photon sources, quantum channels and detectors. A framework is also required for the underlying theoretical security proof which again requires accurate knowledge of all the critical components of the system. The lack of validation and standardisation remains a barrier to the commercialisation of QKD and this naturally falls within the remit of national measurement institutes. Currently, the only initiative for the standardisation of QKD originated in the context of the SECOQC [SECOQC, Alleaume2007, Ghernaouti2009] project of the 6th Framework Programme (FP6) of the European Community, and it is still active. Furthermore there is a strong driver for standardisation of QKD components and systems from the European standards community via an ETSI Industry Specification Group (ISG) on QKD.

The main challenges in QKD technology were the identification of the physical system parameters of quantum communication and the development of appropriate metrics and measurement techniques for their quantification. While the metrological characterisation of classical (non-quantum) communication parameters is well-established, quantum mechanics based quantum communication had not been systematically investigated from the metrological point of view and further development of the 'classical' measurement techniques was necessary to cover parameter ranges which are beyond the interests of classical communication.

The overall aim of the project was the development of metrological techniques, standards and methods to encourage end user adoption and foster the development of new industrial quantum communication technologies. To achieve a maximum impact for the European industry in this area, the project focussed on Quantum Key Distribution technologies [Gisin2002,Dusek2006], the most advanced towards practical application, and set out to develop measurement facilities and standards to operate at telecom wavelengths (around 1.5 micrometres) in single-photon regime. This was technically challenging since no measurement standards existed for photon counting at the telecom wavelengths at that time. In fact, standards, when

existing, operated in the regime of microwatts or above, and were not suitable to be used for measurements at single photon level.

The project technical objectives were the traceable characterisation of:

Emitters

1. Traceable characterisation of photon sources with unknown quantum states, including measurement of the mean number of photons per pulse, reconstruction of the probability of emitting a certain number of photons per pulse, and quantum tomography of the quantum states;
2. Realisation of optimised single-photon sources as a reference for the quantum source;

Channels

3. Traceable characterisation of quantum channels for optical fibre based communication systems, including de-coherence quantification, and quantum process tomography related to the propagation of states inside optical fibres;

Receivers

4. Traceable characterisation of commercial single-photon detectors, including detection efficiency, timing jitter, dead-time, after-pulsing, dark counts and saturation. Identification and standardisation of the definitions specific to quantum detection at single-photon level;
5. Determination of the properties of photon-number-resolving detectors capable of observing more than one photon in a pulse.

Priority was given to work meeting documented industrial needs through the interaction with ETSI-ISG that is working towards the standardisation of QKD. This interdisciplinary group unites experts from various scientific fields, such as quantum physics and metrology, cryptology and information theory from academia, research centres and industry from all over the world [ETSIportal, Langer2009]. Three of the project partners, INRIM, NPL and PTB are members of this group.

3 Research results

In the following we describe the measurement activities and the results obtained in the context of this project. The scope of the work carried out relates to the investigation of the key modules of QKD systems: photon emitters, quantum channels and photon receivers (see Figure 1).

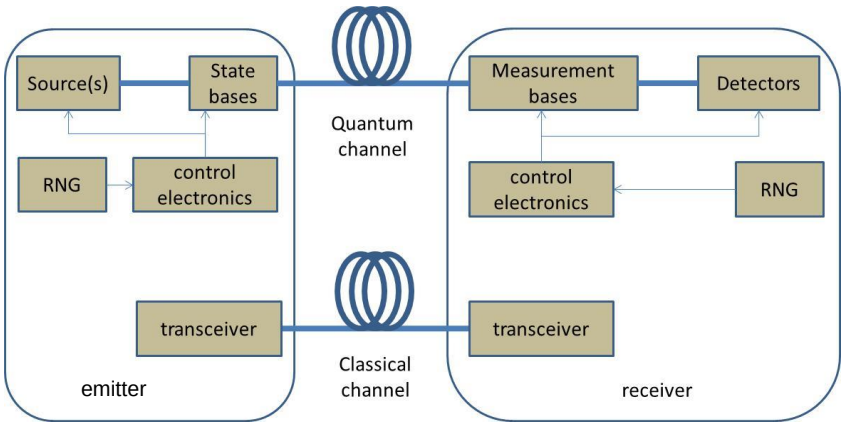

Figure 1: Generic QKD structure. RNG: random number generator

Due to current implementations of QKD systems and unavailability of perfect single-photon sources operating at telecommunication wavelength and room temperature, investigations were mainly focused on the development of characterisation techniques of the light emitted by highly attenuated pulsed lasers and shuttered heralded single-photon source, based on spontaneous parametric downconversion (SPDC) generating individual photons. Parameter studies of the photon receivers were mainly concentrated on

InGaAs/InP semiconductor single-photon avalanche diodes (SPADs) operating in Geiger mode, suitable for single photon counting or timing applications in the near-infrared spectral range (up to 1.65 µm) and in some cases on superconducting nano-wire detection systems (SNSPD) providing very low dark count rates.

3.1 Photon Emitters

A single-photon source will be ideal as a QKD source, if it is able to maintain indistinguishability for photons in all degrees of freedom, except that of encoding; i.e. encoded photons should not be distinguishable through measurement of parameters other than the encoding parameter. However, a perfect single-photon source is yet to be realised; current sources suffer from low efficiencies and require stringent operation conditions such as cryogenic cooling and thus are impractical. For practical QKD, a highly attenuated pulsed laser approximates a single-photon source; this emits optical pulses containing less than one photon per pulse on average. They are suitable for encoding in discrete degrees of freedom, e.g., in polarisation, phase and arrival times. A heralded single-photon source, based on SPDC, also generates individual photons. This is of immediate use in metrology of components and detectors, and is a prospective candidate technology for future QKD sources. A QKD source will also be specified by a photon number distribution P(n). Parameters related to the probability distribution (e.g. mean, variance, g(2), etc.) allow the determination of the multi-photon probability, i.e., the probability that a photon pulse contains more than one photon. Precise quantification of these parameters is fundamental in guarding against the so-called photon number splitting (PNS) attack [Norbert2002] and a few protocols have been developed to protect against it, such as i) decoy state protocols that use intensity modulators with different signal levels, so called signal and decoy states [Hwang2003, Lo2005] and ii) Scarani-Acin-Ribordy-Gisin (SARG) [Scarani2004] or Coherent One Way (COW) [Stucki2005] protocols.

Attenuated lasers

Commercially available pulsed lasers can be used to approximate to a single-photon source using attenuators, where on average there will be a mean photon number <1 so most pulses will have zero photons. Table 1 summarises the source parameters characterised and the techniques used in this project. In some cases different approaches have been investigated. The listed parameters represent all the (relevant) parameters for a pseudo-single-photon source used in QKD systems. Different techniques have been used to prevent eventual biases from being unnoticed, as this was the first time that such quantities were characterised at metrological level.

Table 1: Table of parameters relevant to a commercial QKD source

Parameter	Symbol	Units	Definition	Measurement approach
Mean photon number	μ	Photons/ pulse	Average number of photons per pulse emitted by the sender	a) calibrated detector and commercial attenuator b) reconstruction of probability distribution c) calibrated detector and traceable attenuator based on InGaAs photodiodes d) photon number resolving detector based on commercial single photon detectors in a tree configuration
Mean photon number variation	σ_μ			As above
Source timing jitter	J_S	ps or ns	The uncertainty in the emission time of a photon at the optical output.	Measure FWHM of distribution of photon emission times with respect to pulse generator signal
Source wavelength	λ	nm	Wavelength of photons that are emitted.	Wavemeter
Spectral line width	δ	GHz	Bandwidth of the emitted photons.	Beat note measurement or Fabry-Perot interferometer.
Spectral indistinguishability	s^{ind}	Unitless	The extent to which the encoded states can be distinguished through spectral measurement.	Fabry-Perot interferometer: compare spectra of different encoding states
Polarisation state				Polarisation reconstruction

3.1.1 Traceable characterisation of photon sources with unknown quantum states produced by photon emitter

A QKD source must maintain indistinguishability for photons in all degrees of freedom, except that of encoding. For example, in the polarisation-encoding BB84 protocol, qubits in all four states are required to have exactly the same wavelength, temporal profile, arrival time, etc. Discrimination of these polarisation-encoded qubits can be made possible through polarisation measurement. Indistinguishability in all photon degrees of freedom except that of encoding is the key to prevent any side-channel attack to a QKD system.
A QKD source is also specified by a photon number distribution P(n). This is of prime importance in QKD security and is quantified by two parameters, namely the mean and variance of number of photons per pulse. These parameters determine the multi-photon probability, i.e., the probability that a photon pulse contains more than one photon. Precise quantification of these parameters is fundamental in guarding against the so-called photon number splitting attack.

Within this project we have developed the measurement approaches listed in Table 1.

Measurement of mean photon number and variation in mean photon number of QKD pseudo-single-photon-source

The mean photon number, μ, is defined as the average number of photons per emitted pulse (equation 1).

$$\mu = \frac{P}{f\left(hc/\lambda\right)} 10^{-A} \tag{1}$$

where

P = measured optical output power of the laser (W);

f = repetition rate of the laser pulses (Hz);

hc/λ = photon energy (J);

A = attenuation factor (unitless)

The variance in the mean photon number is defined as the square of the standard deviation of the N measured values.

The following subsection describes the measurement protocols developed and results obtained with the four approaches considered in this project for the estimation of the mean photon number of attenuated pulsed lasers.

Two measurements were developed on laser pulses attenuated with a calibrated commercial attenuator exploiting the following techniques:

a) measurement using a calibrated detector;
b) reconstruction of probability distribution.

The other two measurement techniques were performed using:

c) laser pulses attenuated with a calibrated attenuator based on InGaAs photodiodes in trap configuration measured with a calibrated detector;
d) a photon number resolving detector based on commercial single photon detectors in a tree configuration.

(a) Calibrated detector and commercial attenuator

This measurement approach can be considered as the state-of-the-art measurement technique applicable to any kind of light source. In this case the source comprised a laser driver, laser head, variable attenuator(s) and the optical fibre. The measurement set-up used a detector calibrated against metrology standards traceable to the primary standard for optical radiation, the cryogenic radiometer [Martin1985, Stock2000]. Measurements were carried out at different settings of the variable attenuator. A schematic of the measurement set-up is shown in Figure 2.

An attenuated laser pulse producing pulses with a photon number distribution P(n), where the probability for P(n>1) is non-zero was employed. As described in the introduction to this section, one countermeasure to PNS attacks is to use decoy-state protocols, where the mean photon number of each pulse is randomly switched between two, three or more values. Two methods of measuring μ are described below. The first one is only applicable where every pulse has the same μ value, i.e. when no decoy-state protocol is implemented.

(i) Measurement of average power (indirect measurement)

In the situation where there is only one μ value, or the mean μ value over all μ states is adequate, the detector could be a device that measures mean optical power within some time interval, such as a power meter. In this case, the source is driven at some frequency f = f_{clock}. The electronic delay and frequency divider shown in Figure. 2 are not used and a gate input to the detector is not required. From measurement of the power P, and knowledge of the effective wavelength λ, the mean photon number <μ> was calculated using Eq. (1). The uncertainty in this measurement is dominated by the calibration uncertainty of the power meter. Power meters can be traceably calibrated with an uncertainty (k = 2) varying from 1% at the 100 pW level to 10% at the 1 pW level, i.e. the uncertainty in measuring <μ> is inversely proportional to the power level being measured in the sub-nW regime. At 1550 nm, for f = 1 GHz and <μ> = 0.5, P ~ 64 pW; however, for f = 50MHz and <μ> = 0.5, P ~ 6.4 pW. It is evident that this approach cannot currently provide high accuracy for QKD sources operating at low repetition rates or μ values.

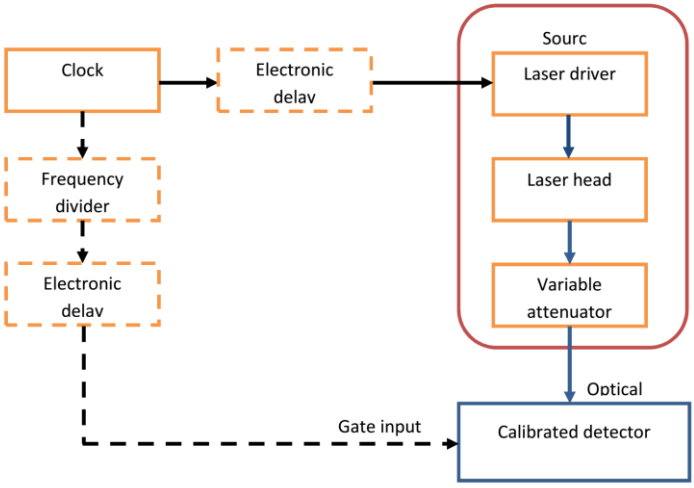

Figure 2: Measurement set-up for standard calibration of a QKD source, comprising a laser driver, laser head and fibre-coupled variable attenuator. Electrical connections are shown in black, optical fibre in blue.

In the case where the decoy state protocol is implemented with at least three values of μ – μ_{signal}, μ_{decoy}, μ_{vacuum} – of known relative frequency, the measurement of average power to determine the mean photon number of these states requires the assumption that $\mu_{vacuum} <<< \mu_{decoy}, \mu_{signal}$. While this assumption may be useful for order of magnitude estimates, it does not allow one to properly test a QKD source and measurement at the photon counting level is required.

(ii) Measurement of photon number per pulse (direct measurement)

The measurement uses a calibrated photon counting detector. In the 1.3 μm and 1.5 μm spectral regions, the majority of non-cryogenically cooled detectors are gated to reduce the dark-count rate. The method can be adapted for continuously active (free running) detectors by time stamping the laser pulses and detection clicks.

The arrival of the laser pulse at the detector has to be synchronised with the detector gate. This was implemented by using low jitter electronics. The detector was gated at the same frequency as the laser. If the laser is operating at a frequency above which the detector was calibrated, a frequency divider can be employed so that the detector is exposed to every pulse (Figure. 2).

The laser pulses must sit entirely within the duration of the detector gate, taking account of any jitter in their arrival. Figure 3 shows the temporal shape of the pulses produced by the light source, which comprised a PicoQuant laser driver (model PDL-800D) and a PicoQuant laser head (model LDH-P-F-N-1550). This was measured, before any attenuation, using a Textronix DCA-J waveform analyser (model 86100C) and a 65 GHz optical head (model 86116B). The pulse width was found to be 85 ps wide (full-width half-maximum - FWHM), and 100 ps wide (1% level). The detector gate width was measured by scanning the electronic delay and recording the number of clicks for a fixed number of pulses. The measured response is shown in Figure. 4, and is the combined effect of the laser pulse profile, the detector gate profile, the temporal response of the detector, and jitter in the pulse arrival and the detector gate. Given that the pulse is 85 ps wide, and the overall jitter was less than 25 ps, it can be deduced that the pulse can be set comfortably within the detector gate. One source of uncertainty will be due to any difference in the width and jitter between the laser pulses that were used to calibrate the detector and those of the laser to be measured. In our tests, the source laser was also used to calibrate the detector, so this factor can be ignored. There is some residual uncertainty due to any (small) difference in the synchronisation between the detector calibration and the source measurement.

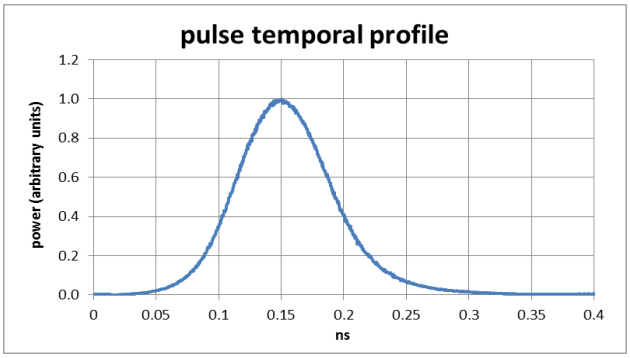

Figure 3. Temporal shape of laser pulse (timebase uncertainty < 10 ps).

The number of clicks for a known number of laser pulses was measured and corrected for the detection efficiency, dark counts, after-pulses, and the assumed Poisson distribution of photons in each pulse (since the photon counter is neither photon-number resolving, nor 100% efficient) [Schmunk2011].

The dominant uncertainty in these measurements is the uncertainty in calibrating the detection efficiency, after-pulsing probability, and dark count probability of the detector. These uncertainties were around 2% (k = 2). The other significant uncertainty component is the stability of the system – for a stable system, measurement times can be made long enough so that the uncertainties in the count statistics make a negligible contribution to the overall uncertainty. This is achievable for high laser repetition rates (e.g. f > 1 MHz, $\mu > 0.001$), but for lower repetition rates (e.g. f = 50 kHz) this could be important, since measurement times of up to 1000 seconds may be needed. (The measurement of μ values of 0.001 is not extreme for QKD systems that employ the decoy state protocol). In cases where the detector calibration uncertainty dominates, uncertainties of 3% (k = 2) are achievable.

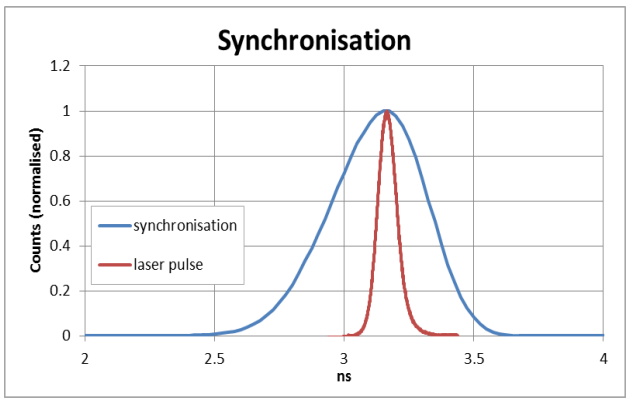

Figure 4. Measured response of detector as function of arrival time of photons

Two commercial variable attenuators were used in the set-up. The first, an OZ Optics manual in-line attenuator (model OZ 560151-18) was used for crude attenuation of the source. The second, a calibrated Hewlett-Packard optical attenuator (model 8158B) with an uncertainty of 1% for attenuations below 50 dB, was used to set the mean photon number to the single photon level. The output of the laser head after the 1st attenuator, was measured using a Hewlett-Packard power meter, which comprised of an optical head (model 81524A), an optical head interface (model 81533B), and a light multimeter (model 8153A). The power meter had been calibrated at 1550 nm traceably to the NPL cryogenic radiometer with an uncertainty of 1% for power levels above 1 nW. The wavelength of the emission was measured using an Anritsu Optical Spectrum Analyser (model MS9717A), whose wavelength had been calibrated using the vibration-rotation spectra of $^{13}C_2H_2$ [Edwards2005]. It was found that the peak wavelength was 1549.60 ± 0.02 nm. For the purposes of these measurements, it was assumed that the response of the power meter was the same at 1549.6 nm as at 1550 nm. Hence the predicted values of μ were around 2%. The predicted values, and the calibration of the photon counting detector, are both traceable back to the same power meter. Therefore, the observed agreement between the two values, while it is to be expected, demonstrates the reliability of the measurement technique.

The following techniques go beyond the state of the art.

(b) Reconstruction of probability distribution by means of on/off technique

The knowledge of the density matrix of a quantum state plays a fundamental role in several fields ranging from quantum information processing to experiments on foundations of quantum mechanics and quantum optics.

Recently, a method has been suggested and implemented in order to obtain the reconstruction of the diagonal elements of the density matrix exploiting the information achievable with realistic on/off detectors, e.g. SPAD detectors operating in Geiger mode [Brida2011], which are only able to discriminate between the presence or the absence of light.

Let us consider a single-mode quantum optical state. All the accessible information on the state can be obtained using the Born trace rule on its density matrix, which, in the photon number basis, reads as follows:

$$\rho = \sum_{n,m} \rho_{n,m} \, |n\rangle\langle m|. \tag{2}$$

In particular, the information about the photon number distribution of the state is given by the diagonal elements of the density matrix, $\rho_{n,n} = \rho_n$. The reconstruction of the ρ_n's for a general quantum optical state is possible upon exploiting the set of binary data obtained by a two-level, on/off, detector. We assumed that our state was revealed by a detector such as InGaAs/InP SPADs operating in Geiger mode with a quantum efficiency $0 < \eta < 1$. If we label 0=off and 1=on as the two possible outcomes, the overall measurement process for this kind of detector can be described by a two-value positive operator-valued measure (POVM) of the form:

$$\Pi_0(\eta) = \sum_n (1 - \eta)^n \, |n\rangle\langle n| \tag{3}$$

$$\Pi_1(\eta) = 1 - \Pi_0(\eta) \tag{4}$$

The off and on probability are thus given by

$p_0(\eta) = \mathrm{Tr}[\,\Pi_0(\eta)\,\rho\,]$ and $p_1(\eta) = \mathrm{Tr}[\,\Pi_1(\eta)\,\rho\,]$.

If we perform K on/off measurements, each one with a different quantum efficiency η_i, we obtain a set of experimental data that is a sample from the overall distribution.

The easiest way to extract the photon distribution from the above relation is via matrix inversion, but this solution is rather inefficient and unstable. A faster and statistically more reliable solution can be found by exploiting the maximum likelihood (ML) and/or other kind of minimisation/maximisation algorithms, i.e. finding the ρ_ns that are most likely to produce the observed data.

In the setup for the reconstruction of the probability distribution of number of photons emitted by a pulsed attenuated laser exploiting the on/off technique there is a source part separated from the detection part. The source part is composed by a pulsed pig-tailed laser whose power is lowered at the single photon level by commercial attenuator(s). In our case the laser used was a diode with a mean optical power of 3 mW at a wavelength of 1550 nm operated in a gated mode providing pulses of about 300 ps. On the detection part an attenuator was used for varying the total quantum efficiency of the detection system composed by the attenuator itself and the traceable calibrated single-photon detector (in our case a click/no-click detector, based on a commercial InGaAs/InP SPADs gated at 300 KHz by the same pulse generator triggering the laser). The whole system was connected by single-mode fibre. Operation parameters should be chosen in order to reduce as much as possible the influence of dark-counts and afterpulses. The outputs of the detector should be sent to a time correlation measurement apparatus in order to further suppress the effect of "erroneous" counts.

The first step was the characterisation of the loss induced by the insertion of the attenuator. The second one was the characterisation of the attenuation levels, i.e. the difference between the nominal and the measured attenuation. For this aim a classical traceable detector was used. All the data was corrected for the background power. Moreover, also repeatability of the attenuation values was investigated.

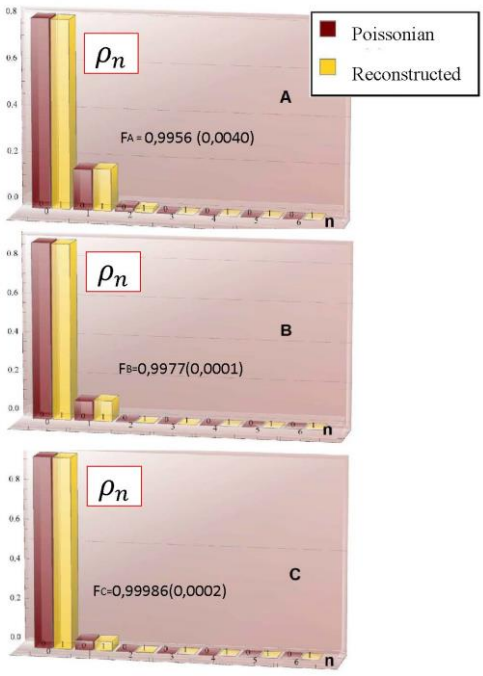

Fig. 5: Photon number distribution of the source for three different mean intensities indicated by A, B and C, compared with the expected Poissonian distributions.

Then, the power of the source was lowered down to the photo counting level and the efficiency of the single photon detection apparatus was varied up to the a number of detection events comparable to the dark counts. In the different quantum efficiency configuration, the data for the tomographic reconstruction were collected applying statistical analysis for the rejection of dark counts.

Once the data were collected the reconstruction algorithm was applied and the results obtained are presented in Figure 5.

The reconstruction algorithms produce useful results in terms of interpretation of the photon number statistics of quantum sources; however the uncertainty associated with this reconstructed distribution is still an open problem. In particular, repeated measurements and reconstructions provide information regarding the reliability of the procedure but do not really provide an evaluation of the uncertainty associated to the reconstructed statistics. One possible solution to this is to associate the repeated reconstructions to Monte Carlo simulations, accounting for the uncertainties contributed by each measurement parameters. This solution works well with a small number of calibrated parameters but with more parameters the process becomes time consuming. In conclusion, we believe that these reconstruction techniques are useful diagnostic tools for example for testing the presence of some unexpected behaviour of the statistical distribution or for some hypothesis testing. For the estimation, with trustable uncertainty, of the mean and variance of the number of photons produced by the source, the direct measurement with calibrated attenuators appears to be the most viable solution.

(c) Calibrated detector and traceable attenuator based on InGaAs photodiodes

In this approach we followed state-of-the art methodology but instead of using a commercial attenuator, we developed and used a traceable fibre-coupled attenuator based on InGaAs. This attenuator is able to measure the input power from which one can calculate the attenuated output power. Therefore, this device allows the mean photon number to be set using an uncalibrated attenuator on the input beam.

The principal attenuator set up based on InGaAs photodiodes in transmission trap configuration with an actively controlled fibre-coupled system was projected and realised. The attenuator is based on 10 mm-InGaAs photodiodes in a polarization-independent configuration. In order to minimise the effects of machining and temperature changes on the performance of the attenuator, a compact housing was developed. The design has been modelled with specific software applications proposing design features which allowed the study of the maximum deflection of the beam within a few micrometres under usual laboratory conditions i.e. temperature fluctuations within (20 ± 2) °C. Using the developed design, the beam

can be attenuated to some extent in 10^{-6} at the wavelength of 1.55 µm. An active controlled fibre coupling has been set up and tested.

Front end electronics for fibre couple attenuator has been designed and manufactured. A five decade switched integrator configuration has been chosen to provide parallel reading from the two InGaAs photodiodes composing the attenuator. The timing circuit is driven by an on-board digital signal processor (DSP). The current voltage conversion factor, i.e. the integration schedule, can be changed remotely through either RS232 or USB interface to provide further measurement flexibility. On-board firmware has been positively tested and the fibre coupled attenuator was then completely characterised.

A test setup for the planned fibre-coupled attenuator was constructed and successfully tested for operation at power range of 10-30 mW. The efficiency loss caused by potential optical misalignment has been calculated by a theoretical model and Matlab simulations. The suitability of the construction is evaluated by a characterisation set-up. The transmission trap was found to be polarisation insensitive. The external quantum efficiency of the transmission trap detector was 87.1% and the responsivity, was 1.09 A/W, at a wavelength of 1.55 µm. A redesigned device achieved an attenuation of 6.2×10^{-6} at 1.55 µm.

With this new device, the estimation of the mean photon number of the pseudo single photon source provided results within the uncertainty of the estimation obtained with the commercial attenuator. This suggests that the calibration of the single-photon detector, necessary to perform this measurement, brings the main contribution to the uncertainty.

(d) Mean photon number and variance measured by means of photon number resolving detector based on commercial single photon detector in tree configuration

An ideal Photon-number-resolving (PNR) detector requires a detection efficiency of unity to unambiguously detect the number of photons in a field. The most promising type is the transition edge sensor [Hadfield2010]. However, these PNR detectors require advanced cryogenic equipment and are hardly accessible or convenient for average laboratories or for end users of future quantum information systems.

Within the MIQC project, a new PNR detection system based on conventional detectors with no intrinsic PNR capability (click/no-click detectors) was developed exploiting the use of spatial multiplexing. The novel detector has been realized experimentally consisting of commercial InGaAs/InP SPADs operating in Geiger mode. The SPADs were arranged in a tree configuration of two or four detectors controlled by an integrated circuit designed to be configured by the customer after manufacturing - hence "field-programmable" (field-programmable gate array or FPGA) (Figure 6).

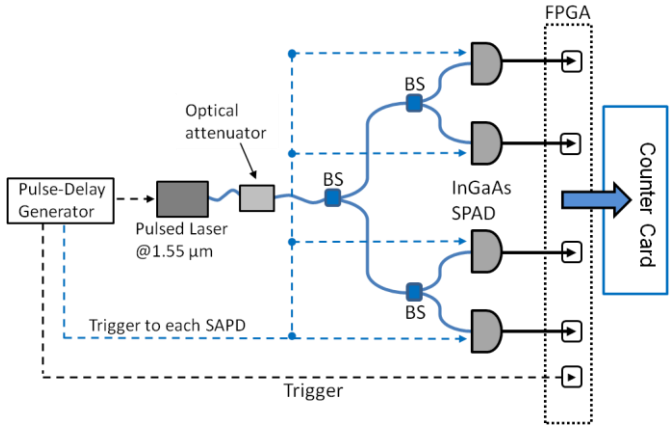

Figure 6. Experimental setup of the PNR detector based on spatially multiplexing exploiting click/no-click detectors in a "tree" configuration (BS: beam splitter based on optical single mode fibres).

As this detector is intrinsically non-linear, it is necessary to carry out a proper characterisation that fully describes the positive-operator-value-measurement (POVM) in order to be able to recover the mean and variance of the (pseudo-)single photon sources from the measurement data. After properly characterising the detection system, as shown later on in this report, a proper estimation of the mean photon number of an attenuated laser source was performed. The achieved uncertainty was compatible with the one obtained with the calibrated detector and commercial attenuator. A typical output from this detector measuring attenuated

laser pulses is shown in Figure 7. The histogram peaks correspond to the probability that the PNR detector records no, one or up to four photons per laser pulse.

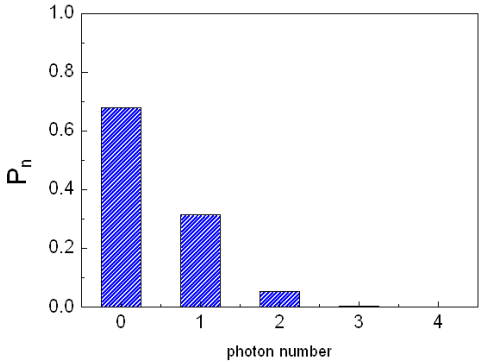

Figure 7: Attenuated laser pulse recorded by the PNR detector: the histogram peaks correspond to the probability (relative frequency) to detect no, one or up to four photons per laser pulse.

Measurement of source timing jitter of QKD pseudo-single-photon-source

The source timing jitter is defined as the uncertainty in the emission time of a photon at the optical output with respect to the pulse generator signal.

In considering an attenuated laser source, two options for jitter measurements were available. Using one approach, the attenuated source with its output at the single-photon level was detected by a superconducting nanowire detector, since the jitter of such detectors is low (< 100 ps) in comparison to other detectors [Hadfield2010]. By correlating many successive detection events with the clock signal triggering the source, a histogram of detection times could be observed. By deconvolving this signal from the detector's inherent jitter, the source jitter was determined. An alternative approach measured the optical output pulse from the source, prior to the attenuator that reduces the flux to the single-photon level. By performing this measurement on laser pulses containing many photons, it was then possible to detect them with a fast photodiode, rather than a photon-counting detector. The photodiode has a higher bandwidth and significantly less jitter than the superconducting nanowire detector.

If measuring the jitter of a single-photon signal using the superconducting nanowire detector, then a measurement uncertainty of < 50 ps was obtained. By measuring the jitter of the laser pulses before attenuation using a fast photodiode, a measurement uncertainty < 10 ps was obtained.

Measurement of source wavelength and spectral line width of QKD pseudo-single-photon-source

Attenuated laser sources used in commercial communication systems operate in the 1.3 μm and 1.5 μm regions of the near-IR spectrum. The calibration of wavemeters and the wavelength scale of optical spectrum analysers is conventionally carried out using a tuneable laser such as external-cavity or distributed feedback laser which gives a single wavelength output. The laser output is locked to molecular vibration-rotation transitions of gas-phase molecules, and, in the 1.5 μm region, CO and $^{13}C_2H_2$ transitions are employed [HC1998, Edwards2005]. The accuracy with which a device can be calibrated depends on the spectral resolution and stability of the device under test, but for a high-quality wavemeter with resolution of 0.1 pm or 1 pm, the achievable uncertainty can be as low as 0.15 pm, or 0.6 pm, respectively (k = 2).

When the laser in the QKD source is driven to emit short optical pulses, typically < 100 ps in duration, the spectral width of the source is $\Delta\lambda_{source}$ ~ 0.1 nm, which corresponds to $\Delta\nu_{source}$ ~ 12 GHz. This will affect the accuracy with which the wavelength can be measured. A wavemeter suitable for use with pulsed sources can measure such a laser's centre wavelength, λ_{source}, with an uncertainty $\Delta\lambda_{source}$ of ~ 0.002 – 0.01 nm, depending on stability, spectral profile and S/N.

It is possible to measure the spectral linewidth of an attenuated laser source by two different methods. Using the light emitted by the pulsed laser source, prior to the attenuator, and beating it against a tuneable narrow-linewidth auxiliary laser, the spectral linewidth can be measured. The tuneable narrow linewidth laser should be stabilised such that its linewidth $\Delta\nu_{stabilised} \leq$ 10 MHz, *i.e.* much narrower than the attenuated source

($\Delta\nu_{source}$). The spectral linewidth of the pulsed laser source will be revealed by the beat note, observable when the auxiliary laser is tuned near the source's optical frequency. Using this beat note method, a resolution of ~ 200 MHz, should be feasible. Note that this method is not suitable for optical pulses at the single-photon level.

The use of a stable, tuneable Fabry-Perot resonator provides another route to measuring the source linewidth. The technique requires that the cavity free spectral range (FSR) is much greater than the source's pulsed laser linewidth, *i.e.* FSR >> $\Delta\nu_{source}$, yet have a linewidth $\Delta\nu_{cavity}$ << $\Delta\nu_{source}$. Consider the design with a cavity of length = 1.0 mm, which has a corresponding FSR = 150 GHz. By choosing a mirror finesse of 250, the cavity resonance linewidth $\Delta\nu_{cavity}$ = 600 MHz sets the spectral resolution of the instrument. When used in transmission mode, the Fabry-Perot cavity can be tuned to resonance with the pulsed laser source to record its spectral profile. When analysing the optical pulses prior to the attenuator, the signal would be measured using a PIN photodiode. The technique is also appropriate for measuring the attenuated laser pulses (containing on average one photon or less), by using a superconducting nanowire detector. For example, with a pulsed laser source operating at 80 MHz repetition rate, and using the nanowire detector, a good signal to noise can be achieved with the cavity resolution stated above. A device constructed following the design described above achieved a FSR of 119 GHz (cavity length of 1.26 mm) and a linewidth of 570 MHz, with an operating range from 1270 nm to 1630 nm.

Measurement of the spectral indistinguishability of QKD pseudo-single-photon-source

The spectral indistinguishability of encoded individual photons is vital to avoid any possibility of detection of the encoded key. However, the spectral profile of the individual photons can be affected by the phase modulator used to implement the phase encoding scheme in the BB84 protocol (and its variants). The encoding modulator's phase is randomly changed between successive laser pulses; and it is essential that this has settled at a constant value prior to the pulse propagating in the modulator, and that further switching occurs afterwards. If the phase switching (or settling) occurs while the laser pulse is propagating through the modulator, then a changing phase shift will be experienced, and the leading edge of the pulse may see a different phase shift from the trailing edge. The spectral characteristics of the laser pulse will be distorted, and will be present on the photons transmitted in the quantum channel. It is therefore possible that with such spectral distortion, the four different encoding phases may be distinguished by spectral means. Spectral measurements are needed to demonstrate that the photons are spectrally indistinguishable, irrespective of the phase encoded onto them.

The Fabry-Perot resonant cavity, detailed above, was used to perform this analysis. The cavity acts as a narrowband spectral filter, and by scanning the cavity length, its resonance frequency is tuned. By accumulating transmitted signals as a function of resonant frequency, the photons' spectral profile was determined. This was done for the encoding phases using the normal switching of the modulator. A spectral distinguishability was evident when there was a difference between these spectral profiles.

Polarisation state reconstruction of QKD pseudo-single-photon-source

Photon polarisation is the quantum mechanical equivalent of the classical electromagnetic light polarisation. The quantum polarisation state vector for a single photon, for instance, is identical with the Jones vector, usually used to describe the polarisation of a classical wave. Thus, it is clear that the quantum state tomography is equivalent to the estimation of Stokes parameters for classical light. The only difference is that instead of measuring light power, what is experimentally observed are the relative detection frequencies of single photon detection, i.e. conditional probabilities of detection of single photons. Investigation of eventual differences induced by power attenuation is absolutely relevant for the characterisation of QKD sources. Furthermore, tomographic reconstruction of the polarization state at the single photon level is obviously more affected by detection imperfections (such as e.g. dark counts and afterpulses) than conventional polarimetry that take advantage of the well-established light detection technology in the macroscopic regime. For this reason proper reconstruction algorithms (e.g. maximum likelihood algorithms) should be employed to reconstruct physically meaningful polarisation state of the single photons.

The problem of the estimation of the uncertainties on Stokes parameters is not obvious in conventional polarimetry and it becomes even more complicated for single-photon detectors operating in Geiger mode (i.e. non photon-number-resolving) that also present some dead time. In our experiments we took care of these distortion factors and we introduced correction factors.

The work on the polarisation tomographic technique helped us to understand if there was a real need of developing such a technique for the actual QKD sources (i.e. attenuated laser) or if it would be enough to measure the polarisation of the laser source just before the attenuation. However, independently of the results of this analysis, in view of the future substitution of the attenuated laser with real single-photon source it is anyway necessary to develop a reliable polarisation state reconstruction technique.

In this perspective the most efficient and reliable solution is the development of a system similar to the actual conventional polarimeter, where a splitting of the beam occurs along different direction and the polarisation measurements are performed in all the needed polarisation basis (i.e. horizontal/vertical, diagonal/anti-diagonal, left- and right-circular). At single-photon level this means that the single photon would be detected in the best case scenario by one of the six single-photon detectors. The total detection efficiency of each detector in this setup is reduced by the splitting of the field, thus this measurement is more affected by dark counts and afterpulses than a measurement where, for example, only two detectors are present and the different polarisation measurement projections are performed in sequence by modifying the polarisation control systems (see Figure 8).

In this sense the single-photon polarimeter we developed is based on bulk optics, i.e. a polarising beam-splitter in fixed position, a quarter and a half-wave plates to control the polarization state and only two single-photon detectors. We confirmed the equivalence of the results of our single-photon polarimeter with a conventional polarimeter (operating a conventional light level) by measuring attenuated and non-attenuated CW laser light with different incoming polarisation.

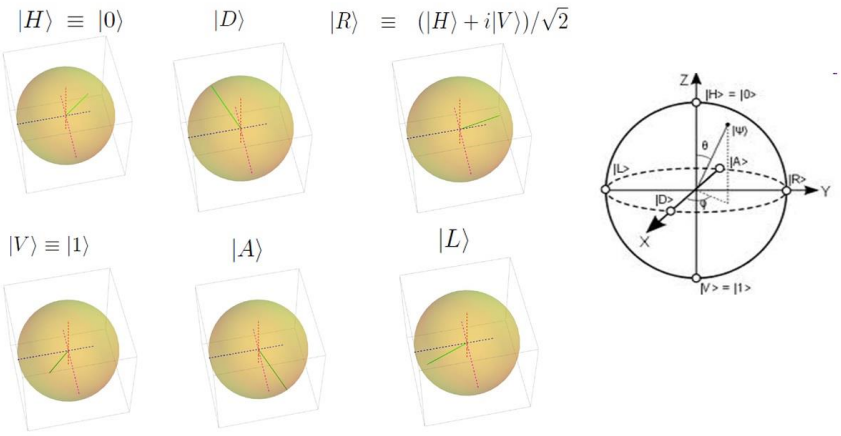

Figure 8: The experimental results: six polarisation states have been reconstructed in single photon regime with tomographic measurements (green vectors).

In Figure 8, states are visualised as Stokes vectors on the Poincare' sphere. States are all orthogonal and with norm equal to 1, confirming that the effect of the propagation in the short fibre is simply a rotation of the Poincare' sphere, without decoherence effects. The results obtained with the conventional polarimeter were completely analogous to the ones showed here, irrespective to a phase rotation due to the different pieces of fibre and attenuator that connects the source to the "conventional" and to the single-photon polarimeter, thus proving the equivalence between the two approach.

Single photon emission characterisation of QKD pseudo-single-photon-source

For a real (practical) single photon source (SPS) the most important characterisation consists in verifying the possibility of having more than one photon emitted by the source. One of the most typical setup used for this aim is known as Hanbury Brown-Twiss interferometer (HBT) operating at single photon level. The HBT is typically realised exploiting two threshold (click/no-click) detectors placed at the output ports of a 50:50 beam-splitter [Grangier1986, Eisaman2011, Migdall2013].

The efficiency of a single-photon source can be described by means of the parameter α proposed by Grangier et al. in ref. [Grangier1986]. This is essentially an "anticorrelation criterion" based on the parameter $\alpha = Q(2)/[Q^{(I)}(1)\, Q^{(II)}(1)]$ where Q(2) is the probability of the coincidence click between the two detectors of the HBT interferometers, while Q(1) is the probability of a click by one of the two detectors ((I), (II) indicate the two detectors after the beam splitter). In the single-photon community the parameter 'α' is

often called second order correlation function $g^{(2)}$ [Grangier1986], but as $g^{(2)}$ has a different definition [Mandel1995], despite the fact that in the few photon regime the two definitions are asymptotically equivalent.

In general it is expected that each “pulse” from the SPS contains ‘n’ photons. Thus, by considering the proper detection model for the click/no-click detectors, the probability of the detector firing due to an optical pulse containing ‘n’ photons and as the probability of observing a coincidence between the two detectors of the HBT due to a single pulse from the SPS should be properly evaluated (see e.g. [Migdall2013]).

It is worth noting that with typical click/no-click detectors the parameter ‘α’ is almost independent from the detection efficiency of the detectors (when very similar between the two detectors), while it can be strongly affected by the presence of dark counts or counts due to stray-light. For this reason, time-correlated-photon-counting measurements techniques can be helpful to provide proper estimation of the background counts. Furthermore, also detectors’ deadtime and HBT interferometer beam-splitter unbalance may bias the estimation of ‘α’ parameter. Proper estimation of these non-idealities are necessary to implement the needed correction factor in order to have a faithful estimation for ‘α’. For examples of proper detection models in HBT interferometers one can refer to Refs [Migdall2013, Brida2011_2].

In conclusion we note that, despite apparently non-useful in the case of SPS based on attenuated laser (because ‘α’ should be equal to one, therefore independent of the intensity of the coherent source), this estimation is important because it provides information about the stability pulse-to-pulse of the pulsed laser based SPS. For this reason, in the context of the project we used this technique to characterise both a pseudo-single-photon-source based on an attenuated laser and a real extremely “low-noise” single photon source that we realised in the context of the project (more detail on this single-photon source is provided in the forthcoming sections).

3.1.2 Realisation of optimised single-photon sources as a reference for the quantum source

In addition to the new measurement techniques contributing to the realisation of single-photon metrology of photon sources at telecom wavelength, we have also realised the following new devices necessary for the deployment of these new measurement techniques:

- *The single-photon polarimeter*

  A complete realisation of the launcher (a pseudo-single-photon source with fully controllable polarisation) and of the single-photon polarimeter based on bulk optical components and single-photon detector was performed. The single-photon polarimeter was mounted and tested (against a conventional polarimeter) obtaining satisfactory agreement. Thus, this single-photon polarimeter was exploited in the tomographic reconstruction of the single-photon polarisation states (exploiting the launcher) before and after propagating over a 25 km fibre length. Then we compared the results with the ones obtained carrying out the same experiment but using a laser beam and a conventional polarimeter for the polarization reconstruction. The results obtained were in good agreement as expected. Thus, we were able to fully describe the evolution of the polarisation inside the optical fibre, for both the single-photon polarimeter based reconstruction for the conventional polarimeter based reconstruction. As we observed that, as expected, there is not any relevant difference on what happens to a conventional laser field and to a single photon propagating in the fibre, we can use either the information obtained from a conventional polarimeter, or the one from a single-photon polarimeter to describe the decoherence process suffered by light propagating in optical fibre.

- *The attenuator based on InGaAs diodes in trap configuration*

  The attenuator based on 10 mm-InGaAs in a polarisation-independent configuration was used in the calibration of single-photon detection probability and in the mean photon number measurement of pseudo-single-photon-sources. In order to minimise the effects of machining and temperature changes on the performance of the attenuator, a compact housing was developed. The design has been modelled with specific software applications proposing design features which allowed the study of the maximum deflection of the beam within a few micrometers under usual laboratory conditions i.e. temperature fluctuations within (20 ± 2) °C. Following the developed design the attenuator was realised, having the beam attenuated to some parts at the wavelength of 1.55 µm. An active controlled fibre coupling has been set up and tested. Front end electronics for fibre couple attenuator has been designed and manufactured. A five decade switched integrator configuration has been

chosen to provide parallel reading from the two InGaAs photodiodes composing the attenuator. The timing circuit is driven by an on-board digital signal processor (DSP). The current voltage conversion factor, i.e. the integration schedule, can be changed remotely through either RS232 or USB interface to provide further measurement flexibility. The attenuator with its read-out electronics was measured (2% uncertainty) using a power meter whose linearity has previously been calibrated with an uncertainty (k=2) < 1%. The electronics was able to read incident power on the front photodiode down to power levels of 5 pW with a noise level < 0.5%. The output mean photon number per pulse of the attenuator can therefore be calculated from the reading of the front photodiode. The mean photon number was also measured with a calibrated photon counter and agreement within 3% was obtained.

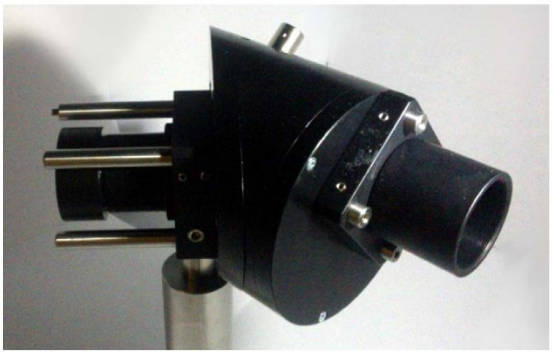

Figure 18: Body of the transmission trap detector–attenuator. Light enters from the leftmost and exits from the rightmost part of the detector. The two 10mm diameter photodiodes were mounted into the trap detector in such a way that reflection from photodiode surfaces takes place at the angle of incidence of 17◦. The planes of incidence of the photodiodes are perpendicular to each other ensuring polarisation insensitivity of the total reflection and attenuation. The reflected, non-absorbed fraction of incoming beam exits from the output aperture of the attenuator at the angle of 34◦ relative to the direction of the incoming beam.

- *The single-photon spectrometer*

  The wavelength of an unattenuated optical source can be measured using a commercial wavemeter. However, with the aim of determining the spectral linewidth and the indistinguishability of single-photon optical pulses we realised a specifically designed cavity spectrometer. The instrument showed a free spectral range of 119.0 GHz and a resolution linewidth of 560 MHz, thus meeting the specified resolution requirement of 1 GHz. Confinement of the cavity in vacuum and dual layer active temperature control reduced the spectrometer drift rate well below practical scan rates, ensuring linearity of scans. Characteristics have been demonstrated at single-photon flux rates, detected by the superconducting nanowire detector. The single-photon spectrometer was used to characterise the spectrally narrow emission of the pseudo-single-photon source based on attenuated pulsed lasers.

3.2 Quantum Channel

The photon emitters and receivers in a QKD system must be connected by a “quantum channel”. Such a channel is not especially quantum, except that it is intended to carry information encoded in an individual quantum system, namely a degree of freedom of a photon. In this project the analysis was restricted to optical fibre as quantum channel, thus all the components so far considered are somehow pigtailed.

3.2.1 Traceable characterisation of quantum channels for optical fibre based communication systems

From the QKD perspective, the quantum channel is, for its definition, out of the control of the sender and of the receiver. Even if the quantum channel is attacked, manipulated, modified by the eavesdropper, the QKD system should be able to ensure the security of the distributed keys. For this reason there are not any critical parameters to be characterised in connection with the security of QKD systems. However, knowledge of the expected behaviour of the quantum channel is of some utility when a QKD link is setup. For this reason all

the relevant parameters can be characterised without the need of operation at single photon level. In this project we calibrated the lab based test-bed based on 50 km of fibre, exploiting well-established calibration techniques. The list of parameters investigated can be found in Table 2. After carrying out the characterisation at conventional (macrosocopic) light level we investigated the roles of these parameters in the de-coherence induced by the propagation of single-photons in the quantum channel.

Table 2: Table of parameters measured for the characterisation of the quantum channel (optical fibre).

Parameter	Symbol	Units	Definition
Spectral attenuation	$\alpha_T(\lambda)$	dB/km	Loss in optical power having traversed through the optical fibre. $\alpha_T(\lambda) = \frac{10}{L}\log\left[\frac{P_2(\lambda)}{P_1(\lambda)}\right]$ Where $P_x(\lambda)$ is the power measured at length L_x, measured in km ($x = 1,2$). L_1 is the whole fibre length and L_2 is the length of the cutback section.
Chromatic Dispersion	$D_{CD}(\lambda)$	ps/nm	$D_{CD}(\lambda) = \frac{d\tau(\lambda)}{d\lambda}$ Variation in the speed of propagation of light wave signal with wavelength
Polarisation Mode Dispersion	PMD(λ)	ps/$\sqrt{km}$	$PMD(\lambda) = \Delta\tau_g(\lambda)/\sqrt{L}$, where $\Delta\tau_g(\lambda)$ is the difference in propagation time between polarization modes.
Polarisation Dependent Loss	PDL	dB	Loss that varies as the polarisation state of the propagating wave changes.
OTDR/Optical length	L	km	It is the optical length of the fibre at a specific wavelength.
OTDR/Attenuation uniformity	D_{AU}	dB/km	$D_{AU} = \alpha_{T,L1}(\lambda) = \alpha_{T,L2}(\lambda)$ where $\alpha_T(\lambda)$ is the spectral attenuation of successive sections of different length L1 and L2 respectively
OTDR/Relative Backscattered power	P_{BS}	Unitless	The ratio between the incident and the back-reflected power by a specific section of the fibre

In fact, when a photon passes through a quantum channel as an optical fibre, the environment acts on it and processes e.g. decoherence can occur, changing the characteristics of the quantum state. Hence, it is of the utmost importance to generate, to manipulate and to characterise photons with high precision to understand their evolution during the propagation through an optical medium. In fact, a QKD source emits individual photons upon which a single bit of information is encoded in a two-level quantum mechanical system (qubit). The qubit is geometrically represented with the Bloch sphere that in optics is known as Poincaré sphere. A common and useful way to encode information is to use polarisation as degree of freedom; the photon with encoded information is then sent through a medium, usually an optical fibre, to the receiver that will infer the polarisation of the photon and get the information encoded. Hence, it is clear that a fundamental step to develop a reasonable QKD source is to have a deep control on the polarisation of the photon to be sent and to measure the polarisation after the interaction with the environment. With this aim, we performed the characterisation of the decoherence effects on the polarisation degree of freedom induced on a single photon propagating both in the lab test-bed (50 km of optical fibre, results in Figure 14) and in a real link in the metropolitan area of the city of Turin (Figure 15). This characterisation of the decoherence was achieved by performing what is called the “quantum process tomography” of the evolution of the state. This was achieved exploiting measurements performed with the single-photon polarimeter already described in the section “Polarisation state reconstruction of QKD pseudo-single-photon-source”.

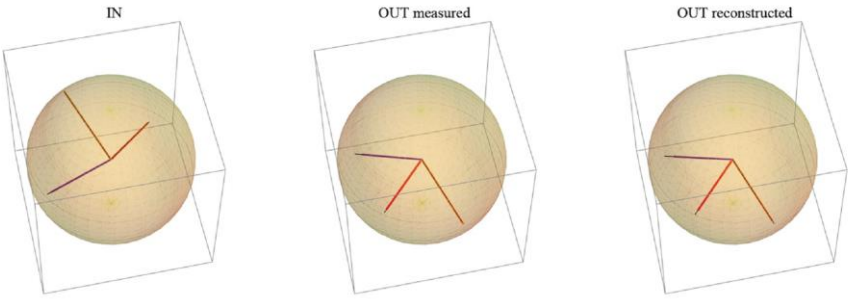

Figure 14: The polarised photons evolve in the quantum channel (50 Km of fibre link). The initial (IN) Horizontal, Diagonal and Right-circular single-photon states are reconstructed after 50 km of propagation (OUT) and are reconstructed using the results of the quantum process tomography (OUT reconstructed). The measured and reconstructed states are almost identical and the decoherence processes start to be evident in both measurements (the difference between the thin black lines and the thick coloured lines). This essentially proves the good quality of our quantum process tomographic reconstruction, i.e. our ability to reconstruct and characterise the evolution of the single-photon state.

Furthermore, in the context of this project we developed a full quantum theoretical model for the decoherence on the polarisation degree of freedom of a single photon travelling in a single mode optical fibre. According to this model, the decoherence is essentially due to the phenomenon of polarisation-mode-dispersion. This model describes the decoherence effect induced by an optical fibre. This fibre can be modelled as an “effective” non-linear media exploiting a representation for the propagation that is essentially based on a stochastic process whose complete description is achieved through a system of coupled Fokker-Planck equations.

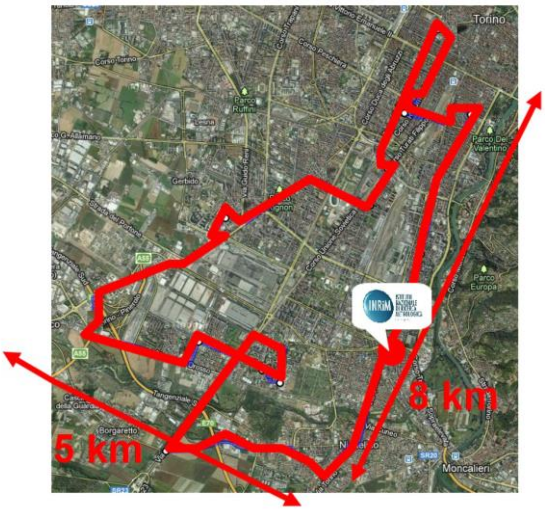

Fig. 15: The metropolitan link under the city of Turin.

Initial and final end of the link are in the Optics division of INRIM, Turin (Italy). This link is low-noise and it is used by INRIM to transfer the time signal. In this second experiment we obtained results analogous to the ones of Fig. 11, but with strongly reduced decoherence effects. This can be explained observing that an underground deployed fibre is, in general, much less affected by vibration that a spool of fibre (the lab test bed where composed of two spools of 25 km of fibre).

New devices

In addition to the measurements performed for the characterisation of the quantum channel, we have developed a certain number of devices in the context of this project that were aimed at improving the knowledge of QKD system. These new devices are listed and described below:

- *The extremely low-noise single-photon source*

We realised a heralded single photon source with extremely low-noise that exploits a fast optical switch to prevent the emission of un-heralded photons. This single photon source presented astonishingly good performances, much better than expected. In particular, this source achieved $g^2(0)=(0.005\pm0.007)$, which is the best result obtained thus far and worldwide for "real" single-photon sources. Furthermore the output noise factor (a figure of merit related to the noise of the source defined as the ratio of the number of noise photons to total photons at the source output channel) was (0.25±0.01)%. These results were achieved due to the collaboration of project participants that provided prototypes of single photon with much lower value of jitter than the corresponding commercial ones (i.e. some tens versus hundreds of picoseconds) and a pulse generator with low raising times (picoseconds) used to control the optical switch. The source was realised to test components and techniques against a real single-photon source instead of the usual pseudo-single-photon source based on pulsed attenuated laser used in the commercial QKD system.

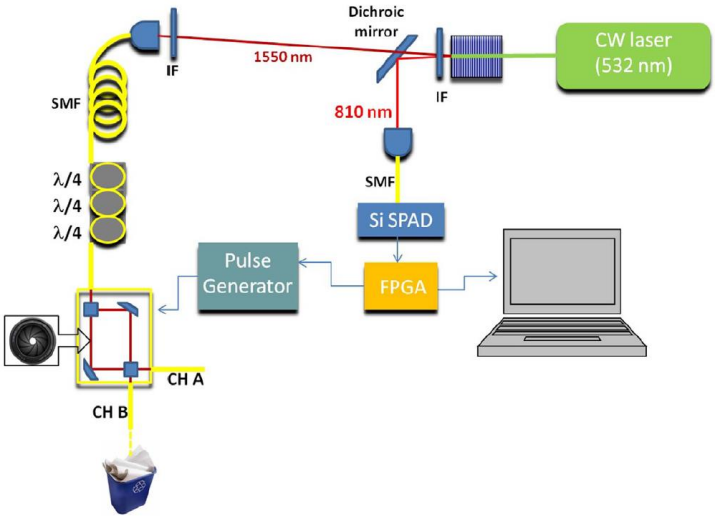

Figure 17: The set-up of the extremely low-noise single-photon source: a CW laser pumps a periodically pulsed lithium niobate (PPLN) crystal producing non-degenerate SPDC. Each signal photon at 810 nm heralds the presence of a correlated photon at 1550 nm. The heralded photon is sent to a FPGA controlled electro-optical shutter (based on lithium-niobate technology) that opens channel (CH) A for a custom time interval only in the presence of a heralding count (revealed via a Si-based SPAD).

- *The photon-number-resolving (PNR) detector based on single-photon detectors in a tree-configuration*

Two versions of the detector-tree based PNR detector were realised, one based on four commercial single-photon-detectors and three beam-splitters, and a second one where the commercial single-photon-detectors were replaced by prototypes. To produce an intelligent control of the gates, inputs and outputs of the PNR detector, a FPGA software and a FPGA board with BNC connectors were developed. This FPGA system was integrated with the detector-tree. First test measurements were successfully performed to match time delays and the outputs of the four detectors controlled by the FPGA device. Two algorithmic approaches were developed, the simplest avoided excessive trigger rate by exploiting a temporal selection of the trigger events, while the other exploited also the information from the detection outputs in order to optimise the measurement time. The complete characterisation of the detection behaviour of this PNR detector was performed and it was also exploited in an experiment aimed at optical occupation mode reconstruction (for more information, see Goldschmidt *et al* 2013).

- *The open-quantum-random-number-generator (open-QRNG)*

  Two QRNGs were chosen to investigate the links between physical parameters and randomness. In some cases these links are evident, e.g. for the open system QRNG based on a beam splitter, if the ratio of the beam splitter is not 50/50, the ratio 0/1 will not be 50/50, which affects randomness. Other links can be more difficult to establish. The analysis took into consideration the noise, beam profile, detection efficiency, after-pulses and cross-talk. Models for the beamsplitter and detector matrix QRNGs were developed. The open-system QRNG has been assembled on a breadboard. By removing the beamsplitter and replacing the straight-through bucket detector with the matrix array, the system could be converted from the beamsplitter QRNG to the matrix detector QRNG, and vice-versa. The open-system QRNGs were physically characterised in terms of the parameters discussed above. Additional software was developed to post-process the output data of the two QRNGs. The randomness produced by these two open-system QRNGs was tested with NIST, Diehard and Dieharder statistical test suites, and both of the QRNGs pass those statistical tests.

3.3 Single-photon receivers

Single-photon receivers are single-photon detectors - optically sensitive devices that probabilistically transform a single photon into a macroscopically detectable signal, most often a voltage pulse of a certain short duration, followed by amplification to a detectable level.

QKD performance can be affected by a number of factors including limited coupling efficiencies, reflection at the device surface, finite absorption probability of the photon within the device, loss of photon generated carriers and insufficient gain of the photon generated carriers. Another source of photon loss is the recovery time or dead time of the detector. A long dead time limits the data rates in a QKD system. To ensure good timing resolution of the detector, the time interval between the absorption of a photon and the generation of an output electrical signal should be short and stable, corresponding to a small time jitter (hundreds of picoseconds). This time jitter is defined as the uncertainty in determining the photon arrival time at the device.

Dark counts can arise from electrical noise in the detection circuit or through the excitation of carriers through processes such as thermal excitation. The effect of after-pulsing leads to further increase of the noise level which an eavesdropper can exploit.

InGaAs Avalanche Photodiodes

InGasAs/InP semiconductor single photon avalanche diodes (SPADs) are suitable for single photon counting or timing applications in the near-infrared spectral range (up to 1.65 µm) [Cova2009, Tosi2009]. Providing good detection efficiency and low time jitter, they can be operated in either free running or gated mode. Due to the narrow band gap (smaller than 1.1 eV) of the infrared sensitive material, which implies high charge carriers, the devices are cooled down to reduce the dark count rate and hence to improve the signal-to-noise ratio. The dark count rate is caused either by spontaneous thermal generation of free carriers due to local crystal defects or by field-assisted mechanisms, which include direct band-to-band and trap-assisted tunnelling. Latter processes become important at higher electric fields. Therefore, the dark count rate is often measured as a function of the temperature or the excess bias voltage. After-pulsing effects caused by carriers trapped into deep levels during the avalanche current flow and released later, determine the technical performance of the SPADs. Typical relaxation times of the carriers are in order of a few microseconds limiting the maximum gating frequency of a InGaAs/InP SPAD to approx. 10 MHz, and therefore the bit rate of a QKD system. Another possible approach is based on superconducting nanowire detectors that have deadtimes of a few nanoseconds. These types of superconducting detectors recently appeared on the market. Table 3 summarises the detectors' parameters characterised and the techniques used for this characterisation.

Table 3: Table of parameters relevant to commercial QKD receivers

	Parameter	Symbol	Units	Definition	Measurement approach
1	Photon detection probability	η		The probability that a photon incident at the optical input will be detected within a detection gate.	Via a calibrated laser light source and a calibrated filter
2	Dark count probability	P_d		The probability that a detector registers a detection event per gate, despite the absence of optical illumination.	As above (1)
3	Afterpulse probability	P_{after}		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.	As above (1)
4	Dead time	T_{dead}	s	The smallest time duration after which the detection efficiency is independent of previous photon detection history.	Via a train of two optical pulses with tuneable temporal separation
5	Recovery Time	T_{rec}	s	The time duration after a photon detection event for the detection efficiency to return to 99% of its steady-state value. This is only important if the detector is passively quenched	As above (4)
6	Timing jitter	T_{jitter}	s	The uncertainty in determining the arrival time of a photon at the optical input.	Measure the FWHM in the distribution of detection times

3.3.1 Measurement techniques for the characterisation of a commercial QKD detector

We have quantified and measured, in a traceable manner, different parameters necessary for a QKD photon detector to be considered a suitable detection technology. Accurate knowledge of the detector performance is critical to QKD performance as the receiver needs to know how many clicks on the detector could be due to detector inefficiencies, after pulsing etc. Having taken these numbers into account any further anomalies can be attributed to the eavesdropper.

In the following we describe the measurement techniques developed in the context of this project in order to characterise the properties of the single-photon detectors.

Measurement of photon detection probability

This work dealt with the detection efficiency of commercial single-photon detectors for QKD. The aim was to establish traceability to national standards for commercial single-photon detectors operating at 1.55 µm. Different techniques and approach were considered:

Measurement of photon detection probability using an attenuated laser with a commercial attenuator and with the attenuator with InGaAs diodes in trap configuration

The photon detection probability is one of the most important parameters specifying QKD systems. It can be measured by following the experiments carried out by Yuan et al. [Yuan2007], which are also suitable for determining the after-pulsing probability and the dark count probability. The SPAD is illuminated by the pulsed laser source attenuated to the low photon level. Both devices are triggered by a pulse generator, whereby the laser pulse frequency is stepped down by a factor R compared to the detector gate rate. The same experimental set-up can be used to measure the after-pulsing probability P_{after}. A time-correlated

photon counting device is used to record a histogram of time delays between the laser trigger and the detector output signal. At zero-time delay the histogram peak is dedicated to the detection events observed under laser light illumination. With the knowledge of the dark count probability P_d and the after-pulse probability P_{after} the photon detection efficiency η can be obtained by measuring the probability P_i to detect a photon at each illuminated gate as a function of the laser power. The latter is described as n photons per laser pulse on average.

$$\eta = \frac{P_i - P_d}{n} \cdot \frac{1}{1+P_{after}} \quad (5)$$

The average number of photons per laser pulse n can be obtained by calibrating the attenuated laser source against a traceable detector standard. The first experiment was performed exploiting a commercial attenuator. An improved measurement was performed exploiting the attenuator based on InGaAs photodiodes in transmission trap configuration described in the subsection “New Devices”.

The detection efficiency of single-photon with the attenuator based on InGaAs photodiodes was measured exploiting the setup shown in Figure 9. The measurements were carried out using passive fibre coupling instead of the active coupling because it was found that the attenuation (output power/input power) with active coupling was significantly better than without active coupling (~ 2.7×10^{-6} compared to ~ 6.2×10^{-6}), but that the variability was much larger (4 % compared to 1.5 % (k=1)).

A pulsed laser operating at 1549.6 nm was used. Agreement between detection efficiency of a photon counter measured using the photodiode attenuator and using the commercial attenuator based system was within 3 %. Investigations suggested that this might be due to the alignment optimisation hunting when there was no power, leading it to re-optimise in a local minimum when power was subsequently re-applied. As noted before, the performance of the device was found to be satisfactory without active coupling and the target uncertainty of 3 % was achieved. However, further investigation into the active coupling may be carried out by participants subsequent to this project.

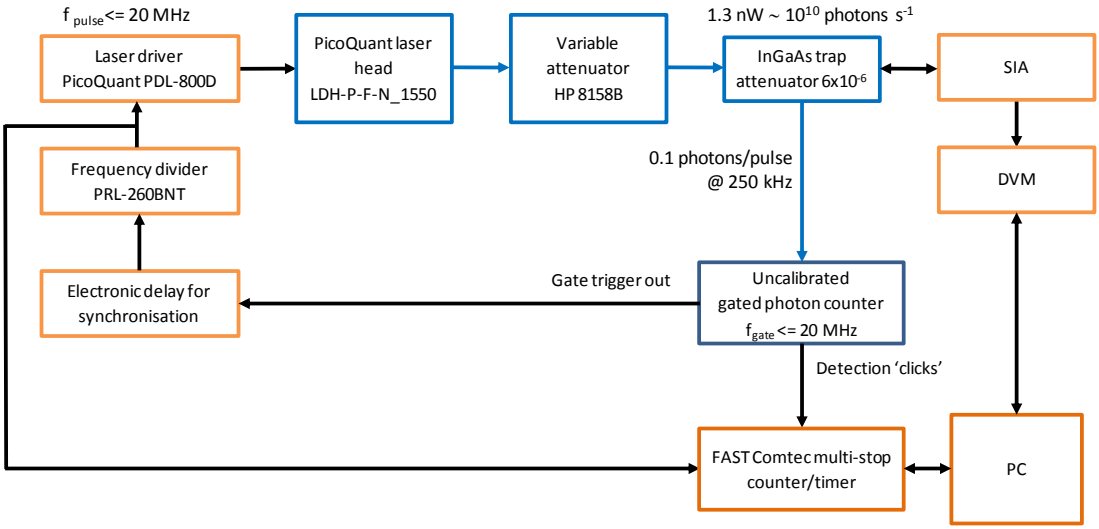

Figure 9: Setup for the determination of the single-photon detector detection efficiency using the variable attenuator.

The whole system allows calibration of commercial InGaAs-SPAD diodes with an uncertainty in the order of 3 %, which is now the state-of-the-art.

Measurement of photon detection probability using a metrology light source (MLS)

A novel reference standard for calibrating photon receivers (fibre coupled single-photon detectors) using an absolute light source based on synchrotron radiation at 1.55 µm was realised in the context of this project. A setup for the passive coupling of the synchrotron radiation from the PTB’s Metrology Light Source (MLS) into a fibre was established, thus providing a novel reference for calibrating photon receivers. In detail, a passive fibre coupling setup had successfully been applied to send the synchrotron radiation to the fibre coupled InGaAs photodiode (secondary standard for radiative power) and to the superconducting nanowire single-

photon detector (SNSPD), which was the device under test. Initial measurements of the coupling efficiency of the setup were found to be stable and independent of the synchrotron ring current. In order to perform the calibration, an InGaAs photodiode was characterised for its use as a reference detector standard for the calibration of the fibre-coupled single-photon detector at the MLS. The spectral responsivity has been interpolated for the wavelength where the detection efficiency calibration of the SNSPD was carried out, i.e. at 1551.97 nm. At this wavelength, the spectral responsivity of the detector was determined to *s*(1551.97 nm) = 1.17836 A/W with *u*(s(1551.97 nm)) = 0.15%. For the test of the polarisation dependence of the responsivity, the detector was rotated against the fibre-coupler and the photocurrent was measured for the positions 0°, 90°, and 180°. Within the relative uncertainty of the measurements (0.125%), no systematic polarisation dependence was observed. These measurements were carried out for laser radiation at a wavelength of 1.55 µm. For the calibration procedure it is necessary to have the reference detector under-filled. In order to validate this, the distance between the detector surface and the fibre tip was optimised by measuring the photocurrent for different distances. Finally, the fibre-coupled SNSPDs was calibrated at the few photon level against the InGaAs photodiode operating at the classical power level taking advantage of the proportionality of radiant power and current of stored electrons of the synchrotron radiation source. For this calibration, the synchrotron radiation (SR) has been monochromatised by a filter with a central wavelength of 1550 nm and fed into a single mode optical fibre (SMF-28) for wavelengths of 1550 nm. The SSPD was current biased to 90% of the critical bias current. To increase the available radiant power of the MLS per stored electron the undulator U180 of the MLS has been used in this calibration campaign. The fibre coupled synchrotron radiation is then connected to the reference detector, a calibrated InGaAs photodiode, and the SNSPD sequentially. The absolute photon rate per stored electron that is coupled into the fibre is determined at a ring current I_{high} of about 1 mA using the reference detector based on an InGaAs detector that has been calibrated traceable to the cryogenic electrical substitution radiometer. At this level the ring current has been measured with a relative standard uncertainty of 5×10^{-3} by parametric current transformers. The ring current was then reduced to approximately one nA. At this ring current (I_{low}), i.e. about thousand stored electrons, the count rate of the SNSPD, normalised to the ring current, has been measured a number of times. The detection efficiency of the SNSPD was determined from:

$$DE_{SNSPD} = c\frac{CR_{SNSPD}S_{ref}E_{Phot}I_{med}\tau}{N_{Ilow}e^{-}i_{ref}} = cDE^{\sim}_{SNSPD}, \qquad (6)$$

with CR_{SNSPD} the measured count rate of the SNSPD, S_{ref} the spectral responsivity of the reference detector, E_{phot} the energy of a photon with a wavelength of 1550 nm, I_{med} the measured ring current in the medium ring current range of the MLS, τ the revolution time of a stored electron of 160 ns, $e-$ the elementary charge, I_{ref} the measured photocurrent of the calibrated reference detector, N_{Ilow} the number of stored electrons and c the correction for the deadtime of the SNSPD, the bandwidth of the synchrotron radiation and the applied bias current. As a result, the detection efficiency of the SNSPD, measured at the entrance of the fibre, at a wavelength of 1552 was DE_{SNSPD} = 15.01 % ± 0.28 %. The main contribution to these overall uncertainties is the uncertainty associated with the polarisation dependence of the detection efficiency of the SNSPD. A target uncertainty of 5 % was achieved.

Measurement of dark count probability

The dark count probability of a detector was measured by recording detection events per gate or per unit time in the absence of photon flux illuminating the detector's sensitive area. To perform the measurements, a counting device records the detector output signal. In order to count only detection events during gates, a time-correlated photon-counting device was used to record the detector output signal. By correlating many dark count events with a clock signal triggering the detector gate, a time delay histogram could be observed. To calculate the dark count probability of the detector, the detected count rate was normalised to the total number of applied gates. The uncertainty in general depends on the uncertainty of the trigger clock signal (that in most cases provides a negligible contribution) and the uncertainty of the counting device (typically plus/minus 1 count), both of which can be calibrated against a traceable frequency standard, as well as the count statistics (that scales as the inverse of the square root of the measurement time, and typically is the dominant uncertainty contribution).

Measurement of after-pulse probability

The after-pulse phenomenon introduces a secondary source of dark counts, with a charge carrier production rate proportional to the trap levels. These levels have fairly long lifetimes and fairly high concentration in

InGaAs/InP SPADs. As a result, the after-pulsing effect can limit the transmission rate of single photons in QKD systems. The after-pulse probability of the SPAD can be measured exploiting a setup similar to the one used for the measurement of the probability of detection.

The pulsed laser repetition rate was scaled down by a factor *R* compared to the detector gating rate, in order to observe detection events in the detector gates lying between the gates corresponding to consecutive laser pulses (*R*-1). A signal time-correlated photon counting technique recorded a histogram of time delays between the laser trigger and the detector output. Peaks at a time delay in this histogram not corresponding to an illuminated gate were generated by photon events caused by the after-pulse effect (and dark counts). By normalising the detected count rate to the total number of applied gates, the after-pulse probability can be calculated from

$$P_{after} = \frac{P_{n-i} - P_{dark}}{P_i - P_{n-i}} \cdot R \tag{7}$$

P_{dark} is the dark count probability, P_i is the probability to detect a photon at each illuminated gate and $P_{n\text{-}i}$ is the probability of a detection event at each non-illuminated detector gate after a previous optical excitation of the detector. The uncertainty is dependent on the uncertainty of the clock frequency and the temporal resolution of the time-correlated photon counter, both of which can be calibrated against a traceable frequency standard, and the uncertainties due to P_{dark} and the count statistics. Uncertainties below the 1% level were achieved.

These measurements are illustrated in Figure 10.

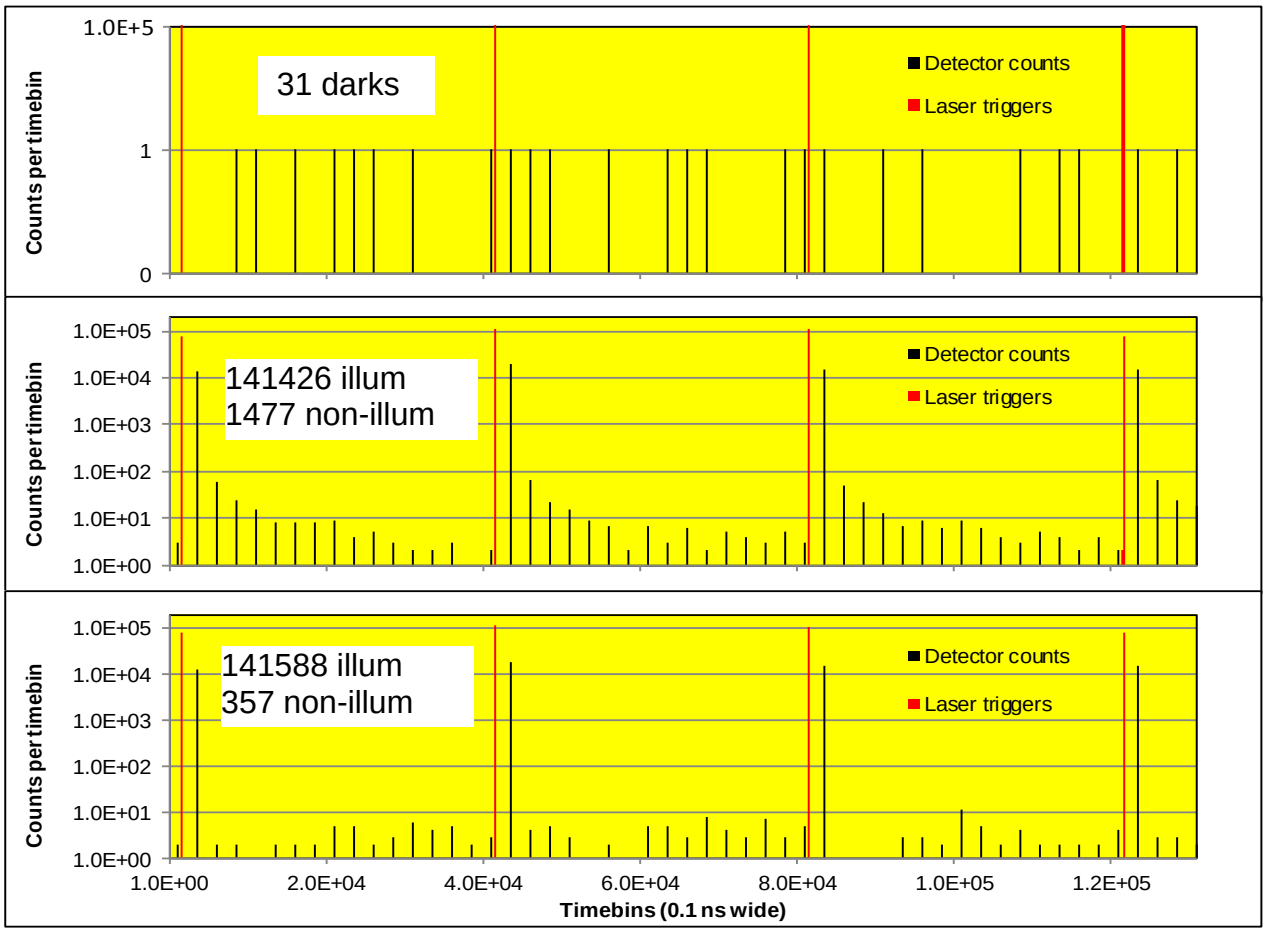

Figure 10: Illustrative data for gated detector calibration.

In the top diagram, the dark count probability is measured. The detector was gated at 4 MHz, while the laser was triggered at 250 kHz. The red lines show the laser triggers, and the black lines the detection events. The detector gate was synchronized with the arrival of the laser pulse, but in the plots the gates are offset for clarity. Note the logarithmic ordinate axis. Data is analysed for the three complete intervals following a laser pulse, i.e. 48 detector gates. The histograms are built from 262144 (2^{18}) sweeps. The top panel (laser blocked) shows the dark counts, from which we obtained P_{dark} = 2.46 x 10^{-6} per gate. In the middle panel (laser unblocked) there is a large number of detections in the gate immediately following the laser (true detections plus dark counts), while in the following gates there are events corresponding to after-pulses and dark counts. This data yields P_{after} = 0.0109, η = 0.28. A similar plot is shown in the bottom panel, in this case leading to P_{after} = 0.0025, η = 0.28. This data was collected using a Princeton Lightwave PGA-602 photon counter. It has the facility to blank a number of detector gates immediately following a detection event, in order to suppress after-pulses. In the middle plot, the blanking was set to zero, i.e. no blanking, whereas in the lower plot the blanking was set to 7 gates. The fact that in the lower plot there are detection events in the 7 detector gates immediately after the illuminated gate is because the detection efficiency is less than 1, and therefore blanking is not activated for every laser pulse, leading to the possibility of dark counts and very long delayed after-pulses from previous events. A full analysis of the data takes account of the time sequence of the events, information that is lost in the histograms. Longer data acquisition times could be used to reduce the uncertainty in the count statistics below the 1% level.

Measurement of dead time and recovery time

The dead time limits the maximum count rate of a single-photon detector and therefore the transmission rate of the QKD system. To measure the dead time a train of double laser pulses at a wavelength of ~1.5 µm were sent to the detector. The pulses should have equal power levels and a variable time separation. The laser pulses, with their relative time delay, were synchronized to the detector gates. The relative time delay between the two laser pulses should not be smaller than the time of two gating periods. In order to determine the probability for simultaneous detection of both pulses, the detector output could be recorded as single waveforms by an oscilloscope over several detection events. The dead time and the recovery time were obtained by measuring this probability as a function of the variable time delay.

Measurement of timing jitter

To ensure good timing resolution of a single photon detector, the time interval between the absorption of a photon and the generation of an output electrical signal should be short and stable, corresponding to a small timing jitter. A common technique to determine this parameter is to measure the full-width half-maximum (FWHM) of the detector's instrument response function. The jitter of the InGaAs SPAD (id201, ID Quantique) was determined by correlating many detection events with the trigger signal of the laser. A time delay histogram could be observed by a time-correlated photon counter (time resolution ~4 ps, Pico Harp 300), from which the detector's response function can be calculated. For that purpose the full-width half-maximum (FWHM) of the laser pulses illuminating the SPAD should be smaller than the SPAD's timing jitter. To prove this the jitter of the pulsed laser (~145 ps) was measured using a superconducting nanowire detector (SSPD). This detector featured a jitter of ~ 44 ps calibrated against the temporal duration of a synchrotron light pulse of ~22 ps from the MLS (Metrology Light Source). The jitter of the SPAD was determined to ~355 ps. Due to the comparable large jitter between of the SPAD's gate signal and the output signal an uncertainty of ~65 ps was calculated.

3.3.2 Characterisation of the photon-number-resolving (PNR) detector based on a tree configuration

The PNR detector based on a tree configuration described in section 3.1 was characterised using different measurement techniques. This was necessary to prove that the novel device, developed and realised in the context of the project, behaves as expected.

In a first investigation, the overall detection efficiency of the PNR detector was investigated. This was characterised by means of traceable calibration of the detection efficiency of the commercial single-photon detectors and passive optical components. The detection efficiency of a detector tree consisting of four InGaAs single photon detector modules was determined by using transfer standards traceable to primary standards. The expanded uncertainty of the detection efficiency achieved is ≤ 2.3 %, thus the target uncertainty of 7 % was achieved.

As an example for the obtained results, the detection efficiency of a PNR detector in passive configuration is shown in Figure 11. The dependence on the mean photon number is clearly observed. Figure 12 shows the corresponding experimental setup.

Finally, the PNR detector efficiency was characterised by means of reconstruction of the behaviour of the PNR detector by means of Quantum Process Tomography. Performing the reconstruction of the behaviour of the PNR detector essentially means being able to recover the Positive Operator-Value Measurements (POVM) of the PNR detector.

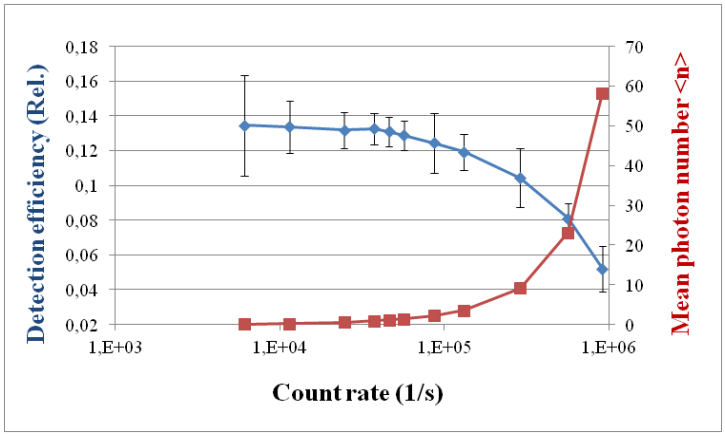

Figure 11. Detection efficiency (left axis, blue) of the photon-number-resolving (PNR) detector in passive configuration as a function of the count rate of the PNR-detector and the corresponding mean photon number <n> (right axis, red).

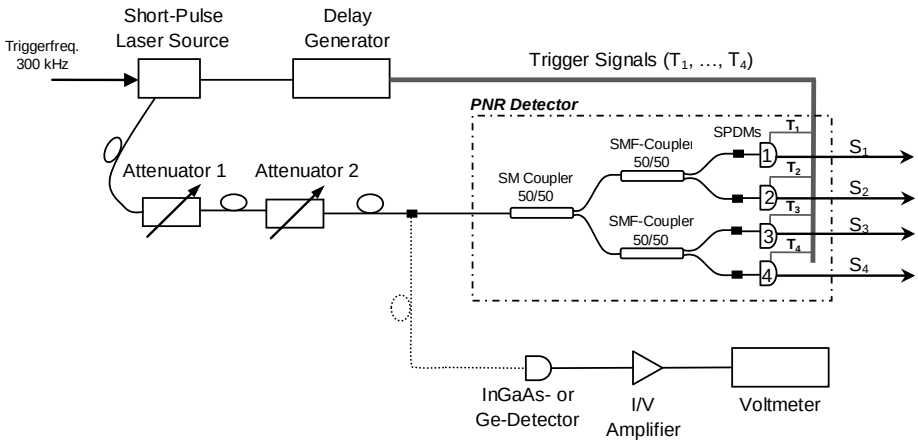

Figure 12. Measurement setup for the calibration of the photon-number-resolving (PNR) detector by using a standard InGaAs- or Ge-photodiode and a short-pulse laser source at a wavelength of λ = 1550 nm.

With a detector-tree configuration, the PNR detector considered in the project is phase-insensitive and we can state that it presents a diagonal POVM of the form:

$$\Pi_n = \sum_m \Pi_{n,m} |m\rangle\langle m| \qquad (8)$$

where the $\Pi_{nm} = \langle m|\, \Pi_n |m\rangle$ element represents the detector tree probability of counting n = 0,1,2,3 4 photons with 'm' impinging photons per pulse. In order to reconstruct these Π_{nm}'s, we probed our device with a set of

J suitably chosen coherent states (of different intensity, but anyway with up to few tens of photon per pulse). In this framework, the response of our PNR detector to the j-th coherent probe can be written as:

$$p_{n,j} = \sum_m \Pi_{n,m} q_{m,j} \tag{9}$$

being $q_{m,j}$ the Poissonian photon statistics with mean photon number μ_j of the j-th coherent state. Once we have estimated the p_{nj} probabilities from the experimental data, to reconstruct the Π_{nm} elements we apply a minimization algorithm to the distances between the two quantities in Eq. (9) for all the values of 'j' (i.e. for all the coherent states measured).

The results of the Π_{nm}'s reconstruction are shown in Figure 13. It is observed that the experimentally reconstructed Π_{nm}'s are in a very good agreement with the theoretically expected values up to N= 40 incoming photons. However, for $N \geq 40$ photons the reconstruction algorithm is not reliable anymore because of the little information at high photon regimes and the truncation of the algorithm at 60 photons. To prove the fidelity between experimental and theoretical results, the root-mean square deviation (RMSD) was calculated. The RMSD obtained between the experimental and the theoretical probabilities, for $N \leq 40$, is larger than 98.31%.

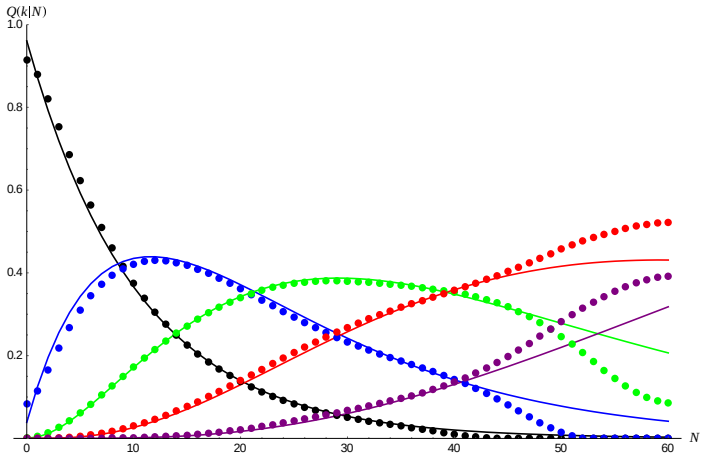

Figure 13. Reconstruction of the mode distribution of the laser optical field using the PNR detector. The dots represent the result of the experimental reconstruction of the Π_{nm} elements, while the solid curves are the expected values evaluated starting from the specific detection model describing the detector tree and from the calibration of each single components (i.e. beam splitters and single-photon detectors). Curves and dots colours: Black: Π_{0N} , Blue Π_{1N}, Green: Π_{2N}, Red: Π_{3N} and Purple: Π_{4N}.

New devices

In addition to the new measurement techniques developed which contributed to the realisation of single-photon-metrology for single-photon detectors operating at telecom wavelength, we realised a new device, more specifically a single-photon-optical-time-domain-reflectometer (single-photon-OTDR), to perform the measurement of back-flashes from single-photon detectors:

- *The single-photon optical-time-domain-reflectometer (single-photon-OTDR)*

  The knowledge about back-flashes are important for the security of a QKD system. For this reason we decided to develop an OTDR operating at single-photon level, because conventional OTDR are not able to detect back-flashes. In fact, this system is able to identify the behaviour of active elements at much lower sensitivities than achievable by commercial OTDR systems. Exploiting this single-photon OTDR, we were able to observe the presence of back-flashes from both a prototype (by PoliMi) and a commercial single photon detector (by ID Quantique). Two versions of OTDR operating at single-photon level were realised. The first exploited a common commercial single-

photon detector (ID Quantique model id201) operating in gated mode. The second, an improved version of the OTDR was realised by exploiting a novel single-photon detector operating in free-running mode (on loan to INRIM from ID Quantique, model id220). This second approach took advantage of the free running and low dark counts level of the id220 and enabled to perform the measurement on long haul fibre at extremely low light level. Furthermore, this improved OTDR operating at the single-photon level exhibits a surprisingly good temporal resolution (less than 150 ps corresponding to approximately 1.5 cm resolution, much better than the typical 50 cm resolution).

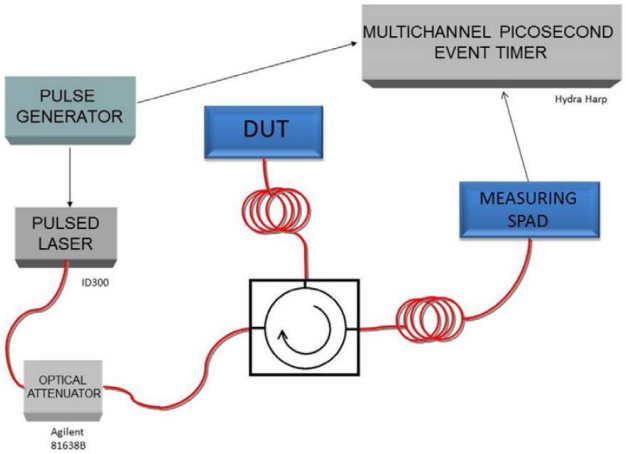

Figure 16: The set-up of the photon-counting OTDR: a commercial pulsed diode laser emitting at 1550 nm, with pulse width shorter than 300 ps, is strongly attenuated with a variable optical attenuator and sent to a pigtailed optical circulator. The optical signal back-reflected from the fibre/device under test (DUT), after passing through the circulator, is detected by means of a single-photon detector based on a free-running InGaAs–InP SPAD. The detector output signal is correlated to the synchronisation signal from the pulsed laser exploiting TCSPC measurement technique.

4 Actual and potential impact

The collaborative work in this project lead to the development of techniques and facilities for the traceable characterisation of single-photon components of QKD systems, in particular single-photon sources and detectors operating in the 1.55 micrometres telecom band. The project outputs set the foundations for a European measurement infrastructure able to validate the performance of QKD systems and technologies that use and manipulate single photons.

4.1 Metrology achievements

The following developments have been realised within this project:

(i) Characterisation of optical pulses produced by photon emitter

- Reliable methods for measuring mean photon number traceably to cryogenic radiometry (the SI);
- Technique for measuring photon number probability distribution using non-PNR detectors;
- Construction and characterisation of an extrinsic PNR detector, comprising four spatially multiplexed non-PNR detectors, and application to measurement of photon number probability distribution;
- Construction and characterisation of a tuneable Fabry-Perot resonator to measure spectral linewidth, and application to measurement of the spectral indistiguishability.

(ii) Characterisation of quantum channel

- Construction of a single-photon polarimeter, and application to measuring evolution of polarization in field-installed single-mode fibre

(iii) Characterisation of single-photon detectors in receiver

- Reliable methods for characterising gated SPADs, SNSPDs, and extrinsic PNR detectors traceably to cryogenic radiometry (the SI);
- Construction and characterisation of a heralded single-photon source, and its application in tests on sources and detectors characterisations;
- Construction and characterisation of a calibrated attenuator to simplify detector characterisation, and application to SPADs;
- Construction of a single-photon OTDR with better temporal resolution and able to identify the behaviour of active elements at much lower sensitivities than commercial OTDR systems. Application of this OTDR to measurement of back-flash from a commercial SPAD (measurement that is possible because of the single photon sensitivity of this OTDR);

These achievements have been reported in the scientific literature (see section 6) so that the user community can access them.

4.2 Dissemination activities:

(i) Scientific publications

23 peer-review papers have been published and 2 are in preparation. In addition, 5 papers have been published as conference proceedings (see section 6).

(ii) Conference presentations

34 oral presentations and 22 poster presentations were given at international conferences in Europe North America and India. In addition, 2 presentations were given at high-level international metrology business meetings, and 18 presentations at national and international workshops.

While the majority of these presentations reported technical results obtained in the project, others were given to promote the work of the project in developing the metrology that would help accelerate the commercial uptake of QKD. A few key conferences are highlighted:

a. QKD-focused conferences – QCrypt2013 and QCrypt2014. A poster on the development of a high-speed quantum random generator, part of which was concerned with the work in this project, was presented at QCrypt2013. Four poster presentations were given at QCrypt2014. These presentations summarised the outcomes of the project, the development of traceability at the single-photon level, the measurement of back-flash from the single-photon detectors used in QKD systems, and the realisation of a heralded single-photon source which can be used to characterise QKD detection systems.

b. Single-photon workshops – SPW2013. Presentations were given on the overall project, on methods for calibrating single-photon SPAD and SNSPD detectors, and on measurements on quantum random number generators and QKD modules. INRIM, NPL, and PTB were members of the scientific committee and contributed to the organisation of scientific programme.

c. Metrology conferences – NEWRAD 2011, NEWRAD 2014. The objectives of the project were presented at NEWRAD 2011, and the results presented in 3 oral and 4 poster presentations at NEWRAD 2014. The 3 oral presentations were among the 23 selected from 162 submissions for publication in a special issue of Metrologia. The presentations showed the advances in single-photon metrology achieved by the project and their application to QKD systems.

d. ETSI post-quantum cryptography workshops. The impact of quantum computing on current algorithmic encryption techniques is a concern that has led to ETSI organising two workshops within the last 13 months to discuss the standardisation and deployment of the next-generation cryptographic infrastructure, in particular, one that will be secure against emerging quantum computing technologies [http://www.etsi.org/news-events/past-events/770-etsi-crypto-workshop-2014]. The consortium was represented at both meetings, showing how the work in this project will enable QKD to address these requirements, and contributing to the wider discussion on next-generation cryptographic infrastructure.

(iii) Lectures

Metrology Summer School. A lecture “Metrology for Quantum Communication Technologies” was presented at the International School of Physics "Enrico Fermi" - Metrology and Physical Constants, which was held in July 2012 at Varenna, Italy. An international audience of PhD students, post-docs, and young scientists attended this summer school. A book compiling all of the lectures was published in 2013 (see Section 6).

(iv) Best practice guide & review article

A best practice guide outlining the measurement procedures to be followed in the characterisation of attenuated-laser single-photon sources and single-photon avalanche photodiodes, and a review article on metrology of single-photon sources and detectors were made available on the project website. The best-practice guide states what equipment and procedures are required to characterise these devices, allowing the users to carry out these measurements by themselves. The review article surveys the different types of single-photon sources and detectors that are available and currently under research, and references the various measurements that can be performed to characterise such devices.

(v) Standardisation

Three project partners (INRIM, NPL, PTB) are members of the ETSI ISG-QKD and attended meetings of the ISG. 7 presentations on the work were given at the ISG-QKD international standardisation meetings and inputs were given to the drafting of 3 documentary standards of ETSI QKD-ISG.

A paper by the ISG, entitled ‘Worldwide Standardisation Activity for Quantum Key Distribution’ has been accepted for presentation at the IEEE GLOBECOM 2014 in December 2014, one of the two flagship conferences for IEEE Communications Society. The paper discusses the ongoing worldwide activity to develop forward-looking standards for QKD in the ETSI ISG-QKD.

(vi) CCPR

The Consultative Committee for Photometry and Radiometry (CCPR) is a Consultative Committee of the International Committee for Weights and Measures (CIPM), and its activities concern measurement standards for optical radiation measurements. Within the Consultative Committee there is a Strategy Group looking at the requirements for single/few-photon metrology that is planning to carry out pilot comparisons in the single-photon regime in order to build confidence in single-photon metrology. Project partners (INRIM, PTB, NPL, CMI, KRISS), who are also members of the Strategy Group on few-photon metrology, have ensured that the telecom region will be covered in such comparisons.

(vii) Project Workshop

At Quantum 2014, held in INRIM, Italy, a session was devoted to the project workshop. Presentations were made on backscattering characterisation of QKD modules, calibration of superconducting single-photon detectors, heralded and defect-generated single-photon sources, and on a public demonstration of a characterised QKD system.

4.3 Training activities

Training was given between partners of the consortium. In particular:

(i) NPL provided a short course on optical radiation and fibre-optics metrology to REG(IDQ);

(ii) PoliMi provided training on the detectors developed to staff at INRIM;

(iii) INRIM provided an introduction to the components of QKD systems to REG(UOULU);

(iv) INRIM provided training on single-photon OTDR to a member of KRISS;

(v) INRIM provided a short course on single-photon sources to a member of KRISS.

In addition, a training package has been created and four on-demand web lectures discussing basic aspects of QKD are online at http://www.activeresearch.eu/; As of August 2014, 69 participants were registered since the lectures went 'live' in March 2014. The web lectures are as follows:

(i). 'Introduction to QKD' by Momchil Peev, Austrian Research Centers GmbH ARC (Austria),

(ii).'Practical QKD' by Gregoire Ribordy, ID Quantique (Suisse),

(iii). 'Security of the QKD' by Norbert Lütkenhaus and Vadim Makarov, University of Waterloo (Canada),

(iv). 'Metrology for QKD' by Christopher Chunnilall, National Physical Laboratory (UK)

4.4 Early impact:

(i) Standards

The Industry Specification Group of the European Telecommunications Standards Institute (ETSI ISG-QKD) is the only known standardisation initiative for QKD systems worldwide [T. Länger, G. Lenhart, ETSI standardisation of quantum key distribution and the ETSI standardisation initiative ISG-QKD, New Journal of Physics, 11, 055051, (2009); http://www.etsi.org/index.php/technologies-clusters/technologies/quantum-key-distribution]. Three National Metrology Institutes (NMIs) involved in this project (INRIM, NPL and PTB) are members of the group and through them the project consortium ensured that the work being carried out was aligned with the industrial requirements. It is recognized that one of the building blocks necessary to achieve QKD systems standardisation is that of traceable measurements at the single-photon level and the project consortium provided the ISG with the experience and expertise on these measurements.

The project partners INRIM, NPL and PTB participated in the review of the published ETSI document "GS QKD 003: Quantum Key Distribution (QKD); Components and Internal Interfaces" (before the project start), and to the drafting of current ETSI documents "DGS/QKD-0011_OptCompChar: Quantum Key Distribution (QKD) Component characterisation: characterising optical components for QKD systems" (NPL is the rapporteur, INRIM contributed writing some sections and reviewing the document, PTB reviewed the document) and "DGS/QKD-0010_ISTrojan: Quantum Key Distribution (QKD) Implementation security: protection against Trojan horse attacks in one-way QKD systems" (NPL, PTB and INRIM reviewed the document).

The work undertaken in this project advances the development of standards which will be used for validating and certifying QKD systems, thereby supporting European QKD manufacturers and the need for secure data transfer.

(ii) Industrial and other user communities

a. The project provided some of the metrological expertise that underpinned the measurement aspects of a public demonstration which involved a characterised QKD over a single field-installed lit fibre. This demonstration was performed by Toshiba Research Europe Limited (a QKD system developer), BT Group plc (the UK's largest network provider), ADVA Optical Networking SE (a provider of data encrypters to network providers), and the project partner NPL. It demonstrated to key users and providers of secure communications that QKD and QKD-secured data can be transmitted over a single fibre and does not need dedicated and expensive dark fibre to be used for the quantum channel in a QKD link. This work makes QKD a more attractive commercial proposition, and will accelerate its commercial deployment.

b. A European company used a facility developed in the project to characterise the relative spectral response of its single-photon detectors. This is of general value for the use of these detectors in a broad range of single-photon applications, and will advance the market take-up.

c. The back-flash from a commercial single-photon detector operating at telecom wavelengths was measured. Back-flash from a QKD detector can provide a side-channel which can be exploited by a quantum-hacker. Knowledge of the back-flash and its characteristics enables appropriate counter-measures to be implemented when this detector is used in QKD systems.

d. The detection probability of commercial single-photon detectors has been measured for a European company as a test of the performance of an internal component.

(iii) Metrological and scientific communities

This project tackled the measurements required for characterising the optical components of QKD systems operating in a benign environment. However, QKD systems are targets for hacking attacks [Lo2014] and for every attack so far identified, counter-measures have been devised. This, as well as work in ETSI ISG-QKD DGS/QKD-0010 (see (i) above), shows that traceable measurements are also required to verify whether such counter-measures have been effectively deployed.

4.5 Long-term impact:

The impact of quantum computing on current algorithmic encryption techniques is a concern that has led to ETSI organising two meetings within the last 13 months to discuss the standardisation and deployment of the next-generation cryptographic infrastructure, in particular, one that will be secure against emerging quantum computing technologies [http://www.etsi.org/news-events/past-events/770-etsi-crypto-workshop-2014]. QKD is currently the only guaranteed solution for future-proofing data against such advances in computing. Although post-quantum encryption algorithms are believed to be resistant to quantum computation, that is not guaranteed by information theory and the laws of physics, as is the security of QKD. QKD will therefore be an important component for the next generation of cryptographic infrastructure. This has led to current work to develop QKD networks in the USA, China, and South Korea; networks in other countries/continents are expected to follow.

Quantum cryptography therefore has great potential to become the key technology for securing confidentiality and privacy of communication in the future ICT world, and thus to become the driver for the success of a series of services in the fields of e-government, e-commerce, e-health, transmission of biometric data, intelligent transport systems, and in many other areas.

Standardisation is one of the key elements for the success of such an initiative and Europe has the potential to lead the development of globally accepted standards and an anticipatory approach that would facilitate the market uptake globally. This project has developed **traceable measurement techniques for the quantum optical components of QKD systems** and participated in the review and drafting of **ETSI pre-standard documents.** This will enable the ETSI ISG-QKD to continue to drive the standardisation process and to achieve the goal of implementing a validation and certification process for QKD systems, ultimately revolutionising data security in ICT.

The project has also demonstrated to the industrial and user community that the necessary metrological foundations for the standardisation of QKD are being developed, thereby providing confidence for the continued development and deployment of this technology.

The measurement techniques and devices developed in this project will also serve the needs of other developing quantum photonics technologies that rely on the production, manipulation and detection of single photons (e.g. single-photon detection for medical and biological, single-photon based microscopy, LIDAR, etc.). European industry has a prominent position in quantum technologies in general and in QKD in particular. Several European SMEs have based their business models on QKD. In addition, a number of industrial players have already invested in QKD R&D projects under the umbrella of the EC Framework Programs 6 and 7 and it is expected that this trend will increase with the Horizon 2020.

This project has therefore made a significant contribution to the foundations of a robust quantum industry that will provide a step change in the telecommunication industry and future-proof data management that will impact on us all.

Through its advancements on QKD technologies, it is expected that this project will have a wider indirect impact in four key areas:

Social, economic and political impact. “Information in many ways equates to geopolitical, social, and economic power. The economic, social, and political well-being of developed countries depends on integrity, confidentiality, and authenticity of sensitive data sent over networks. Corporations and governments have legal responsibilities to their investors, constituents, and customers to preserve the confidentiality of sensitive information. Whether this information consists of military communications, secret government documents, industrial trade secrets, or financial and medical records, interception of information allows adversaries to not only learn about the contents of these communications, but also to discover metadata in patterns within a

network of communicators, to extract general patterns using machine learning, and even to insert false or misleading information or malware into a data stream." [ETSI].

Modern information and communication technologies are present in various social aspects of our lives. Personal data, such as medical records, is increasingly being converted into digital format and there have been some instances where digital storage media have been lost or stolen. As stated in the document published jointly by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" [EUC], the secure transmission of information and the protection of privacy of individuals is important for the data traffic at public institutions, and for strengthening and maintaining the competitiveness of the European economy. This document shows that quantum cryptography is increasingly seen by policy-makers as one way, and maybe the only way, to secure data transmission.

QKD technology remains largely in the first stage of commercialisation, with the technology being offered primarily to government, military, and research institutes. The QKD market is nevertheless expected to expand in the coming years, based on the availability of certified and standardized products, and technology advancements that help extend its application beyond point-to-point connections to cover global communications. Continuous and incremental technology innovation in fibre, protocols and free-space is expected to result in the decline in the price of the equipment and related accessories in the coming years. Global market for QKD is projected to reach $1.0 billion by 2018, driven by the need to secure the transmission of sensitive communications [market].

Environmental impact. Successful deployment of validated QKD systems will encourage and accelerate the use of network communications and services, such as secure video conferencing and secure data transfer of important documents, thereby reducing our dependence on travel- and paper-based communication.

References

[Alleaume2007] R. Alléaume, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter and A. Zeilinger (2007) SECOQC White Paper on Quantum Key Distribution and Cryptography arXiv:quant-ph/0701168;

[Brida2011] G. Brida, M. Genovese, M. Gramegna, A. Meda, F. Piacentini, P. Traina, E. Predazzi, S. Olivares, and M. G. A. Paris, "Quantum state reconstruction using binary data from on/off photodetection," Advanced Science Letters **4**, 1-11 (2011).

[Brida2011_2] G. Brida, I. P. Degiovanni, M. Genovese, A. Migdall, F. Piacentini, S. V. Polyakov and I. Ruo-Berchera, Opt. Expr. 19, 1484 (2011).

[Dusek2006] M. Dusek, N. Lütkenhaus and M. Hendrych, Quantum Cryptography Progress in Optics vol 49 ed E Wolf (Amsterdam: Elsevier 2006) pp 381–454

[Cova2009] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single.photon avalanche diodes and quenching circuits," Journal of Modern Optics **15**, 1267-1288 (2009).

[Edwards2005] C.S. Edwards, H.S. Margolis, G.P. Barwood, S.N. Lea, P. Gill, W.R.C. Rowley, "High-accuracy frequency atlas of $^{13}C_2H_2$ in the 1.5 μm region", Appl. Phys. B **80**, 977-983 (2005)

[Eisaman2011] M. D. Eisaman, J Fan, A. Migdall, S. V. Polyakov, Invited review article: Single-photon sources and detectors., Rev Sci Instrum. 82, 071101 (2011), and ref.s therein.

[ETSI] ETSI White Paper (Quantum Safe Cryptography V1.0.0, October 2014): Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges, ISBN 979-10-92620-03-0

[ETSIportal] http://portal.etsi.org/portal/server.pt/community/QKD/328

[EUC] "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (7 Feb 2013), by European Commission and the High Representative of the Union for Foreign Affairs and Security Policy.

[Ghernaouti2009] Ghernaouti-Hélie S, Tashi I, Länger T and Monyk C 2009 SECOQC Business White Paper arXiv:0904.4073 [quant-ph]

[Gisin2002] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys 74 145–95

[Grangier1986] P. Grangier, G. Roger, and A. Aspect, Europhys. Lett. 11, 173 (1986).

[HC1998] CRC Handbook of Chemistry & Physics, 79th Edition, 1998, p10-236 to 10-240.

[Hadfield2010] R. H. Hadfield, "single-photon detectors for optical quantum information applications," Nature Photonics 3, 696-705 (2010).

[Hwang2003] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. 91, 057901 (2003).

[Langer2009] Länger T, and Lenhart G 2009 Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD, New Journal of Physics 11, 055051

[Lo2005] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. 94, 230504 (2005).

[Lo2014] H.-K. Lo, et al., "Secure quantum key distribution," Nat Phot. **8**, 595 (215).

[market]http://www.prweb.com/releases/quantum_cryptography/quantum_key_distribution/prweb10897723.htm, http://marketpublishers.com/report/industry/other_industries/quantum_cryptography.html

[Martin1985] J. E. Martin, N. P. Fox, and P. J. Key, "A cryogenic radiometer for absolute radiometric measurements," Metrologia 21, 147-155 (1985).

[Migdall2013] A. Migdall, S. V. Polyakov, J. Fan, J. C. Bienfang Ed.s, Single-Photon Generation and Detection, Volume 45: Physics and Applications, (Academic Press; December 2013) and ref.s therein.

[Norbert2002] L. Norbert, and J. Mika, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," New Journal of Physics 4, 44 (2002).

[Scarani2004] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," Phys. Rev. Lett. 92, 057901 (2004).

[Schmunk2011] W. Schmunk, M. Rodenberger, S. Peters, H. Hofer & S. Kück, “Radiometric calibration of single photon detectors by a single photon source based on NV-centers in diamond”, Journal of Modern Optics, 58(14), 1252-1259 (2011)

[SECOQC] http://www.secoqc.net

[Stock2000] K. D. Stock, and R. Heine, "Spectral characterization of InGaAs trap detectors and photodiodes used as transfer standards," Metrologia 37, 449 (2000).

[Stucki2005] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. 87, 194108-194103 (2005).

[Tosi2009] A. Tosi, A. D. Mora, F. Zappa, S. Cova, M. A. Itzler, and X. Jiang, "InGaAs/InP single-photon avalanche diodes show dark counts and require moderate cooling," in Proc. Of SPIE(2009), pp. G1-G-9

[Wang2005] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," Phys. Rev. Lett. 94, 230503 (2005).

[Yuan2007] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," Appl. Phys. Lett. 91, 041114-041113 (2007).

5 Website address and contact details

A website has been established to disseminate the results of the project. It contains a public area that provides the following information from the project - an overview of the project, news items about project activities, publications, presentations, and training material. A members-only area is dedicated to exchange information and reports among the project partners, and includes a digital archive of all presentations, reports and papers from the project. The website is referenced in the Wikipedia page on QKD - http://en.wikipedia.org/wiki/Quantum_key_distribution

Public website address:	http://projects.npl.co.uk/MIQC/, linked from http://www.miqc.org	
Contacts:		
General	Maria Luisa Rastello	m.rastello@inrim.it
Website	Jessica Cheung	jessica.cheung@npl.co.uk

6 List of publications

Articles in peer-reviewed journals:

1. **Quantum and classical characterization of single/few photon detectors**
   M G Mingolla, F Piacentini, A Avella, M Gramegna, L Lolli, I Ruo Berchera, E Taralli, P Traina, M Rajteri, G Brida, I P Degiovanni and M Genovese
   Quantum Matter, Volume 4, p.1-13 (June 2015).

2. **Random Variation of Detector Efficiency: A Secure Countermeasure against Detector Blinding Attacks for Quantum Key Distribution**
   C C Wen Lim, N Walenta, M Legré, N Gisin and H Zbinden
   *IEEE Journal of Selected Topics in Quantum Electronics, **21** (3), pag 6601305 May/June 2015*

3. **Compact two-element transmission trap detector for 1550 nm wavelength**
   A Vaigu, T Kübarsepp, F Manoocheri, M Merimaa, E Ikonen
   Measurement Science and Technology, **26**(5), p. 055901 (March 2015)

4. **Reconstruction of mode structure of faint sources and its applications**
   F Piacentini, E A Goldschmidt, I P Degiovanni, I Ruo Berchera, S V Polyakov, S Kück, G Brida, A Migdall and M Genovese
   Physica Scripta,Volume 2014, Number T163, p. 014024 (December 2014)

5. **Worldwide standardisation activity for quantum key distribution**
   A. Mink, R. Alléaume, T. H. Chapuran, C.J. Chunnilall, I. P. Degiovanni, N. Lutkenhaus, V. Martin, M. Peev, M. Lucamarini, A. Shields, and M. Ward
   IEEE Communications Magazine, Volume: Globecom Workshops (GC Wkshps) 2014, p.656-661 (December 2014)

6. **Metrology for industrial quantum communications: the MIQC project**
   M L Rastello, I P Degiovanni, A G Sinclair, S Kück, C J Chunnilall, G Porrovecchio, M Smid, F Manoocheri, E Ikonen, T Kubarsepp, D Stucki, K S Hong, S K Kim, A Tosi, G Brida, A Meda, F Piacentini, P Traina, A Al Natsheh, J Y Cheung, I Müller, R Klein and A Vaigu
   *Metrologia, **51**(6), S267–S275 (November 2014)*

7. **Traceable metrology for characterising quantum optical communication devices**
   C J Chunnilall, G Lepert, J J Allerton, C J Hart and A G Sinclair
   *Metrologia, **51**(6), S258–S266 (November 2014)*

8. **Traceable calibration of a fibre-coupled superconducting nano-wire single photon detector using characterised synchrotron radiation**
   I Müller, R Klein and L Werner
   *Metrologia, **51**(6), S329–S335 (November 2014)*

9. **Beating Abbe diffraction limit in confocal microscopy via non-classical photon statistics**
   D Gatto Monticone, K Katamadze, P Traina, E Moreva, J Forneris, I Berchera, P Olivero, IP Degiovanni, G Brida, M Genovese
   Physical Review Letters, Volume 113, p. 143602[5] (September 2014)

10. **Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber**
    I Choi, Y R Zhou, J F Dynes, Z Yuan, A Klar, A Sharpe, A Plews, M Lucamarini, C Radig, J Neubert, H Griesser, M Eiselt, C Chunnilall, G Lepert, A Sinclair, J-P Elbers, A Lord, A Shields
    Optics Express **22**(19), 23121-23128 (September 2014) [Open Access]

11. **Metrology of single-photon sources and detectors: a review**
    C J Chunnilall, I P Degiovanni, S Kück, I Müller, A G Sinclair
    Optical Engineering, **53**(8), 081910[17] (August 2014) [Open Access]

12. **Native NIR-emitting single colour centres in CVD diamond**
    D Gatto Monticone, P Traina, E Moreva, J Forneris, P Olivero, I P Degiovanni, F Taccetti, L Giuntini, G Brida, G Amato, M Genovese
    New Journal of Physics, **16**(5), 053005[18] (May 2014) [Open Access]

13) **Measurement facility for the evaluation of the backscattering in fibre: realisation of an OTDR operating at single photon level**
F Piacentini, A Meda, P Traina, K Hong, I P Degiovanni, G Brida, M Gramegna, I Ruo Berchera, M Genovese, M L Rastello
International Journal of Quantum Information, **12**, 1461014[8] (March 2014)

14) **Separable Schmidt modes of a nonseparable state**
A Avella, M Gramegna, A Shurupov, G Brida, M Chekhova, M Genovese
Physical Review A, **89**(2), 023808[8] (February 2014)

15) **Practical implementation of a test of event-based corpuscular model as an alternative to quantum mechanics**
S. V. Polyakov, F. Piacentini, P. Traina, I. P. Degiovanni, A. Migdall, G. Brida, M. Genovese
Foundations of Physics, **43**(8), 913-922 (August 2013)

16) **Fast Active Quenching Circuit for Reducing Avalanche Charge and Afterpulsing in InGaAs/InP Single-Photon Avalanche Diode**
F. Acerbi, A. Della Frera, A. Tosi and F. Zappa
IEEE Journal of Quantum Electronics, **49**(7), 563-569 (July 2013)

17) **Mode reconstruction of a light field by multi-photon statistics**
E. A. Goldschmidt, F. Piacentini, I. Ruo Berchera, S. V. Polyakov, S. Peters, S. Kueck, G. Brida, I. P. Degiovanni, A. Migdall and M. Genovese
Physical Review A, **88**(1), 013822[5] (July 2013)

18) **Reply to comment on the 'Experimental test of an event-based corpuscular model modification as an alternative to quantum mechanics'**
G. Brida, I. P. Degiovanni, M. Genovese, A. Migdall, F. Piacentini, S. V. Polyakov, P. Traina
Journal of the Physical Society of Japan, **82**(8), 086001[1] (July 2013)

19) **Review on recent groundbreaking experiments on quantum communication with orthogonal states**
P. Traina, M. Gramegna, A. Avella, A. Cavanna, D. Carpentras, I. P. Degiovanni, G. Brida and M. Genovese
Quantum Matter, **2**(3), 153-166 (June 2013)

20) **Experimental Test of an Event-Based Corpuscular Model Modification as an Alternative to Quantum Mechanics**
G. Brida, I. P. Degiovanni, M. Genovese, A. Migdall, F. Piacentini, S. V. Polyakov and P. Traina
Journal of the Physical Society of Japan, **82**(3), 034004[5] (February 2013)

21) **An extremely low-noise heralded single-photon source: A breakthrough for quantum technologies**
G. Brida, I. P. Degiovanni, M. Genovese, F. Piacentini, P. Traina, A. Della Frera, A. Tosi, A. B. Shehata, C. Scarcella, A. Gulinatti, M. Ghioni, S. V. Polyakov, A. Migdall and A. Giudice
Applied Physics Letters, **101**(22), 221112[4] (November 2012)

22) **Ancilla-Assisted Calibration of a Measuring Apparatus**
G. Brida, L. Ciavarella, I. P. Degiovanni, M. Genovese, A. Migdall, M. G. Mingolla, M. G. A. Paris, F. Piacentini and S. V. Polyakov
Physical Review Letters, **108**(25), 253601[5] (June 2012)

23) **Experimental realization of counterfactual quantum cryptography**
G. Brida, A. Cavanna, I.P. Degiovanni, M. Genovese and P. Traina
Laser Physics Letters, **9**(3), 247-252 (March 2012) [Free to download]

Conference proceedings:

1) SPIE Photonics Europe, Brussels, 2014:
High performing SPS based on native NIR-emitting single colour centers in diamond
P. Traina, D. Gatto Monticone, E. Moreva, J. Forneris, M. Levi, G. Brida, I. P. Degiovanni, G. Amato,

L. Boarino, P. Olivero, M. Genovese
Proc. SPIE [9136], 913624 (May 2014)

2) SPIE Security & Defense, Dresden, 2013:
Towards a high-speed quantum random number generator
Damien Stucki, Samuel Burri, Edoardo Charbon, Christopher Chunnilall, Alessio Meneghetti, Francesco Regazzoni
Proc. SPIE, [8899] 88990R[6] (October 2013)

3) SPIE Optics & Photonics 2013:
Some recent progresses in quantum tomography realised at INRIM
F. Piacentini, E.A. Goldschmidt, M.G. Mingolla, I.P. Degiovanni, M. Gramegna, I. Ruo Berchera, S. V. Polyakov, S. Peters, S. Kück, E. Taralli, L. Lolli, M. Rajteri, M.G.A. Paris, A. Migdall, G. Brida, M. Genovese
Proc. SPIE, [8875], 88750G (2013)

4) SPIE Optics & Optoelectronics 2013:
An extremely low-noise heralded single-photon source without temporal post-selection
F. Piacentini, P. Traina, A. Della Frera, A. Tosi, C. Scarcella, A. Ruggeri, A. Gulinatti, M. Ghioni, S. V. Polyakov, A. Migdall, A. Giudice, G. Brida, I. P. Degiovanni, M. Genovese
Proc. SPIE, [8873], 87730S (2013)

5) SPIE Security and Defense 2012:
Report on proof-of-principle implementations of novel QKD schemes performed at INRIM
A Avella, G Brida, D Carpentras, A Cavanna, I P Degiovanni, M Genovese, M Gramegna and P Traina
Proc. SPIE, [8542], 8542-65 (2012)

Book chapter:

1) **Metrology for Quantum Communication technologies**
M L Rastello
Proceedings of the International School of Physics "Enrico Fermi", [185], 243-271 (2013)
Editors: E. Bava, M. Kühne, A.M. Rossi
ISBN: 978-1-61499-325-4 (print) | 978-1-61499-326-1 (online)

JRP start date and duration:	01 September 2011, 36 months
JRP-Coordinator: Maria Luisa Rastello, Dr, INRIM Tel: +39 011 39 19 219 E-mail: m.rastello@inrim.it JRP website address: www.miqc.org	
JRP-Partners: JRP-Partner 1 INRIM, Italy JRP-Partner 2 Aalto, Finland JRP-Partner 3 CMI, Czech Republic JRP-Partner 4 Metrosert, Estonia JRP-Partner 5 NPL, United Kingdom	 JRP-Partner 6 PTB, Germany JRP-Partner 7 AIT, Austria JRP-Partner 8 IDQ, Switzerland JRP-Partner 9 KRISS, Republic of Korea JRP-Partner 10 MIKES, Finland
REG-Researcher (associated Home Organisation):	Damien Stucki, Switzerland IDQ, Switzerland
REG-Researcher (associated Home Organisation):	Alberto Tosi, Italy PoliMi, Italy
REG-Researcher (associated Home Organisation):	Anas Al Natsheh, Finland UOULU, Finland

The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union