IOP Publishing | Bureau International des Poids et Mesures Metrologia

Metrologia **51** (2014) S267–S275

Metrology for industrial quantum communications: the MIQC project

M L Rastello[1], I P Degiovanni[1], A G Sinclair[2], S Kück[3], C J Chunnilall[2], G Porrovecchio[4], M Smid[4], F Manoocheri[5,6], E Ikonen[5,6], T Kubarsepp[7], D Stucki[8], K S Hong[9], S K Kim[9], A Tosi[10], G Brida[1], A Meda[1], F Piacentini[1], P Traina[1], A Al Natsheh[11], J Y Cheung[2], I Müller[3], R Klein[3] and A Vaigu[5]

[1] Istituto Nazionale di Ricerca Metrologica (INRIM), Torino, Italy
[2] National Physical Laboratory (NPL), Teddington, UK
[3] Physikalisch-Technische Bundesanstalt (PTB), Braunschweig and Berlin, Germany
[4] Cesky Metrologicky Institut (CMI), Praha, Czech Republic
[5] Centre for Metrology and Accreditation (MIKES), Espoo, Finland
[6] Metrology Research Institute, Aalto University, Espoo, Finland
[7] AS Metrosert (Metrosert), Tallinn, Estonia
[8] ID Quantique SA, Genève, Switzerland
[9] Korea Research Institute of Standards and Science (KRISS), Daejeon, Republic of Korea
[10] Politechnico di Milano, Milano, Italy
[11] Centre for Measurement and Information Systems, University of Oulu, Oulu, Finland

E-mail: i.degiovanni@inrim.it

Received 10 June 2014, revised 17 July 2014
Accepted for publication 6 August 2014
Published 20 November 2014

Abstract

The 'Metrology for Industrial Quantum Communication Technologies' project (MIQC) is a metrology framework that fosters development and market take-up of quantum communication technologies and is aimed at achieving maximum impact for the European industry in this area.

MIQC is focused on quantum key distribution (QKD) technologies, the most advanced quantum-based technology towards practical application. QKD is a way of sending cryptographic keys with absolute security. It does this by exploiting the ability to encode in a photon's degree of freedom specific quantum states that are noticeably disturbed if an eavesdropper trying to decode it is present in the communication channel. The MIQC project has started the development of independent measurement standards and definitions for the optical components of QKD system, since one of the perceived barriers to QKD market success is the lack of standardization and quality assurance.

Keywords: metrology, quantum cryptography, quantum communication

(Some figures may appear in colour only in the online journal)

1. Introduction

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 is the traditional application of cryptography, it is used nowadays to achieve broader objectives, such as authentication, digital signatures and non-repudiation. Security of classical communications relies on making cryptographic keys longer and longer to stay ahead of increases in computing speed—however the successful development of a quantum computer will render this tactic useless [1].

Quantum key distribution (QKD) is essentially the generation of truly random cryptographic keys between two parties that are connected by a quantum channel. This true

randomness means these keys are future proof even in the presence of a quantum computer. Cryptographic keys are the key ingredient to realizing secure communication between the two legitimate parties [1]. 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.

Qualified practical use 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 standardized methodology. QKD offers to guarantee security of a channel only after measurements have been made to ensure the channel has not been compromised. Therefore, the security certification of QKD systems requires standardized properties of optical components such as photon sources, and detectors and a framework for the underlying information theoretical security proofs, which again requires accurate knowledge of all the critical components of the system.

This need for standards has been driven by the QKD industry and academia themselves. The first initiative for the standardization of QKD originated in the context of the SECOQC 'SEcure COmmunication based on Quantum Cryptography' [2] project of the 6th Framework Programme (FP6) of the European Community, and it is still active. Within the European Telecommunications Standards Institute (ETSI) there is an Industry Specification Group (ISG), which is an interdisciplinary group uniting 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 [3, 4].

Irrespective of the underlying technologies, there are quantum devices that appear in most QKD systems, namely sources and detectors. The characteristics of quantum optical components are crucial for security analysis on the quantum optical level. The identification of relevant parameters, standardization and the development of appropriate measurement techniques for their metrological characterization are therefore necessary to enable the efficient specification of generic security requirements for QKD systems. The MIQC project is the first answer of the metrological community to these needs [5].

Although characterization of classical communication parameters is a well-established metrological activity (even if research and optimization are still necessary), for quantum communication further development of these 'classical' measurement techniques is necessary to cover parameter ranges that are beyond the interests of classical communication. These are, for example, power measurements and detector characterization at the single-photon level at telecom wavelengths.

Since an efficient way to attack the channel by an eavesdropper relies on exploiting inefficiencies of the components to hide himself in the system, security of practical QKD systems demands an accurate knowledge of optical and electronic properties of the QKD components. This will allow the sender and receiver to eliminate anomalies due to imperfections and to home in on the eavesdropper.

The MIQC project has developed measurement techniques for the characterization of QKD quantum optical components at telecom wavelengths (around 1.55 µm). In particular the activities have been mainly focused on single-photon sources and single-photon detectors, but also attention has been paid to the characterization of quantum random number generator (QRNG) and to the quantum channels (optical fibres in this case). This was technically challenging, since no measurement standards existed before MIQC for photon-counting technologies at telecom wavelengths. Indeed, where standards were present, they operated in the regime of microwatts or above, and are cumbersome to use for measurements at the single photon level.

2. The QKD system

A QKD system is composed of quantum physical devices (quantum sources, quantum channels and quantum detectors) and classical (and well-established) information technology that is needed for the part of classical communication, during both the realization of the QKD protocol and the subsequent secret communication when the cryptographic key is established (see figure 1) [1].

A QKD source emits individual quanta of light (photons), upon which a single bit of information is encoded. A source suitable for QKD will possess a property such that the encoded bit of information can be recovered faithfully through quantum measurement, but only when the measurement basis is compatible with the encoding basis. The information can be encoded using polarization, phase, detection time, etc.

A single-photon source is ideal as a QKD source, however, a perfect single-photon source is yet to be realized; current sources suffer from low efficiencies and stringent operating conditions, and thus are impractical. For practical QKD, a highly attenuated pulsed laser approximates to a single-photon source; these lasers emit optical pulses containing less than one photon per pulse on average [1, 6, 7]. They are suitable for encoding in discrete degrees of freedom, e.g., in polarization, phase and arrival times. In the following text this attenuated pulsed laser will be referred to as a QKD source. A 'heralded' single-photon source, based on spontaneous parametric down-conversion (SPDC), also generates individual photons. SPDC (producing quantum correlated photon pairs) is realized by pumping a non-linear optical crystal with a laser beam. Detection of one photon of the pair in a specific point in space and at a given wavelength heralds the presence of its twin at the conjugate wavelength and position in space (with respect to the pump). This is of immediate use in metrology of components and detectors [6–8], and is a prospective candidate technology for future QKD sources.

A QKD source must maintain indistinguishability for photons in all degrees of freedom, except that of encoding; i.e. encoded photons must not be distinguishable through measurement of parameters other than the encoding parameter.

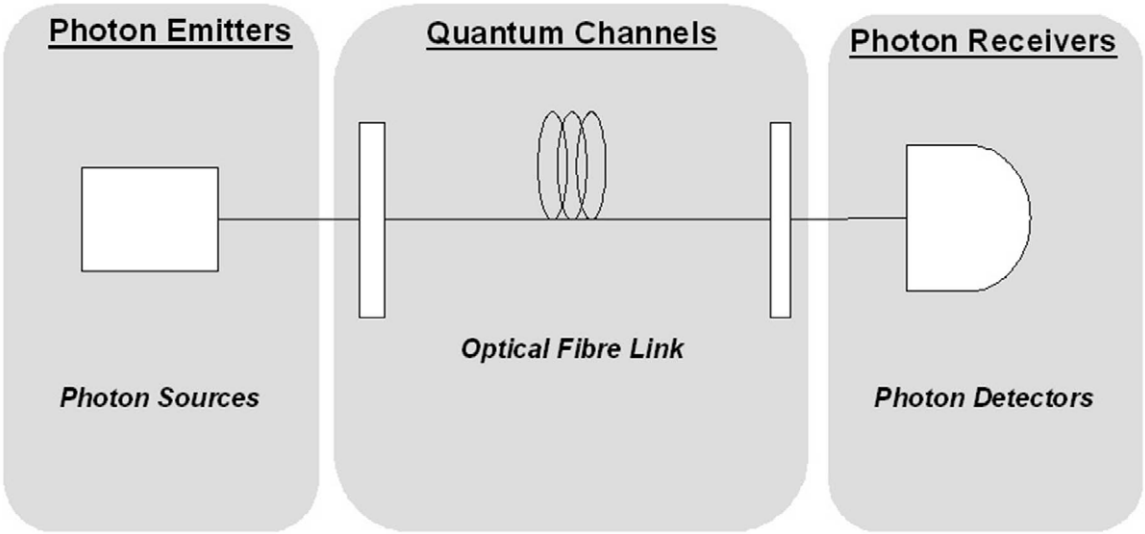

Figure 1. Typical schematic of a QKD system.

For example, in the polarization-encoding BB84 protocol [1], qubits in all four states are required to have exactly the same wavelength, temporal profile and arrival time etc. Discrimination of these polarization-encoded qubits can be made possible through polarization measurement. Indistinguishability in all photon degrees of freedom except that of encoding is the key to prevent any side-channel attack on a QKD system [1].

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 [1, 9].

Single-photon receivers are single-photon detectors, which are 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.

To date there is no single detector that can meet all of the requirements (such as, for example, unit quantum efficiency, photon number resolving (PNR) ability, minimum jitter and dead-time, etc) of any given application and QKD is no exception [7, 10]. There are many different trade-offs to be considered in order to obtain the best performance with a given set of QKD components.

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 absorbed photon. Another source of photon loss is the recovery time or dead-time of the detector. A long dead-time of the single-photon receiver limits the data rates in a QKD system [7, 10]. 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 stable, corresponding to a small time jitter (hundreds of picoseconds) [7, 10]. This time jitter is defined as the uncertainty in determining the photon arrival time at the device.

Moreover, 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 [7, 10].

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 individual quantum systems, namely a degree of freedom of a photon. The quantum channel considered in the context of MIQC project is based on optical fibre since fibre-based QKD is currently the most promising evolution of QKD. The physics of optical fibres has been explored in depth because of their importance for communication, but investigation of the connection between fibre properties and decoherence [11] of photon states used as the information carrier is a fast developing field of interest in the QKD community [1].

The most important parameter to consider is the amount of optical loss as this will lower the key rate, as lost photons cannot be detected, thus the bit of the cryptographic key that they carry is also lost. Having a fixed repetition rate for the pulsed QKD source, these optical losses reduce the detected bit rate of the key, i.e. the number of bits per second exchanged by person A and person B during the key distribution process. The raw key rate decreases with distance along the quantum channel and at some point the detection rate reaches the level of the dark counts of the detectors; this effectively limits the maximal achievable distance [1]. Furthermore, the key signal cannot be amplified. Any lost photons are correlated with the signal and therefore must be counted as information that is leaked to the eavesdropper.

Furthermore, as far as the security is concerned, the quantum channel must be characterized only *a posteriori* because the eavesdropper has full freedom of action on it during

the key distribution process. In fact, at the end of the key distribution process, person A and person B can evaluate the maximum amount of information that can be obtained by the eavesdropper by evaluating the quantum bit error rate (QBER) at the cost of a part of the key [1]. However, knowledge of the *a priori* expected behaviour of the quantum channel is important.

Furthermore, errors and/or information leakage can be introduced by non-proper quantum state preparation, and for this reason QRNGs are therefore tested in the context of this project.

3. The photon emitters

MIQC project provides a measurement framework for the characterization of photon emitters developed for QKD in optical fibre. In the following we will summarize some of the main achievements connected to the characterization of relevant QKD source parameters:

3.1. Photon statistics of emitters

It is of utmost importance to characterize the photon number distribution $P(n)$ of (pseudo) single-photon emitters for QKD. This includes actual sources used in QKD systems, as well as source instruments used in test and measurement of other QKD components. The parameters related to $P(n)$ are very important in the context of QKD security analysis, because of the so-called photon number splitting attack.

So far, three different techniques are used in determining the number of photons present in an optical pulse. In the first instance, pulses of individual photons are clocked out of the attenuated laser source; they are detected using a single-photon detector whose practical quantum efficiency has been calibrated. As all the other aspects of efficiency in the measurement apparatus are known, the mean photon number per pulse is straightforward to determine.

Method 1. The photon source is comprised of a pulsed laser, an uncalibrated attenuator, and a calibrated attenuator. The uncalibrated attenuator was used to set a high power level (100 pW–1 nW), which could be measured with a calibrated power meter. The calibrated attenuator was used to set the mean photon number ($\sim$0.1) at various pulse repetition rates. A calibrated photon-counting detector operating in gated mode was used to measure the mean photon number emitted by this source. Specifically designed and implemented instrumentation for synchronizing, the detector gate with the source was realized; this was achieved with low jitter and resolution down to 11 ps. In order to improve the accuracy, instead of using a commercial calibrated attenuator a specifically designed fibre-coupled transmission trap attenuator was realized (figure 2).

The pointing stability of the light coupling system is ensured by a piezo-based active-controlled fibre-coupling system with feedback loop. The key advantages of using a transmission trap detector are polarization insensitivity and the possibility to use the photodiodes as reference detectors. The attenuator provides a free space attenuation of 3.6×10^{-5} with $k = 2$ uncertainty of 4.4% at the wavelength of 1550 nm. The attenuation was directly measured to be independent of incident power over the range of 10 nW up to 1 mW [12]. While the transmission trap detector is used as a fibre coupled attenuator, as described above, the uncertainty at $k = 2$ level for total attenuation is 3%.

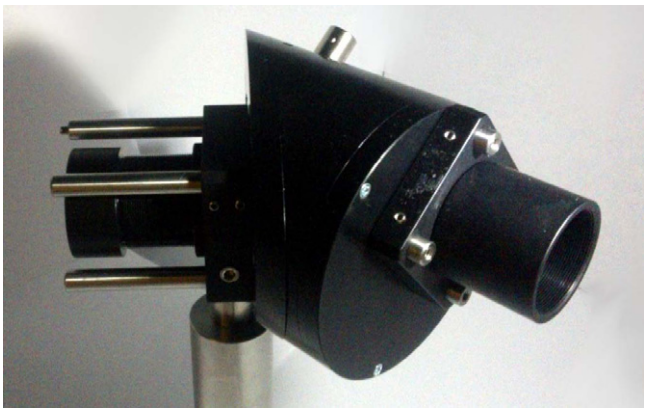

Figure 2. Body of the transmission trap detector–attenuator. Light enters from the leftmost and exits from the rightmost part of the detector. The two 10 mm diameter photodiodes were mounted into the trap detector in such a way that reflection from photodiode surfaces takes place at the angle of incidence of 17°. The planes of incidence of the photodiodes are perpendicular to each other ensuring polarization 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.

Method 2. The second technique is based on photon statistics reconstruction by on/off detection [13]. Measurements of photon counts are made using a single-photon avalanche photodiode for various 'effective' quantum efficiencies. The measured probability $P(0)$ of detecting no photons is used with a maximum likelihood estimator to 'reconstruct' $P(n)$.

Method 3. A third technique for reconstruction of photon statistics distribution based on 'direct' photon counting is under development. It exploits a PNR detector counting up to four photons per pulse exploiting commercial single-photon detectors (SPD) in a tree configuration with four detectors (as shown in figure 3), controlled by an integrated circuit which is designed to be configured by the customer after manufacturing—hence 'field-programmable' (Field-programmable Gate Array or FPGA). FPGA-software as well as an FPGA board controlling the PNR detector input–outputs, were developed, and first test measurements were successfully performed. A very preliminary characterization was performed and this PNR detector was also exploited in an experiment aimed at optical occupation mode reconstruction [14].

Furthermore, instead of investigating the photon statistics of the source, one can identify parameters that describe the quantum behaviour of the individual photons generated by a single-photon source. The relevant parameters are somehow related to the second order degrees of coherence, and are used by the quantum information community to describe the performance of single-photon sources. The single-photon

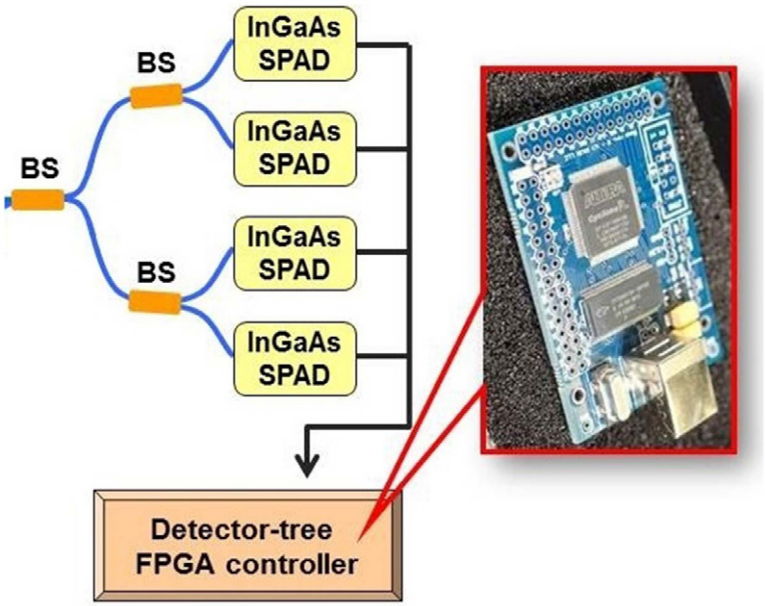

Figure 3. Scheme of the PNR detector based on the detector tree configuration: it is composed of a cascade of three 50 : 50 beam splitters with each output connected to a InGaAs/InP SPAD (single-photon avalanche diode) [15]. The whole system is managed by a FPGA-based control circuit, gating the detectors only when all of them are 'ready' (avoiding dead-time issues) and performing partial real-time processing of the four SPADs counts.

emission property of a single-photon source is described by the second order correlation function $g^{(2)}$, which is measured with a Hanbury Brown–Twiss (HBT) interferometer containing two single-photon detectors [16, 17]. The HBT interferometer was realized and measurements on both an attenuated pulsed laser sources and an almost noiseless heralded single-photon source (figure 4), realized in the context of this project, were performed successfully. In particular, the quasi-noiseless heralded single-photon source [18, 19] is developed exploiting SPDC phenomena and the heralded photon is emitted at 1.55 µm. The novelty of this source resides in its ability to nullify the presence of background counts in the heralded channel without the need of temporal post-selection (typical of the experiment exploiting heralded single-photon source based on SPDC) by means of a fast optical switch in order to prevent the emission of un-heralded photons. With this source astonishingly good performances were achieved, such as e.g. $g^{(2)}(0) = (0.005 \pm 0.007)$ [19], to our knowledge the best $g^{(2)}(0)$ value achieved without temporal post-selection.

3.2. Spectral, temporal and polarization properties of photon emitters

The aim is to develop measurement capabilities for characterizing spectral, temporal and polarization properties of individual photons emitted by (pseudo) single-photon emitters for QKD. The need for photon indistinguishability for all parameters other than that used for encoding requires precise knowledge of parameters such as wavelength, spectral bandwidth, temporal jitter and polarization.

Source timing jitter (the temporal uncertainty in the temporal emission of the light pulse versus the corresponding heralding or reference signal) is measured most accurately and precisely using a high speed photodiode module in a fast oscilloscope, via the optical signal before attenuation to the single-photon level. A timing jitter of 9.1 ps was demonstrated. This was achieved with all instrumentation synchronized to a 10 MHz maser reference. Temporal measurements using photon-counting detectors are limited by the jitter of the detectors (∼80 ps), despite the use of superconducting nanowire detectors providing the highest temporal resolution in detecting single photons at high bit rates.

The polarization state of the weak laser pulsed source is reconstructed by quantum state tomography. Quantum state tomography is a technique which makes repeated measurements on the system under study, in order to build up a picture of the quantum state. So in the case of polarized single photons, a polarization analysis apparatus (a single-photon polarimeter) is used to make repeated measurements over many individual photons, in order to build a statistical picture of the polarization state. The single-photon polarimeter operates as a conventional polarimeter but exploiting single-photon detector instead of conventional ones [20].

The wavelength of the non-attenuated optical source is measured using a commercial wavemeter, but also a specifically designed cavity spectrometer for the purpose of determining spectral linewidth and indistinguishability of single-photon optical pulses was realized. Actual achieved instrument parameters were free spectral range of 119.0 GHz and resolution linewidth = 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 system [21].

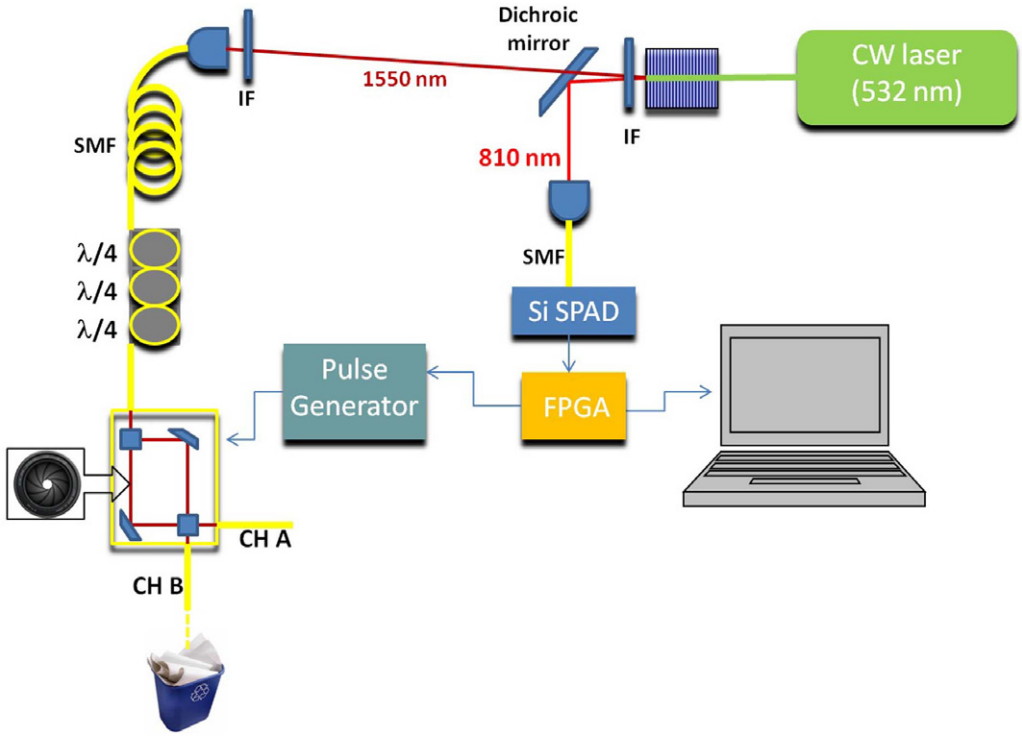

Figure 4. The set-up of the almost noiseless single-photon source: a CW laser pumps a periodically pulsed lithium niobate (PPLN) crystal producing non-degenerate SPDC. Each signal photon at 810 nm heralds the presence of a correlated photon at 1550 nm. The heralded photon is sent to a FPGA controlled 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).

4. Photon receivers

MIQC project also provides a measurement framework for the characterization of photon detectors developed for fibre based QKD. In the context of the MIQC project InGaAs/InP SPADs [15] are essentially the single-photon detector considered unless otherwise stated. In the following we will summarize some of the main achievements connected to the characterization of relevant QKD receiver parameters.

4.1. Detection efficiency of commercial single-photon detectors for QKD

Previously, no reference standards were available at telecom wavelengths at this low level of radiation. To provide traceable calibrations, the transmission trap attenuator described in the previous section was developed. The input power to the attenuator can be measured directly from the photodiodes, from which the low level output can be calculated, and used to calibrate the response of a telecom wavelength photon receiver. Test measurements have demonstrated that this device allows the detection efficiency of an InGaAs SPAD to be traceably measured against the cryogenic radiometer with a relative standard uncertainty of 2%. The detection efficiency of the SPAD was obtained by comparing the photon count rate observed with the incident radiation power of an attenuated pulsed laser at 1.55 µm. The latter was determined by an analogue InGaAs diode calibrated against a thermopile, which again was calibrated against a cryogenic radiometer. Two fibre-coupled variable commercial attenuators decreased the pulsed laser radiation to few photons. The transmittance and linearity of the attenuator system was measured by a cross check diagnostic using the calibrated InGaAs diode. Main contributions to the measurement uncertainty are after-pulsing and dark count probability, linearity of the InGaAs diode, stability of the pulsed laser source as well as the transmittance and linearity of the fibre-coupled attenuators.

4.2. Novel reference for calibrating single-photon detector

The technique is based on the fact that the spectral radiant intensity of synchrotron radiation from electron storage rings is (according to the Schwinger equation) directly proportional to the stored electron beam current, i.e. the number of stored electrons. The photon flux of the dedicated electron storage ring of the PTB, the metrology light source (MLS) can be varied and controlled over 11 orders of magnitude. Thus it is possible to calibrate a SPD (operated at very low photon rate) against a classical radiation detector (operated at a classical photon rate) without using a calibrated attenuator or relying on the linearity over several orders of magnitude of a classical detector [22].

This method provides a novel reference for calibrating photon receivers. To perform traceable measurements an InGaAs photodiode, calibrated against a cryogenic radiometer at 1.55 µm, was used to determine the ratio of photon flux to the stored ring current. At the MLS, the necessary equipment is installed to monitor the source size of the synchrotron radiation over the whole available ring current range [23]. A change of the source size might change the ratio of photon flux and the

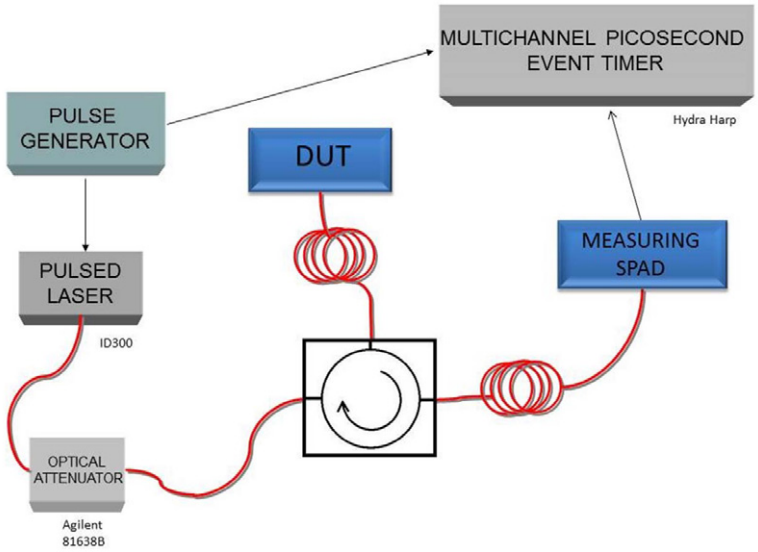

Figure 5. The set-up of the photon-counting OTDR: a commercial pulsed diode laser emitting at 1550 nm, with pulse width shorter than 300 ps, is strongly attenuated with a variable optical attenuator and sent to a pigtailed optical circulator. The optical signal back-reflected from the fibre/device under 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 synchronization signal from the pulsed laser exploiting TCSPC measurement technique.

stored ring current if the ring current is reduced. Within the ring current range used during the calibration of the fibre-coupled SPD no change of the source size has been observed and, thus, of the ratio of photon flux to the stored ring current [24]. Using this ratio the calibration of superconducting nanowire single-photon detectors (SNSPD) was performed at a ring current of 5 nA, corresponding to about 630 000 photons per second, and at wavelength of 1.55 µm. As a result the detection efficiency of the SNSPD was measured at the entrance of the fibre with a combined relative standard uncertainty of 1.9% [24]. The main contribution to these overall uncertainties is the uncertainty associated with the polarization dependence of the detection efficiency of the SSPD.

4.3. Other relevant parameters of commercial single-photon detectors for QKD

Other relevant parameters of commercial single-photon detectors for QKD, such as e.g. jitter, dead-time, back-flash etc should also be measured, other than detection efficiency. The jitter of the SPD (the temporal uncertainty of the emission of the detection signal versus the absorption of the photon by the detector) was determined by correlating many detection events with the trigger signal of the laser. A time delay histogram can be observed by a time-correlated-single-photon-counting (TCSPC) measurement, from which the detector's response function can be calculated.

A similar TCSPC measurement technique is used to estimate the dead-time of single-photon detector (after a detection, the dead-time is time interval during which the detector is not ready to detect another photon), by varying the laser repetition rate.

Back-flashes (photons emitted by the detector itself during the avalanche process in the presence of a detection event) from single-photon detector appears to be a security issue in QKD systems, since they may induce an uncontrolled leak of information on which photon-detector clicks inside the QKD receiver. In order to perform a proper characterization of back-flashes, an optical time domain reflectometry (OTDR) system, operating at single-photon level was developed (figure 5). This system takes advantage of a new free-running SPD based on InGaAs–InP SPAD is able to perform the measurement on long-haul fibres at an extremely low light level, and is also able to identify the behaviour of active elements at sensitivities much lower than achievable by commercial OTDR systems. 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) [25]. With this novel OTDR the presence of back-flashes was confirmed and their spectral and temporal behaviour has been characterized. In particular two different kinds of gated InGaAs–InP SPAD were investigated (one commercial and one prototype): in both cases it was observed that back-flashes present a broad and continuous spectrum of emission, with characteristic temporal profiles. We highlight that from the study of the temporal profiles of the back-flash emission an eventual eavesdropper can obtain information about the detection electronics implemented in the detector.

In the context of the MIQC project, the characterizations of dark counts, after-pulses, etc were performed with straightforward techniques [26].

Furthermore, tens of kilometres of traceably calibrated fibre optic links were used to realize a standard platform for validation, quantification and comparison of different physical components of a QKD system in a 'real' environment. In particular, the platform can be used to test photon emitters and photon receivers and also the effects that the fibre may have on the optical properties of the source. It was also used for the investigation on the connection between fibre properties and decoherence of the photon state used as an information carrier.

5. The quantum random number generator

The QRNG [27] is a physical random number generator (RNG) which is, for example, based on the physics of photons acting on a beam splitter. When the photon arrives at the beam splitter it will either be reflected or transmitted and the outcome is truly random compared with software generated random numbers that are pseudo-random.

The interest in commercial QRNGs goes beyond QKD. Gaming industries are also showing an interest in QRNGs and request certification of the QRNG. Currently, standard software tests such as FIPS and Diehard are applied to the random numbers that are generated [28]. These are used for pseudo-random numbers that are computer generated not physically generated and therefore the tests are not so appropriate for physical RNGs.

In the context of QKD, the QRNG is critical as is ensures the randomness of the choices made in the QKD session and therefore safeguards the security of the session. It is particularly important therefore that there is some independent physical validation of the 'black box' QRNG in addition to software tests to check the randomness of the bit generation.

An RNG can be deterministic (pseudo-random) or 'true'. Deterministic RNGs are based on a mathematical algorithm, while 'true' RNGs can be based on a non-physical process or a physical source of entropy, which can be quantum or non-quantum. Sixteen types of quantum RNG (QRNG) were identified. The difficulty in proving the randomness of a binary sequence was reported and five statistical software suites for testing sequences produced by a deterministic RNG were referenced. The argument that a physical RNG is a true RNG and that verification of the physical process is sufficient to verify the randomness of the produced sequence was highlighted. Thus RNG based on quantum physics, which is intrinsically probabilistic, is the best choice for RNG. Two set-ups for open system QRNG were realized [29]. One comprises LED pulses attenuated to the single-photon level, a 50/50 beam splitter and two detectors. A photon will produce a click on one of the detectors with some probability. One detector will be associated with bit 0 and the other with bit 1. The other comprises attenuated LED pulses and a detector matrix. The detectors of the matrix are grouped in pairs, for each pair one detector is associated with bit 0 and the other with bit 1.

To assess the performances of the QRNGs, the properties of the physical components that require characterization were identified—the spatial profile of the illuminating beam, the relative detection efficiencies of the detectors, their dark count and after-pulse probabilities, and the beam splitter ratio, together with target uncertainties. Measurement techniques were developed and implemented for characterizing these properties at the component level, and in the assembled devices. Raw bit streams are being collected, and their entropy analysed, to test the validity of models relating entropy to the physical characteristics of the devices.

6. Conclusions

This MIQC project lays the *foundations* for a European measurement infrastructure able to validate the performance of QKD systems, and technologies that use and manipulate single photons. Specifications based on the outputs of this project will enable systems to be evaluated and standard measures to be defined, thus helping to shape a validation and certification process for wider implementation of this technology. Engagement with manufacturers has highlighted the importance of characterizing the physical performance of QKD systems in order to assure both suppliers and customers that the devices are operating as intended. The MIQC results will also enable the development of new hardware for manipulating single and few photons, required for next-generation communication systems and quantum networks.

The overall aim of the MIQC project was the development of metrological techniques, standards and methods to facilitate the commercial success of the quantum communication technologies in general, and of QKD technologies in particular.

The technical work developed, refined and applied new metrology to qualify and quantify properties of photon emitters, photon receivers and quantum channels. New methodologies were developed to optimize QKD products for reliable and stable operation. Specifically we:

- Developed a measurement framework for the characterization of photon emitters developed for QKD. Specific operating parameters were quantified, and traceable measurements provided for most of the relevant QKD source parameters.
- Developed a measurement framework for the characterization of photon detectors developed for QKD. The various parameters necessary for a detection technology to be considered a suitable QKD photon detector were quantified and measured in a traceable manner.
- Developed a QKD testbed. Additionally two different types of (open-system) QRNGs—a core component for the security of QKD systems—were developed and characterized. This represents a relevant first step in the development of the standardization of QRNG whose practical interest goes beyond the QKD.

Acknowledgments

This work was funded by the project MIQC (contract IND06) of the European Metrology Research Programme (EMRP). The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys* **74** 145
Dusek M, Lütkenhaus N and Hendrych M 2006 *Quantum Cryptography* (*Progress in Optics* vol 49) ed E Wolf (Amsterdam: Elsevier) pp 381–454
Scarani V *et al* 2009 *Rev. Mod. Phys.* **81** 1301 and references therein
[2] www.secoqc.net

Alléaume R, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H and Zeilinger A 2006 *SECOQC White Paper on Quantum Key Distribution and Cryptography* (arXiv:quant-ph/0701168)
Ghernaouti-Hélie S, Tashi I, Länger T and Monyk C 2009 *SECOQC Business White Paper* (arXiv:0904.4073[quant-ph])
[3] http://portal.etsi.org/portal/server.pt/community/QKD/328
[4] Länger T and Lenhart G 2009 *New J. Phys.* **11** 055051
[5] http://projects.npl.co.uk/MIQC/
[6] Eisaman M D, Fan J, Migdall A and Polyakov S V 2011 *Rev. Sci. Instrum.* **82** 071101 and references therein
[7] Midall A *et al* (ed) 2013 Single-photon generation and detection *Experimental Methods in Physical Science* vol 45 (New York: Academic) and references therein
[8] Dauler E, Migdall A, Boeuf N, Datla R, Muller A and Sergienko A 1998 *Metrologia* **35** 295
Brida G *et al* 2000 *Metrologia* **37** 629
Ghazi-Bellouati A *et al* 2005 *Metrologia* **42** 271
Migdall A *et al* 2002 *Appl. Opt.* **41** 2914
Polyakov S V and Migdall A L 2007 *Opt. Express* **15** 1390
Cheung J Y *et al* 2011 *Opt. Express* **19** 20347
[9] Norbert L and Mika J 2002 *New J. Phys.* **4** 44
Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
Scarani V *et al* 2004 *Phys. Rev. Lett.* **92** 057901
[10] Hadfield R H 2010 *Nature Photon.* **3** 696 and references therein
[11] Nielsen M A and Chuang I L 2011 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[12] Vaigu A, Kübarsepp T, Manoocheri F, Merimaa M and Ikonen E 2014 Traceability at the single photon level for quantum communication *Proc. NEWRAD 2014 Conf. (Espoo, Finland, 2014)* pp 109–10
[13] Zambra G *et al* 2005 *Phys. Rev. Lett.* **95** 063602
[14] Goldschmidt E A *et al* 2013 *Phys. Rev.* A **88** 013822
[15] Tosi A *et al* 2012 *Rev. Sci. Instrum.* **83** 013104
Itzler M A *et al* 2007 *J. Mod. Opt.* **54** 283
[16] Mandel L and Wolf E 1995 *Optical Coherence and Quantum Optics* (Cambridge: Cambridge University Press)
[17] Grangier P, Roger G and Aspect A 1986 *Europhys. Lett.* **11** 173
[18] Brida G *et al* 2011 *Opt. Express* **19** 1484
[19] Brida G *et al* 2012 *Appl. Phys. Lett.* **101** 221112
[20] James D F V, Kwiat P J, Munro W J and White A G 2001 *Phys. Rev.* A **64** 052312
[21] Fitzpatrick C R *et al* 2014 A high-resolution single-photon spectrometer for telecom wavelengths *Opt. Express* in preparation
[22] Müller I, Klein R, Hollandt J and Ulm G 2012 *Metrologia* **49** S152
[23] Klein R, Thornagel R and Ulm G 2010 *Metrologia* **47** R33
[24] Müller I, Klein R M and Werner L 2014 Traceable calibration of a fibre-coupled superconducting nano-wire single photon detector using characterised synchrotron radiation *Proc. NEWRAD 2014 Conf. (Espoo, Finland, 2014)* pp 123–4
[25] Brida G *et al* 2014 Photon-counting optical time-domain refletometry at 1550 nm *Proc. NEWRAD 2014 Conf. (Espoo, Finland, 2014)* pp 105–6
[26] Chunnilall C J, Degiovanni I P, Kück S, Müller I and Sinclair A G 2014 Metrology of single-photon sources and detectors: a review *Opt. Eng.* **53** 081910
[27] Stefanov A *et al* 2000 *J. Mod. Opt.* **47** 595
Jenewein T *et al* 2000 *Rev. Sci. Instrum.* **71** 1675
Stipcevic M *et al* 2007 (arXiv:quant-ph/0609043)
Dynes J F *et al* 2008 *Appl. Phys. Lett.* **93** 031109
Wahl M *et al* 2011 *Appl. Phys. Lett.* **98** 171105
Williams C *et al* 2010 *Opt. Express* **18** 23584
Wayne M A *et al* 2010 *Opt. Express* **18** 9351
Gabriel C *et al* 2010 *Nature Photon.* **4** 711
Shen Y *et al* 2010 *Phys. Rev.* A **81** 063814
Symul T *et al* 2011 *Appl. Phys. Lett.* **98** 231103
Jofre M *et al* 2011 *Opt. Express* **19** 20665
Fürst M *et al* 2010 *Opt. Express* **18** 13029
[28] http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf
www.stat.fsu.edu/pub/diehard/
www.phy.duke.edu/∼rgb/General/dieharder.php
www.fourmilab.ch/random/
www.iro.umontreal.ca/∼simardr/testu01/tu01.html
Killman W *et al* Methodology for true (physical) random number generators (www.bsi.bund.de)
[29] Stucki D, Burri S, Charbon E, Chunnilall C J, Meneghetti A and Regazzoni F 2013 Towards a high-speed quantum random number generator *Proc. SPIE* **8899** 88990R