Metrology Challenges in Quantum Key Distribution

Y Gui, D Unnikrishnan, M Stanley and I Fatadin

National Physical Laboratory, Teddington, United Kingdom

yunsong.gui@npl.co.uk, divya.unnikrishnan@npl.co.uk, manoj.stanley@npl.co.uk, and irshaad.fatadin@npl.co.uk

yunsong.gui@npl.co.uk

Abstract. The metrology of the QKD devices and systems grows increasingly important in recent years not only because of the needs for conformance and performance testing in the standardization, but more importantly, imperfect implementation of the devices and systems or deviations from the theoretical models, which could be exploited by eavesdropper, should be carefully characterised to avoid the so-called side channel attack. In this paper, we review the recent advances in many aspects of the QKD metrology in both fibre based QKD and free space QKD systems, including a cutting edge metrology facility development and application, traceable calibration methods, and practical device characterising technologies, all of which have been contributed by the metrology communities and relative institutions.

1. Introduction

The world's most secure cybersecurity infrastructure relies on the use of digital cryptographic keys. The advancements in quantum computing intensely raises the threat to the security of this infrastructure. Since traditional networking systems are exposed to a variety of attacks, quantum key distribution (QKD) has been proposed to achieve information-theoretical security by harnessing the laws of quantum physics [1].

QKD is considered as the earliest form of secure quantum communication that enables the two communication parties (transmitter and receiver) to share a random secret key immune to eavesdropping. The secret key is created by transmitting and detecting few photon pulses over an authenticated channel. Unique protocols are used whose security can be proven by laws of nature and does not depend on computational complexity. The QKD concept is a solution to the threat from quantum computing technology which utilises the laws of quantum mechanics to perform computations using physical quantum systems differing from the traditional computational bits for solving mathematical problems.

Fig. 1 presents the block diagram of a basic QKD system [2]. In general, a QKD system holds communication channels, QKD protocol and encryption/decryption blocks. In contrast to the current popular cryptographic method of Advanced Encryption Standard (AES), the encryption or decryption process in QKD system is a logical sum of transmitted information and cryptographic keys which enables low latency encrypted communication. The encryption and decryption sections are required to encrypt the information using the secret keys and then to decrypt it back. QKD communication channels such as quantum signal channel (QSCh) and public interaction channel (PICh) are used to send the

photons between the nodes, to transmit the qubits, and to verify the generated shared secret keys using the post-processing methods. An ultimate random secret key is generated between the nodes after post-processing. A QKD protocol is used to establish a secure connection between the nodes by generating secret keys and decrypts the correct information shared between the users during the key generation. An in-depth analysis of QKD is presented in [3] while their practical challenges are reviewed in [4].

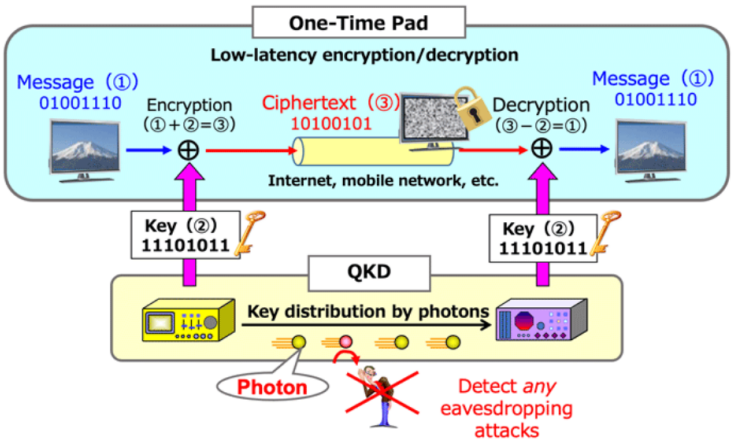

Figure 1. Block diagram of basic QKD system [2].

The most common implementations of QKD systems are the optical fibre based terrestrial QKD system and the free space based terrestrial and satellite QKD implementations [5]. This review paper is organised into four main sections. Section 2 discuss the various implementations of QKD systems. Section 3 discuss the different protocols used in various QKD systems and compares the advantages and vulnerabilities of these protocols in terms of security and key rates. In section 4, the metrology parameters designed to quantify the performance of QKD components, channels and systems is described. Some of the measurement techniques employed to characterise these performance parameters are reviewed in this section as well. The efforts from the UK's National Physical Laboratory (NPL) in QKD metrology through various European initiatives are also summarised in a sub-section.

2. QKD Classification Based on Deployment

2.1. Fibre based QKD

Typically, optical fibre has been considered as a secure mode of transmission due to its advantage of sending optical signals through a guided medium. A basic point-to-point QKD mechanism of transmission over optical fibre is shown in Fig. 2. Here, the quantum transmitter holds a quantum signal source (QSS), random number generator (RNG), and polarization filter (PF) and the quantum receiver comprises of quantum detector (QD), RNG, and PF [6][7]. Various other components are also involved in QKD systems, and the choice of these components are subjected to the QKD protocols being used.

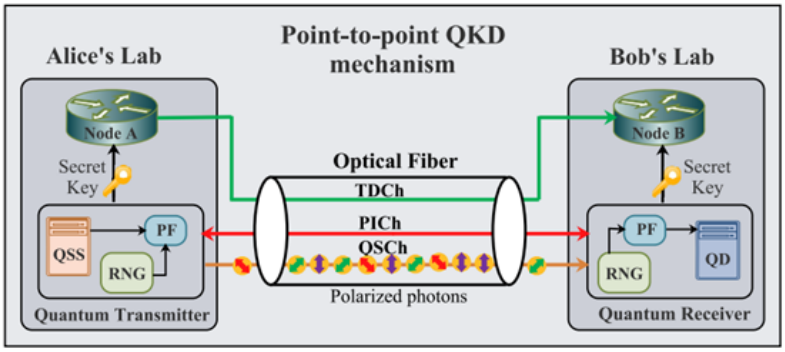

Figure 2. Point-to-point fibre based QKD mechanism [7].

Secure communication is established between transmitter and receiver in the following ways [7][8]:

• On the transmitter side, single photons are sent from QSS [8] to the PF and random bits are generated from RNG and transmitted to the PF. The single photons are polarized, and the bits generated by RNG are encoded with the polarized single photons to obtain qubits. These qubits are transmitted to the receiver through the channel QSCh where qubit synchronization is performed by PICh between transmitter and receiver.

• The quantum receiver measures the received qubits with randomly selected polarization bases. These measured bases are exchanged with transmitter and receiver through PICh for comparison. The qubits with the same polarization bases are then considered for secret key generation. The sequence of bits obtained after the comparison creates the sifted key. A further authentication process is performed via PICh to ensure the correctness of the sifted key and the remaining bits obtained in this process constitute the secret key [9]. The transmitter uses the generated secret key to encrypt the data and transmits the encrypted data to the receiver through traditional data channel (TDCh) where the receiver uses the same key to decrypt the received data [8].

• For data encryption, conventional encryption methods, such as one-time pad [10] and advanced encryption standard (AES) are widely used. In this method, Shannon found that the key length needs to be at least the data size at the minimum [11] and hence this method is not suitable for high bit rate data encryption due to its need for large storage and high execution time. An AES algorithm [12] was proposed as an alternative to overcome this problem, where secret keys of different lengths are used to encode and decode the data. The AES algorithm encrypts the data at smaller key size and low execution time [13][14].

Long distance implementation of fibre based QKD links causes technological hurdles and losses in transmission [15]. Introducing amplification to overcome optical losses will destroy the delicate quantum states used in QKD. Repeated trusted nodes with QKD are primarily incompatible in a practical and economical way. The use of free space medium through satellites to distribute secure keys to ground stations through free-space optical links can be considered as a viable solution for long distance key distribution to reduce propagation losses outside the earth's atmosphere compared to optical fibre.

2.2. Free Space based QKD

The free space based QKD is suitable for implementing both medium range terrestrial QKD links and long-range satellite based QKD links.

Medium-range terrestrial free-space quantum key distribution systems enable widespread secure networked communications in dense urban environments, where it would be infeasible to install many short optical fibre links. Such networks need to perform over a wide range of conditions and their design

must balance key rate maximisation versus robust key generation over the greatest range of circumstances. A terrestrial free space (FS) link is composed of a transmitter (Alice) and receiver (Bob), as shown in Fig. 3 [16]. In this configuration, the transmitter (Alice) consists of 4 emitters of phase randomized weak coherent pulses of the following polarizations: horizontal (H), vertical (V), diagonal (D) and anti-diagonal (A). The signals are mode matched in their spatial, spectral, and temporal degrees of freedom to avoid side channel information that can compromise security. The receiver (Bob) collects the photons using a suitable arrangement of optical elements (the collection optics). The beam-splitter chooses which polarization basis Bob will measure in.

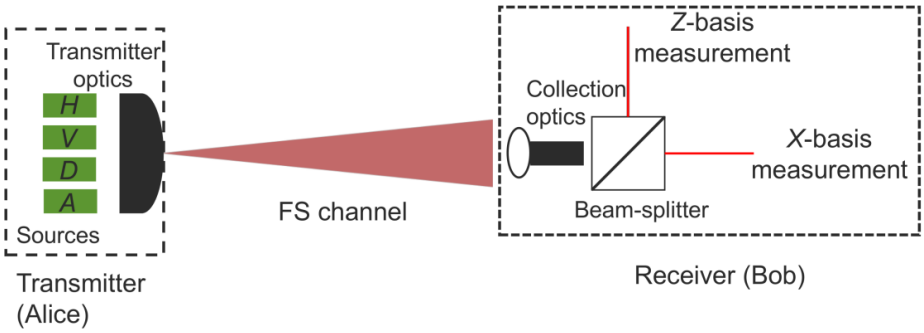

Figure 3. A common terrestrial based free space QKD system, an illustration [16].

In satellite based QKD, satellites placed above the earth's atmosphere are used as intermediate relay nodes to establish a communication link with users on the ground. Attenuation in free space decreases as altitude increases from ground level, becoming negligible in vacuum above the Earth's atmosphere. Thus, satellite based QKD is a promising route for establishing secure communications across global distances.

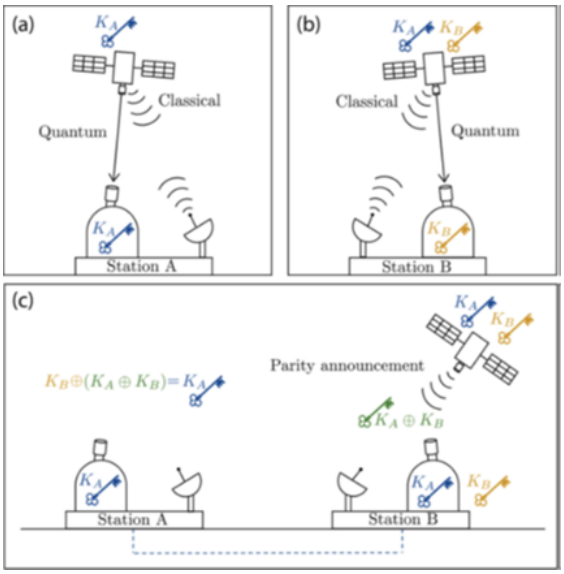

Figure 4. A common satellite based QKD system, an illustration [17].

A general satellite QKD scheme is illustrated in Fig. 4 [17], where the satellite is envisioned as a flying trusted node. The satellite performs QKD functions with individual ground stations and sets up independent secret keys with each of them. At the beginning, the satellite creates a shared secret key K_A with station A by running a QKD protocol as shown as step (a). This involves both classical and quantum communication. Similarly, step (a) is repeated in step (b) to establish a shared secret key K_B with station

B which is located at further distance. The satellite holds both keys while individual stations can only have access to keys of their own. To enable station A and B to share a common key, the satellite combines K_A and K_B and broadcasts their bit-wise parity $K_A \oplus K_B$. In step (c), the satellite widely announces the parity of both keys which allows station B to determine key K_A. Based on this announcement, the stations can retrieve each other's keys as $K_A \oplus (K_A \oplus K_B) = K_B$ and $K_B \oplus (K_A \oplus K_B) = K_A$. This can then be used to encrypt private communications to A and vice versa. This parity announcement does not help potential eavesdroppers to access useful information as original keys are just independent secret strings and their bit-wise parity is a uniformly random string. In this scenario, the satellite must be trusted since it holds all keys and their complete information.

QKD systems implement a cryptographic protocol to transfer quantum keys from transmitter to receiver. The following section discusses various QKD protocols.

3. An Overview of QKD Protocols

QKD consists of a family of cryptographic protocols to transmit a private encryption key between two parties. QKD protocols are mainly designed using two schemes, namely, Prepare and Measure (P&M) scheme, and Entanglement-Based (EB) scheme [22][23][24]. In P&M scheme, the transmitter prepares and send the information as polarized photons to the receiver for their measurement [23][24]. The P&M scheme is based on the Heisenberg's uncertainty principle and the quantum no cloning theorem. BB84 [18,19], Bennett-92 (B92), Six-State protocol (SSP) [25][26], Scarani Acin Ribordy Gisin-04 (SARG04) [27], Differential Phase Shift (DPS) [28][29] and others [30][31] are some of the QKD protocols based on this scheme. In the EB scheme, a source generates entangled quantum states, and sends them to transmitter and receiver [32], where both then measure the received quantum states. The quantum states of both the transmitter and receiver are linked so that the measurement affects each other, and both can easily detect any eavesdropper attack [24]. Ekert-91 (E91) and Bennett Brassard Meermin-92 (BBM92) [33] are some of the QKD protocols based on the EB scheme.

BB84 is known as the first protocol of quantum cryptography published by Bennett and Brassard in 1984 [18]. Individual photons were used for execution protocol and a sequence of single photons carrying qubit states is sent between transmitter (Alice) and receiver (Bob) through a quantum channel as given in Fig. 5. BB84 is vulnerable to a photon number splitting attack, where a pulse containing more than one photon can be split and read by Eve (attacker).

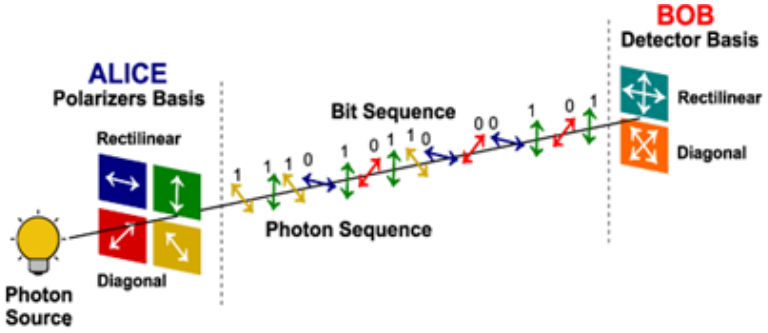

Figure 5. An illustration of BB84 Protocol [19].

Based on Bell's theorem, Ekert [20] proposed the E91 protocol where an entangled pair of photons are used. The photon entanglement principle or entanglement based QKD is used in this protocol where the photons source can be created either by transmitter or receiver. Fig. 6 illustrates E91 protocol where entangled photon source releases a pair of entangled photons from which the transmitter or receiver each receives one particle from every pairs. Similar to the BB84 protocol, the transmitter and receiver in the

E91 protocol choose a random basis for measurement. By using Bell's Inequality test, the presence of eavesdropper can be detected.

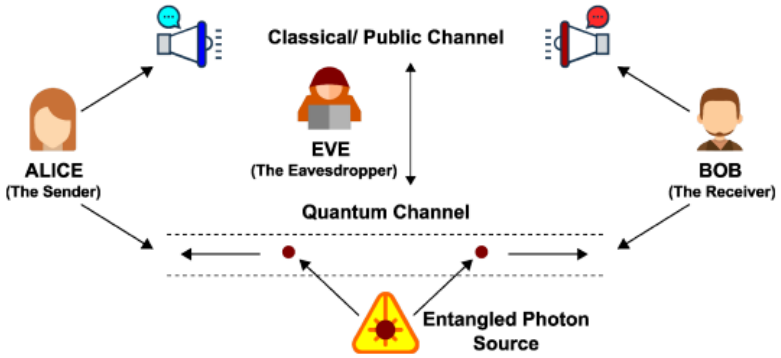

Figure 6. E91 protocol concept [19].

Bennett published the B92 protocol in 1992 [21]. Here, the QKD scheme uses signal photon interference where photons propagate over long distances through optical fibres. B92 is classified as prepare-and measure-based QKD protocol. In contrast to the BB84 procedure which uses one of four photon polarization states, the B92 protocol only uses one of two polarization states. A single non-orthogonal basis can be used in B92 for encoding and decoding QKD protocol without affecting the capacity to detect the presence of eavesdropper.

Year	Name of protocol	Principle Base	References
1984	BB84	Heisenberg's Uncertainty Principle	[18]
1991	E91	Quantum Entanglement	[20]
1992	BBM92	Quantum Entanglement	[33]
1992	B92	Heisenberg's Uncertainty Principle	[21]
1999	SSP	Heisenberg's Uncertainty Principle	[25][26]
2000	Discrete modulation protocol	Heisenberg's Uncertainty Principle	[36]
2001	Gaussian protocol	Heisenberg's Uncertainty Principle	[37]
2003	DPS	Quantum Entanglement	[28][29]
2004	COW	Quantum Entanglement	[31]
2004	SARG04	Heisenberg's Uncertainty Principle	[27]
2011	Entanglement-based QKD	Quantum Entanglement	[38]
2012	MDI-QKD	Principle of entanglement swapping	[39]
2013	S13	Heisenberg's Uncertainty Principle	[40]
2018	Twin-field QKD	Time-reversed Quantum Entanglement	[41]

Table 1. List of QKD protocols.

The QKD protocols can be also categorised as discrete variable (DV)-QKD protocols, continuous-variable (CV)-QKD protocols, and distributed-phase-reference (DPR)-QKD protocols [23]. In DV-QKD protocols, secret keys are generated between transmitter and receiver using the polarization states

of photon or phase to encode the bits. Photon counting and postprocessing methods are used for the detection of individual photons to generate the secret keys [23]. Single photon sources and detectors are required for this implementation with BB84 being the first protocol of this family [34]. Ralph introduced CV-QKD protocol for secure data transmission [35]. The major difference between the DV-QKD and CV-QKD protocol falls in their detection method. CV-QKD protocols substituted the photon counting approach of discrete-variable coding with an efficient coherent detection method (homodyne detection), which is cost-effective and fast. In DPR-QKD protocols, a sequence of coherent states of weak laser pulses is transmitted between transmitter and receiver. The continuous advances in quantum encryption continue to lead to the publications of new QKD protocols. Table 1 summarizes the existing QKD protocols.

Although QKD protocols can be proven unconditionally secure in theory, in practice any deviations of the real system from the idealised model could introduce vulnerabilities. For QKD technology to become a viable real-world solution, end-users need confidence in it, and this requires physical testing.

4. QKD metrology – Importance and Challenges

4.1. Importance of metrology in QKD

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, receivers and other optical components. A framework is required for the underlying theoretical security proof which again requires accurate knowledge of all the critical components of the system. Without the development of this framework, 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 main challenges in QKD technology are 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.

4.2. Metrology of QKD source

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 [43, 44] and are suitable for encoding in discrete degrees of freedom, e.g., in polarization, phase and arrival times. A more popular and promising single-photon source is based on spontaneous parametric down conversion (SPDC) which 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. This is of immediate use in metrology of components and detectors [43-45] and is a prospective candidate technology for future QKD sources.

A QKD source must maintain indistinguishability for photons in all degrees of freedom such as wavelength, spectral bandwidth, temporal jitter, and polarization, except that of encoding, i.e., encoded photons must not be distinguishable through measurement of parameters other than the encoding parameter. Hence it is essential to develop measurement capabilities for characterizing spectral,

temporal and polarization properties of individual photons emitted by (pseudo) single-photon emitters for QKD. Source timing jitter is the temporal uncertainty in the temporal emission of the light pulse versus the corresponding reference signal. This 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. 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, to build up a picture of the quantum state. In the case of polarized single photons, a polarization analysis apparatus is used to make repeated measurements over many individual photons, to build a statistical picture of the polarization state. 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.

Besides the spectral and temporal distinguishability considered in the fibre based QKD, eavesdropper could exploit the spatial mode distinguishability of the emitted pulses as a side channel attack in a free-space QKD system. Spatial filtering is used to overlap the output modes of the laser diodes. By using a spatial resolving detector, the far field of the source could be measured, and indistinguishability could be accessed. The single-photon avalanche diodes (SPAD) array is usually exploited as a sensor array to measure the spatial distribution $P(x)$ of transmitted photons. In [61], after calibrating an electron-multiplying charge-coupled (EMCCD) camera in single-photon level, the EMCCD camera which has higher resolution than SPADs array was used as a spatially resolving detector. After determined the preliminary characterization such as mean value and standard deviation of read noise, and the model of the relationship between the efficiency and the threshold defined in [61], EMCCD camera could be exploited as the spatially resolving detectors according to a similar procedure as SPADs array.

The distinguishability of photons emitted by the single photon source with different time delay is a potential factor of free-space QKD system which could be exploited to perform a side channel attack. The degree of indistinguishability is characterised by using Hong-Ou-Mandel (HOM) two-photon interference (TPI) experiments by exploiting the occurrence of an interference dip which comes from the destructive interference. In [62, 63], Technical University of Berlin (TUB) proposed a HOM type detection system based on the two asymmetric Mach-Zehnder interferometers with variable delay differences between two arms. Two types of quantum dot based single-photon sources and relative characterisations such as emission wavelength, extraction efficiency and the second order correlation function were measured by using the detection system and method.

A QKD source is also specified by a photon number distribution. 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 [46, 47]. Normally, two types of method are used to measure the mean photon number of the single-photon source. The first one is by using a traceable single photon detector such as SPAD. In the case of a laser with high attenuation working at single photon power class, the detector measures the laser pulses directly. In the second method, a traceable analogue detector such as an InGaAs photodiode is used to measure the high-power level of the laser pulse passing through a low value calibrated attenuator, which is then calculated by compensating for an attenuation factor representing the difference in offset from the power level. Based on the first method, in [64], a traceable Transition-Edge Sensors (TES) based measurement procedure and setup for determining the mean photon number and the photon distribution of quantum dot (QD) based emitters was developed. The transition-edge sensors could access the emitted light field and could directly determine the photon distribution. A compact adiabatic demagnetization refrigerator (ADR) was used to provide the low temperature which the detector needs.

The second order correlation function $g^{(2)}(\tau = 0)$ is used to characterise the probability of more than one photon per pulse. In [65], a well-designed measurement system is used to measure the second order correlation function $g^{(2)}(0)$ by exploiting the equivalence between $g^{(2)}(\tau = 0)$ and the α parameter which is measurable by conducting Hanbury Brown and Twiss interferometer (HBT) experiment. The measurement model also considers minimising the impact from accidental jitter of SPD and recording electronics, and the backflash.

Within a QKD emitter, the Quantum Random Number Generator (QRNG) 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 commercial QRNG modules in addition to software tests to check the randomness of the bit generation. To assess the performances of the QRNGs, the properties of the physical components that require characterization were identified such as 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 [76].

4.3. Metrology of QKD receivers

Single-photon receivers are single-photon detectors, which are optically sensitive devices that probabilistically transform a single photon into a macroscopically detectable signal. To date there is no single detector that can meet all the requirements such as unit quantum efficiency, photon number resolving (PNR) ability, minimum jitter, dead time, etc. There are many different trade-offs to be considered to obtain the best performance with a given set of QKD components. QKD performance can be affected by several 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.

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.

In the receiver of free-space QKD system, the detection efficiency of SPAD should be characterised very carefully especially if the receiver contains multiple single photon detectors. In [66], a facility and method which could be used to calibrate the detection efficiency of Si-SPAD detectors was presented. The proposed calibration system used a calibrated Si-diode as comparison with two calibrated neutral density filters and one variable filter to make photon flux level changeable in big dynamic range to fit both detectors. The final detection efficiency of Si-SPAD will be calculated from the signals for measurement of laser power with different filter insertions.

In [67], a laser-based measurement system containing a tuneable ratio splitter is established to characterize the detection efficiency (DE) of Transition-Edge Sensor (TES) single photon counters. The presented calibration procedure consists of two steps. The first step is measuring the power by using a calibrated power meter from the first outport of the beam splitter when the laser operates in the CW mode and the power pumped into the power meter is large enough to be detected. The second step is measuring the photon number by TES from the second output of the beam splitter, when the laser works with an electro-optical modulator (EOM) which is traceable to a cryogenic radiometer to generate the pulsed signal with high repetition rate and then it attenuates to single photon level by passing through a 40 dB attenuator. The detection efficiency is then calculated by using these measured results according to Poisson distribution assumption. National Institute of Standards and Technology (NIST) presented a calibration method/system for free-space and fibre based QKD detector working at a wavelength of

around 851 nm [68]. The devices under test (DUTs) include one free-space SPAD, two optical fibre-coupled Si-SPADs, and one superconducting nanowire single-photon detector (SNSPD). The calibration system used a CW laser and Ti:Sapphire oscillator with 5 nm bandwidth as two sources and a Si-Trap detector (Si-Trap) as power meter. A splitter/attenuator unit formed by a variable fibre attenuator (VFA), a fibre beam splitter (FBS) and a calibrated power meter (monitor) was used to calculate the power of DUT from the value of monitor and the output to monitor ratio was measured by a calibrated power meter pre-measurement. The DE and after pulsing characterization of each SPADs was measured based on the time-tag of the detection events.

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. 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) [48, 49]. 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.

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 a further increase of the noise level which an eavesdropper can exploit [48, 49]. In [69], An analytical model for the measured count rate of a free-running SPAD considering the effects of dark counts and its measurement procedure is established. The model was verified by an experiment for mean photon numbers. The measurement setup contains a laser worked at 1550 nm passing through two variable attenuators and reaching an InGaAs/InP SPAD. The real events and dark counts events can be distinguished based on the arrival times which are detected by a time-to-digital converter and a software-induced gating mechanism. The model is shown to match well with the measurement results in different configurations of the laser repetition frequency.

Back-flashes which are photons emitted by the detector itself during the avalanche process in the presence of a detection event from single-photon detector also appear 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. An optical time domain reflectometry (OTDR) system, operating at single-photon level was developed to characterize backflashes [77]. This system takes advantage of a free-running SPD based on InGaAs–InP SPAD which can 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.

Trojan-horse attacks use non-ideal features of the detectors to adversely affect their expected function. This type of attack can, for example, control the behaviour of the detection system by targeting single-photon detector features, such as detection efficiency mismatch (DEM) between the detectors of the QKD receiver, dead-time, jitter, and switching detection mode into the linear regime by a CW laser.

4.4. Metrology of QKD quantum channels

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 can be based on optical fibre which is the most common for most of the terrestrial QKD networks. Another quantum channel is based on the free space link which is present in some terrestrial networks to connect difficult terrains or

cities with no fibre link connectivity. The free space links are also used to connect ground based QKD systems to satellite based QKD systems and vice-versa for long range intercontinental QKD communication.

For fibre based QKD, 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, the portion 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 Alice and Bob 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 maximum achievable distance [46]. 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, Alice and Bob 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 [46]. However, knowledge of the a priori expected behaviour of the quantum channel is important.

One major practical challenge for QKD commercialisation over fibre is its integration with dense wavelength division multiplexing (DWDM) optical transport. The difficulty arises in the co-propagation of the QKD channel with classical DWDM channels over the same fibre [50]. The ability of DWDM technology to incorporate multiple wavelengths, thereby, increasing the data throughput of the fibre optic channel has made it the core functioning mechanism of optical networks. In addition, erbium-doped fibre amplifiers (EDFAs) can be deployed across optical links to increase the transmission distance. Even the ideal EDFA generates noise which limits the performance of the systems [51]. The source of the fundamental noise in EDFA, is known as Amplified spontaneous emission (ASE), and occurs due to the spontaneous emission from the Erbium doping. The optical bandwidth of the generated ASE noise is on the order of tens of nm and the noise generated by EDFA is dependent on linear gain of the EDFA and spontaneous emission factor. The quantum channel cannot be propagated through the EDFA, as each quantum state of light used subsequently to generate the key information will be irreversibly distorted by the action of amplification and hence an additional multiplexer is utilised for bypassing the ASE noise. The optical bandpass filter (OBPF) is placed after the EDFA to reduce the ASE noise, which can hinder the QKD performance significantly. It is essential to measure this performance degradation and investigate solutions to minimise noise from EDFA.

Another quantum channel effect in fibre based QKD is the Spontaneous Raman scattering (SRS). SRS occurs when a photon is scattered and generates/absorbs a photon with leading/lagging frequency shifts, respectively [52]. Photons from the classical channels can propagate into the quantum channel due to the Raman scattering. The magnitude of power from the generated Raman effect on the quantum channel is proportional to the power of all classical channels and the fibre span [53]. To reduce SRS, it is suggested that the QKD channel propagates at a lower wavelength than those of the classical channels [54, 55]. The effect of SRS on the quantum channel can be reduced by maintaining the optical launch power (OLP) of classical DWDM channels to be far less than ∼22 mW (∼13.4 dBm). The SRS effects have been reported over different fibre spans ranging from 2.7 km [56] to 50 km [57].

Four-wave mixing (FWM) is an effect that occurs when two or more wavelengths exist in the link. In the case of two lasers operating at frequencies $\nu 1$ and $\nu 2$ transmitting data through a single-mode fibre, the non-linear Kerr effect occurring in the fibre due to the change in the refractive index would result in FWM. Therefore, undesired frequency harmonics at $(2\nu 2 - \nu 1)$ and $(2\nu 1 - \nu 2)$ will be generated and the use of a simple filtering technique will not eliminate the FWM effect on the QKD channel. When the QKD is operating at 1550 nm, the presence of two neighbouring DWDM channels strongly influences the performance of the QKD channel. In such a scenario, the effect of the FWM cannot be easily suppressed because the generated harmonics can occur in the QKD frequency spectrum. According to

[58], separation between the QKD channel and classical channels would mitigate the crosstalk effect, which occurs due to FWM.

The variation in the optical intensity of classical data leads to a variation in the refractive index of the fibre. When different wavelengths are transmitted through the fibre, each wavelength's optical phase can be influenced by other wavelengths. Such a phenomenon is referred to as Cross-phase modulation (XPM). Coherent communication is more vulnerable to the XPM effect than non-coherent communication [59, 60]. In this regard, XPM is one of the main impairments to coherent quadrature phase-shift keying (QPSK) systems and quadrature of a carrier also carry information in CV–QKD protocol similar to the QPSK structure.

The free-space QKD channels are impacted by signal transmission through the atmosphere, scattering, absorption, and weather dependence, molecular absorption, aerosol absorption and atmospheric turbulence. Compared with the fibre-based QKD, the higher-level dynamic range of the signal intensity fluctuation disturbed by turbulence via free-space link makes the traditional way to share the time and frequency in fibre-based QKD very challenging. In [75], an MDI-QKD-based free-space QKD system is proposed, which takes an alternative approach, using an ultra-stable crystal oscillator-based reference signal on each of the two Tx sides. To minimize the difference between the two reference sources, a fraction of the arriving photons on the receiving side are used by the SNSPD to measure the time difference between the oscillators of the two Tx. On the other hand, two independent hydrogen cyanide molecule cells are used on each transmitter as the frequency standards and worked with photodiodes (PDs) to precisely calibrate DFB laser diodes (LDs).

In CV QKD system, a fading channel estimation is needed to compensate the channel fading and then restore the transmitted signal. In [70], a pass-loss model which could be used in satellite-based links for quantum key distribution by considering beam effects and weather dependence was presented. Many channel estimation algorithms used in CV QKD system are presented. In [71], a fading channel estimation for open space continuous-variable was proposed. In [72], a compressive sensing-based parameter estimation was proposed. In [73], a channel-parameter estimation over satellite-to-submarine link was proposed and assessed. The evaluation of the algorithm uses a Monte Carlo approach based on the model of free-space QKD channel when modelling the impact of the atmospheric turbulence, surface roughness, zenith angle of the satellite, wind speed, submarine depth was evaluated.

4.5. Metrology of optical components

Side channel attacks can target many of the properties of the elements that compose a QKD system: exploiting SPAD detector back-flashes, wavelength or timing mismatch of multi-diode emitters, the wavelength dependent splitting ratio of beam splitters/couplers, the wavelength dependence of intensity and phase modulators. An eavesdropper can attack a QKD system outside the specifications of its components, for instance by probing a filter’s transmission at 500 nm and/or with high power. The eavesdropper could also try to modify the components’ properties by interacting with them. Components should therefore be characterized over a broad range of wavelength and power, but also after interactions with special signals (wavelength, power etc.) to be sure that the eavesdropper will not have the opportunity to exploit weaknesses of the optical components. Hence broad-band characterization (400 nm - 1600 nm) at high and low power should be performed on passive components such as interference filters, beam splitters, isolators and circulators, and on active components such as InGaAs-SPAD based single-photon detectors operating in Geiger mode (SPDG), intensity modulators, and pin photodiodes.

4.6. NPL efforts in QKD metrology

NPL coordinated with European NMI’s through the ‘Metrology for Industrial Quantum Communication Technologies’ project (MIQC) [42] to address the metrology challenges in QKD to accelerate the commercialisation of the technology. One of the main outcomes of the MIQC project was the

establishment of the first measurement procedures for some specific quantities related to fibre based QKD components such as single-photon sources and single-photon detectors operating in the telecom wavelength around 1550 nm, characterization of quantum random number generator (QRNG) and fibre-based quantum channels. This was technically challenging since no measurement standards existed before MIQC for photon counting technologies at telecom wavelengths. The follow up MIQC2 project developed measurement techniques for the characterisation of the components of free-space QKD systems for ground-air communication mainly in the VIS-NIR range (wavelength range between 400 nm and 950 nm). Currently, a follow up project of the MIQC2 is in progress namely Metrology for testing the implementation security of quantum key distribution hardware (MeTISQ). This project aims to develop traceable methods and protocols for the characterisation of assembled QKD modules (i.e., transmitter and receiver). Traceable characterisation methods for active QKD components focussing on new, free-running or quasi-free-running single-photon detectors for telecom wavelengths (1550 nm) based on (InGaAs/InP SPADs) or superconductors (SNSPDs) will also be developed over the course of the project. Methods to characterise the hardware vulnerabilities of practical QKD systems for prominent attacks targeting single photon detectors will be investigated through this project.

In [74], the measurement method for a CV-QKD (COW) protocol-based chip-scale QKD system was developed. The method was used to characterise an assembled chip-scale full function transmitter and receiver (exclude detector). For the transmitter side, an NPL-calibrated gated SPAD was used to characterize mean photon number per time-bin to the generated pulses by the laser section. In the receiver side, the Mach-Zehnder interferometers (MZIs) and fibre beam splitters with three variable thermo-optic phase shifters (TOPS) was used to control the power ratio among arms are included in the chip. A method using CW light combined with three off chip SPAD are used to optimize the bias of TOPS by characterising the power of detectors with bias of TOPS.

5. Conclusion

Overall, during the past decade, the metrology of QKD technology has seen great progress. In this paper, we summarize the progress in metrology of four aspects: transmitter, receiver, quantum channel and other optical components.

For the transmitter side, the associated metrology facilities and measurement methods that can be used to characterize single-photon sources are introduced for the various implementations of single-photon sources ranging from attenuated pulsed laser, SPDCs to the quantum dot (QD)-based emitters. Critical parameters range from quantum number distribution, spectral, temporal, and polarization properties of single photons emitted by single-photon emitters, to the more important spatial mode distributions in free-space QKD systems.

For the receiver side, a typical two-step measurement method is discussed to characterize the detection efficiency of single-photon detectors. Other fully traceable calibration procedures based on similar methods are also described. Other critical parameters of the receiver, such as dead time, dark count, and flashback, are covered in the discussions.

Regarding the quantum channel, a special case of integrating quantum channels with traffic channels using DWDM technology, the effect of amplified spontaneous emission of EDFA and its associated OBPF is presented in a fibre based QKD system. The non-ideal factors of fibre channel such as SRS, FMW, etc. are also described. A reference signal sharing and synchronization technique is also discussed for a higher-level dynamic range of signal strength fluctuations of turbulent perturbations in free-space quantum channels for free-space QKD systems.

Acknowledgements
This project 20SIP05 KTOC has received funding from the EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme, Funder ID: 10.13039/100014132. This work was also supported by the Department for Business, Energy & Industrial Strategy (BEIS) through the UK National Quantum Technologies Programme, and Quantum Test and Evaluation programme.

6. References

[1] F. Xu et. al., "Secure quantum key distribution with realistic devices," Reviews of modern physics, vol. 92, 2020.
[2] National Institute of Information and Communications Technology, 'Beginning Joint Verification Tests on Quantum Cryptography Technology to Enhance Cybersecurity in the Financial Sector,' joint verification test, Cross-ministerial Strategic Innovation Promotion Program (SIP), January 18, 2021. https://www.nict.go.jp/en/press/2021/01/18-1.html
[3] Scarani, V. et al., The security of practical quantum key distribution. Rev. Mod. Phys. 81, 1301 (2009).
[4] Diamanti, E., Lo, H.-k, Qi, B. and Yuan, Z. Practical challenges in quantum key distribution. Quantum Inf. 2, 16025 (2016).
[5] A. C. Casado et. al., "Free-Space Quantum Key Distribution," Optical Wireless Communications - An Emerging Technology, Springer, 2016.
[6] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," IEEE/OSA J. Opt. Commun. Netw., vol. 9, no. 11, pp. 995–1004, Nov. 2017.
[7] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, 2021.
[8] Y. Zhao et al., "Resource allocation in optical networks secured by quantum key distribution," IEEE Commun. Mag., vol. 56, no. 8, pp. 130–137, Aug. 2018.
[9] E. Kiktenko, A. Trushechkin, Y. Kurochkin, and A. Fedorov, Post-processing procedure for industrial quantum key distribution systems," J. Phys. Conf., vol. 741, no. 1, pp. 1–6, 2016.
[10] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," IEEE J. Amer. Inst. Elect. Eng., vol. 45, no. 2, pp. 109–115, Feb. 1926.
[11] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.
[12] M. Dworkin et al., Advanced Encryption Standard (AES), Federal Inf. Process. Stand., Gaithersburg, MD, USA, Nov. 2001. [Online]. Available: https://www.nist.gov/publications/advanced-encryptionstandard-aes
[13] M. Taha and P. Schaumont, "Key updating for leakage resiliency with application to AES modes of operation," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 519–528, Mar. 2015.
[14] P. Derbez, P.-A. Fouque, and J. Jean, "Improved key recovery attacks on reduced-round AES in the single-key setting," in Proc. Adv. Cryptol. EUROCRYPT, 2013, pp. 371–387.
[15] Imran Khan, Bettina Heim, Andreas Neuzner and Christoph Marquardt,' Satellite-Based QKD,' Optics and Photonics News, The Optical Society, Feb 2018.
[16] T. Brougham and D. K. L. Oi "Medium-range terrestrial free-space QKD performance modelling and analysis", Proc. SPIE 11881, Quantum Technology: Driving Commercialisation of an Enabling Science II, 1188108 (6 October 2021)
[17] Bedington, R., Arrazola, J.M. & Ling, A., 'Progress in satellite quantum key distribution', npj Quantum Information, Aug 2017.
[18] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Comput. Syst. Signal Process., 1984, pp. 175–179.

[19] A. I. Nurhadi and N. R. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," 2018 4th International Conference on Wireless and Telematics (ICWT), 2018, pp. 1-5.
[20] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical review letters vol. 67, pp. 661-663, August 1991.
[21] C. H. Bennett, "Quantum Cryptography using any two Nonorthogonal Sates," Physical review letters vol. 68, pp.3121-3124, June 1992.
[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, Mar. 2002.
[23] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, Sep. 2009.
[24] M. Mafu and M. Senekane, "Security of quantum key distribution protocols," in Advanced Technologies of Quantum Key Distribution, S. Gnatyuk, Ed. Rijeka, Croatia: IntechOpen, 2018, ch. 1.
[25] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett., vol. 81, no. 14, pp. 3018–3021, Oct. 1998.
[26] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," Phys. Rev. A, vol. 59, no. 6, pp. 4238–4248, Jun. 1999.
[27] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett., vol. 92, no. 5, pp. 1–4, Feb. 2004.
[28] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett., vol. 89, no. 3, pp. 1–3, Jul. 2002.
[29] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," Phys. Rev. A, vol. 68, no. 2, pp. 1–4, Aug. 2003.
[30] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, no. 13, pp. 1–5, Mar. 2012.
[31] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," Nov. 2004.
[32] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," Phys. Rev. Lett., vol. 84, no. 20, pp. 4729–4732, May 2000.
[33] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett., vol. 68, no. 5, pp. 557–559, Feb. 1992.
[34] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Comput. Syst. Signal Process., 1984, pp. 175–179.
[35] T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A, vol. 61, no. 1, pp. 1–4, Dec. 1999.
[36] M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A, vol. 61, no. 2, pp. 1–8, Jan. 2000.
[37] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," Phys. Rev. A, vol. 63, no. 5, pp. 1–5, Apr. 2001.
[38] M. Houshmand and S. H. Khayat, "An entanglement-based quantum key distribution protocol," 8th International ISC Conference on Information Security and Cryptology (ISCISC), 2011.
[39] A. Boaron, et al. "Detector-device-independent QKD: security analysis and fast implementation." arXiv preprint arXiv:1607.05435 (2016).
[40] E. H. Serna, "Quantum Key Distribution from a random seed," Quantum Physics, arXiv preprint arXiv:1311.1582, 2013.
[41] Pirandola, S., Laurenza, R., Ottaviani, C. et al. Fundamental limits of repeaterless quantum communications. Nat Commun 8, 15043 (2017).
[42] Rastello, M L, et.al, (2014) Metrology for industrial quantum communications: the MIQC project. Metrologia, 51 (6). S267-S275.
[43] Eisaman M D, Fan J, Migdall A and Polyakov S V 2011 Rev. Sci. Instrum. 82 071101

[44] Midall A et al (ed) 2013 Single-photon generation and detection Experimental Methods in Physical Science vol 45 (New York: Academic)
[45] Dauler E, Migdall A, Boeuf N, Datla R, Muller A and Sergienko A 1998 Metrologia 35 295
[46] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys 74 145
[47] Norbert L and Mika J 2002 New J. Phys. 4 44
[48] Midall A et al (ed) 2013 Single-photon generation and detection Experimental Methods in Physical Science vol 45
[49] Hadfield R H 2010 Nature Photon. 3 696
[50] Eriksson, T.A., Hirano, T., Puttnam, B.J., et al.: 'Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels', Commun. Phys., 2019, 2, (1), p. 9, doi: 10.1038/ s42005-018-0105-5.
[51] Caves, C.M.: 'Quantum limits on noise in linear amplifiers', Phys. Rev. D, 1982, 26, (8), pp. 1817–1839
[52] Collins, M., Clark, A., Xiong, C., et al.: 'Random number generation from spontaneous Raman scattering', Appl. Phys. Lett., 2015, 107, (14), p. 141112
[53] Subacius, D., Zavriyev, A., Trifonov, A.: 'Backscattering limitation for fiberoptic quantum key distribution systems', 2005, p. 011103
[54] Mlejnek, M., Kaliteevskiy, N.A., Nolan, D.A.: 'Reducing spontaneous Raman scattering noise in high quantum bit rate QKD systems over optical fiber', arXiv preprint arXiv:1712.05891, 2017
[55] Bahrani, S., Razavi, M., Salehi, J.A.: 'Wavelength assignment in hybrid quantum-classical networks', Sci. Rep., 2018, 8, (1), p. 3456, doi: 10.1038/ s41598-018-21418-6
[56] Ribeiro, L., Quirino, S., Toledo, A., et al.: 'Spontaneous Raman scattering in optical fiber: experimental measurement'. AIP Conf. Proc., São Pedro, Brazil, 2008, vol. 1055, no. 1, pp. 159–162
[57] Feng, C., Rao, Z., Jin, S., et al.: 'Research on measurement of optical fiber Raman gain coefficient'. 2010 6th Int. Conf. on Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, China, 23–25 September 2010, pp. 1–4
[58] Ciurana, A., Martínez-Mateo, J., Peev, M., et al.: 'Quantum metropolitan optical network based on wavelength division multiplexing', Opt. Express, 2014, 22, (2), pp. 1576–1593
[59] Kumar, R., Qin, H., Alléaume, R.: 'Coexistence of continuous variable QKD with intense DWDM classical channels', New J. Phys., 2015, 17, (4), p. 043027.
[60] Chen, Y., Shen, Y., Tang, G.-Z., et al.: 'Impact of cross-phase modulation induced by classical channels on the CV-QKD in a hybrid system', Chin. Phys. Lett., 2013, 30, (11), p. 110302
[61] A. Avella, I. Ruo-Berchera, I. P. Degiovanni, G. Brida, and M. Genovese, "Absolute calibration of an EMCCD camera by quantum correlation, linking photon counting to the analog regime," Opt. Lett. 41, 1841-1844 (2016)
[62] S. Fischbach, et.al, "Single Quantum Dot with Microlens and 3D-Printed Micro-objective as Integrated Bright Single-Photon Source", ACS Photonics 2017 4 (6), 1327-1332
[63] S. Fischbach, et.al, "Efficient single-photon source based on a deterministically fabricated single quantum dot - microstructure with backside gold mirror", Appl. Phys. Lett. 111, 011106 (2017)
[64] Schmidt, M., von Helversen, M., López, M. et al. Photon-Number-Resolving Transition-Edge Sensors for the Metrology of Quantum Light Sources. J Low Temp Phys 193, 1243–1250 (2018).
[65] E Moreva, "Feasibility study towards comparison of the g(2)(0) measurement in the visible range", Metrologia, vol. 56, no. 1, Jan 2019.
[66] López M, Hofer H, Kück S. Detection efficiency calibration of single-photon silicon avalanche photodiodes traceable using double attenuator technique. J Mod Opt. 2015 Dec 8;62(sup2):S21-S27.
[67] Schmidt, M., von Helversen, M., López, M. et al. Photon-Number-Resolving Transition-Edge Sensors for the Metrology of Quantum Light Sources. J Low Temp Phys 193, 1243–1250 (2018).
[68] T. Gerrits, A. Migdall, J. C Bienfang, J. Lehman, S. W. Nam, J. Splett, I. Vayshenker and J. Wang, "Calibration of free-space and fiber-coupled single-photon detectors", Metrologia, vol. 57, no. 1, Dec 2019.

[69] H. Georgieva, "Detection of ultra-weak laser pulses by free-running single-photon detectors: Modeling dead time and dark counts effects", Appl. Phys. Lett. 118, 174002 (2021)
[70] C. Liorni, H. Kampermann and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence", New Journal of Physics, vol. 21, Sept 2019.
[71] L. Ruppert, "Fading channel estimation for free-space continuous-variable secure quantum communication", New Journal of Physics, vol. 21, Dec 2019
[72] Feng Jing, Xiaowen Liu, Xingyu Wang, Yijie Lu, Tianyi Wu, Kai Li, and Chen Dong, "Compressive sensing-based parameter estimation for free-space continuous-variable quantum key distribution," Opt. Express 30, 8075-8091 (2022)
[73] Y. Guo, C. Xie, P. Huang, J. Li, L. Zhang, D. Huang, and G. Zeng, "Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution", Phys. Rev. A 97, 052326, May 2018.
[74] Vaquero-Stainer, A; Kirkwood, R A; Burenkov, V; Chunnilall, C J; Sinclair, A G; Hart, A; Semenenko, H; Sibson, P; Erven, C; Thompson, M G (2018) Measurements towards providing security assurance for a chip-scale QKD system. Proceedings of SPIE, 10674. 106741A
[75] Yuan Cao, Yu-Huai Li, Kui-Xing Yang, Yang-Fan Jiang, Shuang-Lin Li, Xiao-Long Hu, Maimaiti Abulizi, Cheng-Long Li, Weijun Zhang, Qi-Chao Sun, Wei-Yue Liu, Xiao Jiang, Sheng-Kai Liao, Ji-Gang Ren, Hao Li, Lixing You, Zhen Wang, Juan Yin, Chao-Yang Lu, Xiang-Bin Wang, Qiang Zhang, Cheng-Zhi Peng, and Jian-Wei Pan, "Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution", Phys. Rev. Lett. 125, 260503 – Published 23 December 2020.
[76] A. Tomasi, A. Meneghetti, N. Massari, L. Gasparini, D. Rucatti and H. Xu, "Model, Validation, and Characterization of a Robust Quantum Random Number Generator Based on Photon Arrival Time Comparison," in Journal of Lightwave Technology, vol. 36, no. 18, pp. 3843-3854, 15 Sept.15, 2018.
[77] Meda, A., Degiovanni, I., Tosi, A. et al. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. Light Sci Appl 6, e16261 (2017).