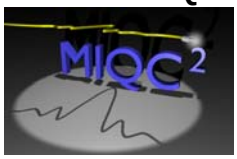

FINAL PUBLISHABLE REPORT

Grant Agreement number	14IND05
Project short name	MIQC2
Project full title	Optical metrology for quantum-enhanced secure telecommunication
Period covered (dates)	From 1 June 2015 To 30 May 2018
Coordinator	
Name, title, organisation	Dr Ivo Pietro Degiovanni, INRIM
Tel:	+39 011 3919245
Email:	i.degiovanni@inrim.it
Website address	http://empir.npl.co.uk/miqc2/
Other partners	

INRIM, Italy
Aalto, Finland
CMI, Czech Republic
Metrosert, Estonia
NPL, UK
PTB, Germany
PoliMi, Italy
Toshiba, UK
TUB, Germany
UBER, Germany
IDQ, Switzerland
KRISS, Republic of Korea
METAS, Switzerland
MPD, Italy
UniGE CH, Switzerland

TABLE OF CONTENTS

1 Executive summary

Quantum Key Distribution (QKD) is essentially the generation of perfectly secure random keys between two parties that communicate by an open quantum channel. This enables the parties to establish a secret key from short pre-shared secret and public exchanges, something which has never been shown to be possible with classical, non-quantum means. With increasing amounts of data being transmitted and stored online, there is an increasing need to secure that data. Researchers in the field consider QKD as the only truly secure key distribution technology (except secret courier) since it is secured by the laws of physics. Interestingly, conventional asymmetrical cryptography, which is almost exclusively used for key distribution today, could be rendered insecure by the advent of extremely powerful computers, including quantum computers, or new mathematical insights.

The aim of this project has been to accelerate the development and commercial success of QKD technologies. the key results achieved in this project were:

- The development of measurement techniques for characterising and validating counter-measures to quantum hacking strategies (such as side-channel and Trojan-horse attacks) in order to ensure the security of real fibre-based QKD systems operating at telecom wavelength (i.e. around 1550 nm). The project activities have been carried on in close collaboration with “quantum” companies and the Industry Specification Group on QKD of the European Telecommunications Standards Institute (ETSI ISG-QKD). To ensure the validation of the measurements at single-photon level at telecom wavelength, MIQC2 consortium carried on two pilot studies towards measurement comparisons (the measurement quantities considered are the detection efficiency of single-photon detectors, and a statistical parameter describing the photon emission of light sources operating at the few-photon kevel).
- The development of measurement techniques for characterising components used in free-space QKD systems for, e.g., ground-air communication. This required the development, or improvement, of calibration methods for single-photon sources, detectors, and other relevant optical components such as polarisation encoder and attenuator in the VIS-NIR spectral region (in general, around 850 nm: the wavelength typically used in free-space quantum communications). To ensure the validation of these measurements at single-photon level, MIQC2 consortium carried on two pilot studies somehow analogous to the ones at telecom wavelength, but in the VIS-NIR.
- The establishment of the foundations of the metrology required for next-generation QKD systems based on the entanglement of photons. The MIQC2 consortium,for example developed new sources of entangled photons andrealized measurement techniques for characterising quantum states (i.e. witnessing and quantifying the amount of entanglement and “non-classicality”).
- The contribution to international guidelines and standards with specific focus on the ETSI Industry Specification Group for QKD (ETSI ISG-QKD). In particular, MIQC2 consortium led the drafting of four Group Specification documents for QKD, focusing on the characterisation of optical components in QKD systems, and on verification through measurement of countermeasures against Trojan-Horse and Side-Channel attacks.
- The initial steps towards the realisation of the European Metrology Network for Quantum Technologies under the EURAMET umbrella. This started from an investigation on the possibility of establishing a metrology network for Quantum Photonics between the partners of the project. The Metrology Network aims to coordinate the scientific and technological efforts of the European Metrology Institutes to face the challenges posed by the quantum technologies revolution.

2 Need for the project

EMPIR 14IND05 MIQC2 was designed to build on the existing metrological framework, established by EMRP IND06 MIQC for assessing QKD and its components, so that we better understand how QKD components, counter-measures to attacks, and new types of QKD which are in principle more robust to attacks, perform in an adversarial environment. This impacts on QKD manufacturers and component manufacturers helping them to develop reliable and characterised components, fundamental for producing more reliable and trusted QKD systems. This in turn provides assurance to end users, who do not necessarily care about the technological details of QKD, but need to know that QKD systems have been rigorously tested in all conditions and that the industry is governed by agreed, rigorous standards. This project aimed at meeting these measurement challenges, or at least several of them, as well as engaging with bodies such as ETSI to draft paper standards to provide assurance to end users.

One of the main outcomes of the EMRP IND06 MIQC project was the establishment of the first measurement procedures for some specific quantities related to QKD components, namely pseudo single-photon sources, and detectors, operating in a benign environment (i.e. not subject to hacking attacks). A transformation of these results into a reliable, efficient and market-oriented metrological approach is necessary for maintaining the leading role of Europe in the quantum communication field. This is in essence the need of the activities carried on in EMPIR 14IND05 MIQC2.

Proofs of absolute security for QKD often assume perfect implementation of the theory, but systems can be vulnerable to side-channel and Trojan-horse attacks due to flaws in their experimental implementation. This is exactly where MIQC2 has impact on. Indeed, ad-hoc strategies and counter-measures have been developed to counter these attacks. QKD security analyses are now addressing the use of practical devices and counter-measures to attacks; measurements have been developed to test whether devices truly meet the stipulated requirements flowing from these analyses.

QKD exploiting satellites appears to be the only viable solution for achieving QKD worldwide, thus a metrological infrastructure able to provide appropriate characterisation of optical components for free-space QKD is absolute necessary. EMPIR 14IND05 MIQC2 substantially moved forward the development of such an infrastructure.

Entanglement, as in entangled states or entangling measurements, has a central role in a new generation of QKD technologies. This ranges from the realization of quantum repeaters and the development of quantum networks, to the practical application of (measurement-) device-independent QKD. Substantial research activities in the context of MIQC2 aimed at building the measurement infrastructure necessary for these futuristic technologies.

3 Objectives

The aim of this project is to accelerate the development and commercial success of QKD technologies. The main objectives addressed in this project are:

1. The development of efficient measurement techniques for characterisation of counter-measures to side-channel and Trojan-horse attacks in fibre-based QKD systems, and the realisation of pilot measurement comparisons to validate the techniques
2. The development of new high-speed (sine-gated) single-photon detectors for fibre-based QKD and the relative calibration technique
3. The development of measurement techniques for the characterisation of the components of free-space QKD systems for ground-air communication, and the realisation of pilot measurement comparisons to validate techniques developed
4. The development of measurement techniques for characterising the “quantumness” of quantum states
5. To provide two Best-Practice Guides, one on characterisation of counter-measures to side-channel and Trojan-horse attacks, and one on characterisation of components of free-space QKD systems
6. Contribute to impact - via contributions to international guidelines/standards and showcase examples of early uptake by end users

4 Results

Objective 1: Metrology for counter-measures to side-channel and Trojan-horse attacks in fibre-based QKD systems

The first objective of the project was the development of efficient, cost-effective measurement techniques for characterizing and validating counter-measures to side-channel and Trojan-horse attacks, and the identification of additional parameters or components that must be accurately characterised in order to ensure the security of real fibre-based QKD systems operating in the third telecom spectral window (i.e. around 1550 nm). This has been performed in collaboration with “quantum” companies and standardization bodies, in particular the Industry Specification Group on QKD of the European Telecommunications Standards Institute (ETSI ISG-QKD).

Despite the unconditional security of QKD protocols, practical QKD implementations may suffer from technological and protocol-operational imperfections that an eavesdropper (Eve) could exploit in order to remain undetected. Ranging from Trojan-horse attacks where the eavesdropper can extract some information from the QKD process by exploiting specific non-idealities or weaknesses of QKD optical components, to unexpected leakage of information in side-channels, a variety of eavesdropping attacks have been devised and sometimes implemented, which exploit the differences between the theoretical model and the practical implementation. The technical results connected to this objective have largely contributed to the project's impact, fostering the development of new standard protocols and the updating of the existing ones in close collaboration with the ETSI ISG-QKD.

Characterising counter-measures to Trojan-horse and side-channel attacks

The aim of this group of activities was to identify the vulnerabilities of QKD components to Trojan-horse and side-channel attacks, and to characterize the efficacy of counter-measures to such attacks. All these attacks invariably exploit some non-ideal behaviour of the components of real QKD systems. The Trojan-horse attacks use non-ideal features of the QKD components (mostly the detectors) to adversely affect their expected function. This type of attack can, for example, control the behaviour of the detection system by targeting real 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. 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.

A counter-measure against Trojan-horse attacks requires filters and 'watchdog' detectors. To ensure that the counter-measure is efficient, it is necessary to check that the filter will block light with wavelengths outside of the wavelength detection range of the detector. It also needs to ensure that the properties of the components will not be altered by bright-light or special wavelength pulses. Broad-band characterization (400 nm - 1600 nm) at high and low power should be performed on passive components such as interference filters, beamsplitters, 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. In addition, the performance of intensity and phase modulators for countering bright pulse and DEM attacks should be performed.

Activities specific to SPDGs carried on in MIQC2 to measure their gate time detection efficiency (DE) dependency (to prevent DEM attacks), to develop electronic circuitry to defeat attacks, to characterise their back-flash emission, and to develop the ability to monitor their DE in the single-photon regime when installed in a commercial QKD system.

The development of a low-photon-flux reference-detector for telecom wavelengths based on a thermoelectrically-cooled state-of-the-art InGaAs detector in conjunction with a custom-made high-sensitivity switched-integrator amplifier improved the noise performance at very low light level (around fWs).

The side-channel information remaining after the implementation of countermeasures to reduce information disclosed to Eve will be investigated. This information will be integrated into the model of prepare-and-measure QKD, leading to a modified security proof which accounts for the disclosed information.

Specifically, the most interesting results achieved by the MIQC2 consortium are

- The characterization of the splitting-ratio of pigtailed beam-splitter, as a countermeasure against multi-wavelength attacks, using a tunable OPO laser facility in conjunction with a dual synchronized detection system that allow to compensate for the OPO pulse by pulse instability (up to 40%). Using this measurement procedure, the statistical spread of the splitting ratio was as low as 200 ppm to in the spectral range between 1260nm and 1650nm.
- The characterization of the optical transmission of key optical components of QKD systems (interference filters, wavelength division multiplexing filters, optical isolators and circulators). In

particular optical transmission of a polarization maintaining (PM) circulator and of a standard (not PM) circulator at discrete wavelengths (850 nm, 1310 nm and 1540 nm) have been performed. The optical transmission of interference filters, wavelength division multiplexing filters and optical isolators in the optical domain ranging from 700 nm to 1640 nm have been characterized. Astonishing results have been obtained: serious discrepancies, with respect to the ideal behaviour, have been found at hundreds of nanometers from the nominal operation wavelength. The results is that only proper combination of these devices accurately characterised may provide the necessary protection of QKD systems. The measurement techniques here developed represent an early uptake, since METAS is developing a calibration service based on that.

- The characterisation of the extinction ratio of typical intensity modulator that could be used for restoring the security against attacks exploiting bright illumination. The characterisation was performed at the single-photon level (simulating the condition of operation) exploiting a single-photon heralded source at 1550 nm (15 nm bandwidth). The extinction ratio has been evaluated to be 0.001(0.002). Similar result was obtained using conventional calibration using laser light.
- The investigation on the vulnerability of SPDGs to bright pulse attacks outside their normal light level range of operation. Specifically, the SPDG tested was the id220 by IDQ. It was successfully calibrated under various level of illumination. The measurements were performed at 1310nm and at 1550nm. The count rate of the SPDG was measured when varying the optical power of a reference source. This allowed to identify the threshold level of the potentially dangerous linear detection regime.
- The calibration of the spectral responsivity and of the linearity of a PIN diode used against Trojan horse attack. This PIN detector is used in IDQ QKD emitters to calibrate the output power of the device. The proper measurement of this value is essential for security of the key exchange. Identical photodiodes with similar electronics were used in IDQ Clavis2 QKD system to attempt to detect Trojan horse attack with CW light. The spectral responsivity was calibrated in the spectral range between 700 nm and 1640 nm and the linearity was calibrated at 1310 nm and 1550 nm. A dedicated measurement system was developed for this purpose.
- The characterisation of the back-flash emission in order to quantify and then suppress possible information leakage that Eve could gain on the internal behaviour of the Bob's QKD receiver. It was demonstrated that backflash light emitted by single-photon detectors may contain a substantial amount of information of potential interest for an eavesdropper. Possible countermeasures are identified. A relevant publication was originated by this activity [Light: Science & Applications (2017) 6, e16261].
- The realisation of a calibration procedure for the detection efficiency of the detectors used in QKD prototypes as a function of time within the detection temporal gate, defining a reliable mitigation against detection efficiency mismatch attacks. The calibration procedure developed is based on detection efficiency measurements -as codified in the ETSI document ETSI GS QKD 011 V1.1.1 (2016-05) and tested in this project- taking advantage of a sub-nanosecond-pulsed laser at 1550 nm. The detection efficiency measurements have been performed by setting 15 different delays (with 1 ns incremental step) of the peak of counts within the detector (id210) gate window, preliminarily set at 15 ns. As expected the measured values are stable except close to the gate edges: it is enough to have detections 1 ns inside the gate window to avoid detection efficiency mismatch attacks, from the detector point of view.
- The realisation of a broadband watchdog detector as a counter measure against Trojan horse attacks. It consists on a hybrid-trap that uses Si and InGaAs photodiodes to measure light in the broad wavelength range from 400 nm to 1600 nm. The broadband watchdog detector has been tested and characterized using a combination of pulsed laser light beams at wavelengths 685 nm and 1550 nm. The NIR light was pulsed with frequency 100 MHz and the VIS light was pulsed at three frequencies (1, 10 and 20) MHz. These tests demonstrated that the Si-photodiode can record light to which InGaAs-photodiode is blind and vice-versa. This feature can be exploited to monitor for 'side' beams in the optical system.
- The realisation of a new secure front-end circuit for InGaAs/InP SPADs exploiting a configurable system based on a FPGA (for controlling the main critical signals) and on a custom integrated circuit (designed to operate an InGaAs/InP SPAD) has been perfomed. Specifically: avalanches during dead time are fully rejected; advanced synchronization/deskew avoids efficiency mismatch attacks; bias voltage/current and temperature are constantly monitored. The instrument has been assembled and

fully characterized. The effectiveness of the implemented counter-measures was demonstrated against the following attacks: i) efficiency-mismatch attacks (the residual mismatch is less than 10 ps); ii) after-gate attacks; iii) blinding attacks.

- The realisation and characterisation a low-photon-flux reference detector in the IR spectral region (LOFIR) comprising a thermoelectrically-cooled state-of-the-art fibre-coupled InGaAs detector in conjunction with a custom-made high-sensitive switched-integrator amplifier. The LOFIR achieved excellent noise performances (<2 fW noise at 1550 nm). The LOFIR was calibrated in terms of spectral responsivity of from 900 nm to 1700 nm in the free space configuration using the double-monochromator based facility developed for the calibration of SPDs in the 1550 nm region.
- The analysis and extension of the previous security model for prepare-and-measure QKD schemes to encompass more general side channels, not only those related to the Trojan-horse attack. This situation identifies the “leaky sources”. Indeed, it was demonstrated that, even in presence of a leaky source it is possible to guarantee the full security of a QKD system. Measurements and solutions to increase the final key rate of the system were devised, such as e.g. the phase randomizer against the Trojan horse attacks, or the Hanbury Brown and Twiss measurement to rigorously characterize the photon statistics of a QKD light source. Furthermore, the security model to account for the non-zero information leakage that remains even after the implementation of the countermeasures has been extended. This research is summarized in the papers Tamaki et al., New J Phys. [18], 065008 (2016) and Dynes et al., arXiv:1711.00440.

Novel high-rate single-photon detectors for fibre based QKD

In addition to countermeasures to Trojan-horse and side-channel attacks, it is necessary to consider a new class of periodic-high-rate-gate single-photon detectors developed since the EMRP IND06 MIQC project.

InGaAs/InP SPAD single-photon detectors are generally used in gated-mode, where the detector is turned on (above its breakdown voltage) for only a few nanoseconds. Each gate is followed by a long hold-off period (up to few tens of microseconds) to limit after-pulsing. Recently, a SPAD has been developed to allow free-running operation of InGaAs/InP SPADs by reducing the avalanche charge with an integrated passive fast-quenching resistor, but its throughput is limited to below 1 Mcount/s.

To overcome the intrinsic low throughput of the standard gating technique due to its long hold-off time, different fast-gating methods have been developed, some based on sub-nanosecond square-wave gate signals, while others are based on gigahertz sine wave gating.

These techniques enable InGaAs/InP SPADs to operate at high count rates, due to a strong reduction in the after-pulsing probability and hence of the required hold-off time, but they are suitable only for periodic optical signals with a short duration (below 1 ns) because of their limited “on” time, as is the case for QKD.

A photon-counting system based on InGaAs/InP SPADs sinusoidally-gated at more than 1 GHz was developed. The main features are: i) very low after-pulsing (around few percent); ii) high dynamic range (maximum count rate > 100 Mcount/s), high detection efficiency (> 30 % at 1550 nm), low noise (per-gate dark count rate < 1 x 10^{-4}) and low timing jitter (< 100 ps). Such electronic circuit solution was developed with a differential read-out for reading the avalanche pulses with low time jitter and a feedback control loop for long-term stability. In order to guarantee fast avalanche quenching, the gate signal is at frequency > 1 GHz, but it is tunable in a wide range (900-1400 MHz) for synchronization with different external laser systems and for selecting the best trade-off between after-pulsing and detection efficiency. The excess bias is adjustable for optimizing the main SPAD parameters, like photon detection efficiency, dark count rate, after-pulsing, timing jitter. The system can be controlled remotely from a PC and proved long-term stability.

During the development of this sine-gate module, a few problems emerged due to the demanding specifications of the system under development in terms of frequency and phase shift. The most important problem was solved by employing a new PLL (just introduced into the market) that experimentally demonstrated to guarantee low noise and correct synchronization with an external laser source.

A first prototype has been assembled and its experimental characterization demonstrated that the aforementioned goals have been achieved with a noise level at the readout node of < 1 mV (thanks to a gate feed-through suppression of more than 50 dB) and an avalanche amplitude > 12 mV (at V, = 7 V).

The above-described unexpected difficulties have delayed the realization of a first fully-working prototype of the detectors only at the very end of the project. Thus, it was impossible to start developing a completely new characterization technique during the lifetime of the project. Because of the interest in the characterization of

such novel detectors, the members of the Consortium will carry on this activity exploiting their own resources outside the lifetime of the project.

Pilot studies for the measurements of detection efficiency and source photon statistics for validating the calibration facilities at telecom

As a route to the validation of the measurement facilities, developed in the framework of this project, four European NMIs (INRIM, PTB, NPL and CMI) started two pilot studies on two key measurands in the 1550 nm region correlated with fibre-based QKD systems, i.e. the detection efficiency of single-photon detectors, and the Glauber second-order auto-correlation function of a pseudo single-photon source. Measurement protocols and procedures were developed on purpose.

Specifically,

- the pilot study towards a comparison on the measurements of detection efficiency of SPADs in the 1550 nm region, exploited a free-running InGaAs/InP SPAD-based detector. An excellent agreement (within the uncertainty) was obtained. The Pilot study was carried on jointly in the INRIM labs. The results will be disseminated by presentations at conferences and meetings, and a paper is in preparation;
- the pilot study towards a comparison on the measurements of the Glauber second order autocorrelation function achieved a good agreement within the uncertainty. The source used for this test was a CW heralded single-photon source emitting real single photons at 1550nm. The Pilot study was carried on jointly in the INRIM labs. The results will be disseminated by presentations at conferences and meetings, and a paper has been already submitted.

Objective 2: Metrology for components of free-space QKD system

The second objective of the project was the development of measurement and characterization facilities within the Consortium for components of free-space QKD devices. This included metrology for single-photon sources and detectors as well as relevant optical components. Within the scope of this project, we defined visible-light QKD as the spectral range where silicon-based detectors are applicable, i.e. as the wavelength range between 400 nm and 950 nm.

Specifically, MIQC2 consortium developed measurement facilities for detectors, sources and components relevant for free-space QKD, identified in analogy with the work carried on within the EMRP IND06 MIQC, for fibre-based QKD (i.e. at telecom wavelength, and not in the VIS-NIR as in this case). Furthermore, new components for free-space QKD were developed when necessary, and pilot studies for the validation of the measurement facilities by carrying out comparisons of selected measurands have been carried on.

Measurement facilities for detectors for free-space QKD

Different facilities for the calibration of the detection efficiency of free-space single-photon detectors in the VIS-NIR spectral range are established:

- **Double monochromator-based facility**. A double monochromator-based calibration facility and a reference detection setup for low photon fluxes traceable to the primary radiometry standard, the cryogenic radiometer, is developed. The transfer detector used was a low-noise thermally cooled miniature Si photodiode reflection trap developed on purpose. The double monochromator-based calibration facility has been proven able to perform spectral characterization of detection efficiency, linearity and spatial uniformity of free space Si SPAD. The same facility has been used to characterize the standard for low photons fluxes for the infrared spectral range (LOFIR).
- **Laser-based facility.** A laser-based calibration facility has been established, based on the precise beam attenuation method using in-situ calibrated neutral density filters and, subsequently Si-photodiodes in trap-configuration. The laser-based facility was used for the comparison of the detection efficiency of Si-SPAD detectors using only the calibrated neutral density filter. The upgrade with the attenuator based on Si photodiodes is ready.

Measurement facilities for sources for free-space QKD

Characterisation of sources used in QKD systems is also of high importance. Therefore measurement facilities for the characterization of sources suitable for free-space QKD have been established. Specifically, the more interesting activities carried on by the consortium this context are:

- The characterization of the photon statistics distribution of a single-QD-based single-photon source, developed in the context of this project. This has been achieved thanks to the realization of a measurement system based on 2 TES-photon counters operated in a portable millikelvin refrigerator, whose detection efficiency has been calibrated (within MIQC2) with an uncertainty < 1 %. The results of this activity were published in T. Heindel et al., Nat. Commun. 8, 14870 (2017).
- The characterization of two types of single-photon source – (a) an InGaAs quantum dot with a distributed Bragg reflector below it and a microlens and micro-objective above it; (b) an InGaAs quantum dot with a gold mirror below it and a microlens above. The emission wavelength, extraction (out-coupling) efficiency into a numerical aperture of 0.4, and $g^{(2)}(0)$ value were measured to be [$\lambda_{emission}$ = 918 nm, $\eta_{extract}$ = (40 ± 4)% , $g^{(2)}(0) < 0.02$] for (a) [relative publication: ACS photonics 4, 1327 (2017] and [$\lambda_{emission}$ = 947.1 nm, $\eta_{extract}$ = (18 ± 2)% , $g^{(2)}(0) = 0.015 \pm 0.009$] for (b) [relative publication: Appl. Phys. Lett. 111, 011106 (2017)].
- Lifetime and coherence measurements on InGaAs quantum dot with a distributed Bragg reflector below it and a microlens and micro-objective above it was performed, reporting a spontaneous emission lifetime of 1.2 ns and a coherence time of about 0.7 ns for the neutral exciton. Indistinguishability measurements were performed by using a Hong-Ou-Mandel (HOM) interferometer developed in the context of the project. Measurements with single-photon avalanche photodiode non-photon-number-resolving detectors at the output ports of the HOM interferometer yielded an interference visibility of (84 ± 7) %. Measurements with TES photon-number-resolving detectors at the output ports of the HOM inferred an interference visibility of (95 ± 5) %.
- The characterisation of the spatial modes of emitted/transmitted photons of a single photon source, exploiting different kinds of spatially resolving detectors (i.e. an EMCCD, and a SPAD Array). EMCCD are efficient detectors (100 % fill factor, > 90 % quantum efficiency), while SPAD arrays have fast timing capabilities. The two elements of information have been merged. SPAD array and EMCCD were used to measure the spatial mode of a fibre-coupled heralded single-photon source. A model of SPAD and EMCCD operated in On/Off regime has been developed and validated by experimental results [Optics Letters 41 (8), 1841 (2016)]. Then, the uncertainty on the spatial distribution of the mode and its characteristic parameters has been evaluated as a function of the parameter of the detectors, i.e. noise count probability and Quantum Efficiency.

Measurement facilities for components used in free-space QKD

It is important to consider also components other than sources and detectors which are relevant for free-space QKD. Within this project, the focus was on the characterisation of the main components, i.e. polarization controllers with respect to the degree of polarization, intensity modulators with respect to modulation depth, attenuators with respect to transmission. Specifically:

- The setup and characterization of a system for polarization control based on quartz plates analogous to the one used in free-space QKD systems with respect to encoding degree of freedom (the polarization) has been carried on. Within the activity it was realised also a single-photon polarimeter to perform the quantum state tomography at single photon level. The tomographic reconstruction of the polarisation state emitted by the QKD transmitter has been successfully completed.
- 2 intensity modulators (model: iXblue Photline NIR-MX800-LN-10, 10 GHz Mach-Zehnder intensity modulators designed for operation in the 800 nm wavelength band) used in free-space QKD systems were characterised with respect to modulation depth. The measurements report for these modulators an overall extinction ratio >27 dB, and an overall insertion loss value of 5.4 dB. Furthermore, also a MEMS-based attenuator used in free-space QKD systems were characterised i.e. it was measured the effective attenuation against the nominal attenuation was performed. The attenuation showed the excellent linear behaviour, demonstrating the good quality of the device.

Pilot studies for the measurements of detection efficiency and source photon statistics for validating the calibration facilities in the VIS-NIR (for free-space QKD)

As a route to the validation of the measurement facilities, developed in the framework of this project, four European NMIs (INRIM, PTB, NPL and CMI) started two pilot studies on two key measurands in the VIS-NIR spectral region of interest for free-space QKD, i.e. the detection efficiency of single-photon detectors, and the Glauber second-order auto-correlation function of a single-photon source.

Specifically,

- the pilot study towards a comparison on the measurements of detection efficiency of SPADs in the VIS-NIR proposed in this project has attracted the interest of the radiometric community. This pilot study become part of the worldwide comparison on Si-SPAD single-photon detection efficiency carried on by the task-Group on Single-Photon Measurements inside the CCPR (CCPR WG-SP-TG11, CCPR-WG-SP-TG7). PTB, NPL and CMI have already carried out their measurements. INRIM suffered some technical problem during the measurement, and it will join this comparison after the end of the project.
- the pilot study towards a comparison on the measurements of the Glauber second order autocorrelation function achieved a good agreement within the uncertainty. The source used for this test was a pulsed single photon source based on silicon-vacancy in diamond emitting real single photons in the VIS-NIR. The Pilot study was carried on jointly in the INRIM labs. The results will be disseminated by presentations at conferences and meetings, and a paper has been already submitted.

New components for the metrology for free space QKD systems

- For increased security and performance of commercial free-space QKD systems, a new radiometric standard has been investigated and developed. Specifically, the feasibility of an induced-junction photodiode with predictable detection efficiency (developed in the iMERA+ qu-Candela) as an integrated primary standard for commercial QKD systems has been tested. This predictable photodiode delivers inherent SI traceability to customers without the need for external calibration. It should increase the security of commercial QKD systems against detector-control attacks such as, for example, detector-blinding of single-photon detectors. Furthermore, the performance of the QKD system can be validated at any time using the integrated primary standard when verifying the detection efficiency of the single photon detectors. To achieve this, the first stage is to verify the predictability of induced-junction photodiodes at near “single photon power level” (i.e., at about 1 Million photons per second) based on the results obtained in the IMERA+ qu-Candela. This has been done by determining the linearity of induced-junction photodiodes down to the “single photon power level”, thus extending the range of linear operation verified within the IMERA+ project qu-Candela by three orders of magnitude down to a power level of 0.3 pW. With this aim a low noise photocurrent amplifier for biased photodiodes, suitable for the measurement of photon fluxes of about 1 Million photons per second, was developed, and a traceable calibration of the amplifier gain was achieved. Reliable linearity measurements slightly above the noise level has been performed by using synchrotron radiation whose power can be varied over 11 orders of magnitude in a controlled way. Using this novel detector as a reference, the detection efficiency of the commercial free-space SPAD was determined, the results was in excellent agreement with the reference value within the measurement uncertainty.
- Efficient single-photon sources represent a breakthrough for quantum technologies in general, not only for QKD. In MIQC2 efficient free space single photon sources based on deterministic quantum dot-micro-lenses with a photon extraction efficiency of 41 % for a numerical aperture (NA) of 0.4 were realized. A photon extraction efficiency of > 50% is predicted for an NA = 0.9 (see S. Fischbach et al., ACS Photonics 4, 1327-1332 (2017)). To improve the performance of this sources the flip-chip process has been developed and flip-chip bonded quantum dot membrane structures were realized. Based on these structures, deterministic quantum dot – micro-mesas with an extraction efficiency of 18% into a numerical aperture (NA) of 0.4 and an predicted extraction efficiency > 60 % for an NA of 0.8 have been reported (S. Fischbach et al., Appl. Phys. Lett. 111, 011106 (2017)). Numerical simulations indicated that an anti-reflection coating will not improve the extraction efficiency because it will suppress a slight cavity effect in the structures which is used to achieve efficient photon extraction. Efficient fiber-coupled single photon sources based on deterministic quantum dot micro-lenses were also realized (see S. Schlehahn at al. Scientific Reports 8, 1340 (2018), arXiv1703.10536) but the predicted efficiency was not achieved. Moreover, the development of direct single-mode fiber-coupling using on-chip fiber-chucks in combination with high-NA microobjectives, which are realized by 3D two-photon laser writing into polymer, is presently being pursuit and will allow to further improve the extraction efficiency in the future.

Objective 3: Metrology for next generation (entanglement-based) QKD

Following Ekert’s seminal paper proposing a QKD protocol (E91) exploiting entanglement and Bell’s inequality, and subsequent proof-of-principle experiments, the role of entanglement in QKD has, for a long time, been mainly academic rather than practical. In recent years the hacking of standard (non-entanglement-based) QKD has made an impact in the scientific literature and popular press. All of these attacks are based on the gap

between the ideal of the security proofs of standard prepare and measure QKD protocols, such as BB84, assuming generally perfect sources and detectors, and the implementation of QKD with real devices. Imperfection in real sources and detectors can be exploited by eavesdropper to obtain information regarding the crypto-key distributed. Even if countermeasures have been identified for known quantum hacking attacks, a new paradigm for removing a priori the problem is highly desirable.

Recently, it has been demonstrated that it is possible to construct QKD protocols whose security can be proven without making any assumptions about the behaviour of the devices. In these new approaches, classified as Device-Independent (DI-) and Measurement-Device-Independent (MDI-) QKD, the key ingredient is the non-local correlations achievable by measuring entangled states. Therefore, entanglement is regaining a central role in practical QKD.

DI-QKD offers the strongest form of security since it requires minimal assumptions (such as detector calibration to overcome the detection loophole), but its practical implementation remains extremely challenging. However, since hacking attacks concentrate mainly on the detectors, the invention of MDI-QKD was a highly acclaimed solution. The first implementations of MDI-QKD were based on Bell-state analyser.

Security aside, a limiting factor for practical QKD systems is the channel capacity in the operation bandwidth of single photon detectors, which is reduced over long distances. One way to overcome this limit is by encoding multi-dimensional quantum information on a single photon. While photonic spatial modes of a paraxial beam have been widely used for this purpose, multiple spatial modes of multicore or multimode optical fibres could provide practical advantages for optical fibres over free space communication channels.

Aspects connected to these novel approach to QKD have been considered in MIQC2, and some interesting results have been achieved. Namely:

- MIQC2 developed metrics and measurement apparatus for rigorous quantification of entanglement for families of quantum states that are relevant in QKD protocols. Specifically, non-maximally (tuneable) entangled two-photons states in polarization have been prepared exploiting spontaneous parametric down-conversion These states represent the typical non-ideal output of a two-photon source. The states were first reconstructed by standard quantum state tomography. Then, the optimal estimators for entanglement quantifiers (e.g. concurrence and negativity) have been evaluated experimentally. The results are compared with the theoretical model. In addition, the “geometric discord” has been also estimated by an optimal measurement for the same family of states. Geometric discord is an approximation of the discord and measure a type of “quantumness” that does not coincide with entanglement in general. This experiment confirmed the validity of the theory, showing that optimal entanglement estimation is doable in a simple way for states which are relevant for QKD.
- A similar measurement apparatus for entanglement quantification of photon pairs emitted by the exciton-biexciton cascade of a quantum dot – microlens was successfully assembled and exploited. This apparatus has peculiar requirements due to the nature of the exciton-biexciton emission. In particular it required the use of fast superconducting nanowire single photon detectors (SNSPDs) with a temporal resolution of 70 ps. The obtained entanglement fidelities were approximately 84 % (corresponding negativity: ~40%) under pulsed excitation.
- MIQC2 developed also an asymmetric source of polarization-entangled photons, based on type-II down-conversion in a Sandwich-fold-configuration, with signal and idler photons at 894 nm and 1310 nm, respectively. The two-colour two-photon source was characterized in terms of fidelity to the target maximally entangled state. This kind of source can be useful for free-space QKD. In this sense, it is under test in Berlin connecting two building tens of km apart.
- In DI-QKD, security is based on the unconditional violation of Bell inequalities, namely to ensure that Alice and Bob share genuine quantum correlated states. One of the difficulties is due to the detection loophole: if the detection efficiency of correlated pairs is less than a certain threshold, the detected events may not represent a fair sample of the total ensemble, leading to an apparent larger correlation. MIQC2 consortium investigated the role of the detection efficiencies in the estimation of Bell inequalities violation. It turns out that unbalanced efficiencies can distort the values estimated in usual experimental situation, allowing violation of quantum bound as well as hiding the possible decoherence of the entangled state (supposed to be induced by Eve’s action). This work will also impact on other measurements where Bell inequality violations are used as a metric.
- The consortium investigated the possibility of exploiting the “weak measurement” paradigm to perform a “non-destructive” characterisation of a Bell’s inequality violation. A huge amount of work to investigate weak measurements and their applications has been carried on. This has been very profitable from general scientific point of view with possible fundamental return in quantum enhanced

metrology. The following publications report on the studies carried on in the MIQC2 framework [Phys. Rev. Lett. 116, 180401 (2016), Phys. Rev. Lett. 117, 170402 (2016); Nature Physics 13, 1191–1194 (2017)].

- The high-rate, fibre-based, single-photon detector device independent (DDI) QKD has been realized by a MIQC2 consortium member. In short, DDI-QKD is a simpler version of MDI-QKD based on only one photon instead of two. Secret key rates up to 104 Hz have been achieved for short distances (20 Km) and a maximum distance of about 90 km has been reached. The security analysis has been also completed (A3.2.5). For this setup the performance was limited by the relatively slow detectors and the rather high QBER due to the difficult alignment of the interferometer. A paper has been published [J. Appl. Phys. 120, 063101 (2016)].
- The consortium investigated the possibility of enlarging the Hilbert space (i.e. the alphabet) of in-fibre QKD by exploiting multi-spatial modes of single-photon propagation and the creation of states entangled in their spatial degrees of freedom. Indeed, using a SLM-based technique high-dimensional entanglement between two photons propagating in multi-core fibres was generated. The entanglement considered is in the spatial degree of freedom, given by the different cores of the fibres. The state have been characterised by performing quantum state tomography, and by evaluating a generalized concurrence (Phys Rev A 80, 022317 (2009)) for multi-dimensional bipartite state. A paper has been published: Sci Rep 7, 4302 (June 2017).

5 Impact

The project contributed to: 29 peer reviewed publications (20 open access); 125 conference presentations (93 talks [39 invited] and 32 posters); 6 conference paper publications; 2 early uptakes and 12 exploitable results. The Single Photon Workshop 2015 (SPW2015) was successfully organised at the University of Geneva (CH) in July 2015. There were around 200 attendees. The consortium contributed also to the organisation of the Single Photon Workshop 2017 (SPW2017) at University of Colorado in the USA (approximately 250 attendees). Furthermore, as a side event of SPW2017 the consortium organised a successful Lecture Course entitled “Single-photon metrology and its application to quantum technologies” dedicated mainly to PhD and early Postdoc Researchers (40 attendees). A partner of MIQC2 consortium was designated to host the following Single Photon Workshop 2019 (SPW2019, Italy, summer/fall 2019).

A parallel symposium on the topic of ‘Assurance and Certification for Quantum Communication Technologies’, co-organised by MIQC2 and the ETSI ISG-QKD, was held at QCrypt2017, Cambridge (UK), in September 2017.A Special Symposium on “Metrology for Quantum Communications” was held at the Quantum Technologies Conference of the SPIE Photonics Europe 2018 Meeting in Strasbourg (FR), in April 2018. 5 presentations were given (approximately 50 attendees).

Web-lectures have been realised and published on the MIQC2 website (http://empir.npl.co.uk/miqc2/), with periodical updates. These lectures cover the topics of single-photon sources and detectors, discrete-variable and measurement-device independent QKD, and an overview of the European metrology effort for quantum cryptography. A Webpage for ‘European single-photon metrology has been created (http://empir.npl.co.uk/quantumphotonics/). This gives the overall perspective on European metrology for single-photons and related technologies, e.g. quantum communications.

Impact on relevant standards

TREL, IDQ, INRIM, NPL, and PTB, in the context of the ETSI ISG-QKD, contributed to the drafting of pre-standards and standards concerned with characterisation, validation, and certification of the optical layer of QKD systems and networks (The Impact report details 18 engagements with the ETSI ISG-QKD). Two Standardisation Documents have been already published. The ETSI Group Specification document “ETSI QKD GS 011 – Component characterisation: characterising optical components for QKD systems”– was published by ETSI in May 2016. This document took about 2 years to compose, and the work on the initial drafts was supported by EMRP projects IND06-MIQC and EXL02-SIQUTE. This document is, to our knowledge, the first measurement (pre-) standard for a quantum 2.0 technology. Since it is focussed on the

characterisation of attenuated laser sources and gated single-photon detectors, it is also relevant to all quantum optical technologies utilising these devices.
The ETSI Group Report document “ETSI GR QKD 003 – Quantum Key Distribution (QKD); Components and Internal Interfaces” was published by ETSI in March 2018. Two other documents currently in draft receive support from this project, in particular:

-ETSI GS QKD 010: Implementation Security - Protection against Trojan horse attacks in one-way QKD systems (Rapporteur TREL)

- ETSI GS QKD 013: Characterisation of QKD transmitter modules (Rapporteur INRIM).

Impact on industrial and other user communities
In the project consortium there are two key European QKD manufacturers (IDQ and TREL), as well as single-photon detector manufacturers (MPD and IDQ), and having as collaborators (members of the stakeholder advisory board) an organisation working in the field of information security (CAENqS), and of single photon detector (PicoQuant). These ensured that the work was aligned with the industrial requirements during the lifetime of the project. For example, investigation of backflashes from single-photon detectors have been carried on in collaboration with TREL, and part of the investigation has been performed on detectors by IDQ, and prototypes provided by MPD in collaboration with PoliMi. Moreover, it should be noted that the published security analyses, derived inside this consortium to improve the protection of the QKD apparatus from quantum-hacking attacks, can lead to: (i) exploitation of the results by QKD manufacturers (impact on industry); and (ii) a required measurement standard and service for establishing whether the required optical isolation is achieved (impact on metrology).

Two project outputs have been exploited – an improved system by MPD for pigtailing their fibre-coupled single-photon detectors (based on tests performed with the set-up developed at INRIM to characterise fibre-couple single-photon detectors), and a new measurement service offered by METAS (based on their work to characterise various passive devices used as countermeasures).
In addition, six results on attack vulnerabilities and their countermeasures – on Trojan-horse attacks, back-flash, photon-source emission instabilities and three aspects of bright-pulse attacks – are expected to be exploited by QKD manufacturers to make their systems more secure, and may also lead to the need for measurements by certification laboratories to confirm the effectiveness of counter-measures.
Four prototypes developed in the context of this project (a lab-prototype of single-photon OTDR, a fast gated detector, a new secure front-end circuit for SPADS against quantum hacking and a stand-alone quantum dot based single-photon source) are considered as possible commercial interest.

Finally, two Best Practice Guides have been prepared to be open access: the *"Best practice guide on characterisation of counter-measures to side-channel and Trojan-horse attacks"*, and the *"Best Practice Guide on characterisation of components of free-space QKD systems".* These are downloadable for free from the MIQC2 website

Impact on the metrological and scientific communities

Eight members of the project are also members of the Consulting Committee on Photometry and Radiometry (CCPR), and have been working to incorporate photon-based quantities into its strategic planning. Furthermore, seven members of the project are members of the EURAMET Technical Committee for Photometry and Radiometry ensuring that CCPR and EURAMET are kept informed about the progress of the project and that CCPR & EURAMET roadmaps address the needs of the single-photon and QKD communities. It should be mentioned that this project triggered the establishment of the informal comparison on detection efficiency of single-photon detector in the VIS-NIR under the umbrella of the task group on “Single-Photon Radiometry” within the working group “Strategic Planning” of the Consultative Committee for Photometry and Radiometry. In a worldwide effort, 11 NMIs (6 are partners of this project), agreed on a technical protocol to carry out the informal comparison on the detection efficiency of Si-SPADs (coordinated by PTB, the comparison started in May 2016).

Moreover, a pilot study on measurement of detection efficiency in the photon counting regime at 1550 nm have been performed, together with two pilot-studies on the measurement of the $g^2(0)$-values (Glauber second order correlation function) for pulsed and CW light sources (emission at single-photon level) in the VIS and at telecom spectral region, respectively. Three papers reporting the results of these comparisons will be publicly available

on MIQC2 web portal and on the arXiv.org portal, and will be disseminated to CCPR, EURAMET TC PR (and their relevant working groups), ETSI and IEC meetings.

It is worth noting that the strategic analysis promoted between the European NMI partners of the consortium (INRIM, NPL, PTB, CMI, Aalto, Metrosert and METAS) returned a unanimous and synergetic vision about the creation of a European Metrology Virtual Institute for Quantum Photonics (lately renamed: European Metrological Network for Quantum Photonics). A structure able to coordinate the European metrological effort in the field of quantum photonic technologies, and to exploit in a cooperative and efficient way the resources available.

Beyond the project objectives, and in harmony with the EURAMET decision to develop internal structures called European Metrology Networks (EMN), the Consortium proposed the creation of the EMN for Quantum Technologies that broaden the scope beyond Quantum Photonics. EURAMET approved the proposal and the EMN for Quantum Technologies (EMN-Q) is under construction.

6 List of publications

1. O. Dietz, C. Müller, T. Kreißl, U. Herzog, T. Kroh, A. Ahlrichs, O. Benson, “A folded-sandwich polarisation-entangled two-color photon pair source with large tuning capability for applications in hybrid quantum systems”, Applied Physics B 122, 33, (2016). dx.doi.org/10.1007/s00340-015-6275-x

2. F. Piacentini, A. Avella, P. Traina, L. Lolli, E. Taralli, E. Monticone, M. Rajteri, D. Fukuda, I. P. Degiovanni, G. Brida “Towards joint reconstruction of noise and losses in quantum channels”, Quantum Meas. Quantum Metrol. 3, 27–31 (2016). https://doi.org/10.1515/qmetro-2016-0005

3. F. Piacentini, A. Avella, M. P. Levi, R. Lussana, F. Villa, A. Tosi, F. Zappa, M. Gramegna, G. Brida, I. P. Degiovanni, M. Genovese, “Experiment investigating the connection between weak values and contextuality”, Phys. Rev. Lett. 116, 180401 (2016). dx.doi.org/10.1103/PhysRevLett.116.180401

4. Avella, I. Ruo-Berchera, I. P. Degiovanni, G. Brida, M. Genovese, "Absolute calibration of an EMCCD camera by quantum correlation, linking photon counting to the analog regime", Optics Letters 41, 1841 (2016). dx.doi.org/10.1364/OL.41.001841

5. K. Tamaki, M. Curty, M. Lucamarini, “Decoy-state quantum key distribution with a leaky source”, New J. Phys. 18, 065008 (2016). dx.doi.org/10.1088/1367-2630/18/6/065008

6. Boaron, B. Korzh, R. Houlmann, G. Boso, C. C. Wen Lim, A. Mortin, H. Zbinden, “Detector-device-independent quantum key distribution: Security analysis and fast implementation”, J. Appl. Phys. 120, 063101 (2016). dx.doi.org/10.1063/1.4960093

7. V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, S. Sajeed, “Creation of backdoors in quantum communications via laser damage“, Phys. Rev. A 94, 030302(R) (2016). dx.doi.org /10.1515/qmetro-2016-0005

8. F. Piacentini, M. P. Levi, A. Avella, E. Cohen, R. Lussana, F. Villa, A. Tosi, F. Zappa, M. Gramegna, G. Brida, I. P. Degiovanni, M. Genovese, “Measuring incompatible observables by exploiting Sequential Weak Values“, Phys. Rev. Lett. 117, 170402 (2016). dx.doi.org/10.1103/PhysRevLett.117.170402

9. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, M. Genovese, “Quantifying the backflash radiation to prevent zero-error attacks in quantum key distribution”, Light: Science & Applications 6, e16261 (2017). dx.doi.org/10.1038/lsa.2016.261

10. T. Heindel, A. Thoma, M. von Helversen, M. Schmidt, A. Schlehahn, M. Gschrey, P. Schnauber, J.-H. Schulze, A. Strittmatter, J. Beyer, S. Rodt, A. Carmele, A. Knorr, and S. Reitzenstein,“A bright triggered twin-photon source in the solid state“, Nature Communications 8, 14870 (2017). dx.doi.org/10.1038/ncomms14870

11. S. Fischbach, A. Schlehahn, A. Thoma, N. Srocka, T. Gissibl, S. Ristok, S. Thiele, A. Kaganskiy, A. Strittmatter, T. Heindel, S. Rodt, A. Herkommer, H. Giessen, S. Reitzenstein, “Single Quantum Dot with Microlens and 3D-Printed Micro-objective as Integrated Bright Single-Photon Source“, ACS Photonics 4, 1327-1332 (2017). dx.doi.org/10.1021/acsphotonics.7b00253

12. Hee Jung Lee, Sang-Kyung Choi, Hee Su Park, "Experimental Demonstration of Four-Dimensional Photonic Spatial Entanglement between Multi-core Optical Fibres", Scientific Reports 7, 4302 (2017). doi:10.1038/s41598-017-04444-8

13. T Jakubczyk, V Delmonte, S Fischbach, D Wigger, D Reiter, Q Mermillod, P Schnauber, A Kaganskiy, J Schulze, A Strittmatter, S Rodt, W Langbein, T Kuhn, S Reitzenstein, J Kasprzak, “Impact of Phonons on Dephasing of Individual Excitons in Deterministic Quantum Dot Microlenses“, ACS Photonics 3, 2461–2466 (2016). dx.doi.org/10.1021/acsphotonics.6b00707

14. F. Piacentini, A. Avella, E. Rebufello, R. Lussana, F. Villa, A. Tosi, M. Gramegna, G. Brida, E. Cohen, L. Vaidman, I. P. Degiovanni, M. Genovese; "Determining the quantum expectation value by measuring a single photon“, Nature Physics (2017). https://doi.org/10.1038/nphys4223

15. *M. Klaas, E. Schlottmann, H. Flayac, F. P. Laussy, F. Gericke, M. Schmidt, M. v. Helversen, J. Beyer, S. Brodbeck, H. Suchomel, S. Höfling, S. Reitzenstein, and C. Schneider; "Photon-Number-Resolved Measurement of an Exciton-Polariton Condensate“, Physical Review Letters 121, 047401 (2018). https://doi.org/10.1103/PhysRevLett.121.047401*

16. *Schlehahn, S. Fischbach, R. Schmidt, A. Kaganskiy, A. Strittmatter, S. Rodt, T. Heindel and S. Reitzenstein; "A stand-alone fiber-coupled single-photon source“, Scientific Reports 8, 1340 (2018). https://doi.org/10.1038/s41598-017-19049-4*

17. F. Piacentini, A. Avella, M. Gramegna, R. Lussana, F. Villa, A. Tosi, G. Brida, I. P. Degiovanni, M. Genovese; "Investigating the Effects of the Interaction Intensity in a Weak Measurement", Scientific Reports 8, 6959 (2018). https://doi.org/10.1038/s41598-018-25156-7

18. J. Forneris, D. Gatto Monticone, P. Traina, V. Grilj, G. Brida, G. Amato, L. Boarino, E. Enrico, I. P. Degiovanni, E. Moreva, N. Skukan, M. Jakšić, M. Genovese, P. Olivero; "Electrical stimulation of non-classical emission diamond color centers by means of sub-superficial graphitic electrodes", Scientific Reports 5, 15901 (2015). https://doi.org/10.1038/srep15901

19. B. Rodiek, M. López, H. Hofer, S. Kück; "The absolutely characterised nitrogen vacancy center-based single-photon source – measurement uncertainty of photon flux and angular emission properties", J. Phys.: Conf. Ser. 972, 012008 (2018). DOI: 10.1088/1742-6596/972/1/012008

20. M. Genovese; "A few reflections on protective measurements and more“, Journal of Physics: Conference Series 880 (1), 012012 (2017); DOI: 10.1088/1742-6596/880/1/012012

7 Website address and contact details

Project website address: http://empir.npl.co.uk/miqc2/

Project Coordinator: Ivo Pietro Degiovanni

INRIM, Strada delle cacce 91,10135 Torino, Italy

Tel: +39 011 3919245

E-mail: i.degiovanni@inrim.it

Impact Coordinator: Christopher Chunnilall

NPL, Hampton Road, Teddington, Middlesex, TW11 0LW, United Kingdom

Tel: +44 020 8943 6872

E-mail: christopher.chunnilall@npl.co.uk