Annex I – JRP protocol

Version Date: 13 May 2015

14IND05 MIQC2

Optical metrology for quantum-enhanced secure telecommunication

Start date: 01 June 2015

Duration: 36 months

Coordinator
Ivo Pietro Degiovanni
INRIM

Glossary

CCPR	consultative committee for photometry and radiometry
DE	detection efficiency
DEM	detection efficiency mismatch
DDI-QKD	detector device independent QKD
DI-QKD	device independent QKD
InGaAs	indium gallium arsenide
ISG	industry specification group
ICT	information and communication technology
SI	international system of units
MDI-QKD	measurement device independent QKD
NMI	National Metrology Institute
NIR	near-infrared
QD	quantum dot
QKD	quantum key distribution
QRNG	quantum random number generator
R&D	research and development
Si	Silicon
SPAD	single photon avalanche diodes
SPS	single photon source
SME	small and medium-sized enterprises
SNSPD	superconducting nanowire single photon detector
VIS	visible

Contents

Section A: Key Data

A1 SUMMARY DATA

Coordinator contact details:

Coordinator	Ivo Pietro Degiovanni
Address	INRIM, Strada delle cacce 91,10135 Torino, Italy
Phone:	+390113919250
Email:	i.degiovanni@inrim.it

Participant details:

a. Partners (participants who will accede to the Grant Agreement)

no.	Participant Type	Short Name	Organisation legal full name	Country
1	Internal Funded Partner	INRIM	Istituto Nazionale di Ricerca Metrologica	Italy
2	Internal Funded Partner	Aalto	Aalto-korkeakoulusäätiö	Finland
3	Internal Funded Partner	CMI	Cesky Metrologicky Institut Brno	Czech Republic
4	Internal Funded Partner	Metrosert	AS Metrosert	Estonia
5	Internal Funded Partner	NPL	NPL Management Limited	United Kingdom
6	Internal Funded Partner	PTB	Physikalisch-Technische Bundesanstalt	Germany
7	External Funded Partner	PoliMi	Politecnico di Milano	Italy
8	External Funded Partner	Toshiba	Toshiba Research Europe Limited	United Kingdom
9	External Funded Partner	TUB	Technische Universität Berlin	Germany
10	External Funded Partner	UBER	Humboldt-Universität zu Berlin	Germany
11	Unfunded Partner	IDQ	ID Quantique SA	Switzerland
12	Unfunded Partner	KRISS	Korea Research Institute of Standards and Science	Republic of Korea
13	Unfunded Partner	METAS	Eidgenössisches Institut für Metrologie METAS	Switzerland
14	Unfunded Partner	MPD	Micro Photon Devices S.R.L.	Italy
15	Unfunded Partner	UniGE CH	University of Geneva	Switzerland

Financial summary:

	Internal Funded Partners	External Funded Partners	Unfunded Partners	Total
Labour (€)	960 789.00	307 600.00	351 700.00	1 620 089.00
Subcontracting (€)				
T&S (€)	47 871.00	21 670.00	23 000.00	92 541.00
Equipment (€)				
Other Goods and Services (€)	57 859.00	41 000.00	30 000.00	128 859.00
Large Research Infrastructure (€)				
Indirect (€)	53 325.95	92 567.50	101 175.00	247 068.45
Total eligible costs (€)	1 119 844.95	462 837.50	505 875.00	2 088 557.45
Total eligible costs as % of Total	54 %	22 %	24 %	
EU Contribution (€)	**1 119 844.95**	**462 837.50**		**1 582 682.45**
EU Contribution as % of Total	71 %	29 %	0 %	
Months	172.7	81.5	57.5	311.7

A2 WORK PACKAGES SUMMARY

WP No	Work Package Title	Active Partners (WP leader in bold)	Months
WP1	Counter-measures and novel optical components for commercial fibre-based QKD	**CMI**, INRIM, Aalto, Metrosert, NPL, PTB, PoliMi, Toshiba, IDQ, METAS, MPD, UniGE CH	128.4
WP2	Metrology for commercial components for free-space QKD	**PTB**, INRIM, Aalto, CMI, Metrosert, NPL, PoliMi, TUB, MPD	79.4
WP3	Metrology for next generation (entanglement-based) QKD	**INRIM**, NPL, TUB,UBER, KRISS, UniGE CH	61.2
WP4	Creating Impact	**NPL**, all partners	28.3
WP5	Management and Coordination	**INRIM**, all partners	14.5
		Total months	311.7

Section B: Overview of the Research

B1 SCIENTIFIC AND/OR TECHNICAL EXCELLENCE

B1.a Summary of the project

Overview

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 [1-3].

Need

Fibre and free-space QKD systems use real devices, which do not have the ideal characteristics envisaged by the initial QKD concept. This means that those practical systems can be vulnerable to one or more of the many quantum hacking attacks proposed and/or demonstrated [4-20]. Counter-measures against these attacks have already been identified, but their effectiveness should be ensured by rigorous characterisation of the optical components – this will be addressed by the consortium.

Another approach against these attacks is represented by entanglement-based QKD techniques e.g. device-independent (DI) QKD, measurement-device-independent (MDI) QKD, etc. The development of entanglement characterisation and quantification techniques is essential in order to provide the metrological framework for next-generation (entanglement-based) QKD systems.

Addressing these challenges requires collaboration with industrial QKD providers, network providers and standardisation bodies, and will build upon the results of EMRP JRP IND06 MIQC [21] (which addressed some of the metrology requirements of fibre-based QKD operating in an attack-free environment, in particular related to the calibration of source and detectors) and IMERA-Plus JRP qu-Candela [22] (which set up the infrastructure to provide the traceability for measurements at single-photon level to the primary radiometric standards operating at the “macroscopic” light level in the visible).

Objectives

The aim of this project is to accelerate the development and commercial success of QKD technologies. This presents a number of metrological challenges, which result from the current and predicted development and deployment trajectories of QKD technologies.

Following the considerations above, the key 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 dedicated calibration techniques for new high-speed single-photon detectors for fibre-based QKD
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 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

Progress beyond the state of the art

The current state-of-the-art for QKD industry uses fibre communications (typically providing hundred-kilometre point-to-point QKD links). The development of a worldwide network can be achieved only through ground-air (ground-satellite) communication and this will be the next stage for QKD R&D efforts.

Proper standardisation of QKD assisted with calibration of the relative optical components is the best option towards market success. The process of realising a proper European metrological infrastructure for QKD optical components has been already started in the EMRP project IND06 MIQC where techniques to characterise specific optical components of fibre-based QKD systems were developed, despite the fact that an effective comparison between different NMIs on this measurement techniques was not performed. In the context of this project two pilot-comparisons will be carried out inside this project. Furthermore, new characterisation techniques for optical components in fibre-based QKD systems not considered in EMRP project IND06 MIQC (such as those used for counter-measures against hacking techniques based on "side-channel" attacks) will be developed.

This project will also develop measurement techniques required for calibrating the specific optical components and devices for free-space QKD systems that (even if built on the traceability of measurements in the visible at single-photon level developed in the context of IMERA-Plus JRP qu-Candela) will be beyond the current state-of-the-art. Also, the development of suitable techniques for entanglement quantification relevant to the needs of QKD go beyond the state of the art, and it will benefit from research activities carried out in this field by the quantum optical community.

Results

Objective 1

The main expected results connected to Objective 1 are the validation of the measurement techniques developed for optical components operating at single photon level at telecom wavelength by the success of the measurements comparison; and a better understanding of the effectiveness of the countermeasures developed against side-channel hacking attacks by the development of suitable characterisation techniques.

Objective 2

The main expected result connected to Objective 2 is the development of a dedicated technique for performing a reliable measurement of the quantum efficiency of the novel high-speed single-photon detector for QKD.

Objective 3

Two main expected results are connected to Objective 2. The first one is the development of a measurement infrastructure based on different measurement techniques and traceability chains able to characterise QKD components, such as single-photon sources and detectors for free-space QKD (i.e. in the VIS-NIR). The second one is the validation of the measurement techniques developed by the success of the measurements comparison in the VIS-NIR.

Objective 4

The main expected result connected to Objective 4 is the development of methods for quantifying entanglement; for characterising entanglement-based QKD systems, such as, e.g., different practical implementations of the Device-Independent-QKD paradigm.

Objective 5

The main expected results of objective 5 is the dissemination to industry and users of the efficient measurement techniques for characterisation the optical components of a QKD system by means of the two Good Practice Guides that will be written**.**

Impact

In addition, the project will organise workshops and/or conferences, present the project's results at conferences and in high-impact-factor scientific journals. Knowledge will also be disseminated by developing training courses and an advisory board consisting also of industry stakeholders will regularly meet to exchange information with the consortium and ensure that the project is delivering relevant results.

Furthermore, the NMI partners into this project will investigate on the possibility of creating a "Joint Virtual European Metrology Centre for Quantum Photonics".

Impact on relevant standards

Toshiba, INRIM, NPL, and PTB, in the context of the ETSI ISG-QKD, will contribute to the drafting of pre-standards and standards concerned with characterisation, validation, and certification of the optical layer of QKD systems and networks. The list of the actual projected documents is in Table B.1 of section B2.b

Impact on industrial and other user communities

In the project consortium there are two key European QKD manufacturers (IDQ, and Toshiba), as well as single-photon detector manufacturers (MPD and IDQ), and having as collaborators (members of the stakeholder advisory board) a standardisation body (ETSI), two satellite-related companies (AIRBUS, SES), and several organisations working in the field of information security and quantum technology (THALES, NICT, CAENqS) ensures that the work is aligned with and will impact on industrial requirements during the lifetime of the project. In addition, it ensures that practical (i.e. cost-effective and efficient) measurements are developed and disseminated through two Best-Practice measurement guides.

Impact on the metrological and scientific communities

In addition of the possible creation of "Joint Virtual European Metrology Centre for Quantum Photonics", eight members of the Consortium are 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 Consortium 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.

B1.b Overview of the scientific and technical objectives

The objectives of this project are:

1. **To develop and validate measurement techniques for characterising and validating counter-measures to side-channel and Trojan-horse attacks (WP1).**

   The development of the above techniques 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) will be performed in collaboration with "quantum" companies and standardisation bodies, e.g. the Industry Specification Group on QKD of the European Telecommunications Standards Institute (ETSI ISG-QKD) [23]. The validation of the measurement techniques will be achieved by carrying out two pilot comparisons between INRIM, PTB, CMI and NPL. These pilot comparisons will measure relevant measurands, i.e. the quantum efficiency of single-photon detectors and the second-order Glauber auto-correlation function of pseudo single-photon sources at telecom wavelength, that will ensure the traceability of all the other measurements carried on for achieving this objective. (WP1)

2. **To develop a dedicated calibration technique for new type of single-photon detectors for fibre-based QKD, with target uncertainty of 2 % (WP1).**

   The development of a dedicated technique for calibrating (i.e. measuring the quantum efficiency) the novel "high-speed" single-photon detectors for fibre-based QKD it is necessary since these kind of detectors appears to be the most viable solution to increase the key-rate production (one of the critical point of the actual commercial QKD systems). These new detectors are different from the ones considered in **EMRP IND06 MIQC** (InGaAs SPADs operating in Geiger mode, SNSPDs), they are based on InGaAs SPADs operated with fast-gating (e.g. sine-gating) (WP1)

3. **To develop and validate measurement techniques for characterising components of free-space QKD systems (e.g. ground-air communication) (WP2).**

   This will require the development, or improvement, of calibration methods for single-photon sources, detectors, and other relevant optical components such as polarisation encoders and attenuators (but also quantum random number generators) at the wavelengths used in free-space light communications which typically lie in the 400 nm – 950 nm VIS-NIR spectral region. The validation of the measurement techniques developed will be achieved by carrying out two pilot comparisons between INRIM, PTB, CMI and NPL. The two pilot comparisons will be devoted to the measurement of the quantum efficiency of single-photon detectors and on the measurement of the second-order Glauber auto-correlation function on pseudo-single-photon-source in the VIS-NIR (i.e. for free-space QKD). (WP2)

4. **To develop measurement techniques for characterising entanglement and/or "quantumness" of quantum states (WP3).**

   The establishment of the foundations of the metrology is required for next-generation QKD systems based on the entanglement of photons. The development of measurement techniques for characterising quantum states, i.e. witnessing and quantifying the amount of entanglement and/or quantumness, is essential to foster the real-world deployment of these technologies (WP3).

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 (WP4).**

   Best-Practice Guides will disseminate efficient measurement techniques needed by industry and users (WP1 and WP2).

6. **Contribute to impact - via contributions to international guidelines/standards and showcase examples of early uptake by end users (WP4)**.

   The contribution to impact through inputs to international guidelines and standards with a specific focus on the following standards organizations and committees.

   - ETSI ISG-QKD – drafting of Group Specification documents (pre-standards) and standards, in particular on the characterisation of optical components in QKD systems, and on verification through measurement of Countermeasures against Trojan-Horse and Side-Channel attacks;
   - CCPR – pilot comparison of single photon detector detection-efficiency measurement and active contribution by the members of the consortium to the creation of a Task-Group on Single-Photon Measurements inside the CCPR;
   - CCPR and EURAMET – ensuring that metrology roadmaps reflect the requirements of the QKD community

The project's outcomes will provide assurance to end users of the conformance to standards of QKD components, thereby promoting market uptake of the technology and ultimately revolutionising data security in ICT. This will set the foundations for a robust quantum industry in Europe that will provide a step change in the telecoms industry and future secure data management that will impact on us all.

Furthermore, in the context of the project, we will continue the investigation into the possibility of establishing the "**Joint Virtual European Metrology Centre for Quantum Photonics**" between the NMIs partners of the project. The idea behind the formation of such a centre is that the national budgets for establishing a new metrological field such as quantum photonics will be not sufficient to cope with the metrological challenges, and therefore a joint, coordinated, effort is necessary. This investigation will include gathering evidence in support of this approach, agreement between all partners to form such a centre, establishing objectives, and identifying the formal steps necessary to establish such a centre by finalising a co-operation and collaboration agreement between the members of the centre.

B1.c List of deliverables

Relevant objective	Deliverable number	Deliverable description	Deliverable type	Partners (Lead in bold)	Delivery date
1	D1	Validated measurement techniques for characterising counter-measures to side-channel and Trojan-horse attacks	Validation document	**CMI**, INRIM, Aalto, Metrosert, NPL, PTB, PoliMi, Toshiba, IDQ, METAS, MPD, UniGE CH	May 2018 (M36)
2	D2	Validated measurement technique for calibrating new type of single-photon detectors for fibre-based QKD, with target uncertainty of 2 %	Validation document	**INRIM,** PoliMi, UniGE CH, NPL, PTB, CMI	May 2018 (M36)

3	D3	Validated measurement techniques for characterising components of free-space QKD systems	Validation document	**PTB**, INRIM, Aalto, CMI, Metrosert, NPL, PoliMi, TUB, MPD	May 2018 (M36)
4	D4	Report showing the measurement techniques that characterise quantum states	Report	**INRIM**, NPL, TUB, UBER, KRISS	February 2018 (M33)
5	D5	Two Best Practice Guides, one on characterisation of counter-measures to side-channel and Trojan-horse attacks (WP1), and one on characterisation of components of free-space QKD systems (WP2)	Best Practice Guides	**PTB**, CMI, INRIM, Aalto, Metrosert, NPL, PoliMi, Toshiba, TUB, IDQ, KRISS, METAS, MPD, UBER and UniGE CH	May 2018 (M36)
6	D6	Evidence of contributions to an improved draft standard ETSI ISG-QKD and recommendations for an update to CCPR. Examples of early uptake of project outputs by instrumentation manufacturers and/or end-users.	Reporting documents	**NPL**, all partners	May 2018 (M36)
N/A	D7	Delivery of all technical and financial reporting documents as required by EURAMET	Reporting documents	**INRIM**, all partners	May 2018 (M36) +60 days

B1.d Need for the project

“Information in many ways equates to geopolitical, social, and economic power. The economic, social, and political well-being of developed countries depends on integrity, confidentiality, and authenticity of sensitive data sent over networks. Corporations and governments have legal responsibilities to their investors, constituents, and customers to preserve the confidentiality of sensitive information. Whether this information consists of military communications, secret government documents, industrial trade secrets, or financial and medical records, interception of information allows adversaries to not only learn about the contents of these communications, but also to discover metadata in patterns within a network of communicators, to extract general patterns using machine learning, and even to insert false or misleading information or malware into a data stream.” [3].

ICT forms a world-wide market of 2600 billion of Euro [24]. There are currently 9 billion public key and 19 billion symmetric key deployments annually, and their combined total is expected to hit 50 billion by 2020 as we move towards ‘the internet of things/everything’ by 2020 [25].

The impact of quantum computing on current algorithmic encryption techniques is a concern that has led to ETSI organising two meetings within the last 13 months to discuss the standardisation and deployment of the next-generation cryptographic infrastructure, in particular, one that will be secure against emerging quantum computing technologies [26].

QKD is currently the only guaranteed option for future-proofing our data against such advances in computing. Although post-quantum encryption algorithms are believed to be resistant to quantum computation that belief is not guaranteed by information theory and the laws of physics, as is the security of QKD. This has led to current work to develop QKD networks in the USA, China, and South Korea (see Section B1.e), and networks in other countries/continents are expected to follow. Nonetheless, implementing QKD depends on real devices, which have imperfections, and counter-measures are required to maintain the security of QKD systems.

The schematic in Fig. B.1 represents the stakeholders of QKD. This project aims to build on the existing metrological framework, established by 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 will help QKD manufacturers and component manufacturers to develop reliable and characterised components which will lead to reliable and trusted QKD systems. This is turn will provide 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 will meet these measurement challenges as well as engaging with bodies such as ETSI to draft paper standards to provide assurance to end users.

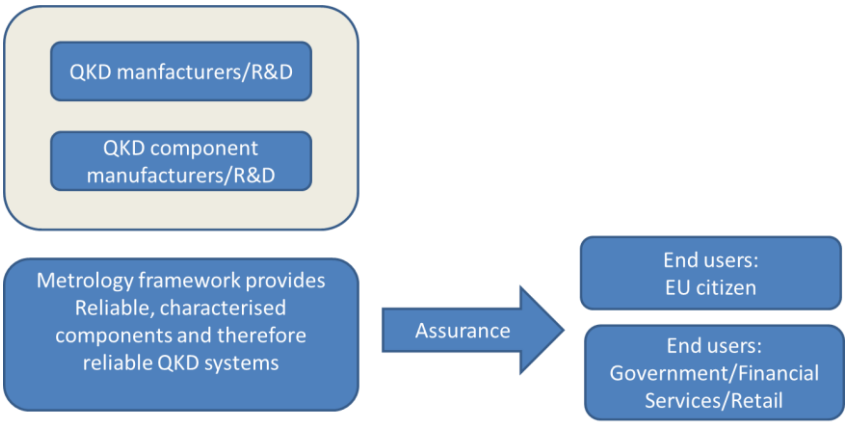


Fig. B.1

The need for QKD and supporting metrology to provide trust is aptly described in the report entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", recently published jointly by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy [27].

The section "Fostering R&D investments and innovation" states that "R&D can support a strong industrial policy, promote a **trustworthy** European ICT industry, boost the internal market and reduce European dependence on foreign technologies. R&D should fill the technology gaps in ICT security, prepare for the next generation of security challenges... " European industry has a prominent position in quantum technologies in general, and in QKD in particular. QKD, with its strong long-term security provision is an important building block for dependably secure communication networks.

The document also states that "The EU should make the best of the Horizon 2020 Framework Programme for Research and Innovation… Horizon 2020 will support security research related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address inter-operability among network and information systems." QKD perfectly fits this description, since it is able to create a secure end-to-end communication link, although inter-operability issues need to be addressed. Widespread adoption of QKD requires that systems are trusted by its users, which is usually achieved in a complex assurance process including security specification, evaluation and certification according to a standardised methodology, as well as inter-operability of QKD systems from different manufacturers and with existing networks [28]. **A specific requirement for the security certification of QKD systems is a standardised set of properties of optical components that should be traceably calibrated according to specified standards.**

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.

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 [29]. 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 will be needed 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 [30,31], but a **metrological infrastructure able to provide appropriate characterisation of optical components for free-space QKD is still lacking**.

Entanglement, as in entangled states or entangling measurements, has a central role in a new generation of QKD technologies. This ranges from the realisation of quantum repeaters [32] and the development of quantum networks, to the practical application of (measurement-) device-independent QKD [33-35]. **A measurement infrastructure needs to be developed to address these technologies.**

B1.e Progress beyond the state of the art

QKD is today no longer confined to laboratories. QKD networks have been realised in metropolitan area in all five continents, e.g. in Vienna Austria (SECOQC) [36], in Tokyo (Japan) (UQCC) [37], in Switzerland [38], in USA [39], in China [40]. Of particular note is the current 560 M RMB project by China to build a 2000 km fibre QKD network from Shangahi to Beijing, supplemented by ground-satellite QKD to reach more distance parts of China such as Ulumuqi [41].

QKD was used to secure elections in Geneva, Switzerland [42], and for public security during the 2010 World Cup [43], for government communications [44], etc. The viability for QKD to operate in existing telecom fibre networks has also been demonstrated [45] and a point-to-multipoint QKD link has recently been demonstrated [46].

Commercial products or industrial prototypes for point-to-point QKD are available from SMEs and large companies, e.g. ID Quantique SA (Suisse), SeQureNet (France), Toshiba Research Europe (UK), Selex Finmeccanica (Italy), QuintessenceLabs (Australia). Several other companies have active research programmes on QKD or are members of the ETSI ISG-QKD, including Thales, Qinetiq plc, Swisscom SA, Telefonica SA, SK Telecom, Applied Communication Sciences, Arche Finanz GmbH, Hewlett-Packard, Mitsubishi Electric RCE, etc

Despite this strong industrial interest in QKD, proven also by recent commercial agreements [47] and strong expected market development showed in several studies [48], the standardisation process of QKD systems is just at the initial phase, as is the development of a measurement framework for the characterisation of the physical (optical) components inside the QKD system. Specific activities related, in particular, to the characterisation of sources and detectors for fibre-based QKD has been already carried on in the context of EMRP IND06 MIQC project, but these do not address the issues that are evolving such as the new components, new materials that will make entangled based QKD more viable; new research into side channel attacks.

The following subsection describes the state of art of metrology for QKD and the next one how this project goes beyond state of the art.

State of the art

The EMRP JRP IND06 MIQC has developed the techniques to characterise specific optical components of fibre-based QKD systems, e.g. pseudo-single-photon sources based on attenuated lasers, and commercial single photon detectors based on avalanche photodiodes operating in Geiger mode

The metrological techniques to characterise the components for free-space QKD systems are yet to be developed. The results of the IMERA-Plus JRP qu-Candela can be used to provide traceability to the photon-counting regime at wavelengths in the visible spectral range. However, the measurement techniques required for calibrating the specific optical components and devices of free-space QKD systems will be, in most of the cases, beyond the current state-of-the-art.

Accurate characterisation of entangled states, development of measurement techniques for entanglement quantification and/or witnessing, and for estimating the entangling-process efficiency are new requirements in metrology, and essentially no specific work has been performed in that direction.

One industrial partner (Toshiba) and three NMIs (INRIM, NPL, PTB) are members of the ETSI ISG-QKD, the chair of which is currently held by Toshiba. This ISG has so far published 5 Group Specification documents. One of the current documents in draft “DGS/QKD-011 Component characterisation: characterising optical components for QKD systems” directly benefits from the results of EMRP IND06 MIQC.

Beyond the state of the art

Despite the fact that the EMRP JRP IND06 MIQC has developed the techniques to characterise specific optical components of fibre-based QKD systems, an effective comparison between different NMIs has not yet performed. Two pilot-comparisons will be carried out inside this project.

Optical components such as those used for counter-measures against hacking attacks to fibre-based QKD system will need traceable calibration techniques. As novel and attack-specific measurements have to be investigated, it is obvious that these activities go beyond the state-of-the-art.

Furthermore new detector technology for fibre-based QKD may require new calibration techniques, together with devices to enable networking and higher data rates. Also this activity will be carried on.

The metrological techniques to characterise the components for QKD are yet to be developed.

The results of the IMERA-Plus JRP qu-Candela can be used to provide traceability to the photon-counting regime at wavelengths useful for free-space QKD systems (visible). In this project we will develop measurement techniques required for calibrating the specific optical components and devices of free-space QKD systems that will be beyond the current state-of-the-art.

The development of suitable techniques of characterisation of entangled states, of entanglement quantification and/or witnessing, and of estimation the entangling-process efficiency relevant to the needs of QKD will benefit from extensive research by the quantum optical community, where several interesting results have been already demonstrated. But the development of these techniques represents completely new tasks for metrology, and it will be carried out within this project.

Toshiba, INRIM, NPL, and PTB, in the context of the ETSI ISG-QKD, will provide metrology leadership for the drafting of pre-standards and standards concerned with characterisation, validation, and certification of the optical layer of QKD systems and networks. The current ETSI programme of drafting a series of Group Specification documents concerned with implementation security against hacking attacks will directly benefit from input from this project, as well as specifications concerned with characterisation of assembled modules, and updates of existing documents. Measurements need to be specified and implemented in an efficient and cost-effective way so that industry and end-users can access them at an affordable cost.

B2 POTENTIAL OUTPUTS AND IMPACT FROM THE PROJECT RESULTS

B2.a Projected impact of the project

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

Several European SMEs have based their business models on QKD. In addition a number of industrial players have already heavily invested in QKD R&D as part of projects under the umbrella of the EC Framework Programmes 6 and 7, and it is expected that this trend will increase in the context of Horizon 2020. This makes it clear that there is increasing need for standardisation for QKD, since there is now a critical mass of interested parties in Europe.

The outputs from this project will:

- contribute to the necessary metrological foundations for the standardisation of QKD through trusted bodies such as NMIs, that has already started in the context of EMRP JRP IND06 MIQC;
- provide assurance to end users of the conformance to standards of QKD components;
- provide assurance to end users that the QKD components have been tested in hostile conditions and that countermeasures are in place against side-channel attacks;
- promote market uptake of the technology.

Successful deployment of QKD will also kick start the quantum industry and ultimately revolutionise data security in ICT – there are already related areas of research which are being pursued by academia to take QKD to the next phase and towards global communication – such as device-independent (entanglement-based) QKD and free-space QKD.

The presence in the consortium of the two key European QKD manufacturers, namely IDQ and Toshiba, as well as single-photon detector manufacturers (MPD and IDQ), and having as collaborators (and members of the stakeholder advisory board) a standardisation body (ETSI), two satellite-related companies (AIRBUS, SES), and several organisations working in the field of information security and quantum technology (THALES, NICT, CAENqS) ensures that the work is aligned with, and impacts on, industrial requirements. Each individual NMI will contribute to the project, developing specific skills on the basis of their background, leading to the realisation of a European NMI network able to provide a full QKD measurement infrastructure. The possibility that this infrastructure will lead to the "**Joint Virtual European Metrology Centre for Quantum Photonics**" will be investigated.

The wider indirect impact of the project can be assessed in three areas as follows:

Social impact

Modern information and communication technologies permeate more and more various social aspects of our lives. Governments are increasingly converting data into digital format such as medical records and there have been some instances where digital storage media have been lost or stolen. The secure transmission of information and the protection of privacy of individuals gain more and more importance for the data traffic at public institutions and for strengthening and maintaining the competitiveness of the European economy, as it is clearly stated in the already mentioned document published jointly by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". This document show that quantum cryptography is increasingly seen by politics and economics as one way, and maybe finally the only way, to obtain secure data transmission in real life. QKD systems are considered as potential key technologies to protect the right to privacy in the processing of personal data, and single-photon sources, and **the metrology infrastructure developed in this project will have a key role in the quality assurance of this technology**.

Furthermore, large companies and government have security officers who monitor the technologies employed, to ensure the security of their communications networks. These companies and government know that there are sometimes security weaknesses in QKD implementation, and that counter measures can be used to supress these weaknesses. **If NMIs can validate the countermeasures it will be of great value to commerce and government**.

Financial impact

QKD technology remains largely in the first stage of commercialization, with the technology being offered primarily to government, military, and research institutes. The QKD market is nevertheless forecast to expand in the coming years, based on the availability of certified and standardised products, and technology advancements that help extend its application beyond point-to-point connections to cover global communications. Continuous and incremental technology innovation in fibre, protocols and free-space, is expected to result in the decline in the price of the equipment and related accessories in the coming years. Global market for QKD is projected to reach $1.0 billion by 2018, driven by the need to secure the transmission of sensitive communications [48].

Standardisation is one of the key elements for the success of this initiative: a European lead in developing globally accepted standards and an anticipatory approach would facilitate the growth of these markets, both in Europe and abroad. The ETSI ISG-QKD aims to drive this **standardisation process, which needs, as a critical key element, dedicated traceable measurement techniques for the quantum optical components of QKD systems**. A first step in this direction was performed by the project EMRP IND06 MIQC, and this project aims to continue the effort in this direction.

B2.b Projected intermediate impact on relevant standards

With the expertise and resources from the consortium, this project will respond to the needs addressed in European directives:

The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal of the European Communities, 31.7.2002, L 201/37*. Here, the Commission specifically emphasises security in the Information Technology and Communications (ICT) in Article 4 ("Security"): "*The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard the security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented*."

In Europe, the Industry Specification Group of the European Telecommunications Standards Institute (ETSI ISG-QKD) is the only known standardisation initiative for QKD systems [28,49]. It is recognised that one of the building blocks necessary to achieve QKD systems standardisation is that of traceable measurements at the single-photon level. For this reason, in the ISG-QKD there are three NMIs participating in this project: INRIM (since the inception of the ETSI ISG-QKD), NPL (since 2010), PTB (since 2011).

ETSI itself supports this project by participating as a Toshiba is also a member, and the current chairman of the ETSI ISG-QKD. As a consequence, the work of this project will directly influence the current and future

versions of the (pre-) standard ETSI Group Specifications listed in Table B.1, as well as additional pre-standards and standards that may follow these documents.

A specific requirement for the security certification of QKD systems is a standardised set of properties of optical components that should be traceably calibrated according to specified standards. The proposed work will provide assurance to end users of the conformance to standards of QKD components, thereby promoting market uptake of the technology and ultimately revolutionising data security in ICT.

Intermediate impact will be realised during and at the end of the project by inputs to international guidelines and standards with a specific focus on the following standard-organizations and committees (WP4):

Table B.1

Standards Committee / Technical Committee / Working Group	**Partners involved**	**Likely area of impact / activities undertaken by partners related to standard / committee**
ETSI-ISG-QKD	INRIM, NPL, PTB, Toshiba	Information will be provided to the updated or revised Group Specification document GS QKD 003: Quantum Key Distribution (QKD); Components and Internal Interfaces
ETSI-ISG-QKD	INRIM, NPL, PTB, Toshiba	Information will be provided for the development of the final, updated or revised drafted Group Specification document DGS/QKD-0011_OptCompChar: Quantum Key Distribution (QKD) Component characterisation: characterising optical components for QKD systems (Rapporteur: NPL)
ETSI-ISG-QKD	INRIM, NPL, PTB, Toshiba	Information will be provided for the development of the final, updated or revised drafted Group Specification document DGS/QKD-0010_ISTrojan: Quantum Key Distribution (QKD) Implementation security: protection against Trojan horse attacks in one-way QKD systems (Rapporteur: Toshiba)
Task-Group on Single-Photon Measurements inside the CCPR (CCPR-WG-SP-TG11, CCPR-WG-SP-TG7)	CMI, INRIM, NPL, PTB	Partners will provide input with a specific focus on detection-efficiency measurement of single-photon detectors

B2.c Projected intermediate impact on industrial and other user communities

The presence in the consortium of the two key European QKD manufacturers, namely IDQ, and Toshiba, as well as single-photon detector manufacturers (MPD and IDQ), and having as collaborators (and members of the stakeholder advisory board) a standardisation body (ETSI), two satellite-related companies (AIRBUS, SES) and several organisations working in the field of information security and quantum technology (THALES, NICT, CAENqS) ensures that the work is aligned with and will impact on industrial requirements during the lifetime of the project. In addition, it ensures that practical (i.e. cost-effective and efficient) measurements are developed.

The intermediate impact can be summarised as follows:

- The development of counter-measures and expanded security proofs which enhance the implementation security of QKD systems;
- Methods for characterising new types of single-photon detector;
- Best-practice disseminated to industrial and user community.

The specific outputs that will have intermediate impact are listed below. They are influenced by the outputs of WP1, since this work package is focussed on current commercial QKD systems.

- the development of counter-measures against side-channel and Trojan-horse attacks on fibre QKD systems (WP1);
- expanded security proofs which better encompass real device characteristics (WP1);
- an artefact for embedding traceability to the SI within QKD modules (WP1) ;
- a measurement from WP1 being demonstrated on a commercial device to show the practicality of the techniques developed (WP4);
- methods to characterise free-space QKD components (WP2);
- dissemination of the results of comparisons of core measurements in the visible and telecom regimes (WP4);

- best-practice disseminated (WP4):
  - publicly-available Best-Practice guides;
  - two1-day meetings with seminars and talks;
  - one symposium;
  - web-lectures;
  - presentations at single-photon workshops and other appropriate conferences.

B2.d Projected intermediate impact on the metrological and scientific communities

The project will influence the work within:

The Consulting Committee on Photometry and Radiometry (CCPR): All six funded partners as well as two unfunded partners of the consortium are members of the CCPR and have been working to incorporate photon-based quantities into its strategic planning. INRIM chairs the Task Group on SI.

EURAMET Technical Committee for Photometry and Radiometry (TC-PR): All six funded partners of the consortium, plus METAS, are members of the TC PR.

Through this membership the project will ensure 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.

A general objective of the project is investigating the possibility of establishing the "**Joint Virtual European Metrology Centre for Quantum Photonics**" between the partners of the project. The idea behind the formation of such a centre is that the national budgets for establishing a new metrological field such as quantum photonics will be not sufficient to cope with the metrological challenges, and therefore a joint, co-ordinated, effort is necessary. This investigation will include gathering evidence in support of this approach, agreement between all partners to form such a centre, establishing objectives, and identifying the formal steps necessary to establish such a centre by finalising a co-operation and collaboration agreement between the members of the centre.

Intermediate impact can be summarised as follows:

- Support for the development of free-space QKD, through providing metrology of components, and new devices, for free-space QKD;
- A measurement infrastructure developed for characterising entanglement-based QKD systems;
- Ensuring that CCPR & EURAMET address the needs of the single-photon and QKD communities.

The specific outputs that will have intermediate impact are listed below. These are dependent on the outputs of WP2 and WP3, which are more focussed on research to accelerate the development of commercial QKD systems.

- metrology of components for free-space QKD (WP2);
- new devices for free-space QKD (WP2);
- methods for quantifying entanglement (WP3);
- a measurement infrastructure developed for characterising entanglement-based QKD systems (WP3);
- a security proof for DI-QKD using hyper-entanglement (WP3);
- the results from WP2 and WP3 disseminated through web presentations (WP4);
- inputs to international guidelines and standards with a specific focus on the activity listed in Table B.1 (WP4);
- updating CCPR & EURAMET roadmaps to include the measurement needs of the single-photon and QKD communities (WP4);
- Go/no-go decision on establishing a "Joint Virtual European Metrology Centre for Quantum Photonics" (WP5).

B3 THE QUALITY AND EFFICIENCY OF THE IMPLEMENTATION

B3.a Overview of the consortium

This consortium brings together 6 European NMIs, 2 non-European NMIs as unfunded partners, 4 academic research institutes both as funded and unfunded partners, and 3 "quantum" industries.

It combines the metrological excellence in the fields of quantum communication, single-photon metrology and radiometry of the participating national metrology institutes (CMI, INRIM, METROSERT, AALTO, NPL,

PTB, KRISS, METAS), the technological and market-leading excellence of industrial partners (IDQ, Toshiba, and MPD) and the outstanding high-level university institutes (TUB, UBER, PoliMi, UniGE CH).

Specifically:

- INRIM brings expertise in developing traceable methods for characterising single-photon sources and detectors. INRIM brings also expertise in generating, manipulating, characterising photonic quantum entanglement, and in expertise in cryogenic single photon detectors, particle detectors and electronics
- PTB brings expertise in developing traceable methods for characterising single-photon sources and detectors, and also in cryogenic single photon detectors, particle detectors and electronics
- NPL brings expertise in developing traceable methods for characterising single-photon sources and detectors. Furthermore NPL brings expertise in fibre-optic metrology, and in coupling single-photon measurements to fibre-coupled high bit-rate quantum key distribution components and modules. NPL brings also expertise in generating, manipulating and characterising photonic quantum entanglement.
- METAS brings expertise in fibre-optic metrology and characterisation, and in cryogenic single photon detectors, particle detectors and electronics.
- Metrosert brings expertise in detector characterisation, and in the development of highly-defined, high-quality attenuators based on semiconductor devices.
- Aalto brings expertise in detector characterisation, and in the development of highly-defined, high-quality attenuators based on semiconductor devices.
- CMI brings expertise in the field of developing highly-precise, high-gain, high-stability electronics necessary for traceable radiometry at low photon fluxes.
- KRISS brings expertise in characterisation of optical fibres, generation of entangled photon pairs, and measurement of high-dimensional entangled states in optical fibres.
- TUB brings expertise in the field of the fabrication of deterministic single-photon sources. TUB has also expertise in the quantum optical study of non-classical light sources and their application in QKD.
- UBER brings expertise in generation as well as characterisation of single- and few-photon states, in the design and implementations of photon-pair sources with specific optical properties (e.g. photon wavelength and line-width), and in quantum information tasks with single photons, such as quantum algorithms, multiplexed single-photon QKD, and photon conversion.
- UniGE CH brings experience in single-photon counting at telecom wavelengths, and QKD. UniGE CH also developed a quantum radiometer based on quantum cloning and has the tools to characterise the single-photon detectors precisely. In recent years it developed a complete high-clock-rate QKD prototype including efficient post-processing and finite-key analysis.
- IDQ brings expertise in photon-counting, electronics and software development to develop quantum communication systems. IDQ will also bring customer views on quantum hacking and counter-measures.
- PoliMi brings expertise in the design, characterisation and exploitation of single-photon detectors and associated electronics, in particular for the near-infrared wavelength range (up to 1700 nm).
- MPD brings expertise in the design and production of single-photon counters for the visible and infrared range, spanning a range from 400 nm to 1600 nm, both for free-space and fibre-coupled applications.
- Toshiba brings expertise in the design, characterisation, and operation of high bit rate quantum key distribution components and systems for fibre-optic networks.

The combined and mutual effort of the partners with scientific excellence and complementary expertise in all aspects of this project will generate powerful synergies and lead to the successful delivery of the objectives of this project. This consortium brings together larger European NMIs which have broad experience and expertise in photon techniques in general with smaller NMIs, who will make highly focussed, well-defined contributions to specific tasks. Furthermore, the inclusion of leading academic partners and industrial partners will ensure the development of an appropriate metrology framework for current and future QKD systems, in addition to NMIs being able to influence the development of QKD systems through best practice measurements that are not always considered in R&D. Due to this combined effort of all partners being the

leaders in their specific field of research and technology, the delivered results will be much larger than the sum of its parts.

The project is designed to limit the unnecessary duplication of skills and facilities. The efforts are divided among the partners such that the specific experience of each partner is optimally exploited.

The project management will be overseen by the coordinator from INRIM. INRIM has a well-established project coordination experience and has successfully managed and delivered many projects. To enhance the effectiveness of the project management, a project management board will be established consisting of one formal representative from each WP.

Section C: Detailed Project Plans by Work Package

C1 WP1: Counter-measures and novel optical components for commercial fibre-based QKD

The aim of this work package is to characterise and validate counter-measures to side-channel and Trojan-horse attacks in order to ensure the security of fibre-based QKD systems. This activity is carried on in strict collaboration with the 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 [4-20]. The technical results of this WP will contribute to the project's impact to foster the development of new standard protocols and the updating of the existing ones in close collaboration with the ETSI ISG-QKD. In addition the outcomes of this WP will contribute to the formation of a Joint Virtual European Metrology Centre for Quantum Photonics (in WP4 and WP5).

Task 1.1 will experimentally characterise and verify counter-measures to Trojan-horse and side-channel attacks, as well as will develop devices for these purposes. Components will be characterised to assess their vulnerability to such attacks, and a security proof which takes account of information leakage after the application of counter-measures in the prepare-and-measure architecture will be developed. This task will focus on components and counter-measures for commercial fibre-based QKD systems, and will require the development of new measurement facilities and procedures to support the development of measurement protocols and standards in co-operation with companies and standardisation bodies active in this field.

Task 1.2 will focus on a new type of high-count-rate single-photon detector for fibre-based QKD driven by very narrow gate signals (few hundreds of picoseconds) to minimise after-pulsing. Specific measurement techniques will be developed for their characterisation.

Task 1.3 deals with the validation of the measurement facilities by carrying out comparisons of selected measurands among the consortium.

C1.a Task 1.1: Characterising counter-measures to Trojan-horse and side-channel attacks

The aim of this task is to identify the vulnerabilities of QKD components to Trojan-horse and side-channel attacks, and to characterise 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 [7-9], dead-time [10], jitter, and switching detection mode into the linear regime by a CW laser [4-6]. 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 [15], the wavelength dependent splitting ratio of beam splitters/couplers [16,17], the wavelength dependence of intensity and phase modulators [17,19]. 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. To limit the maximum power an eavesdropper can inject in QKD system, an optical fuse would be useful. The optical fuse should also be characterised under various conditions to determine its properties, e.g. the breaking power as a function of the wavelength. Components should therefore be characterised over a broad range of wavelength and power, but also after interactions with special signals (e.g. wavelength, power) 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 must also be made sure that the properties of the

components will not be altered by bright-light or special wavelength pulses. Broad-band characterisation (400 nm – 1600 nm) at high and low power will therefore be performed on passive components such as interference filters, beamsplitters, isolators and circulators, and on active components such as InGaAs-SPAD based single-photon detector operating in Geiger mode (SPDG), intensity modulators, fibre fuses and pin photodiodes. A device to detect such high-power attacks over wavelengths from the visible to the infrared will be devised, constructed and tested. In addition, the performance of intensity and phase modulators for countering bright pulse and DEM attacks will be performed.

Activities specific to SPDGs will be to measure their gate time 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 aims to improve the noise performance achieved in EMRP JRP IND06 MIQC by one order of magnitude. This device can be integrated by QKD manufacturers into their systems, to provide SI traceability for calibration/test routines for detection efficiency and emitted mean photon number. A double monochromator-based calibration facility will be constructed to perform broadband spectral characterisation (1280 nm – 1650 nm) of detection efficiency (DE) and linearity of fibre-based single-photon detectors.

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.

Activity number	**Activity description**	**Partners (Lead in bold)**
A1.1.1	CMI together with NPL will measure the splitting-ratio of beam-splitter as a countermeasure against multi-wavelength attacks.	**CMI,** NPL
A1.1.2	IDQ together with METAS will characterise at least two isolators and/or circulators possibly coupled with spectral filters to avoid leakage of information.	**IDQ,** METAS
A1.1.3	IDQ together with METAS will perform the broadband spectral characterisation (400 nm – 1600 nm) of interference filters used against multi-wavelength attack (source side and receiver side)	**IDQ**, METAS
A1.1.4	METAS together with IDQ will test the vulnerability of SPDGs to bright pulse attacks. (METAS will probe SPDGs outside their normal specification to establish their vulnerability to attacks, such as the bright-light attack).	**METAS,** IDQ
A1.1.5	INRIM will characterise, at a fixed wavelength (1550 nm), the extinction ratio of typical intensity modulator that could be used for restoring the security against attacks exploiting bright illumination.	**INRIM**
A1.1.6	METAS and UniGE CH, in collaboration, will evaluate the use of an optical fuse to protect against hacking. UniGE CH will perform the investigations on the availability of optical fuses (as prototypes or commercial products) and METAS identify the physical properties that will have to be characterised.	**METAS,** UniGE CH
A1.1.7	IDQ together with METAS will characterise the variable optical attenuator over a broad spectrum (400 nm – 1600 nm).	**IDQ,** METAS
A1.1.8	IDQ together with METAS will characterise at least two types of PIN diodes used against Trojan horse attack over a broad spectrum (400 nm – 1600 nm) and various input power ranging from microW up to hundreds of mW.	**IDQ,** METAS
A1.1.9	INRIM, PoliMi, MPD, NPL and Toshiba will collaborate in 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, and characterise ways of mitigating against detection efficiency mismatch attacks. INRIM will perform this activity with the collaboration of NPL that has already some experience in time resolved measurement. MPD, PoliMi and Toshiba, as detector developers and manufacturers, will provide fundamental input in the realisation of the measurement technique, and in the interpretation of results.	**INRIM,** PoliMI, MPD, NPL, Toshiba

A1.1.10	INRIM will characterise back-flash emission from the spectral, polarization, temporal point of view in order to suppress leakage of information that Eve could gain on the internal behaviour of the Bob's receiver. MPD, Toshiba and PoliMi, as detector developers and manufacturers, will provide fundamental input in the interpretation of results, as well as they will provide at least 2 detectors to be investigated.	**INRIM,** PoliMi, MPD, Toshiba
A1.1.11	METROSERT, in collaboration with Aalto and CMI, will realise a counter-measure based on a fibre-coupled attenuator based on Si and InGaAs photodiodes in a hybrid tunnel trap configuration with pc interface able to monitor macroscopic light pulses at wavelengths ranging from VIS-NIR up to telecom wavelengths.	**Metrosert,** Aalto, CMI
A1.1.12	Aalto in collaboration with METROSERT and CMI will characterise the trap-based attenuator spectrally (VIS and NIR up to 1500nm).	**Aalto,** Metrosert, CMI
A1.1.13	PoliMi together with MPD will develop a new secure front-end circuit for InGaAs/InP SPADs that will be able to detect attacks by monitoring voltages, currents, SPAD temperature, etc. and accepting only avalanche pulses when the SPAD is ON, i.e. only during the gate ON time, thus avoiding attacks during the dead-time.	**PoliMi**, MPD
A1.1.14	IDQ, NPL and CMI will synchronise attenuated laser pulses of fixed mean photon number and temporal extent with the bias gates of the SPDGs within a commercial IDQ QKD detector module and measure the detection efficiency of the SPADs.	**NPL,** IDQ**,** CMI
A1.1.15	CMI together with NPL will construct and calibrate a low photon flux reference detector for 1550 nm comprising a thermoelectrically-cooled state-of-the-art fibre-coupled InGaAs detector in conjunction with a custom-made high-sensitive switched-integrator amplifier.	**CMI,** NPL
A1.1.16	CMI together with NPL will develop a double monochromator-based calibration facility to perform spectral characterisation of detection efficiency (DE) and linearity of fibre-based single-photon detectors (SPDs) in the 1550 nm region.	**CMI,** NPL
A1.1.17	NPL together with INRIM will measure the properties of phase modulators, used in phase-encoding QKD system, as a function of time, as is needed for bit-mapping based counter-measure against DEM attacks.	**NPL,** INRIM
A1.1.18	Toshiba together with NPL will work on understanding the implementation security of prepare-and-measure QKD schemes. The side-channel information remaining after the implementation of counter-measures to reduce information disclosed to Eve will be investigated.	**Toshiba**, NPL
A1.1.19	Toshiba together with NPL will construct a security model for prepare-and-measure QKD which includes the device properties yielding side-channel information even after the implementation of counter-measures, and develop a security proof for this model	**Toshiba**, NPL

C1.b Task 1.2: Characterising novel high-rate single-photon detectors for fibre based QKD

The aim of this task is to characterise new high-count-rate single-photon InGaAs SPADs operated with narrow gates 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 [50], 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 [51-55].

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 with very low after-pulsing (few percent), high dynamic range (maximum count rate of few hundreds of 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) will be developed, and will be fully characterised in terms of performance and vulnerability to Eve attacks.

The special mode of operation of this new kind of high count rate single-photon detector requires new characterisation techniques to be developed through collaboration between NMIs and manufacturers that are members of the consortium.

Activity number	Activity description	Partners (Lead in bold)
A1.2.1	PoliMi together with UniGE CH will develop a photon-counting system based on InGaAs/InP SPADs sinusoidally-gated at more than 1 GHz, with very low after-pulsing (expected around few percent), high dynamic range (maximum count rate no more than few hundreds of 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).	**PoliMi**, UniGE CH
A1.2.2	INRIM, in collaboration with PoliMi and NPL, will characterise the photon detection efficiency within the gate window for InGaAs/InP SPADs sinusoidally-gated at more than 1 GHz.	**INRIM**, PoliMi, NPL

C1.c Task 1.3: Validation of facilities by measuring two key measurands (the detection efficiency of single-photon detectors and Glauber second-order auto-correlation function of a pseudo single-photon source) at the telecom wavelength (1550 nm)

The aim of this task is to validate the NMIs facilities used in the framework of this project by measuring two key measurands in the 1550 nm region correlated with fibre-based QKD systems, i.e. the detection efficiency of single-photon detectors (A1.3.1) (in collaboration with the CCPR Few Photon Task groups CCPR-WG-SP-TG7 and -TG11), and the Glauber second-order auto-correlation function of a pseudo single-photon source (A1.3.2). The measurement protocols for the comparisons will be agreed among the participants. The results will be disseminated by publications in appropriate journals and presentations at conferences and meetings of appropriate organizations, see Task 4.1 within WP 4 (Impact).

Activity number	Activity description	Partners (Lead in bold)
A1.3.1	PTB, INRIM, NPL and CMI will each perform a pilot comparison on the measurement of detection efficiency of single-photon detectors at a selected wavelength in the 1550 nm region (expected uncertainty agreement: better than 4 %).	**PTB,** INRIM, NPL, CMI
A1.3.2	PTB, INRIM and NPL will each perform a pilot comparison on the measurement of the second-order Glauber auto-correlation function of a pseudo-single-photon-source at a selected wavelength in the 1550 nm region (expected uncertainty agreement: better than 4 %).	**PTB,** INRIM, NPL
A1.3.3	CMI, INRIM, Aalto, Metrosert, NPL, PTB, PoliMi, Toshiba, IDQ, METAS, MPD and UniGE CH will analyse the outcomes of A1.1.1 - A1.1.17, A1.3.1, and A1.3.2 and generate a validation document describing the validation of measurement techniques for characterising counter-measures to side-channel and Trojan-horse attacks. CMI, INRIM, Aalto, Metrosert, NPL, PTB, PoliMi, Toshiba, IDQ, METAS, MPD and UniGE CH will review the validation document which CMI will then submit to coordinator as D1. The coordinator will then submit the validation document to EURAMET as D1 'Measurement techniques for characterising counter-measures to side-channel and Trojan-horse attacks developed and validated'.	**CMI,** INRIM, Aalto, Metrosert, NPL, PTB, PoliMi, Toshiba, IDQ, METAS, MPD, UniGE CH
A1.3.4	INRIM, PoliMi, UniGE CH, NPL, PTB, and CMI will analyse the outcomes of A1.2.1, A1.2.2, A1.3.1, and A1.3.2 and generate a validation document describing the validation of dedicated measurement technique for calibrating new type of single-photon detectors for fibre-based QKD, with target uncertainty of 2 %. INRIM, PoliMi, UniGE CH, NPL, PTB, and CMI will review the validation document which INRIM will then submit to coordinator as D2. The coordinator will then submit the validation document to EURAMET as D2 'Dedicated measurement technique for calibrating new type of single-photon detectors for fibre-based QKD, with target uncertainty of 2 % developed and validated'.	**INRIM,** PoliMi, UniGE CH, NPL, PTB, CMI

C2 WP2: Metrology for commercial components for free-space QKD

The aim of this work package is to establish measurement and characterisation facilities within the consortium for components of free-space QKD devices, with the goal to contribute a significant part to the Joint Virtual European Metrology Centre for Quantum Photonics (see WP4). This includes metrology for single-photon sources and detectors as well as relevant optical components. Within the scope of this project, we define 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.

The first three tasks deal with the measurement facilities for detectors, sources and components relevant for free-space QKD. These measurands, and their corresponding target uncertainties, are derived from the former work within the EMRP IND06 MIQC, where the measurement and characterisation requirements for fibre-based QKD (i.e. at telecom wavelength, and not in the VIS-NIR as in this case) were defined. The fourth task deals with the validation of the measurement facilities by carrying out comparisons of selected measurands among the consortium. The outcomes of these tasks lead directly to the formation of a Joint European Virtual Centre for Measurements for Quantum Communication (in WP4). The fifth task is devoted to the development of new components for free-space QKD.

C2.a Task 2.1: Measurement facilities for detectors for free-space QKD

The aim of this task is to establish measurement facilities - using different methods - among the partners dealing with detectors, their detection efficiencies (DE) and corresponding uncertainties relevant for free-space QKD (i.e. in the VIS-NIR).

Facilities for the calibration of the detection efficiency of free-space single-photon detectors in the VIS-NIR spectral range will be established using different methods: (i) a double monochromator-based calibration facility and a reference detection setup for low photon fluxes traceable to the primary radiometry standard, the cryogenic radiometer, will be developed. This detection system will be based on a small-area low-noise Si detector in conjunction with custom-made high-sensitivity readout electronics able to perform at about 5×10^3 photons/s/Hz$^{1/2}$ noise equivalent in photons at a wavelength of 700 nm (A2.1.1); (ii) a laser-based calibration facility will be established, based on the precise beam attenuation method using in-situ calibrated neutral density filters and Si-photodiodes in trap-configuration, aiming for an uncertainty in the DE below 0.5 %. (A2.1.2); (iii) a transition edge sensor (TES)-based measurement system for the characterisation of single-photon sources will be developed with an uncertainty in measured DE of < 2 %. This uncertainty includes the coupling between free-space and the fibre entrance of the TES (A2.1.3). TES-photon counters provide intrinsic photon-number state resolution. TES-detector technology had been worked on within the IMERA-Plus JRP qu-Candela. Since then, the quantum efficiency, wavelength range and operability of TES-detectors have improved significantly. Therefore, the project aims to set up a 2-channel TES-detector system in a portable millikelvin refrigerator. The system DE will be in excess of 90 % in the wavelength range of 800 nm to 950 nm. This is a drastic improvement in comparison to that achieved within IMERA-Plus JRP qu-Candela (system DE ca. 1 %). This system will be able to characterise the photon number distribution (PND) of single photon sources and will be used to investigate the photon number distribution (Task 2.2) of single photon sources made from deterministic quantum dot micro-lenses (Task 2.4).

Activity number	**Activity description**	**Partners (Lead in bold)**
A2.1.1	Metrosert will develop a thermally cooled miniature Si photodiode reflection trap for measurement of detection efficiency (DE) and linearity of free space single photon detectors at 700 nm.	**Metrosert**
A2.1.2	CMI will develop a double monochromator-based calibration facility to perform spectral characterisation of DE, linearity and spatial uniformity in free space. MPD will provide two state of the art commercially available PDM photon counters, with visible range sensitivity and DCR < 50 c/s for this test.	**CMI**, MPD
A2.1.3	PTB, with the input of Metrosert and Aalto will develop a laser-based facility for the calibration of the detection efficiency of single-photon detectors, provided by MPD (A2.1.2), with a standard uncertainty < 0.5 % using in-situ calibrated neutral density filters and an attenuator based on Si-photodiodes in trap configuration developed by Metrosert and characterised by Aalto.	**PTB**, Metrosert, Aalto

A2.1.4	PTB in collaboration with INRIM will develop and set up a measurement system with 2 TES-photon counters operated in a portable millikelvin refrigerator and to determine its system detection efficiency with an uncertainty < 2 %.	**PTB,** INRIM

C2.b Task 2.2: Measurement facilities for sources used in free-space QKD

The aim of this task is to establish measurement facilities among the partners dealing with the sources, and their corresponding measurands and uncertainties, relevant for open-space QKD.

Characterisation of sources used in QKD systems is also of high importance. Therefore, within this task, measurement facilities for the characterisation of sources suitable for free-space QKD will be established. This includes: the mean number of photons emitted by a pseudo-single-photon-source, typically an attenuated laser, suitable for free-space QKD with an expanded uncertainty of 1 %, which is a factor of three smaller than obtained in MIQC for infrared wavelengths (A2.2.1); the determination of the photon number distribution using the new TES-device (A2.2.2); and the determination of the single-photon spectrum by extending the high-resolution single-photon spectrometer towards visible wavelengths (A2.2.3). The newly-developed sources for free-space QKD applications (A2.2.5) will be characterised: in A2.2.4 with respect to the photon out-coupling efficiency, the quantum nature in terms of the $g^{(2)}(0)$-value and the emission spectra; in A2.2.5 with respect to the spatial modes of the transmitted photons; and in A2.2.6 with respect to the indistinguishability of the emitted photons.

Activity number	**Activity description**	**Partners (Lead in bold)**
A2.2.1	PTB together with INRIM will develop a measurement facility for characterising the mean number of photons emitted by a pseudo-single-photon-source suitable for open-air QKD with an expanded uncertainty of 1 %.	**PTB**, INRIM
A2.2.2	Using the device set up developed in A2.2.1 PTB together with TUB will perform the characterisation of a single-QD-based single-photon source (A2.5.5-A2.5.7) by measuring photon distribution functions.	**PTB**, TUB
A2.2.3	NPL will extend the high resolution single-photon spectrometer developed in EMRP IND06 MIQC, which covers 1270 nm to 1630 nm to cover the 700 nm – 1000 nm spectral region. A stable high-resolution scanning Fabry-Perot cavity, which can be interchanged with the existing telecom wavelength cavity in the previously built temperature-stable, low vacuum, vibration-free housing will be designed and constructed; and tested with attenuated laser pulses.	**NPL**
A2.2.4	NPL together with PTB and input from TUB will characterise at least two single-photon sources developed in A2.5.5-A2.5.7. This includes the determination of the photon out-coupling efficiency, the quantum nature in terms of the $g^{(2)}(0)$-value, the photon number distribution function as well as the emission spectra using the high resolution single-photon spectrometer constructed in A2.2.3.	**NPL**, PTB, TUB
A2.2.5	INRIM and NPL, in collaboration with PoliMi (providing a detector prototype and the expertise for its operation) and TUB (providing a prototype source and the know-how on how to operate it) will characterise the spatial modes of emitted/transmitted photons of a single photon source, exploiting different kinds of spatially resolving detectors (e.g. EMCCD, SPAD Array). EMCCD are efficient detectors (100 % fill factor, > 90 % quantum efficiency), while SPAD arrays have fast timing capabilities. The two elements of information will be merged.	**INRIM**, NPL, PoliMi, TUB
A2.2.6	NPL together with TUB will measure the lifetime and coherence time of photons emitted by fibre-coupled single-photon emitters created in task 2.5 and characterised in A2.2.4; and determines the degree of indistinguishability of the single photons emitted from the devices developed in task 2.5.	**NPL**, TUB

C2.c Task 2.3: Measurement facilities for components used in free-space QKD

The aim of this task is to establish measurement facilities among the partners for components other than sources and detectors which are relevant for open-space QKD. Within this project, the focus is on 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, and quantum random number generators.

Activity number	Activity description	Partners (Lead in bold)
A2.3.1	INRIM with the help of NPL and/or PTB will characterise at least one system for polarisation control (based on plates and/or Pockell's cells) used in free-space QKD systems with respect to degree of polarization.	**INRIM**, NPL, PTB
A2.3.2	CMI, in collaboration with INRIM and/or PTB will characterise at least 2 intensity modulators used in free-space QKD systems with respect to modulation depth.	**CMI**, INRIM, PTB
A2.3.3	PTB, with the input from INRIM and NPL will characterise the attenuating power of at least one kind of attenuator used in free-space QKD systems with respect to transmission.	**PTB**, INRIM, NPL
A2.3.4	NPL will use the QRNG open-system architecture developed in EMRP IND06 MIQC to further investigate how the properties of the single-photon detectors (dark counts, deficiency, after-pulsing, dead-time etc.) and photon pulses affect the measured entropy, and hence the results of specific software tests.	**NPL**

C2.d Task 2.4: Validation of facilities by measuring two measurands (the detection efficiency of single-photon detectors and $g^{(2)}(0)$-value of sources) used in free-space QKD

The aim of this task is to validate the measurement facilities between the partners. The validation takes place by performing selected pilot studies and comparisons of the two most relevant measurands, i.e. the detection efficiency of single-photon detectors (A2.4.1) and the $g^{(2)}(0)$-value of sources (A2.4.2) used in free-space QKD, i.e. in the VIS-NIR spectral region. The partners will establish common and agreed measurement protocols for the comparisons. The reports of the pilot studies will be disseminated by publications in appropriate journals and presentations at conferences and meetings of appropriate organisations see Task 4.3 within WP4 (Impact).

Activity number	Activity description	Partners (Lead in bold)
A2.4.1	PTB, INRIM, NPL and CMI will each perform a pilot comparison on the measurement of detection efficiency of single-photon detectors at a selected wavelength in the VIS-NIR spectral region (expected uncertainty agreement: better than 2 %).	**PTB**, INRIM, NPL, CMI
A2.4.2	PTB, INRIM and NPL will each perform a pilot comparison on the measurement of the second-order Glauber auto-correlation function of a pseudo-single-photon-source at a selected wavelength wavelength in the VIS-NIR spectral region (expected uncertainty agreement: better than 2 %).	**PTB**, INRIM, NPL

C2.e Task 2.5: Development of new few-photon detector and validation of measurement techniques for characterising components of free-space QKD systems

The aim of this task is to develop new components for QKD systems which have the potential to be implemented into QKD systems.

For increased security and performance of commercial free-space QKD systems, a new radiometric standard will be developed and investigated. Specifically, the feasibility of an induced-junction photodiode with predictable detection efficiency (developed in the iMERA-Plus qu-Candela as an integrated primary standard for commercial QKD systems will be tested. This predictable photodiode will deliver inherent SI traceability to customers without the need for external calibration. It will 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-Plus JRP qu-Candela. This will be 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-Plus JRP qu-Candela by three orders of magnitude down to a power level of 0.3 pW. Reliable linearity measurements slightly above the noise level will be performed by using synchrotron radiation whose power can be varied over 11 orders of magnitude in a controlled way. The second stage is to demonstrate measurement of the detection efficiency of a commercial free-space single photon detector based on Si-SPAD against a predictable induced-junction photodiode. (A2.5.1 – A2.5.4)

In addition, efficient single-photon sources based on deterministic quantum dot (QD) micro-lenses will be developed and optimised with respect to their out-coupling efficiency and quantum optical features. These non-classical light sources will be based on InGaAs quantum dots emitting in the wavelength range of 910 nm – 950 nm. Single preregistered quantum dots will be integrated deterministically into high quality micro-lenses by means of in-situ electron beam lithography [56]. This unique technique enables accurate alignment of pre-registered QDs in the centre of micro-lenses whose shape can be tailored precisely to maximise their photon out-coupling efficiency. The single-photon sources will be optimised to interface them with photon-number-resolving single-photon detectors in A2.1.4. Initially this will be achieved via free space coupling; during the project low-temperature coupling of single- photon emission directly, i.e. inside the cryostat, into single mode fibres will be developed. Apart of the user friendliness, single-mode fibre coupling will also be beneficial for free space QKD because it ensures an ideal beam profile and, moreover, single-mode coupling is usually required for the polarization optics in the transmitter unit of QKD systems [57]. Applying suitable mirror sections (distributed Bragg reflector or Au mirror by using a flip-chip process) at the substrate side of the QDs and anti-reflection coating at the upper surface, photon extraction efficiencies exceeding 50 % shall be achieved with high yield. The quantum nature of emission from single QDs in micro-lenses shall be reflected in $g^{(2)}(0)$-values below 1 % and a corresponding Fock-type photon distribution function will be determined in collaboration with PTB in activity A2.2.4. Optimised sources will also be provided to INRIM in order to characterise their spatial profile in A2.2.5. Further quantum optical studies will be performed in A2.2.6 to assess the degree of indistinguishability of single photons, and the visibility of polarization entangled photon pairs emitted from such quantum dot micro-lenses (WP3).

Activity number	**Activity description**	**Partners (Lead in bold)**
A2.5.1	PTB together with CMI will set up of a “few photon detector” based on a temperature stabilised induced-junction photodiode.	**PTB,** CMI
A2.5.2	CMI will develop a low noise photocurrent amplifier for biased photodiodes, suitable for the measurement of photon fluxes of about 1 Million photons per second. PTB in collaboration with CMI will verify the above, and contribute to realise a traceable calibration of the amplifier gain.	**PTB,** CMI
A2.5.3	PTB will measure the linearity of the few-photon detector (from A2.5.1) down to a photon flux of about 1 Million photons per second by using synchrotron radiation. For this purpose it will be taken advantage of the fact that the power of synchrotron radiation can be varied over 11 orders of magnitude in a controlled way by changing the ring current of the synchrotron.	**PTB**
A2.5.4	PTB will measure the detection efficiency of a commercial free-space single photon detector based on Si-SPAD (available at PTB) by comparison against the few-photon detector based on the predictability (from iMERA-Plus T1.J2.3 ‘Candela: Towards quantum-based photon standards’) and linearity (from A2.1.2) of induced junction photodiodes.	**PTB**
A2.5.5	TUB will grow and process at least 20 efficient single photon sources using MOCVD epitaxy and in-situ electron beam lithography.	**TUB**
A2.5.6	TUB will develop efficient free space (photon extraction efficiency > 50 %) and fibre coupled (photon extraction efficiency > 20 %) single photon sources based on deterministic quantum dot-microlenses. PTB will support this activity by sharing their expertise in the efficient fibre coupling of TES detectors. TUB will apply the same approach for the fibre coupling of SPSs.	**TUB,** PTB
A2.5.7	TUB will develop flip-chip process for a back-side Au mirror and anti-reflection coating to enhance the photon outcoupling efficiency beyond 50 %.	**TUB**

A2.5.8	PTB, INRIM, Aalto, CMI, Metrosert, PoliMi, TUB, MPD and NPL will analyse the outcomes of A2.1.1 – A2.1.4, A2.2.1 – A2.2.6, A2.3.1- A2.3.4, A2.4.1, A2.4.2 and A2.5.1-A2.5.4 and generate a validation document describing the validation of measurement techniques for characterising components of free-space QKD systems. PTB, INRIM, Aalto, CMI, Metrosert, PoliMi, TUB, MPD and NPL will review the validation document which PTB will then submit to coordinator as D3. The coordinator will then submit the validation document to EURAMET as D3 'Measurement techniques for characterising components of free-space QKD systems developed and validated'.	**PTB**, INRIM, Aalto, CMI, Metrosert, NPL, PoliMi, TUB, MPD

C3 WP3: Metrology for next generation (entanglement-based) QKD

The aim of this work package is to foster the development of a measurement infrastructure for entanglement-based (next-generation) QKD systems. The consortium intends to: develop methods for the measurement and the quantification of the amount of entanglement in bi-partite qubits system; provide a platform for the development and characterisation of entanglement-based QKD (for example, Measurement-Device-Independent QKD); investigate exploiting new degrees of freedom of the photons in fibre, namely spatial modes.

Following Ekert's seminal paper [58] proposing a QKD protocol 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. As discussed in WP1, 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 ideality of the security proofs of standard protocols, such as BB84, which assume generally perfect sources and detectors, and the implementation of QKD with real devices. Real sources and detectors always have "side" channels revealing information on the result of the measurements, and often their response can be manipulated unbeknown to legitimate users. Even if countermeasures have been found for each specific hacking attack proposed to date, 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-) [59, 60] and Measurement-Device-Independent (MDI-) QKD [61-63], 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 stronger 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. Very recently, a much simpler MDI-QKD (termed detector-device independent QKD, DDI-QKD) scheme using hyper-entanglement has been proposed, and a proof-of-principle experiment has been realised by a member of this consortium UniGE CH) [64].

Reference-frame-independent (RFI) QKD was originally conceived using entangled states to overcome the need for a shared reference frame [Boileau2004], but has since been implemented with weak coherent states and polarization encoding over free-space and fibre [Wabnig2013, Zhang2014], opening a route to incorporating QKD in handheld devices.

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.

In Task 3.1, INRIM, supported by NPL and KRISS, aims to further develop the theoretical tools and experimental procedures available for characterising entangled states and performing entanglement estimation. The consortium will theoretically investigate optimal (in terms of accuracy) entanglement estimation of states used in QKD protocols. An experimental procedure for reaching optimal or quasi-optimal POVM measurement will be tested. The expertise of TUB and UBER will be used to characterise entangled states by quantum tomography of solid-state (quantum dots) and asymmetric SPDC entangled sources.

In Task 3.2 we aim to support the development of DI-QKD, MDI-QKD, and RFI-QKD in the European Community by establishing rigorous measurement tools for estimating the uncertainty in measuring violations of Bell inequalities, such as, e.g., CHSH, as a function of the efficiency of the detectors and the

characterisation of a real Bell-state optical analyser setup (INRIM, NPL). This task will also support the effort to improve the speed of an MDI-QKD scheme recently proposed by UniGE CH and make a more complete security analysis of this scheme. Finally, the consortium (in particular KRISS) will study 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.

C3.a Task 3.1: Entanglement and quantumness quantification

The aim of this task is to develop metrics and measurement apparatus for rigorous quantification of entanglement for those families of quantum states that are relevant in QKD protocols. This is a challenging task, since in quantum mechanics entanglement is not an observable. The amount of entanglement can be indirectly inferred by an estimation procedure, i.e. by measuring appropriate observables and then statistically processing their outcomes by suitable estimators; however, all the entanglement measures are only suitable solutions when specific families of entangled states are considered [68][Brida2010]. This task intends to evaluate the ultimate bound on accuracy, i.e. the smallest value of the entanglement parameter that can be discriminated, and to determine and implement the optimal measurement achieving these bounds.

Activities A3.1.1-2 will theoretically investigate the optimal, i.e. the most accurate, entanglement measure that could be applied for the state used in QKD. Activity A3.1.3 is its experimental implementation. Other quantumness quantifiers, even non-entanglement ones, are investigated in A.3.1.4. The relation of entanglement and/or quantumness quantifier with the performance of QKD, for instance in terms of channel capacity, is the aim of A3.1.5. In activity A3.1.7 UBER will develop an asymmetric source of polarization entangled photons, based on type-II down-conversion and phase matching and compensation in a Sagnac-type configuration, with signal and idler photon at 894 nm and 1310 nm, respectively. Full quantum tomography of the entangled states will be performed by TUB and PTB. In A3.1.6 for a source of exciton-biexciton cascade of deterministic quantum dot [69], and the degree of entanglement (possibly related to the measure established in the A3.1.1-2) evaluated.

Activity number	Activity description	Partners (Lead in bold)
A3.1.1	INRIM will review the state of the art for entanglement measurements relevant for QKD applications, and will evaluate the quantum Fisher information (i.e. the uncertainty of their estimation) of the various entanglement measures for different families of two-qubit entangled states used in QKD.	**INRIM**
A3.1.2	INRIM with the support of NPL will identify among the entanglement measures from A3.1.1 one of particular interest for the states used in QKD (expected uncertainty level cannot is hard to be declared since this will be the first time that this measurement will be carried on from the metrological point of view). Calculation of the quantum Cramer-Rao bound and the investigation of the optimal POVM will be carried on	**INRIM,** NPL
A3.1.3	INRIM with the support of NPL will perform the experimental estimation of the entanglement according to the measure identified in A3.1.2. The states tested will be maximally entangled states, and states originated from such states after experiencing some decoherence effects.	**INRIM**, NPL
A3.1.4	INRIM with input from KRISS will find other “Quantumness” quantifiers of interest, even non-entanglement related (e.g. quantum discord), and their relationship with other informational quantities, such as the mutual information and the fidelity to a target state.	**INRIM,** KRISS
A3.1.5	INRIM will study proper metrics and will quantify the channel capacities and rates of the considered QKD schemes as functions of the quantum resource (e.g. entanglement, quantum discord).	**INRIM**
A3.1.6	TUB together with PTB will determine the degree of entanglement, according to the results from A3.1.1-2, of photon pairs emitted from the exciton-biexciton cascade of deterministic quantum dot – microlenses (via quantum tomography)	**TUB,** PTB
A3.1.7	UBER will develop an asymmetric source of polarization entangled photons with signal and idler photon at 894 nm and 1310 nm, respectively, for evaluating the performance of the device constructed in A3.1.8. This device will be used in perspective in a free-space transmission line over 500 m in Berlin together with the Heinrich-Hertz-Institute.	**UBER**

A3.1.8	UBER will develop a portable tomography system to quantify polarization entanglement according to the results in A3.1.1-3. The system will be able to measure the density matrix of the two-photon state of different sources (depending on the detectors: both photons at around 890 nm, both at 1310 nm, or one at each wavelength). The system will be tested together with TUB and PTB.	**UBER,** PTB, TUB

C3.b Task 3.2: Metrology for next generation QKD: DI-QKD, MDI-QKD and RFI-QKD, and encoding in new degree of freedom

The aim of this task is to investigate and develop metrological tools that are building blocks for the characterisation of components and parameters of interest for newer forms of QKD. In addition, the potential of using non-conventional codifying degrees of freedom in fibres, in particular spatial ones, will be investigated with the aim of enhancing the channel capacity.

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. In this regard, a rigorous method to estimate uncertainty in Bell inequalities which takes into account the detection efficiency uncertainty would allow a more reliable and shared assertion on the closure of the detection loophole in a particular DI-QKD scheme. Activity A3.2.1 will address this point. This work will also impact on other measurements where Bell inequality violations are used as a metric

MDI-QKD schemes are currently more feasible commercially and, so far, are based on the principle of the Bell state analyser. Therefore, a proper characterisation of a realistic optical Bell state analyser will be performed in A3.2.3. In addition, an innovative MDI-QKD scheme based on hyper-entanglement (DDI-QKD) will be pursued within this task (see activities A3.2.4-5).

Another assumption usually made in standard QKD is that Alice and Bob share a common reference frame in order to exchange meaningful information on the bases used. This is not the case in reference-frame-independent (RFI) QKD. In A3.2.6 methods to characterise the independent reference frames of such devices will be established.

The last three activities consider and develop a theoretical and experimental study about the use of spatial degrees of freedom for QKD. In particular, multimode fibre can propagate tens of spatial modes. Codifying information and sharing entanglement on a d-dimensional Hilbert could improve QKD secure bit rate.

Activity number	**Activity description**	**Partners (Lead in bold)**
A3.2.1	INRIM and NPL will collaborate in developing a rigorous method to estimate uncertainty in Bell inequalities (e.g. CHSH and other Bell inequalities), accounting for the detection efficiency uncertainty. This will be done in order to close the detector loophole in DI-QKD, and find the most suitable inequalities for specific values of the detection efficiencies.	**INRIM**, NPL
A3.2.2	INRIM will investigate the possibility of exploiting the “weak measurement” paradigm to perform a “non-destructive” characterisation of a Bell’s inequality violation.	**INRIM**
A3.2.3	NPL together with TUB will develop appropriate metrics and measurement apparatus to quantitatively characterise (i.e. measurement of the optical components and evaluation, with uncertainties, of required corrections to Bell-state measurement data, to their entangling power estimation, or to the estimation of the degree of indistinguishability of single photons) of a realistic optical Bell state analyser, namely the Hong-Ou-Mandel interferometer.	**NPL**, TUB
A3.2.4	UniGE CH will realise high-rate single-photon of detector device independent QKD. DDI-QKD is a much simpler version of MDI-QKD. UNIGE CH performed already a first proof of principle experiment of DDI-QKD. UNIGE CH will implement a full scale, high rate QKD system based on this principle.	**UniGE CH**
A3.2.5	UniGE CH will perform a more complete secure analysis of the single-photon MDI-QKD (DDI-QKD) scheme. UNIGE CH will investigate and clarify the underneath assumptions and consider variants allowing for fewer assumptions.	**UniGE CH**
A3.2.6	NPL will develop efficient schemes for characterising the reference frames used for coding in compact RFI QKD transmitters and receivers.	**NPL**

A3.2.7	KRISS with input from INRIM will develop an experimental technique for measurement of quantum states over multiple spatial modes of an optical fibre. Projection measurement to arbitrary quantum superposition states of single photons will be demonstrated.	**KRISS**, INRIM
A3.2.8	KRISS with input from INRIM to develop a theory to estimate the multi-dimensional entanglement between spatial modes of different optical fibres.	**KRISS**, INRIM
A3.2.9	KRISS assisted by INRIM will perform an experimental measurement of entanglement (or quantumness) between multimode optical fibres, based on the quantumness quantifier developed in A3.1.1-4. Spatially entangled photon pairs will be generated through PDC.	**KRISS**, INRIM
A3.2.10	INRIM, NPL, PTB, TUB, UBER and KRISS will review the outcomes of A3.1.1 – A3.1.8, A3.2.1 - A3.2.3, and 3.2.6 - 3.2.9 and prepare a report on measurement techniques for characterising quantum states. INRIM, NPL, PTB, TUB, UBER and KRISS will review the report, which INRIM will then submit to the coordinator as D4. The coordinator will then submit the report to EURAMET as D4 'Measurement techniques for characterising quantum states developed'.	**INRIM**, NPL, TUB, PTB, UBER, KRISS

C4 WP4: Creating Impact

The aim of this work package is to ensure that the results achieved by the project are provided to the stakeholders and end-user community in a timely and appropriate manner, and that input and feedback is obtained from these communities.

The primary beneficiaries of the outputs of this project will be the QKD community, but the wider community exploiting single-photon states – see [70] – will also derive significant benefits from the methods, devices, calibration facilities and measurement protocols developed.

The activities of the partners within this work package shall ensure that the projected impact and the benefits described in section B2 will be realised. The activities are described in detail below.

C4.a Task 4.1 Knowledge Transfer

The aim of this task is to ensure that the results achieved by the project are adequately and appropriately communicated to the stakeholders and end-user community, and that input and feedback is obtained from this community. Additional specific tasks include carrying out an analysis of the benefits likely to accrue from establishing a joint virtual metrology centre for quantum photonics, and scoping the opportunities for exploiting the results of this project more widely.

Advisory board (NPL, all partners)

An advisory board of at least 10 members, which will include representatives from industry, the user community, ETSI, EURAMET and CCPR, will be formed. The aim of the advisory board is to assess the needs of the various interested parties and feed these into the project; this latter activity will be carried out in WP5.

Membership will not be limited to the EU, in order to ensure that developments outside the EU are recognised and responded to.

Project webpage (NPL, all partners)

The existing MIQC JRP webpage on the NPL website, with public access and a part restricted for partners only, will be expanded and updated regularly to provide the following information from the MIQC2 project: an overview of the project, news items about project activities, publications, presentations, and training material. The usage statistics of the website will be monitored to ensure effective and targeted stakeholder engagement. Link to Facebook, and/or other networking sites, will be investigated.

The part of the website with restricted access will be dedicated to exchange information and reports among the partners. It will also include a digital archive of all presentations, reports and papers from the project.

Presentations at key conferences (all partners):

The following key conferences are expected to take place during the lifetime of this project: QCrypt (2015, 2016, 2017), the 8th Single Photon Workshop (2017), the International Conference on New Developments and Applications in Optical Radiometry – NEWRAD (2017), Quantum Computing, Metrology, and

Communications – QCMC (2016), the Quantum Conferences in memory of Carlo Novero – Quantum (2016, 2018).

Further relevant conferences may be identified during the lifetime of the project. The work within this project should result in at least 25 conference contributions, of which at least 8 will be from WP1, at least 5 from WP2, and at least 4 from WP3.

It is expected that some of the conference presentations will result in published conference papers. The authors of the conference papers will clearly acknowledge the financial support provided through EMRP as required by EURAMET.

Peer reviewed publications (all partners):

The partners will submit at least 10 papers to peer-reviewed journals, from which at least 4 will be from WP1, at least 3 from WP2 and at least 3 from WP3, during the course of the project. Target journals include Physical Review Letters, Physical Review A, Applied Physics, Optics Express, Applied Optics, Metrologia, International Journal of Quantum Information or any other similar. The authors of the peer reviewed papers will clearly acknowledge the financial support provided through the EMPIR as required by EURAMET, and ensure that a minimum of green open access is provided for these publications.

Trade journals (all partners):

The partners recognise the importance of disseminating research results beyond their scientific peers, and at least two articles will be submitted to popular magazines such as Physics World and Wired. Suggested contents are ‘Hacking attacks, counter-measures and their verification’, ‘Measurements for ensuring security of QKD systems’.

Liaison with CCPR and EURAMET P&R committees (All NMI partners)

These two committees guide and direct optical metrology within the world, and in Europe. The partners will ensure these committees are kept informed of the results of MIQC2, and will aim to exert their maximum influence to ensure support for single-photon metrology within these groups. The partners will ensure that metrology roadmaps accurately reflect the measurement needs of the QKD community.

Pilot comparisons (PTB, CMI, INRIM, NPL)

The results of the pilot-comparisons carried out in WP1 and WP2 will be disseminated via published papers, information on the website, direct communication with CCPR, ETSI, IEC and companies manufacturing photon counters, QKD systems, and single-photon technologies in order to demonstrate the validity of the developed measurement facilities to characterise QKD systems and other single-photon technologies.

ETSI (Toshiba, INRIM, NPL, PTB)

Close interaction with ETSI will be pursued, and critical input provided to the drafting of pre-standards and standards concerned with the optical layer of QKD systems (see Section B.2.b).

Joint Virtual European Metrology Centre for Quantum Photonics (INRIM, all NMI partners)

As stated in Section B, a general objective of the project is investigating the possibility of establishing the “**Joint Virtual European Metrology Centre for Quantum Photonics**” between the partners. A strategic analysis for the creation of this Centre will be carried out, which will include consultation with stakeholders and CCPR, and report on the need and proposed terms-of-reference for this Joint Centre.

Wider exploitation (INRIM, All partners)

Finally, in order to seek the maximum benefit for the work carried out in this project, a study will be carried out into where other fields can benefit from the techniques and artefacts that have been developed.

Activity number	**Activity description**	**Partners (Lead in bold)**
A4.1.1	The partners will create an advisory board of at least 10 members. This will include representatives from industry, the user community, ETSI, EURAMET and CCPR. The aim of the advisory board is to assess the needs of the various interested parties and feed these into the project.	**NPL**, all partners
A4.1.2	NPL will create and maintain the project website with public and private access. NPL will monitor its usage statistics on a quarterly basis. All partners will provide content for the website on a regular basis.	**NPL**, all partners

<table>
<tr><td>A4.1.3</td><td>The partners plan to present at least 25 presentations at relevant international conferences. Likely conferences are: QCrypt, ETSI QuantumSafe Crypto Workshop, QCMC, Carlo Novero, Single Photon Workshop, NEWRAD</td><td>INRIM, all partners</td></tr>
<tr><td>A4.1.4</td><td>The partners will submit at least 10 papers to peer-reviewed journals during the course of the project. Target journals include Optics Express, Metrologia.</td><td>INRIM, all partners</td></tr>
<tr><td>A4.1.5</td><td>The partners will submit at least 2 articles in magazines for industrial readership, e.g. Physics World and Wired.</td><td>NPL, all partners</td></tr>
<tr><td>A4.1.6</td><td>The partners will liaise with CCPR and EURAMET P&R.
CMI, INRIM, NPL and PTB will also carry out a comparison of single-photon detection efficiency for the task-Group on Single-Photon Measurements inside the CCPR (CCPR-WG-SP-TG11, CCPR-WG-SP-TG7).
The results of the project will be disseminated to CCPR (in particular CCPR WG-SP and CCPR WG-KC) and EURAMET TC PR, and their relevant working groups. This will ensure CCPR & EURAMET metrology roadmaps accurately reflect the measurement needs of the QKD community.</td><td>Aalto, all partners</td></tr>
<tr><td>A4.1.7</td><td>PTB together with CMI, INRIM and NPL will disseminate the results of the pilot-studies on measurement of detection efficiency in the photon counting regime at 810 nm or 850 nm, and 1550 nm. Likely dissemination activities are: published papers, information on the website, direct communication with CCPR, ETSI, IEC and companies manufacturing photon counters and QKD systems.</td><td>PTB, CMI, INRIM, NPL</td></tr>
<tr><td>A4.1.8</td><td>PTB together with INRIM and NPL will disseminate the results of the pilot-studies on measurement of the $g^2(0)$-values of sources. Likely dissemination activities are: published papers, information on the website, direct communication with CCPR, ETSI, IEC and companies manufacturing photon counters and QKD systems as well as prospective providers of single-photon sources.</td><td>PTB, INRIM, NPL</td></tr>
<tr><td>A4.1.9</td><td>Toshiba together with NPL, INRIM and PTB will continue participating in ETSI Industry Standardization Group on QKD, providing metrology leadership for the drafting of pre-standards and standards concerned with characterisation, validation, and certification of the optical layer of QKD systems and networks.
<table>
<tr><th>Standards Committee / Technical Committee / Working Group</th><th>Partners involved</th><th>Likely area of impact / activities undertaken by partners related to standard / committee</th></tr>
<tr><td>ETSI-ISG-QKD</td><td>INRIM, NPL, PTB, Toshiba</td><td>Information will be provided to the updated or revised Group Specification document GS QKD 003: Quantum Key Distribution (QKD); Components and Internal Interfaces</td></tr>
<tr><td>ETSI-ISG-QKD</td><td>INRIM, NPL, PTB, Toshiba</td><td>Information will be provided for the development of the final, updated or revised drafted Group Specification document DGS/QKD-0011_OptCompChar: Quantum Key Distribution (QKD) Component characterisation: characterising optical components for QKD systems (Rapporteur: NPL)</td></tr>
<tr><td>ETSI-ISG-QKD</td><td>INRIM, NPL, PTB, Toshiba</td><td>Information will be provided for the development of the final, updated or revised drafted Group Specification document DGS/QKD-0010_ISTrojan: Quantum Key Distribution (QKD) Implementation security: protection against Trojan horse attacks in one-way QKD systems (Rapporteur: Toshiba)</td></tr>
</table>
The current ETSI programme of drafting a series of Group Specification documents concerned with implementation security against hacking attacks will directly benefit from input from this project, as well as specifications concerned with characterisation of assembled modules, and updates of existing documents.</td><td>Toshiba, NPL, INRIM, PTB</td></tr>
<tr><td>A4.1.10</td><td>The partners will carry out strategic analysis for the creation of the Joint Virtual European Metrology Centre for Quantum Photonics. A go/no-go decision on the creation of the Joint Virtual European Metrology Centre for Quantum Photonics will be taken in the context of activity A5.1.4.</td><td>INRIM, all partners</td></tr>
<tr><td>A4.1.11</td><td>The partners will carry out paper-study to identify other fields that can benefit from the techniques and artefacts developed within this project. Results of this study will be used to update A4.3.1, to inform CCPR Strategy Group, and for publication in a popular scientific magazine.</td><td>INRIM, all partners</td></tr>
</table>

C4.b Task 4.2 Training

A demonstration of measuring the adjustable detection efficiency of the detectors used in a commercial device, in order to verify security against attacks exploiting bright illumination, will be carried out. This will show that the measurements developed in this project have been devised in such a way as to allow their efficient and cost-effective application to the commercial systems they are intended for.

The consortium will provide training to industrial developers, measurement laboratories, users, and standards bodies by: providing freely-available progress reports on the work in WP1 and WP2 on the project website at the 18-month point; providing freely-available best-practice guides summarising the work in WP1 and WP2 on the project website at the 36-month point; organising two one-day meetings on metrology for QKD with contributions from members of the project and from the extended QKD community; filming these contributions and providing them free of charge on the project website; organising a 1-day symposium on the project during a suitable international conference. The two meetings and one symposium should take place approximately at M18, M27 and M36, with the symposium being either the second or third event. Finally, the 4 lectures on QKD created by EMRP IND06 MIQC are to be expanded by at least two new lectures – one on counter-measures to hacking attacks, the second on advanced metrology for QKD.

The Single Photon Workshop, a workshop dealing with the topic of single-photon sources and detectors with a special session on absolute single-photon sources, will most likely be held in 2017, to follow the one that will be held at UniGE CH in 2015.

Activity number	**Activity description**	**Partners (Lead in bold)**
A4.2.1	IDQ together with NPL and CMI will demonstrate the measuring of adjustable detection efficiency of the detectors used in a commercial device, in order to verify security against attacks exploiting bright illumination. This will be based on the work carried out in A1.1.14.	**IDQ,** NPL, CMI
A4.2.2	The partners will provide two progress reports, freely available on the project website, (one each for WP1 and WP2) in November 2016 (M18). Target audience will be ETSI, measurement laboratories and R&D.	**CMI,** all partners
A4.2.3	PTB, CMI, INRIM, Aalto, Metrosert, NPL, PoliMi, Toshiba, TUB, IDQ, KRISS, METAS, MPD, UBER and UniGE CH will review the outcomes of WP1 and produce a Best Practice Guide on characterisation of counter-measures to side-channel and Trojan-horse attacks. PTB will submit the Best Practice Guide to coordinator as part of D5. PTB, CMI, INRIM, Aalto, Metrosert, NPL, PoliMi, Toshiba, TUB, IDQ, KRISS, METAS, MPD, UBER and UniGE CH will review the outcomes of WP2 and produce a Best Practice Guide on characterisation of components of free-space QKD systems. PTB will submit the Best Practice Guide to coordinator as part of D5. The coordinator will then submit both Best Practice Guides to EURAMET as D5 'Two Best-Practice Guides, one on characterisation of counter-measures to side-channel and Trojan-horse attacks (WP1), and one on characterisation of components of free-space QKD systems'. Both Best Practice Guides will be available to the target audience (e.g. ETSI, measurement and R&D laboratories) for free on the project website.	**PTB,** all partners
A4.2.4	Partners will organise two 1-day meetings with training seminars and talks (aiming at a minimum of 10 attendees). These should take place approximately Oct 2016 (M17), and either Aug 2017 (M27) or Apr 2018 (M35). Venues will be decided in project meetings.	**NPL**, all partners
A4.2.5	Partners will organise a symposium on QKD measurements during a suitable international conference (aiming at a minimum of 20 attendees). This should take place approximately Aug 2017 (M27) or, most likely, May 2018 (M36).	**NPL,** all partners
A4.2.6	NPL will film training seminars and lectures carried out in the 1-day meetings, and provide recorded material on the project website.	**NPL**
A4.2.7	INRIM with input from all partners will expand the web lectures on QKD, created by IND06 MIQC, to cover the new areas researched by this project. Results will be published on the project website.	**INRIM**, all partners

A4.2.8	UniGE CH together with INRIM, NPL and PTB will co-organise the Single Photon Workshop in 2015 and in 2017. The aim of these workshops is to bring together a broad range of people with interests in single-photon technology and its applications thus disseminating progress in the field. The target audience will comprise scientists from NMIs and universities as well as manufacturers and users of products in the field of single photon technology. The typical number of participants is 100 - 150 people. An exhibition of single photon products and technology will also be held. Partners will help organise the scientific programme, as well as assist in editing a special journal issue, which will include papers dealing with the most interesting topics of the workshop..	**UniGE CH,** INRIM, NPL, PTB

C4.c Task 4.3 Uptake and Exploitation

The aim of this task is to ensure that the results of this project provide the maximum benefit to the QKD, single-photon, and wider, communities. This will be achieved by converting intellectual property (most probably through licencing agreements) into new products for the implementation and testing of QKD systems.

Exploitation is specifically addressed by a plan to exploit intellectual property developed in this project (specified in the consortium agreement). This plan will be reviewed and updated at every project meeting. Contract negotiations will start with possible manufacturers on licensing any appropriate Intellectual Property Rights produced within this project, mainly, but not limited to, the “low photon flux reference detector”, the “fibre-coupled attenuator”, the “front-end circuit for detecting attacks” (WP1), the “single-photon spectrometer”, the “few photon detector” (WP 2) and “a new architecture for MDI-QKD” (WP3).

Activity number	Activity description	Partners (Lead in bold)
A4.3.1	Exploitation plan for the research related to MIQC2 reviewed and updated at every project meeting.	**NPL,** all partners

All IP and potential licencing/exploitation will be handled in accordance with the grant agreement and the consortium agreement.

C5 WP5: Management and Coordination

This WP addresses the management and coordination of the project. It is structured into 3 separate tasks: these are Project Management, Project Meetings and Project Reporting.

C5.a Task 5.1: Project management

Activity number	Activity description	Partners (Lead in bold)
A5.1.1	The project will be managed by the coordinator from INRIM. He will be supported by the project management board consisting of two representatives from each partner; including the leaders of each work package. The PMB will guide the project, attend the project meetings, organise the progress meetings at their local institutes and call additional meetings if needed to ensure the overall project’s success.	**INRIM**, all partners
A5.1.2	The work package leaders will report on the ongoing progress to the co-ordinator by e-mail and telephone conferences.	**INRIM**, all partners
A5.1.3	The coordinator, with support from the partners, will manage the project’s risks to ensure timely and effective delivery of the scientific and technical objectives and deliverables.	**INRIM**, all partners
A5.1.4	INRIM together with NPL, PTM, CMI, Aalto, Metrosert and METAS will discuss a go/no-go decision on creating a Joint Virtual European Metrology Centre for Quantum Photonics, together with agreement and implementation of terms of reference as appropriate. This discussion will take place at the project meeting on August 2017 (M27).	**INRIM**, NPL, PTM, CMI, Aalto, Metrosert, METAS
A5.1.5	The consortium will ensure that any ethics issues identified (see Section D.3) are addressed.	**INRIM**, all partners

C5.b Task 5.2: Project meetings

Activity number	Activity description	Partners (Lead in bold)
A5.2.1	The kick-off meeting involving all partners will be held approximately one month after the start of the project.	**INRIM**, all partners
A5.2.2	There will be five formal project meetings. These meetings include the kick-off, mid-term [around November 2016 (M18)] and final meeting [around May 2018 (M36)]. The meetings will be held prior to reporting. The meetings will review progress and will be used to ensure partners are clear as to their role for the next period. The location of the meetings will rotate among the partners. Where possible, meetings may be held as satellite meetings to important conferences or committee meetings.	**INRIM**, all partners
A5.2.3	In addition, technical meetings of work package groups may be held whenever necessary, and will be arranged on an ad-hoc basis.	**INRIM**, all partners

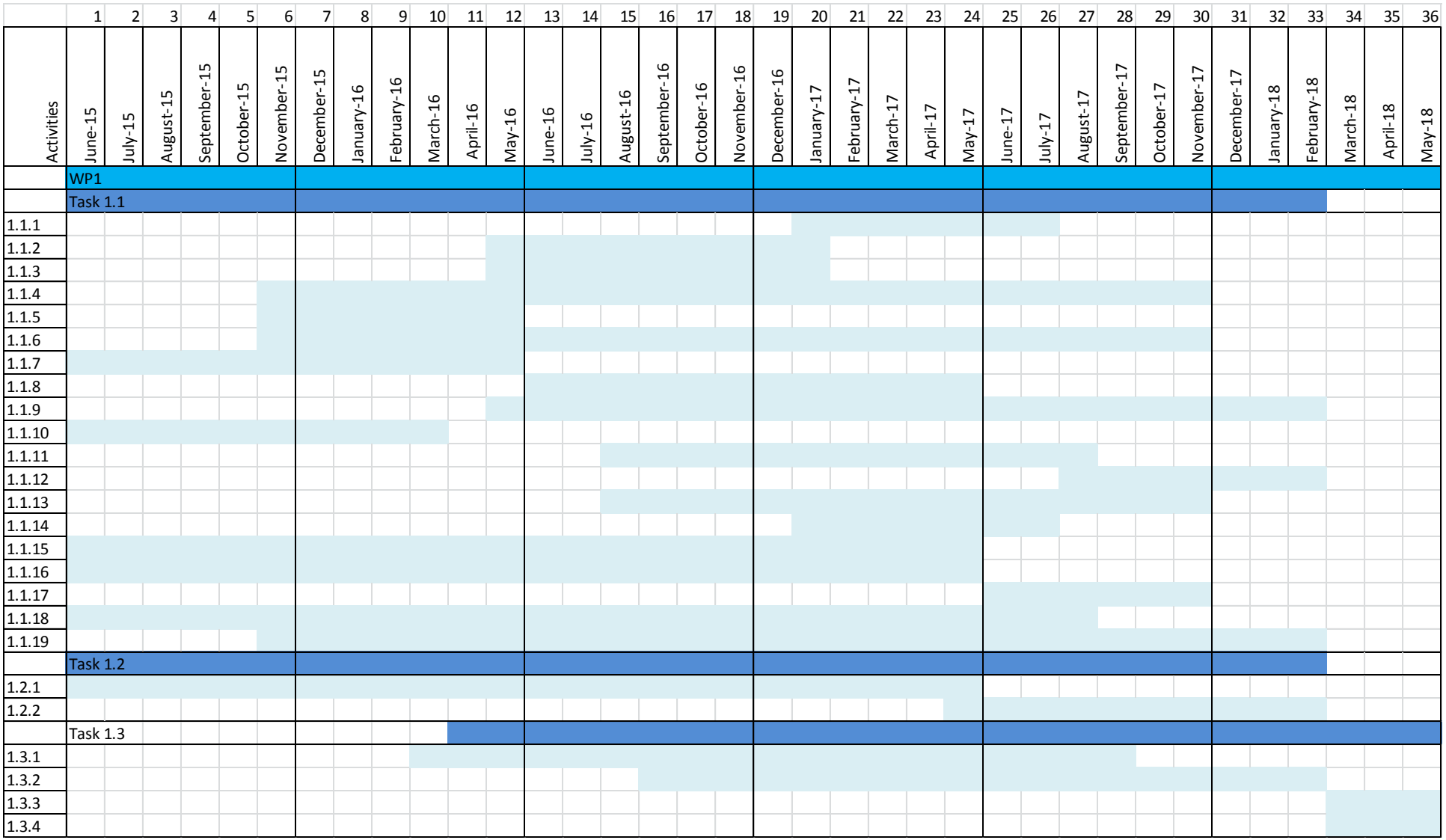
C5.c Task 5.3: Project reporting

Activity number	Activity description	Partners (Lead in bold)
A5.3.1	One month after the signature of the grant agreement a publishable summary will be produced and submitted to EURAMET.	**INRIM**, all partners
A5.3.2	Following Article 17 and 20 of the grant agreement, information will be submitted to EURAMET, in accordance with the procedures issued by them to enable EURAMET to comply with its obligations to report on the programme to the European Commission. • Progress reports will be submitted at months 9, 27 (February 2016, August 2017; + 45 days), 18, 36 (November 2016, May 2018; + 60 days) • Impact/Output reports will be submitted at the same times. All partners will provide input to these reports and the coordinator will provide these and updated publishable summaries to EURAMET. Payment requests will be submitted to EURAMET as appropriate. A report on the assessment of the potential for dual use applications of the results and outcomes of the project and where applicable how dual use risks can be mitigated will be written and submitted to EURAMET at month M36 (May 2018 + 60 days) (see section D3).	**INRIM**, all partners
A5.3.3	Periodic Reports (including financial reports and questionnaires) will be delivered at months 18 and 36 (November 2016, May 2018; + 60 days) in accordance with Article 20 of the grant agreement. All partners will provide input to these reports and the coordinator will provide these to EURAMET.	**INRIM**, all partners
A5.3.4	Final Reports will be delivered at month 36 (May 2018 + 60 days) in accordance with Article 20 of the grant agreement. All partners will provide input to these reports and the coordinator will provide these to EURAMET.	**INRIM**, all partners

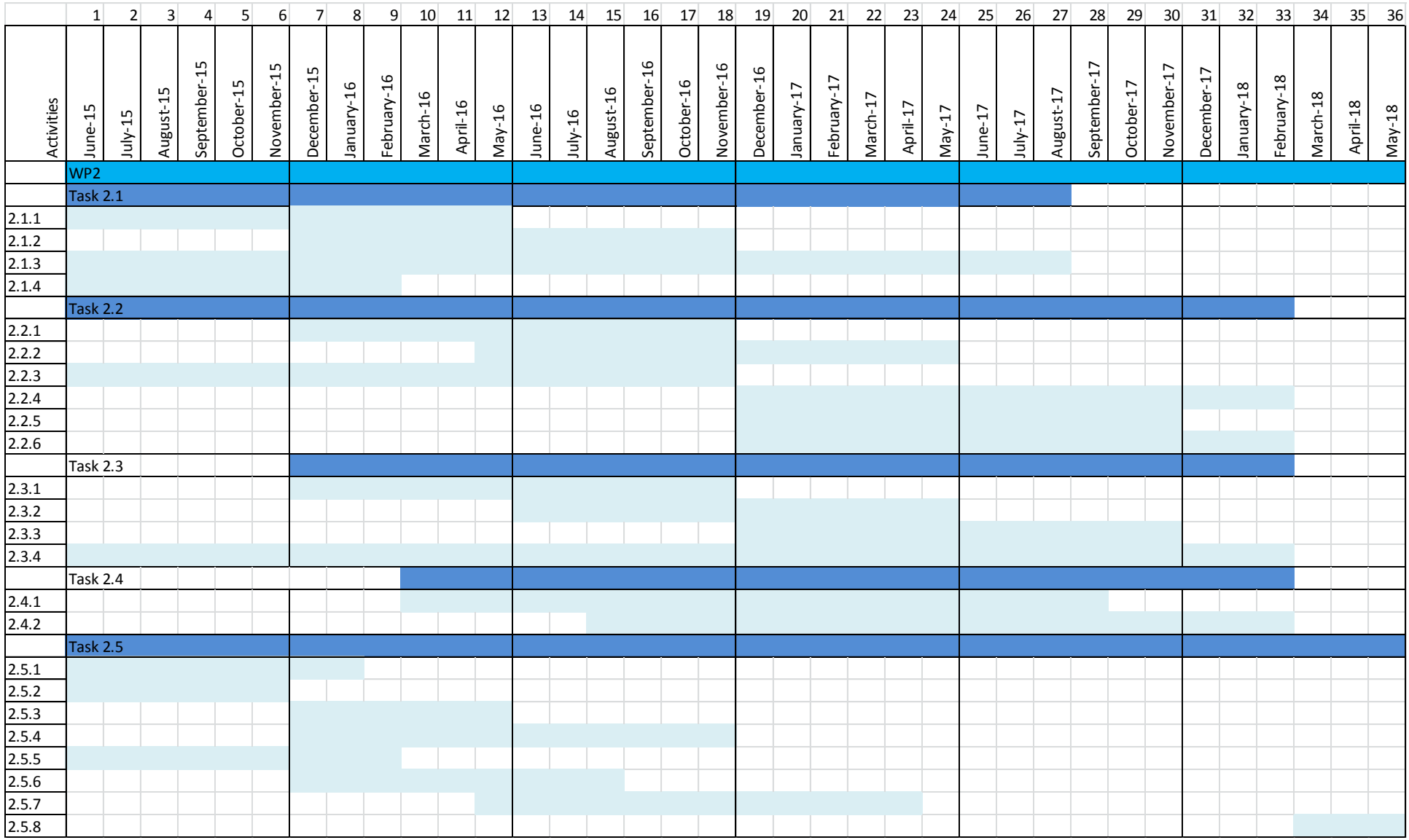
Formal reporting will be in line with EURAMET's requirements and will be submitted in accordance with the Reporting Guidelines.

C6 GANTT CHART

WP1



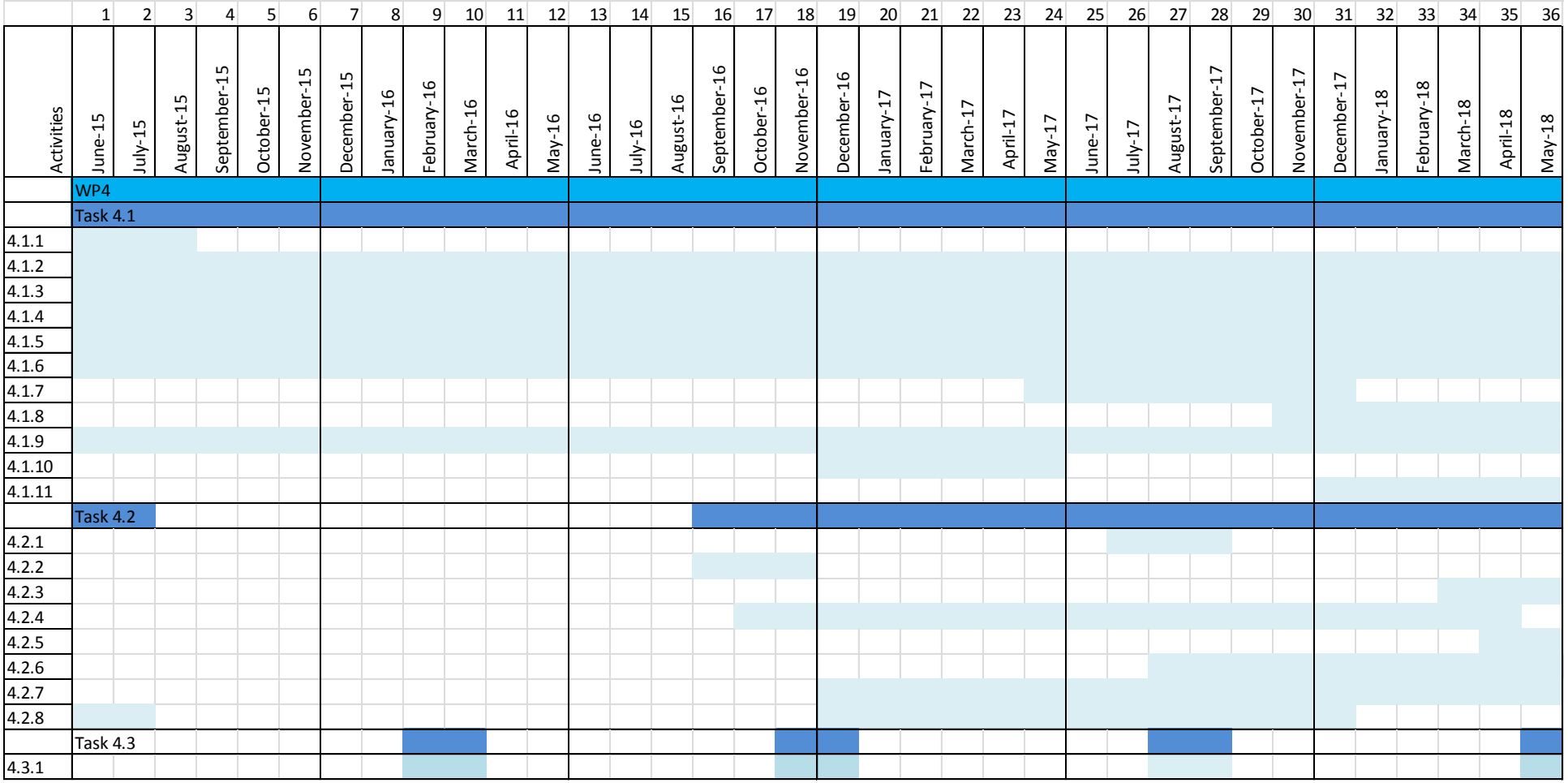
WP2


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
Activities
June-15 July-15 August-15 September-15 October-15 November-15 December-15 January-16 February-16 March-16 April-16 May-16 June-16 July-16 August-16 September-16 October-16 November-16 December-16 January-17 February-17 March-17 April-17 May-17 June-17 July-17 August-17 September-17 October-17 November-17 December-17 January-18 February-18 March-18 April-18 May-18
WP2
Task 2.1
2.1.1
2.1.2
2.1.3
2.1.4
Task 2.2
2.2.1
2.2.2
2.2.3
2.2.4
2.2.5
2.2.6
Task 2.3
2.3.1
2.3.2
2.3.3
2.3.4
Task 2.4
2.4.1
2.4.2
Task 2.5
2.5.1
2.5.2
2.5.3
2.5.4
2.5.5
2.5.6
2.5.7
2.5.8

WP3

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Activities	June-15	July-15	August-15	September-15	October-15	November-15	December-15	January-16	February-16	March-16	April-16	May-16	June-16	July-16	August-16	September-16	October-16	November-16	December-16	January-17	February-17	March-17	April-17	May-17	June-17	July-17	August-17	September-17	October-17	November-17	December-17	January-18	February-18	March-18	April-18	May-18
	WP3																																			
	Task 3.1																																			
3.1.1																																				
3.1.2																																				
3.1.3																																				
3.1.4																																				
3.1.5																																				
3.1.6																																				
3.1.7																																				
3.1.8																																				
	Task 3.2																																			
3.2.1																																				
3.2.2																																				
3.2.3																																				
3.2.4																																				
3.2.5																																				
3.2.6																																				
3.2.7																																				
3.2.8																																				
3.2.9																																				
3.2.10																																				

WP4


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
Activities
June-15 July-15 August-15 September-15 October-15 November-15 December-15 January-16 February-16 March-16 April-16 May-16 June-16 July-16 August-16 September-16 October-16 November-16 December-16 January-17 February-17 March-17 April-17 May-17 June-17 July-17 August-17 September-17 October-17 November-17 December-17 January-18 February-18 March-18 April-18 May-18
WP4
Task 4.1
4.1.1
4.1.2
4.1.3
4.1.4
4.1.5
4.1.6
4.1.7
4.1.8
4.1.9
4.1.10
4.1.11
Task 4.2
4.2.1
4.2.2
4.2.3
4.2.4
4.2.5
4.2.6
4.2.7
4.2.8
Task 4.3
4.3.1

WP5

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Activities	June-15	July-15	August-15	September-15	October-15	November-15	December-15	January-16	February-16	March-16	April-16	May-16	June-16	July-16	August-16	September-16	October-16	November-16	December-16	January-17	February-17	March-17	April-17	May-17	June-17	July-17	August-17	September-17	October-17	November-17	December-17	January-18	February-18	March-18	April-18	May-18
	WP5																																			
	Task 5.1																																			
5.1.1	X																																			
5.1.2																																				
5.1.3																																				
5.1.4																											X									
5.1.5																																				
	Task 5.2																																			
5.2.1		X																																		
5.2.2									X									X									X									X
5.2.3																																				
	Task 5.3																																			
5.3.1	X																																			
5.3.2									X									X									X									X
5.3.3																		X																		X
5.3.4																																				X

Section D: Risk and Risk Mitigation

D1 SCIENTIFIC/TECHNICAL RISKS

Risk (description)	Likelihood and impact of occurrence	Mitigation	Contingency
Task 1.1: the hybrid attenuator based on Si- and InGaAs-photodiodes with fibre coupling cannot be realised. The fibre coupling of the attenuator will fail. Its performance will also be dependent on the mechanical parameters, i.e. declination angle between diode surface and chip edges.	Likelihood without mitigation: High Impact: The impact is medium as validated measurements can still be made with commercial attenuators, but with weaker performance. Likelihood after mitigation: Low	A design specification will be written to ensure all the risk factors are assessed. The hybrid tunnel-type attenuator based on photodiodes will be fabricated by Metrosert which has experience in photodiode based attenuators. In addition, Aalto has successfully demonstrated the functioning of the control of fibre coupling.	Provide traceable on-line monitoring of bright pulses via calibrated commercial variable optical attenuators.
Task 1.1: Optical components not available from the expected provider	Likelihood without mitigation: Low Impact: Some of the planned measurements cannot be performed Likelihood after mitigation: Very low	Find another manufacturer, because components used to implement counter-measures are standard optical components.	None required as the risk is low and mitigation should avoid the need for action.
Task 1.1: Broadband spectral characterisation of some QKD components can't be realised over the complete spectral range required	Likelihood without mitigation: Medium Impact: Potential attacks exploiting spectral regions not tested cannot be excluded Likelihood after mitigation: Low	The QKD component spectral characterisation can be split among different project participants.	Optical pass band filters can be used to cover unexplored spectral regions.
Task 1.1: Development of a new SPAD front-end circuit that includes monitoring of operational conditions is unsuccessful	Likelihood without mitigation: Medium Impact: No validation of counter-measures to attack implemented in the detector. Likelihood after mitigation: Low	The monitoring of operational conditions will be performed simply by acquiring voltage values in few points of the front-end circuit.	Currently available SPAD can be used in conjunction with external monitoring equipment. An alternative approach will be considered.
Task 1.1: Development of a new security proof is not able to include all side-channel information leakage	Likelihood without mitigation: Medium Impact: Some side-channels remain outside security proof. Likelihood after mitigation: Medium	No mitigation inside the project, but stimulating activity inside the community to develop a more comprehensive security proof, or new counter-measures able to seal information leakage that cannot be treated by security proof.	No contingency. The new security proof will be effective only on a subset, albeit as exhaustive as possible, of all possible side channel leakages.
Task 1.2: Poor and unstable performance of the photon-counting system based on InGaAs/InP SPADs sinusoidally-gated at more than 1 GHz for very low after-pulsing and high count rate.	Likelihood without mitigation: Medium Impact: Non-efficient characterisation of novel high-rate single-photon detectors for fibre based QKD Likelihood after mitigation: Low	The development of this system will be focused more on the stability and suitability to QKD systems rather than on the pure performance.	A previous generation high-count rate system will be employed for preliminary characterisations.
Task 2.1: Development of calibration facility for the SPAD detection efficiency calibration fails.	Likelihood without mitigation: Medium Impact: There will be no validation of the detection efficiency calibration of single-photon detectors. Likelihood after mitigation: Low	The consortium has enough experience and knowledge in this field, so that other partners will provide significant support or even take over.	Even if the calibration facility is not be set-up, other partners will try to develop similar facilities for determining detection efficiency.

Task 2.4: Pilot comparison is not be finished during the lifetime of the project	Likelihood without mitigation: Medium Impact: Results of the pilot comparison will be published after the project limiting the impact of the project Likelihood after mitigation: Low	It is expected that at least some measurements of the pilot comparison will be finished. These results will then be published.	Only part of the measurement setups will be validated. The pilot comparison needs eventually to be finished after the project.
Task 2.5: The few photon detector does not properly work for the low photon fluxes used in free-space QKD	Likelihood without mitigation: Medium Impact: No absolute detector available. Likelihood after mitigation: Low	A few photon detectors, that required calibration relative to cryogenic radiometry, would have to be used instead.	The result of the task would be that the few photon detector is not suitable for QKD applications.
Task 2.5: In-cryo coupling of single photon sources to single mode fibres does not properly work due to demanding alignment requirements (alignment accuracy: < 5 µm).	Likelihood without mitigation: Medium Impact: Non-ideal interfacing to single-mode coupled TES detectors Likelihood after mitigation: Medium	In-cryo coupling of single photon sources to multi-mode fibres (alignment accuracy: ~ 50 µm) and external coupling to single mode fibres.	Use free-space optics to extract emission from single photon sources and use external single-mode fibre coupling.
Task 3.1: Optimal POVM for entanglement estimation either cannot be identified or cannot be realised experimentally	Likelihood without mitigation: Medium Impact: non optimal quantification of entanglement has to be performed. Likelihood after mitigation: Low	It is expected that at least a quasi-optimal measurement will be possible for polarization entangled states in A3.1.8. Quantum state tomography is still performed as a quantum state characterisation in both A3.1.6 and A3.1.8.	No further action is required, as the risk after mitigation is low.
Task 3.1: Compensation crystal parameters for asymmetric source of polarization entangled photons deviate from values provided in literature.	Likelihood without mitigation: Medium Impact: Delay of completion of the source. Likelihood after mitigation: Low	Parameters have to be adopted according to first characterisation of the source. Additional crystals have to be ordered.	Compensation crystals of different lengths and width as well as additional temperature control will be implemented to achieve compensation phenomenological in an experimental approach.
Task 3.1: Portable tomography system to quantify polarization entanglement lacks required stability	Likelihood without mitigation: Medium Impact: Delay of completion of the tomography system. Likelihood after mitigation: Low	An optical breadboard with improved passive stability will be used as optical base plate; we will fabricate special home-made mechanical holders for critical components in the setup.	If problems of stability remain, the conditions, where the system is used have to fulfil a certain standard, e.g. standard laboratory conditions in terms temperature stability.
Task 3.2: The search for a rigorous methods to estimate uncertainty in the Bell's inequalities accounting also for the detection efficiency uncertainty fails	Likelihood without mitigation: Medium Impact: The impact will be on the DI-QKD schemes but no impact for other activities of the project Likelihood after mitigation: Low	To mitigate the risks we will consider several types of Bell's inequalities. Probably some of them are more suitable for the scope.	Adopting a conservative approach to be reasonable sure of Bell' s inequalities violation: to reduce as much as possible the uncertainty and pushing the quantum efficiency well above the theoretical low limit
Task 3.2: Spatial degree of freedom result to fragile or unstable to codify qubits and propagate entanglement in fibre.	Likelihood without mitigation: Medium Impact: Not relevant for the developments of other activities of the project Likelihood after mitigation: Low	Effort will be considered in the stabilisation and instability compensation of the in fibre by a feedback control	Even if entanglement cannot be propagated in spatial degree of freedom in fibre, we could study a more robust type of non-classical correlation.

D2 MANAGEMENT RISKS

Risk (description)	Likelihood and impact of occurrence	Mitigation	Contingency
Key personnel are lost to the project.	Likelihood without mitigation: Medium None of the team members are planning to leave or retire within the project, although the possibility of ill-health or unforeseen circumstances cannot be discounted. Impact: The loss of key team members would create difficulties in delivering the project, or specific tasks or deliverables. Likelihood after mitigation: Low	Although each team member has valuable experience that is not replicated exactly by other team members, the grouping of experts within the consortium should minimise the technical areas where knowledge is held by a single person. All the partners will identify back-ups for key workers wherever possible to reduce the overall risk to the project. Project plans will be shared within the consortium and results and methodology will be documented.	If a key member leaves the project, then the partner concerned will be responsible for appointing a replacement. However this may still lead to a delay in delivery.
Complexity of managing a large consortium of participants.	Likelihood without mitigation: Medium Impact: Failure to fully cooperate or communicate effectively within the consortium could endanger efficient delivery of the project. Likelihood after mitigation: Low	The partners are all experienced at co-operating in complex multinational projects. Many have previously developed close relationships through collaborating within other European consortia; in particular the NMIs (and most of the non-NMI partners) have already well-established relations due long lasting collaboration inside previous projects (e.g. IMERA-Plus qu-Candela, EMRP IND06 MIQC). Regular communication and feedback, both in the project meetings and in between, will ensure that potential problems are identified at an early stage and that all partners are clear on their roles.	WP leaders will play an important role in flagging up potential problems to the coordinator and the project management board, who will then decide on the best course of action to take. If necessary, work will be reassigned to an alternative partner, or parts of the work re-scoped in agreement with EURAMET.
Insufficient collaboration between partners. Collaboration between the partners delivering to the work packages is insufficient due to lack of communication and dislike between the partners of the consortium	Likelihood without mitigation: Medium Most of the partners in each WP have shown to be able to collaborate well in the past projects (e.g. IMERA-Plus q-Candela, EMRP IND06 MIQC), however, the new partners will have to be incorporated into the project. Impact: Project deliverables will be delayed or even fail. Likelihood after mitigation: Low	Regular project meetings will be held ensuring a high level of collaboration and communication	The coordinator and the WP leaders will work as much as possible to minimise this risk as far as possible. However, small delays in the deliverables might still be unavoidable. If necessary, work will be reassigned to an alternative partner, or parts of the work re-scoped in agreement with EURAMET.
Inter-dependencies between technical activities and tasks are too complex	Likelihood without mitigation: Medium Impact: Tasks are delayed or are not possible to deliver. Likelihood after mitigation: Low	Technical meetings run by WP leaders have been scheduled to ensure proper sharing of knowledge. The interdependencies between tasks will be considered at meetings to ensure that this is addressed properly in the planning of the work. The technical WPs will be closely managed by their WP leaders to ensure that they deliver their own outputs.	In most cases, activities on the critical path have some overlap in time and there each one includes some independent work. Thus a delay in the output of one deliverable does not necessarily cause an immediate delay in another.

IPR: Intellectual Property Rights Problems dealing with Intellectual Property (IP) ownership and/or exploitation might occur and could be a source of potential conflict.	Likelihood without mitigation: Medium Impact: Disagreement between the partners could delay the progress of the project (in implementing the work and publishing results). Likelihood after mitigation: Low	All partners will sign the grant agreement and consortium agreement, which includes IP clauses.	Independent arbitrators will be used in the event of disagreement between partners.

D3 ETHICS

The EMPIR Ethics Review 2014 has given project 14IND05 MIQC2 “Conditional ethics clearance”.

Third Countries

The consortium will ensure that any partners or collaborators from Third Countries fully adhere to H2020 ethics standards, no matter where the research is carried out. The consortium will also, in the case of dual use applications, clarify whether any export licence is required for the transfer of knowledge or material.

Data protection

The consortium will ensure that all participants in training activities and meetings give a valid informed consent for the processing of personal data.

Dual use

The ethics reviewers identified that the project aims to address the security of data transfers through a technique called Quantum Key Distribution. The objectives do not have direct dual use implications but the research may also impact military communication and may even imply a risk of misuse by non-democratic regimes and terrorist organisations. In particular the project will also research hacking methods and the measures to be taken to secure the communication. As the dual use issue / misuse risk is not directly linked to the immediate / short term objectives of the project, the consortium must in particular address the indirect and distant implications and this must to be assessed and monitored throughout the project life time by the consortium as a contractual obligation

The consortium will assess and report on the potential of dual use applications and, if applicable, how dual use risks can be mitigated. The report will be submitted after the grant signature, with the last technical report. As the dual use issue is an ongoing issue it will be continuously assessed during the entire course of the project.

Section E: References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).

[2] 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. 81, 1301 (2009).

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

[4] I. Gerhardt et al., Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. commun. 2, 349 (2011).

[5] L. Lydersen et al., Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Phot. 4, 686 (2010).

[6] L. Lydersen et al., Controlling a superconducting nanowire single-photon detector using tailored bright illumination, New J. of Phys. 13, 113042 (2011).

[7] Y. Zhao et al., Quantum hacking: experimental demonstration of time-shift attack against practical quantum key distribution systems, Phys. Rev. A 78, 042333 (2008).

[8] Chi-Hang Fred Hung et al., Security proof of quantum key distribution with detection efficiency mismatch, Quant. Inf. & Comp. 9, 131 (2009).

[9] N. Jain et al., Device calibration impacts security of quantum key distribution, Phys. Rev. Lett. 107 110501 (2011).

[10] L. Lydersen et al., Secure gated detection scheme for quantum cryptography, Phys. Rev. A 83, 032306 (2011).

[11] H. Weier et al., Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors, New J. Phys. 13 073024 (2011).

[12] Ilja Gerhardt et al., Experimentally Faking the Violation of Bell's Inequalities, Phys. Rev. Lett. 107, 170404 (2011).

[13] F. Acerbi et al., Fast Active Quenching Circuit for Reducing Avalanche Charge and Afterpulsing in InGaAs/InP Single-Photon Avalanche Diode, IEEE J. Quant. Elect. 49, 563 (2013).

[14] A. Lamas-Linares et al., Breaking a quantum key distribution system through a timing side channel, Opt. Express 15, 9388 (2007).

[15] Sebastian Nauerth et al., Information leakage via side channels in freespace BB84 quantum cryptography, New J. Phys. 11, 065001 (2009).

[16] Hong-Wei Li et al., Attacking practical quantum key distribution system with wavelength dependent beam splitter and multi-wavelength sources, Phys. Rev. A 84, 062308 (2012).

[17] Mu-Sheng Jiang et al. , Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states, Phys. Rev. A 86, 032310 (2012).

[18] Chi-Hang Fred Fung et al., Phase-Remapping Attack in Practical Quantum Key Distribution Systems, Phys. Rev. A 75 032314(2007).

[19] Feihu Xu et al., Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. 12, 113026 (2010).

[20] Shi-Hai Sun, Mu-Sheng Jiang, Lin-Mei Liang, Passive faraday mirror attack in practical two-way quantum key distribution system, Phys. Rev. A 83, 062331 (2011).

[21] http://projects.npl.co.uk/MIQC/project.html

[22] http://www.quantumcandela.net/

[23] http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution.

[24] Net!Works White Paper on "Economic impact of the ICT sector" (October 2012) [http://www.networks-etp.eu/fileadmin/user_upload/Publications/Position_White_Papers/Net_Works_White_Paper_on_economic_impact_final.pdf]

[25] docbox.etsi.org - /Workshop/2014/201410_CRYPTO/S01_Setting_the_Scene/preneel.pdf, accessed on 2014.10.08

[26] http://www.etsi.org/news-events/past-events/770-etsi-crypto-workshop-2014

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

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

[29a] http://qolah.org/research/crypto/hacking/hack.html.

[29b] http://www.youtube.com/watch?v=5kUARd_y53w, http://www.vad1.com/lab/.

[30] S. Nauerth, et al., Air-to-ground quantum communication, Nature Photonics 7, 382–386 (2013).

[31a] http://spectrum.ieee.org/aerospace/satellites/commercial-quantum-cryptography-satellites-coming

[31b] https://www.sciencenews.org/article/quantum-cryptography-takes-flight

[31c] http://spectrum.ieee.org/tech-talk/aerospace/satellites/china-unveils-secret-quantum-communications-experiment

[32] http://quantumrepeaters.eu/index.php/qcomm/quantum-repeaters

[33] Hoi-Kwong Lo, et al., Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. 108, 130503 (2012)

[34] A. Rubenok, et al., Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attack, Phys. Rev. Lett. 111, 130501 (2013), presenting a 20 km prototype link.

[35] Yang Liu, et al., Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. 111, 130502 (2013) presenting a 50 km prototype link.

[36] M Peev et al., The SECOQC quantum key distribution network in Vienna, New J. Phys. 11 075001 (2009), http://www.secoqc.net/html/technology/network.html

[37] http://www.uqcc.org/QKDnetwork/index.html

[38] D. Stucki et al., Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New J. Phys. 13, 123001 (2011).

[39] http://www.battelle.org/our-work/national-security/tactical-systems/quantum-key-distribution

[40] T.-Y. Chen et al., Metropolitan all-pass and inter-city quantum communication network, Opt. Express 18, 27217 (2010).

[41] www.docbox.etsi.org - /Workshop/2014/201410_CRYPTO/S01_Setting_the_Scene/Gisin.pdf, accessed on 2014.10.08

[42] http://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election.html

[43] http://www.foxnews.com/scitech/2010/06/21/world-cup-security-uses-physics-thwart-hackers/

[44] http://www.computerworld.com.au/article/278658/aussie_govt_considers_quantum_leap_secure_comms

[45] I. Choi et al., Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber, Opt. Express 22, 23121 (2014).

[46] http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/About-Quantum-Information-Group/PRESS-RELEASE-Quantum-Cryptography-Goes-Mainstream/

[47] http://www.lanl.gov/discover/news-release-archive/2014/September/09-02-secure-computing.pdf

[48a] http://www.prweb.com/releases/quantum_cryptography/quantum_key_distribution/prweb10897723.htm

[48b] http://marketpublishers.com/report/industry/other_industries/quantum_cryptography.html

[49] http://www.etsi.org/index.php/technologies-clusters/technologies/quantum-key-distribution

[50] T. Lunghi, C. Barreiro, O. Guinnard, R. Houlmann, X. Jiang, M. A. Itzler, and H. Zbinden, Free-running single-photon detection based on a negative feedback InGaAs APD, J. Modern Opt. 59, 1481 (2012).

[51] A. Restelli, J. C. Bienfang, and A. L. Migdall, Time-domain measurements of afterpulsing in InGaAs/InP SPAD gated with sub-nanosecond pulses, J. Modern Opt. 59 1465 (2012).

[52] N. Namekata, S. Adachi, and S. Inoue, BUltra-low-noise sinusoidally gated avalanche photodiode for high-speed single-photon detection at telecommunication wavelengths, IEEE Photon. Technol. Lett. 22, 529 (2010).

[53] K. A. Patel, J. F. Dynes, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, Gigacount/second photon detection with InGaAs avalanche photodiodes, Electron. Lett. 48 111 (2012)

[54] J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, 2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution, Proc. SPIE 7681 “Advanced Photon Counting Techniques IV”, 76810Z (2010).

[55] Y. Liang, E. Wu, X. Chen, M. Ren, Y. Jian, G. Wu, and H. Zeng, Low-timing-jitter single-photon detection using 1-GHz sinusoidally gated InGaAs/InP avalanche photodiode, IEEE Photon. Technol. Lett., 23 887 (2011).

[56] M. Gschrey, F. Gericke, A. Schüßler, R. Schmidt, J.-H. Schulze, T. Heindel, S. Rodt, A. Strittmatter, and S. Reitzenstein, In situ electron-beam lithography of deterministic single-quantum-dot mesa-structures using low-temperature cathodoluminescence spectroscopy, Appl. Phys. Lett. 102, 251113 (2013).

[57] T. Heindel et al., Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range, New J. Phys. 14, 083001 (2012).

[58] Artur Ekert. Quantum cryptography based on Bell’s theorem, Phys. Rev. Lett. 67 , 661-663 (1991).

[59] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. 98, 230501(2007).

[60] Umesh Vazirani and Thomas Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. 113, 140501 (2014).

[61] Feihu Xu, Marcos Curty, Bing Qi and Hoi-Kwong Lo, Practical aspects of measurement-device-independent quantum key, New Journal of Physics 15, 113007 (2013).

[62] Akihiro Mizutani, Kiyoshi Tamaki, Rikizo Ikuta, Takashi Yamamoto & Nobuyuki Imoto, Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol, Scientific Reports 4, 5236 (2014)

[63] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. 112, 190503 (2014).

[64] Ch. Lim, B. Korzh, A. Martin, F. Bussières, R. Thew, and H. Zbinden, Detector Device-Independent Quantum Key Distribution, arXiv:1410.1850 [quant-ph].

[65] J-C Boileau, R Laflamme, M Laforest, and C R Myers, Robust Quantum Communication Using a Polarization-Entangled Photon Pair, Phys. Rev. Lett. 93, 220501 (2004).

[66] J Wabnig, D Bitauld, H W Li, A Laing, J L O Brien, and A O Niskanen, Demonstration of free-space reference frame independent quantum key distribution, New J. Phys. 15 073001 (2013).

[67] P Zhang, K Aungskunsiri, E Martin-Lopez, J Wabnig, M Lobino, R W Nock, J Munns, D Bonneau, P Jiang, H W Li, A Laing, J G Rarity, A O Niskanen, M G Thompson, and J L O'Brien, Reference-Frame-Independent Quantum-Key-Distribution Server with a Telecom Tether for an On-Chip Client, Phys. Rev. Lett. 112, 130501 (2014).

[68] G. Brida, et al., Experimental Estimation of Entanglement at the Quantum Limit, Phys. Rev. Lett. 104, 100501 (2010).

[69] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, Regulated and Entangled Photons from a Single Quantum Dot, Phys. Rev. Lett. 84, 2513 (2000).

[70] C J Chunnilall, I P Degiovanni, S Kück, I Müller, A G Sinclair, Metrology of single-photon sources and detectors: a review, Opt. Eng., 53(8) 081910 (2014).