EMPIR Call 2014 – Industry and Research Potential

Selected Research Topic number: **SRT-i28**
Version: 1.0

Title: Optical metrology for quantum enhanced secure telecommunication

Abstract

Quantum enhanced secure telecommunication is based on Quantum Key Distribution (QKD) which is essentially the generation of random keys between two parties that communicate by an open quantum channel. QKD can be considered as the only truly secure key distribution technology (except secret courier) as conventional asymmetrical cryptography, which is currently used for key distribution, can be rendered insecure e.g. with the use of quantum computers. Therefore, QKD technology could be used to support the competitiveness of European industry and provide improved data security in banking, commerce, government, and the transmission of personal data, i.e. medical records. However, to achieve this, a European metrology infrastructure for quantum optical technologies such as QKD, and standards for QKD are needed.

Keywords

Quantum cryptography, quantum key distribution, single photon, quantum technology, entanglement

Background to the Metrological Challenges

A Joint Communication from the European Commission to the European Parliament and Council, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace” (7 Feb 2013) explicitly names the development of cryptography as an area for support. Currently, cryptography by QKD networks has been used to secure elections in Switzerland, for public security during the 2010 World Cup and for government communications. However, widespread adoption of QKD requires validated systems that are trusted by end users, and to achieve this, QKD systems need to undergo assurance process including security specification, evaluation and certification according to a standardised methodology, as well as inter-operability of QKD systems with existing networks. In addition, QKD standards for calibration, such as standardised sets of optical components, are required.

The current state-of-the-art for QKD can be based on the achievements of iMERA-Plus JRP T1.J2.3 ‘Candela: Towards quantum-based photon standards’ (qu-Candela) and EMRP JRP IND06 ‘Metrology for Industrial Quantum Communication Technologies’ (MIQC).

JRP IND06 MIQC has developed techniques to characterise and validate optical components for 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. However, traceable calibration techniques are required for optical components such as those used for counter-measures against hacking attacks. Proofs of absolute security for QKD often assume perfect implementation of the theory behind QKD; however, QKD systems can be vulnerable to side-channel and Trojan-horse attacks due to flaws in their experimental implementation. This means that counter-measures need to be developed to counteract these hacking attacks, as well as tests of the effectiveness of the counter-measures.

QKD exploiting satellites appears to be the only viable solution for achieving QKD worldwide. The results of the iMERA-Plus JRP qu-Candela have been used to provide traceability for photon-counting regimes at wavelengths in the visible spectral range. However, measurement techniques for calibrating and validating the components of open-air QKD systems still need to be developed.

Entanglement, as in entangled states or entangling measurements, has a central role in the next generation of QKD technologies. This ranges from the development of quantum repeaters and quantum networks, to the practical application of (measurement-) device-independent QKD. However, accurate characterisation of entangled states, development of measurement techniques for entanglement quantification and/or witnessing, and for estimating the entangling-process efficiency are required.

EURAMET-MSU
National Physical Laboratory
Hampton Road, Teddington,
Middlesex, TW11 0LW, UK

Phone: +44 20 8943 6666
msu@npl.co.uk
www.euramet.org

Objectives

Proposers should address the objectives stated below, which are based on the PRT submissions. Proposers may identify amendments to the objectives or choose to address a subset of them in order to maximise the overall impact, or address budgetary or scientific / technical constraints, but the reasons for this should be clearly stated in the proposal.

The JRP shall focus on the development of metrological capacity in quantum optical technologies.

The specific objectives are

1. 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 work must include collaboration with “quantum” companies and standardisation bodies, e.g. the Industry Specification Group on QKD of the European Telecommunications Standards Institute (ETSI ISG-QKD).
2. To develop characterisation, validation, and calibration methods for single-photon sources, detectors, and other relevant optical components (e.g. polarisation controllers, intensity modulators) used in open-air visible-light QKD for their characterisation and validation.
3. To develop measurement techniques for next generation QKD systems based on the entanglement of photons. Namely, to develop the metrology of entangled photons (measurements of quantum states and of the amount of entanglement) and of other “quantumness” quantifiers.
4. To liaise with telecommunication stakeholders and end users in order to define best-practice and to implement the efficient and cost-effective measurements developed by the project to support the development of new, innovative products, thereby enhancing the competitiveness of EU industry

Proposers shall give priority to work that meets documented industrial needs and include measures to support transfer into industry by cooperation and by standardisation. An active involvement of industrial stakeholders is expected in order to align the project with their needs – both through project steering boards and participation in the research activities.

Proposers should establish the current state of the art, and explain how their proposed project goes beyond this.

In particular, proposers should outline the achievements of EMRP JRP IND06 ‘Metrology for Industrial Quantum Communication Technologies’ (MIQC) and iMERA-Plus JRP T1.J2.3 ‘Candela: Towards quantum-based photon standards’ (qu-Candela) and how their proposal will build on these.

EURAMET expects the average EU Contribution for the selected JRPs to be 1.5 M€, and has defined an upper limit of 1.8 M€ for any project.

EURAMET also expects the EU Contribution to the external funded partners to not exceed 30 % of the total EU Contribution to the project. Any deviation from this must be justified.

Any industrial partners that will receive significant benefit from the results of the proposed project are expected to be unfunded partners.

Potential Impact

Proposals must demonstrate adequate and appropriate participation/links to the “end user” community, describing how the project partners will engage with relevant communities during the project to facilitate knowledge transfer and accelerate the uptake of project outputs. Evidence of support from the “end user” community (e.g. letters of support) is also encouraged.

You should detail how your JRP results are going to:

- Address the SRT objectives and deliver solutions to the documented needs,
- Drive innovation in industrial production and facilitate new or significantly improved products through exploiting top-level metrological technology,
- Improve the competitiveness of EU industry,
- Feed into the development of urgent documentary standards through appropriate standards bodies,
- Transfer knowledge to the telecommunications sector.

You should detail other impacts of your proposed JRP as specified in the document “Guide 4: Writing Joint Research Projects”

You should also detail how your approach to realising the objectives will further the aim of EMPIR to develop a coherent approach at the European level in the field of metrology and include the best available contributions from across the metrology community. Specifically the opportunities for:

- improvement of the efficiency of use of available resources to better meet metrological needs and to assure the traceability of national standards
- the metrology capacity of EURAMET Member States whose metrology programmes are at an early stage of development to be increased
- organisations other than NMIs and DIs to be involved in the work

Time-scale

The project should be of up to 3 years duration.