EMPIR Call 2017 – Industry, Fundamental, Normative and Research Potential

Selected Research Topic number: **SRT-i21**
Version: 1.0

Title: Co-ordinated metrology to support a European test and certification infrastructure for quantum cryptography

Abstract

Secure communication is essential to individuals, businesses and governments. However, some form of current encryption is still insecure. Quantum key distribution (QKD) can be used to secure future communications. The metrology for characterising QKD components was developed in previous projects EMRP IND06 (MIQC) and EMPIR 14IND05 (MIQC2) but further development is required to establish a testing and certification infrastructure for quantum-secured communications. Therefore, proposals in response to this SRT should build the metrological tools to develop QKD transmitter and receiver modules, their secure operation in a real environment, and the metrological infrastructure necessary for establishing European testing and certification facilities.

Keywords

Quantum cryptography, quantum key distribution (QKD), single photon, quantum technology

Background to the Metrological Challenges

The Digital agenda for Europe states: “The establishment of standards will be key for the development and maturing of quantum technologies. Standards are needed to address a global market and support the emergence of supply chains and quantum technology eco-systems. Important work has already been started at the level of quantum communications, namely for Quantum Key Distribution. (…) The European Telecommunications Standards Institute (ETSI) will play a key role at global level in this effort (...)”. [1]

QKD researchers, industry and National Metrology Institutes formed the ETSI Industry Specification Group (ISG) on QKD (ETSI ISG-QKD) to define those standards. However, despite the strong industrial and governmental support for QKD, the development of testing and certification capacity to support its widespread adoption and commercialisation has only just started. Previous projects (EMRP IND06 (MIQC) and EMPIR 14IND05 (MIQC2)) developed methods for characterising the quantum-layer components, namely the single-photon sources and detectors, of fibre and free-space QKD systems. However, further work is still needed to support the metrological infrastructure necessary for establishing QKD technologies.

The current work plan of the ETSI ISG-QKD includes documents on counter-measures to Trojan-horse attacks (one type of attack on QKD systems), resistance to other types of attacks, characterisation of QKD transmitter modules, and characterisation of newly commercially available free-running solid-state and superconducting single-photon detectors. There also is a need to develop the metrological expertise and facilities to characterise QKD modules and apply that expertise to the drafting of documents by the ETSI ISG-QKD. This would provide the metrology infrastructure necessary for establishing a testing and certification infrastructure for quantum-secured communications, giving service-providers and end-users the confidence to help QKD mature into a fully-fledged European industry and revolutionising the information and communication technology (ICT) data security in Europe.

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 protocol.

The JRP shall focus on the development of validated calibration and characterisation methods to support a European test and certification infrastructure for quantum cryptography technologies.

EURAMET MSU, Hampton Road, Teddington, Middlesex, TW11 0LW, UK
Phone: +44 20 8943 6666 Email: msu@npl.co.uk
msu.euramet.org

The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

The specific objectives are

1. To develop validated methods for the characterisation of hardware vulnerabilities for practical Quantum Key Distribution (QKD) implementation security. To develop measurement techniques for the characterisation of the counter-measures implemented to nullify such vulnerabilities.
2. To develop validated methods for the characterisation of assembled QKD transmitters and receivers, in accordance with the specifications of the European Telecommunications Standards Institute Specification Group (ISG) on QKD (ETSI ISG-QKD).
3. To develop traceable calibration and characterisation methods for free-running or quasi-free-running single-photon detectors for telecom wavelengths based on semiconductor or superconductor technologies.
4. To develop the necessary metrological infrastructure for novel QKD devices, such as Device-Independent, Measurement-Device-Independent, Phase-Distributed and Continuous-Variable QKD.
5. To facilitate the take up of the technology and measurement infrastructure developed in the project by communication service providers, standards developing organisations (e.g. ETSI ISG-QKD) and end users (e.g. governments, private companies, public institutions, etc.).

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 the iMERA-Plus T1.J2.3 ‘Candela: towards quantum-based photon standards’ (Qu-Candela), EMRP JRP IND06 ‘Metrology for Industrial Quantum Communication Technologies’ (MIQC) and EMPIR JRP 14IND05 ‘Optical Metrology for Quantum-Enhanced Secure Telecommunication’ (MIQC2) and how their proposal will build on those.

EURAMET expects the average EU Contribution for the selected JRPs in this TP to be 1.5 M€, and has defined an upper limit of 1.8 M€ for this 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 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,
- Feed into the development of urgent documentary standards through appropriate standards bodies,
- Transfer knowledge to the ICT sector.

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

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.

Additional information

[1] *DIGITAL AGENDA FOR EUROPE: A EUROPE 2020 INITIATIVE, "WORKSHOP ON QUANTUM TECHNOLOGIES AND INDUSTRY",*
Final Report (6 May 2015, DG CONNECT, Avenue de Beaulieu 25, B-1049 Brussels), page 16 [available at http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=10237]