EMPIR Call 2019 – Energy, Environment, Normative and Research Potential

Selected Research Topic number: **SRT-n11**
Version: 1.0

Title: Metrology for testing the implementation security of quantum key distribution hardware

Abstract

Quantum technologies represent a major opportunity and at the same time a considerable challenge for European industry with respect to innovation and security for high-tech products. Quantum key distribution (QKD), in which Europe is the world-leader, represents a reliable candidate for the security of confidential communications between parties, preventing unauthorised access to data. However, despite strong industrial and governmental support for QKD, the development of testing, standardisation and certification capacity to support its widespread adoption and commercialisation is still in its infancy. Research is needed (i) to develop and implement robust, SI-traceable measurements at the single-photon level, to test the security of QKD systems in a real (i.e. adversarial) environment; and (ii) to provide documented input to ETSI ISG-QKD for drafting measurement standards for QKD technologies.

Keywords

Quantum Communication, Quantum cryptography, quantum key distribution, Standardisation, Single Photon, Quantum Technology, implementation security

Background to the Metrological Challenges

Quantum communications can increase data security on networks, reduce theft of sensitive information and promote trust in network-based products and services.

Quantum key distribution (QKD), in which Europe is the world-leader, represents a reliable candidate to secure future communications. In fact, QKD techniques provide primitives that are intrinsically quantum-safe, as they are based on the laws of nature rather than computation complexity. It allows key sharing over optical fibre or free-space links and can be used in a general Cyber Security framework or as a complement to current security systems. The QKD resilience from every possible attack based on quantum computers also guarantees future-proof security from attacks brought by any classical computer, including powerful supercomputers.

There is now a critical mass of European industry developing QKD systems and QKD components, and the QKD market is forecast to expand significantly in the near-term. However, the cost of transitioning to quantum safe technologies is typically high. Historically, widespread adoption of any technology is not economically feasible without standardisation. The expected growth in the future market for quantum devices assumes the availability of certified and standardised products, and technology advancements that help extend its application beyond point-to-point connections to cover global communications. Europe leads in developing globally-accepted standards and an anticipatory approach would facilitate the growth of these markets, both in Europe and worldwide. Therefore, QKD researchers, industry and National Metrology Institutes formed the ETSI ISG-QKD to define those standards. 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 layer of QKD systems. Moreover, this standardisation effort is in alignment to the Strategic Research Agenda of the Quantum Flagship.

The goal of this SRT is to build on the work of EMRP MIQC and EMPIR MIQC2 and stimulate the realisation of additional metrological techniques appropriate to real-world use, and required for standardisation, thereby accelerating the development and commercial success of QKD technologies.

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

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

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 development of SI-traceable measurements, at the single-photon level, to characterise QKD systems and technologies aligned with the actual standardisation development work of the ETSI Industry Specification Group on QKD.

The specific objectives are

1. To develop measurement standards for practical QKD Implementation Security, focusing on methods to characterise the hardware vulnerabilities of practical QKD Systems, and the counter-measures implemented against them, in order to verify their operation within the bounds of the security proofs.
2. To provide a substantial contribution to the development of traceable methods and protocols for characterisation of assembled QKD modules (i.e. transmitter and receiver), in line with ETSI documents and needs.
3. To provide a substantial contribution to the development of traceable characterisation methods for active QKD components, in line with ETSI Group Report QKD 003 (QKD; Components and Internal Interfaces), focussing on methods relevant for new, free-running or quasi-free-running single-photon detectors for telecom wavelengths based on semiconductor or superconductor technologies, promising a substantial improvement in QKD key rate.
4. To contribute to the standards development work of the ETSI Industry Specification Group on QKD to ensure the outputs of the project are being aligned technically and temporally with their needs, in a form that can be easily incorporated into the standards at the earliest opportunity.

The proposed research shall be justified by clear reference to the measurement needs within strategic documents published by the relevant Regulatory body or Standards Developing Organisation or by a letter signed by the convenor of the respective TC/WG. EURAMET encourages proposals that include representatives from industry, regulators and standardisation bodies actively participating in the projects. The proposal must name a “Chief Stakeholder”, not a member of the consortium, but a representative of the user community that will benefit from the proposed work. The “Chief Stakeholder” should write a letter of support explaining how their organisation will make use of the outcomes from the research, be consulted regularly by the consortium during the project to ensure that the planned outcomes are still relevant and be prepared to report to EURAMET on the benefits they have gained from the project.

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

In particular, proposers should outline the achievements of the EMRP IND06 MIQC and EMPIR 14IND05 MIQC2 projects and how their proposal will build on those.

EURAMET expects the average EU Contribution for the selected JRPs in this TP to be 0.8 M€ and has defined an upper limit of 1.0 M€ for this project.

EURAMET also expects the EU Contribution to the external funded partners to not exceed 30 % of the total EU Contribution across all selected projects in this TP.

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 quantum technology 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.