European Partnership on Metrology
Call 2023 –Fundamental Metrology, Industry, Normative and Research Potential

Selected Research Topic number: **SRT-i01**
Version: 1.0

Title: QKD next generation metrology: supporting QKD networks deployment

Abstract

Quantum key distribution (QKD), in which Europe is the world leader, is a hardware-based technology requiring physical measurement for its security assurance. The target environments of European quantum communication networks (e.g., EuroQCI) requiring investigation are the long-haul and metropolitan-range distances. There is a need to boost testing and certification for innovative QKD solutions such as Twin-Field and Continuous-Variable QKD, as well as investigate entanglement-based approaches that will be at the heart of the forthcoming quantum internet. This will address current and emerging measurement needs and will follow indications emerging from quantum communication standardisation efforts (e.g., by ETSI ISG-QKD and CEN/CENELEC FGQT) and is coherent with the EMN-Q strategic research agenda.

Keywords

Quantum Communication, Quantum Key Distribution (QKD), Twin-Field QKD, Continuous Variable QKD, Quantum Internet, entanglement, time/frequency transfer with fibres

Background to the Metrological Challenges

In an ever more interconnected world, cryptographic protection of data-in-transit to prevent eavesdropping becomes increasingly important. Quantum cryptography provides the absolute strongest protection against eavesdropping, and, for this reason, this field has witnessed tremendous attention in the last two decades.

Advances in quantum computation threaten the security of common classical cryptographic techniques. New cryptographic techniques exist which protect against this threat. They include ‘quantum-secured’ communication protocols based on the quantum properties of light that prevent eavesdropping (e.g., QKD) as well as new classical ‘quantum-safe’ computational techniques designed to resist quantum attacks. A combination of these two techniques provides the strongest protection and these fields have witnessed tremendous attention in the last two decades.

The EuroQCI and national quantum communication networks require a substantial metrological effort to develop SI-traceable measurements for their QKD systems. For such pan-European infrastructures, solutions able to distribute quantum cryptographic keys over long distances are of utmost importance, as well as being able to perform local distribution of cryptographic keys in metropolitan areas. For these specific objectives, there are new QKD approaches, which go beyond the current commercial point-to-point QKD solutions.

The QKD market forecast is to expand exponentially in the coming years, thanks to the planned EuroQCI and the other European national quantum communication networks deployment. Standardisation and certification are 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 worldwide. The ETSI ISG-QKD and CEN/CENELEC FGQT aim 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 aligned to the Strategic Research Agenda of the Quantum Flagship, while the dedicated traceable measurements for the QKD systems quantum optical layer are the core of the Quantum Communication roadmap of the Strategic Research Agenda of the European Metrology Network for Quantum Technologies (EMN-Q).

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 traceable measurement and characterisation of the next-generation quantum key distribution (QKD) systems for quantum communication networks in Europe.

The specific objectives are:

1. To investigate the metrological techniques required to support the development of fibre-based measure-device-independent QKD (MDI-QKD) protocols, such as twin-field QKD (TF-QKD), to establish efficient long-haul links between metropolitan networks with a reduced number of trusted nodes. To develop appropriate real-world testbeds to model and test the correlation between the communication channel length stabilisation and the transmission rate at a given loss, taking into account the estimation (at the single-photon level) of the noise photons that are present in the channel.
2. To develop dedicated measurement protocols for the characterisation of TF-QKD transmitter and receiver modules. To develop measurement methods tailored to the components and modules of TF-QKD systems, with specific focus on the estimation of losses (i.e., detection efficiencies, insertion losses, optical attenuation) and noise (detector dark counts, channel filtering factors).
3. To develop standards for fibre-based continuous-variable QKD (CV-QKD), based on homodyne detection techniques, and to support the development of prototypes and commercial products aimed at serving metropolitan-scale networks. To measure physical security parameters, characterise hardware vulnerabilities, and the countermeasures implemented against these vulnerabilities.
4. To investigate the metrological techniques required to support the development of entanglement-based QKD over standard optical fibre by characterising the co-propagation of QKD and time synchronisation signals. To optimise entanglement distribution by measuring the polarisation correlation of the entangled photons and using this to stabilise the polarisation of the propagating photons.
5. To facilitate the take up of the technology and measurement infrastructure developed in the project by standards developing organisations (ETSI ISG-QKD, CEN/CENELEC FGQT), by the European Metrology Network for Quantum Technologies and end users (e.g. QKD manufacturers).

These objectives will require large-scale approaches that are beyond the capabilities of single National Metrology Institutes and Designated Institutes. 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 EMRP IND06 MIQC, EMPIR 14IND05 MIQC2 and EMPIR 19NRM06 MeTISQ projects and how their proposal will build on those.

EURAMET expects the average EU Contribution for the selected JRPs in this TP to be 1.9 M€ and has defined an upper limit of 2.3 M€ for this project.

EURAMET also expects the EU Contribution to the external funded beneficiaries to not exceed 35 % of the total EU Contribution across all selected projects in this TP.

Any industrial beneficiaries that will receive significant benefit from the results of the proposed project are expected to be beneficiaries without receiving funding or associated 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,
- Facilitate improved industrial capability or improved quality of life for European citizens in terms of personal health, protection of the environment and the climate, or energy security,
- 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 the Partnership 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.