European Partnership on Metrology
Call 2025 – Health, Integrated European Metrology, Regulation and Research Potential

Selected Research Topic number: **SRT-s03**
Version: 1.0

Title: Metrology for QKD to support quantum communication infrastructure deployments

Abstract

As quantum computation advances, traditional cryptographic techniques are becoming insufficiently secure. Today, Quantum Key Distribution (QKD) provides the strongest possible security for distributing encryption keys and will be vital to both the security of the forthcoming 'quantum internet' and the implementation of the European quantum communication Infrastructure (EuroQCI), relying on quantum-secure ways to exchange data. Proposals addressing this topic should develop traceable methods for the testing and certification of innovative QKD solutions over metropolitan and long-haul distances, including continuous variable QKD, twin-field QKD and entanglement-based fibre QKD. Proposals should also develop the metrological techniques required to establish efficient fibre links for long-haul distances which are low-noise and highly stable.

Keywords

Continuous Variable QKD, Quantum Communication, Quantum Internet, Quantum Key Distribution, Quantum Networks, Single Photon, Twin Field QKD, Continuous Variable QKD, Entanglement-Based Fibre QKD.

Background to the Metrological Challenges

Advances in quantum computation threaten the security of traditional cryptographic techniques. A combination of Quantum Key Distribution (QKD), which provides the strongest possible security for distributing encryption keys, and new computational algorithms, designed to resist quantum attacks, provides the most robust protection. For this reason, quantum and traditional cryptography has witnessed tremendous attention in the last two decades and is the focus of work emerging from quantum communication standards groups such as CEN/CENELEC JTC 22 'Quantum Technologies', ETSI Industry Standardisation Group on QKD (ETSI ISG-QKD) and IEC/ISO JTC 3 'Quantum Technologies'. QKD has also been highlighted as part of the Strategic Research Agenda of the European Metrology Network for Quantum Technology [1].

QKD primitives are intrinsically quantum-safe, as they are based on the laws of nature. They allow key sharing over optical links and can be used on their own or as a complement to current security systems. QKD also provides future-proof security, immune to technological or scientific advances. This is the technology upon which European quantum communication networks under development, such as the European Quantum Communication Infrastructure (EuroQCI), are based. As of June 2019, all 27 EU Member States have signed the EuroQCI Declaration, signalling their commitment to the initiative, which is considered strategic to strengthen EU technological sovereignty and competitiveness, and aims to be fully operational by 2027. The goal of EuroQCI is to secure European public communication assets against cyber threats. This includes protecting sensitive government communications, as well as safeguard encryption systems and critical infrastructures, e.g. smart energy grids, telecommunications networks, healthcare facilities, etc. To enable such pan-European infrastructures, solutions for distributing cryptographic keys in metropolitan areas and over long distances, which go beyond current commercial point-to-point discrete-variable QKD (DV-QKD) solutions, are vital.

Continuous-variable QKD (CV-QKD) with Gaussian modulation of quantum coherent states is an effective solution for QKD over relatively short distances (<50 km). Its advantage over DV-QKD lies in efficient, high-rate, cost-effective detection using homodyne receivers as opposed to single-photon counters. Many experiments have demonstrated the feasibility of CV-QKD with coherent states and a number of companies have developed CV-QKD systems as prototypes or products. However, traceable measurement methods (with

EURAMET MSU,
Email: part.msu@euramet.org
Metpart.eu

European Partnership Co-funded by the European Union
METROLOGY PARTNERSHIP EURAMET

target uncertainties of 3 %) are required for physical security parameters (such as laser amplitude/phase noise, channel losses, shot and excess noise, modulation depths and accuracy, quantum efficiencies, electronic noise), as well as to characterise hardware vulnerabilities and their counter-measures. Additionally, a preliminary comparison on measuring homodyne detection parameters (e.g. quantum efficiencies) is required to demonstrate confidence in these developed methods.

Twin-field QKD (TF-QKD) promises high key rates over longer distances (>500 km in laboratory tests). However, real-world networks introduce additional noise due to environmental fluctuations and crosstalk from adjacent fibres. TF-QKD requires highly-coherent photon sources and optical-path length stabilisation for single-photon interference. Solutions have emerged from frequency metrology to improve transmission efficiency, as seen in European fibre networks, but for market success, metrics and techniques to address phase noise, phase stabilization, and transmitter/receiver characterisation are needed. Efficient long-haul fibre links need to be established between metropolitan networks with a reduced number of trusted nodes. This will require the development of metrological techniques for noise reduction in long-haul fibres and characterisation of TF-QKD modules and internal hardware (i.e. single-photon detectors, attenuated lasers, fast phase and intensity modulators, etc.), with a specific focus on the estimation of losses and noise and phase stability.

Entangled systems, in which each subsystem cannot be considered a separate entity and a measurement on one object affects the others, can also be used for QKD. When an entangled pair of objects is shared between two parties, anyone intercepting either object alters the overall system, revealing their presence (and the amount of information obtained). This kind of QKD is a prerequisite for a future ‘quantum internet’ and companies developing QKD-systems based on entanglement are already on the market, but the required metrological basis and metrics do not exist.

Since QKD systems perform security functions, security assurance is essential for their deployment. EuroQCI and national quantum communication networks require a substantial metrological effort to develop SI-traceable measurements for testing and validating quantum hardware. The European Commission has pushed QKD researchers, industry and National Metrology Institutes to create standards, and a testing and measurement infrastructure for QKD. It is timely that the supporting metrology should now be implemented to support these novel QKD solutions through their product lifecycle, from conception, to new device development, design, testing, implementation, certification and deployment for real applications.

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 proposal shall focus on the development of traceable measurements for Quantum Key Distribution.

The specific objectives are

1. To develop metrology for fibre-based continuous-variable QKD (CV-QKD) in the telecom band, based on weak coherent states and homodyne/heterodyne detection techniques, to support the development of prototypes and commercial products to serve metropolitan-scale networks. This includes traceable measurements of physical security parameters, characterisation of hardware vulnerabilities and counter-measures implemented against these vulnerabilities, with a typical target uncertainty of 3 %.
2. To investigate the metrological techniques and develop the dedicated measurement protocols required to support the development of fibre-based measure-device-independent QKD (MDI-QKD) protocols in the telecom C-band, such as twin-field QKD. This includes efficient long-haul fibres links between metropolitan networks with a reduced number of trusted nodes, metrological techniques for noise reduction in long-haul fibres and characterising TF-QKD modules and internal hardware.
3. To develop the metrology required for entanglement-based fibre QKD in the telecom O- and C-bands. This includes characterising (with target uncertainty of 3 %), entangled photon-pair sources (EPPSs), and the co-propagation of QKD and background photons in the channel. Additionally, optimising entanglement distribution by measuring the correlation of the entangled photon observable (e.g. polarisation), stabilising this over the fibre link distance and validating the results.
4. To demonstrate the establishment of an integrated European metrology infrastructure and to facilitate the take up of the technology and measurement infrastructure developed in the project by the measurement supply chain, standards developing organisations (CEN CENELEC, ETSI, IEC, ISO) and end users (EuroQCI, QKD system developers).

These objectives will require large-scale approaches that are beyond the capabilities of single National Metrology Institutes and Designated Institutes. To enhance the impact of the research work, the involvement of the larger community of metrology R&D resources both within and outside Europe, plus engagement with existing European research infrastructures and European Partnerships is recommended. A strong industry involvement is expected in order to align the project with their needs and guarantee an efficient knowledge transfer into industry and end users. Where relevant, proposals are encouraged to build on, or seek collaboration with, existing projects and develop synergies with other relevant European, national or regional initiatives and funding programmes. In particular, links are encouraged with (i) the projects funded under earlier relevant topics of the Horizon Europe programme; or (ii) other relevant European Partnerships.

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 and EMPIR projects IND06 MIQC, 14IND05 MIQC2 and 19NRM06 MeTISQ and how their proposal will build on those.

Proposers should note that the programme funds the activity of researchers to develop the capability, not the required infrastructure and capital equipment, which must be provided from other sources.

EURAMET expects the average EU Contribution for the selected JRPs in this TP to be 2.1 M€ and has defined an upper limit of 2.6 M€ for this proposal.

EURAMET also expects the EU Contribution to the external funded beneficiaries to not exceed 25 % 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 proposal's 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 security and communication sectors.

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 Metrology 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.

Timescale

The project should be of up to 3 years duration.

Additional information

The links provided in this section are only correct at the time of publication up until the end of the Call year.

These references have been provided by EURAMET.

[1] EMN Quantum Technologies Strategic Research Agenda https://www.euramet.org/research-innovation/metrology-partnership/strategic-research-and-innovation-agendas.