EMRP Call 2010 – Industry & Environment

Topic number: SRT-26i

Title: Metrology for industrial quantum communication technologies

Abstract

Today's society faces a challenge of developing future proof data security and data transfer. This challenge can be met, in principle at least, by the use of quantum communication technologies. The quantum industry comprises of a number of well-established companies with quantum research groups, supplemented by smaller spin off companies and university research groups. Quantum communication technology is now close to market, and despite Europe's leading position in quantum key distribution (QKD) technologies, there are currently no methods to ensure that these quantum devices meet the demands of QKD. The industry requires the development of specific and challenging measurement techniques, to ensure devices conform to standards, and the proposed JRP should aim to provide the necessary measurement infrastructure to foster development and market take up of quantum communication technologies; setting a foundation for a robust quantum communication industry.

Conformity with the Work Programme

This Call for JRPs conforms to the EMRP 2008, in the sections on "Photometry and Radiometry" p12

> "Quantum-photon based standards for optical radiation. Communication technologies, high speed communication, quantum computing require characterisation and development of single photon sources, detectors, optical fibres and all-in fibre distribution",

and p34

> "Towards Quantum-photon based standards for optical radiation: the development and validation of quantum optical metrology tools for communication technologies, quantum computing and cryptography is a long-term goal of the EMRP. Single photon sources, detector characterisation and application, will include photon counting from very low levels to conventional radiometry."

Keywords

Quantum Cryptography, Quantum Key Distribution, Single Photon Source, Single Photon Detector, Photon Number Resolving Detector, Optical Fibre

Background to the Metrological Challenges

Data protection, privacy and security are important issues to prevent unauthorised access to communications, and secure confidentiality of communications. Quantum Key Distribution (QKD) is essentially the generation of perfect random keys between two parties that are connected by a quantum channel. QKD with its strong long-term security perspective is an important building block for dependably secure communication networks. It has the potential to increase usability and acceptance for typical services of the Information Society of today and in the near and long term future.

The European Commission supports the standardisation of QKD not only from the technological point of view, but also from the business point of view. The lead market initiative aims to accelerate the emergence of innovative market areas through the close coordination of innovation policy instruments.

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

Phone: +44 20 8943 6666
emrpA169@npl.co.uk
www.euramet.org

EMRP
European Metrology Research Programme
Programme of EURAMET

The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union

Irrespective of the technologies used, there are quantum devices that appear in most QKD systems, each of these components require the relevant properties to be identified that may be subject to standardisation. Sources, quantum channels and detectors play an especially important role in quantum information theoretical security proofs, which are ultimately based on assumptions on particular properties of these components. The characteristics of quantum optical components are crucial for security analysis on the quantum optical level. The identification of relevant resources, their standardisation and the development of appropriate measurement techniques for their metrological characterisation enable the efficient specification of generic security requirements for QKD systems.

Scientific and Technological 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 JRP protocol.

The overall aim of the JRP is to foster development of new industrial quantum communication technologies aimed at achieving maximum impact for the European industry in this area. Successful development of such new technologies and products requires a solution to a number of metrological challenges in QKD technologies.

The specific objectives are

1. Traceable characterisation of photon sources with unknown quantum states, including measurement of the mean number of photons per pulse, reconstruction of the probability of emitting a certain number of photons per pulse, and quantum tomography of the quantum states.

2. Realisation of optimised single-photon sources as a reference for the quantum source.

3. Traceable characterisation of quantum channels for optical fibre based communication systems, including decoherence quantification, quantum process tomography related to the propagation of states inside optical fibres, and non-local evolution of an entangled state propagating in optical fibre.

4. Traceable characterisation of commercial single-photon detectors, including quantum efficiency, timing jitter, dead-time, after-pulsing, dark counts and saturation. Identification and standardisation of the definitions specific to quantum detection at single-photon level.

5. Determination of the properties of photon-number-resolving detectors capable of observing more than one photon in a pulse. Identification and standardization of the definitions specific to quantum detection at few-photon level.

Proposers shall give priority to work that meets documented industrial needs and that which supports transfer into industry e.g. by cooperation and/or by standardisation.

Proposers should establish the current state of the art, and explain the scientific and technological steps of their proposed project that go beyond this. Proposers must ensure that they are familiar with the existing EURAMET funded Joint Research Projects (link below); proposers must explain how their project builds on and differs from the previously funded work.

- T1.J2.3 Qu-Candela “Candela: towards quantum-based photon standards” http://www.quantumcandela.org/

Potential Impact

Proposals must demonstrate adequate and appropriate participation/links to the “end user” community. This may be through the inclusion of unfunded JRP partners or collaborators, or by including links to industrial/policy advisory committees, standards committees or other bodies. Evidence of support from the “end user” community (e.g. letters of support) is encouraged.

Where a European Directive is referenced in the proposal, the relevant paragraphs of the Directive identifying the need for the project should be quoted and referenced. It is not sufficient to quote the entire Directive per se as the rationale for the metrology need. Proposals must also clearly link the identified need in the Directive with the expected outputs from the project.

In your JRP submission please detail the impact that your proposed JRP will have on the following Directives (full references at end)

- Directive 2002/58/EC " Concerning the processing of personal data and the protection of privacy in the electronic communications sector"
- Directive 1999/93/EC "on a Community framework for electronic signatures"

You should also detail other impacts of your proposed JRP as detailed in the document "Guidance for writing a JRP"

You should detail how your JRP results are going to:

- feed into the development of standards through appropriate standards bodies
- transfer knowledge to the secure communications sector.
- Link to the EC's "ICT Standardisation Work Programme" http://ec.europa.eu/enterprise/sectors/ict/files/2010-2013_ict_standardisation_wp_en.pdf
- link to and build on the existing EMRP funded project Qu-Candela.

You should also detail how your approach to realising the objectives will further the aim of the EMRP to develop a coherent approach at the European level in the field of metrology. 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 Member States and countries associated with the Seventh Framework Programme whose metrology programmes are at an early stage of development to be increased
- outside researchers & research organisations other than NMIs and DIs to be involved in the work

Time-scale

The project should be of 3 years duration.

Additional information

Most of the references were provided by PRT submitters; proposers should therefore establish the relevance of any references.

Directives:

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF

[3] The European Commission's "ICT Standardisation Work Programme 2010 – 2013 http://ec.europa.eu/enterprise/sectors/ict/files/2010-2013_ict_standardisation_wp_en.pdf

Other References:

[4] Dusek M, Lütkenhaus N and Hendrych M 2006 Quantum Cryptography Progress in Optics vol 49 ed E Wolf (Amsterdom: Elsevier) pp 381–454

[5] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys 74 145–95

[6] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) 2007 Off. J. Eur. Union D Celex number 52007DC0228

[7] http://www.secoqc.net ; Alléaume R, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H and Zeilinge A 2006 SECOQC White Paper on Quantum Key

Distribution and Cryptography arXiv:quant-ph/0701168; Ghernaouti-Hélie S, Tashi I, Länger T and Monyk C 2009 SECOQC Business White Paper arXiv:0904.4073 [quant-ph]

[8] http://portal.etsi.org/portal/server.pt/community/QKD/328

[9] Länger T, and Lenhart G 2009 Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD, New Journal of Physics 11, 055051

[10] http://math.nist.gov/quantum/overview.html

[11] EMRP funded project T1.J2.3 Qu-Candela "Candela: towards quantum-based photon standards" http://www.quantumcandela.org/