Publishable Summary for 19NRM06 MeTISQ
Metrology for Testing the Implementation Security of Quantum Key Distribution Hardware

Overview

Most of the world's cybersecurity infrastructure is based on the exchange and use of digital cryptographic keys. This has been very effective so far, however advances in quantum computing have dramatically raised the threat to this infrastructure. Quantum Key Distribution (QKD) is considered as the unique information-theoretic secure key distribution technology, as it relies on fundamental laws of quantum mechanics. This project aims to develop robust, SI-traceable measurements, at the single-photon level, to characterise QKD systems and technologies. The developed methods will be used to lead the drafting of measurement specifications and standards by the ETSI Industry Specification Group on QKD.

Need

Data is one of the world's most valuable commodities – affecting every person, every company, every government, everywhere. Never before has it been so important to store and communicate this data in a secure manner. The race is on to develop and establish cryptographic systems safe against the development of the quantum computer. A quantum computer will - in principle - be able to decrypt all the confidential information which was previously encrypted. Government security agencies have called for a move to a quantum-safe solution: QKD represents a building block for high security information and communication technology systems.

QKD operates in the single-photon regime, and distributes secret digital keys over optical links. Uniquely, it provides protocols whose security can be proven by the laws of nature, rather than by relying on unproven assumptions about the computational resources available to an adversary. Although QKD protocols can be proven unconditionally secure in theory, *in practice* any deviations of the real system from the idealised model could introduce vulnerabilities.

For QKD technology to become a viable real-world solution, end-users need confidence in it, and this requires its physical characterisation (i.e. metrological characterisation of physical parameters of the practical QKD system devices).

The industry is developing rapidly, and a metrological effort is now highly requested to: (i) characterise QKD modules, their vulnerabilities and counter-measures to them, together with documentary standards on measurement for practical QKD Implementation Security: (ii) develop traceable methods and protocols for characterisation of assembled QKD modules of complete QKD systems; (iii) develop traceable characterisation methods for active QKD components, such as recently-commercialised novel detectors for QKD, and that promise higher speed rate in QKD sessions.

Objectives

This project focuses on the development of SI-traceable measurements, at the single-photon level, to characterise QKD systems (assembled transmitter and receiver modules) and technologies aligned with the actual standardisation development work of the ETSI Industry Specification Group on QKD.

The specific objectives of the project are:

1. To develop and document measurement procedures for practical assessment of QKD Implementation security, focusing on methods to characterise the hardware vulnerabilities of practical QKD systems

for at least 2 prominent attacks (e.g. detection efficiency mismatch, bright light or back-flashes) targeting single photon detectors, and the current best engineering practice to mitigate them.

2. To provide a substantial contribution to the development of traceable methods and protocols for the 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 (1550 nm) based on semiconductor or superconductor technologies, promising a substantial improvement in QKD key rate with target uncertainties of 2 %.
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.

Progress beyond the state of the art and results

Despite a strong industrial drive, the development of a certification infrastructure to support the widespread adoption and commercialisation of QKD has just begun. The previous projects EMPR IND06 MIQC and 14IND05MIQC2 developed methods for characterizing the quantum-layer components, i.e., all the parts that compose a QKD module and contribute to its overall behaviour. However, the test of the components can hardly lead to the certification of the complete QKD modules, because an assembled QKD device is not simply related to the sum of its inner components.

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 and receiver modules, and characterisation of newer, commercially available, free-running single-photon detectors. This project is closely aligned with this work-plan and will therefore directly benefit the designated Chief Stakeholder of this project, ETSI.

In more detail, the expected results for each objective are described in the following.

To develop measurement standards for practical QKD Implementation Security (Objective 1)

The project develops methods to characterise hardware vulnerabilities on the receiving side of practical QKD systems, where active components like sensitive single-photon detectors (such as fast-gated single-photon detectors) are placed, and develop and characterise countermeasures to nullify them.

To provide a substantial contribution to the development of traceable methods and protocols for characterisation of assembled QKD modules (Objective 2)

The characterisation at the single-photon level of whole assembled QKD modules, as proposed in this project, is new and the methods developed will feed into a work-item recently initiated by the ETSI ISG-QKD (on characterisation of QKD transmitters) and a planned work-item on receivers. The objective will be accomplished by developing the necessary measurement methods and instrumentation, and introducing a testing modality in existing QKD modules that allows a third, independent, party to test the most important features of such modules.

To provide a substantial contribution to the development of traceable characterisation methods for active QKD components (Objective 3)

Single-photon detector technology is evolving rapidly. New, free-running or quasi-free-running single-photon detectors for telecom wavelengths based on semiconductors (InGaAs/InP SPADs) or superconductors (SNSPDs) promise a substantial improvement in QKD key rate, but their properties and operation modes present many measurement challenges. It is particularly important to develop measurement techniques for the new SNSPD detectors, which have extremely high efficiency and low jitter.

To contribute to the standards development work of the ETSI Industry Specification Group on QKD (Objective 4)

The main expected results related to this objective are to select from among the available methods that are amenable to standardisation, the ones that offer the best route to test the vulnerabilities of practical assembled QKD modules and increase their security. These methods are essential to develop the certification process for QKD and are aligned with the current work plans of the ETSI ISG-QKD.

Impact

The outputs from this project will contribute to the necessary metrological foundations for the certification of QKD, which already started with the previous projects EMRP IND06 MIQC and EMPIR 14IND05 MIQC2, and hence the work of the ETSI ISG-QKD to drive this certification process, which needs dedicated traceable measurement techniques (standards) to promote market uptake of the technology.

Impact on industrial and other user communities

There is now a critical mass of European industries developing QKD systems and QKD components (QT Ecosystem). The presence, in this consortium, of two key European QKD manufacturers (ID Quantique and TOSHIBA), as well as single-photon detector manufacturers (MPD and ID Quantique), and of a standardisation body (ETSI) as Chief Stakeholder, ensures developed measurement procedures are suitable, practical and economic for adoption by industry and certification laboratories, and will impact on industrial requirements during the lifetime of the project.

In this scenario, the MeTISQ project will directly support relevant user communities, on the basis of their specific needs, by means of the following expected outputs: (i) development of methods to characterise hardware vulnerabilities, and the current best engineering practice to mitigate them, as identified in the ETSI ISG-QKD documents on implementation security; (ii) substantial contribution to the development of traceable methods and protocols for the characterisation of the performance of assembled QKD modules; (iii) development of characterisation techniques both for SNSPDs, and fast-gated SPADs.

These methods are essential to a certification process able to provide assurance on QKD-based security solutions, leading in turn to increased confidence in the security of fibre QKD systems, and improved competitiveness of European quantum industry.

Impact on the metrology and scientific communities

The seven NMI partners of this project are members of the Consultative Committee on Photometry and Radiometry (CCPR), and they have incorporated photon-based quantities into the strategic planning of the CCPR. They are also members of the EURAMET Technical Committee for Photometry and Radiometry, and thus able to influence the work within this committee. The same seven partners are also members of the recently established European Metrology Network for Quantum Technologies (EMN-Q). Input from its engagement with stakeholders and the development of its Strategic Research Agenda will be used by this project to guide any re-adjustment of this project's work-plan to meet evolving requirements. The relationship with EMN-Q will provide a link to the EU Quantum Flagship.

Impact on relevant standards

This project will enable Europe to continue leading the development of measurement-related QKD standards, appropriate to European and global market needs.

The MeTISQ project is closely aligned with the work-plan of ETSI Industry Standardisation Group on QKD (ETSI ISG-QKD), the longest existing international standardisation initiative for QKD. In particular, Toshiba (TEUR), ID Quantique, INRIM, NPL, and PTB are all active members of the ETSI ISG QKD and TEUR is the current Chair, providing metrology leadership for the drafting of specifications and standards concerned with characterisation, validation, and certification of the optical layer of QKD systems and networks. The strong collaboration with ETSI ISG-QKD activities will continue for the duration of the project, and project objectives may be modified in line with indications from the ETSI ISG-QKD. The outcomes from this project will directly influence the current and future versions of the (pre-standard) ETSI ISG-QKD documents.

Longer-term economic, social and environmental impacts

The outputs of this project will support the development of a European test and certification infrastructure to enable the deployment of QKD. A European lead in developing globally accepted standards and an anticipatory approach will aid the development of the quantum communication ecosystem and achieving the projected growth in market value of QKD technologies (establishment of QKD-based secure communication; future Pan-European Quantum Communications Infrastructure).

Deployment of validated QKD systems will encourage and accelerate the use of network communications and services *(e.g. secure video conferencing and secure data transfer of important documents, thereby reducing need to travel to face-to-face meetings).*

List of Publications: -

<table>
<tr><td colspan="2">Project start date and duration:</td><td>1 September 2020, 36 Months</td></tr>
<tr><td colspan="3">Coordinator: Marco Gramegna, INRIM Tel: +390113919245 E-mail: m.gramegna@inrim.it
Project website address: www.euramet.org/project-19nrm06</td></tr>
<tr><td colspan="2">Chief Stakeholder Organisation: ETSI - European Telecommunications Standards Institute</td><td>Chief Stakeholder Contact: Hakim Mkinsi</td></tr>
<tr><td>Internal Funded Partners:
1. INRIM, Italy
2. Aalto, Finland
3. CMI, Czech Republic
4. Metrosert, Estonia
5. NPL, United Kingdom
6. PTB, Germany</td><td>External Funded Partners:
7. IDQ, Switzerland
8. MPD, Italy
9. PoliMi, Italy
10. TEUR, United Kingdom</td><td>Unfunded Partners:
-</td></tr>
<tr><td colspan="3">RMG: -</td></tr>
</table>