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

Overview

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. 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. This project aims to develop robust, SI-traceable measurements, at the single-photon level, to characterise quantum key distribution (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 expertise gained in developing the measurements for practical QKD implementation security will be used to lead the drafting of measurement specifications and standards by the European Telecommunications Standards Institute Industry Specification Group on QKD (ETSI ISG-QKD), the principal stakeholder of this project.

Need

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. Therefore, to prevent disruption in the confidentiality of our cybersecurity systems, the time for action is now. Finding new solutions that protect against quantum attacks is a hot topic for everyone in the cybersecurity industry. Further, the implementation of new solutions requires a significant investment and trust. This trust is provided by standardisation and certification.

Tools for characterising devices and modules to advance their development, alongside standards and certification to provide independent assurance to end-users (corporate, government, banks and financial institutions, network providers, medical centres, data centres, etc.), will accelerate market take-up, maintain European competitiveness in the provision of quantum-safe technologies and ultimately protect the data of every citizen. Government security agencies have called for a move to a quantum-safe cryptographic solution. New cryptographic techniques defined as "quantum safe" are under development to protect against the threat brought to conventional cryptography by a quantum computer or by a sudden progress in solving complex mathematical problems. These techniques include algorithmic encryption, often called "post-quantum cryptography" (PQC), and schemes based on the principles of physics, most notably "quantum key distribution (QKD)". 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, such as the mean photon number statistics, the characterisation of light signals at the single-photon level, spectral/temporal properties of emitted single-photons and of the detectors, the degree of indistinguishability between supposed identical qubits, etc.). Earlier projects EMRP IND06 MIQC and EMPIR 14IND05 MIQC2 improved traceability in the photon-counting regime and developed measurements to characterise QKD components. Their outputs were implemented into published ETSI Group Specification GS QKD 011.

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 ISG-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

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 14IND05 MIQC2 developed methods for characterizing quantum-layer components. 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 attacks on QKD systems, characterisation of QKD 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, and is bringing advances in different areas, concerning:
1) development of 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 SPAD) are placed, and identification and characterisation of countermeasures to nullify them;

2) characterisation at the single-photon level of whole assembled QKD modules is new and the methods developed will feed into the ETSI ISG-QKD work-item on characterisation of QKD transmitters and a planned work-item on receivers;

3) development of dedicated measurement techniques for new, free-running or quasi-free-running single-photon detectors for telecom wavelengths based on semiconductors (InGaAs/InP SPADs) or superconductors (SNSPDs), devices that promise a substantial improvement in QKD key rate;

4) selection 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.

Results

The expected and preliminary results for each declared objective of the project are described in the following:

1. *To develop measurement standards for practical QKD Implementation Security:*

In order to develop methods to characterise hardware vulnerabilities in QKD systems, and to identify countermeasures to nullify them, an apparatus to characterise the phase relationship between pulses emitted by QKD transmitters was recently developed and is being used to test QKD modules. In parallel, measurement activities to investigate back-flash emission of both new-generation free-running and fast-gated InGaAs/InP SPADs started. Two main outputs were completed and published as co-authored joint open access peer-reviewed publications (listed in the bibliography section), as described in the following:

a) An experimental study on real-world implementation of Twin-Field QKD as anti-hacking-detectors solution. TF-QKD represents one of the most promising technique for the practical implementation of distribution of intrinsically secure encryption keys by optical means on long-distance fibers. The operated approach took advantage of interferometry techniques derived from frequency metrology, and by exploiting a suitable solution designed in the project for the simultaneous key streaming and channel length control, the TF-QKD communication was demonstrated on a 206 km field-deployed fiber with 65 dB loss. This technique permits to reduce the quantum-bit-error-rate contributed by channel length variations to <1%, representing an effective solution for real-world quantum communications. It is worth to notice that this research allowed also the first tests of coexistence in the same Quantum Backbone fibre infrastructure of both Quantum Time Distribution and QKD.

b) An experimental study on the detection of ultra-weak laser pulses by free running single-photon detectors allowed the characterisation of the detection efficiency of a fibre-coupled free-running InGaAs-Single-Photon Avalanche (SPAD) detector (ID 220) and a gated InGaAs-SPAD (ID 201). The setup was based on the double attenuator technique And the characterisation performed at 1550 nm, mean photon numbers up to 10, and relative uncertainty of less than 2 %. The model will be useful to detect any deviation from the ideal behaviour that can be exploited by an eavesdropper to gain information about the system.

Moreover, in the context of Objective 1, advances in the studies on implementation security are going to be reached. In general, the outcomes from both the reported and future results are are potentially useful to update the current stable draft versions of ETSI DGS/QKD 010 and DGS/QKD 013 documents.

2. *To provide a substantial contribution to the development of traceable methods and protocols for characterisation of assembled QKD modules:*

A polarimeter operating at single-photon level exploiting two fibre-coupled single-photon detectors and dedicated electronics allowing synchronisation with the QKD transmitters was developed. Two early uptakes of exploitable results of the project emerged in achieving this objective, as descibed in the following:

a) The realisation of a Trusted Node for QKD implemented in the Italian Quantum Backbone (I-QB), infrastructre realised, deployed and coordinated by a partner of the consortium. The Trusted Node station integrating classical cryptography with QKD systems was completed in collaboration with an external Company operating in the industry of telecommunication protection and cybersecurity, part of one of the major European telecom operators. This facility consists of 2 Commercial QKD point-to-point links plus the classical communication system able to create a common crypto-key between site A and site C (given site B the trusted node). The quantum fiber-optic I-QB infrastructure uses commercial fibers, and is deployed all along the Italian peninsula for a total length of 1850 km. Originating from fibre-optic infrastructure used for the dissemination of precise time and frequency signals generated by atomic clocks, it is being upgraded to include quantum channels suitable for QKD.

b) The realisation, in collaboration between partners of the Consortium and Telsy, a Company operating in the industry of telecommunication protection and cybersecurity, of a portable optical time domain reflectometer (SP-OTDR) apparatus, operating at single-photon level in the telecom wavelengths (1310 nm and 1550 nm). The SP-OTDR results to be a fundamental and invaluable device exploitable for the investigation of possible weak points of practical implementations of QKD systems, optical links and networks, allowing their characterisation at photon counting regime with an unprecedented precision.

Both the trusted node for QKD implemented in the I-QB and the SP-OTDR are completed, operational and already included in the platform of facilities and services that the EMN-Q will provide to users and stakeholders.

Moreover, it is worth to mention that in the context of Objective 2, advances in the definition of necessary measurement methods and instrumentation, together with testing modality -under development in the context of this project - in existing QKD modules allowing a third, independent, party to test the most important features of such QKD modules are going to be reached. To this purpose, relevant degrees of freedom that could be studied by implementing a repetitive test pattern in the evaluation of the QKD transmitter were envisaged, and preliminary measurements performed. Outcomes from both these reported and future results are potentially useful to update the current stable draft versions of ETSI DGS/QKD 010 and DGS/QKD 013 documents.

3. *To provide a substantial contribution to the development of traceable characterisation methods for active QKD components:*

In the context of objective 3, two different facilities were completed for traceable calibration and characterisation of single-photon detectors based on both superconductor (SNSPD: superconducting nanowire single-photon detector) and semiconductor (InGaAs/InP SPAD) technologies, together with the realisation of a novel fast-gated detector, where a period wave enables an InGaAs/InP SPAD at a repetition frequency higher than 1 GHz, as described in the following:

a) The set-up of calibration facility based on the double attenuator calibration method traceable to the cryogenic radiometer for the calibration of the detection efficiency of SNSPD at the wavelength of 1550 nm has been set-up. The facility is equipped with a polarisation controller for evaluating the detection efficiency polarisation dependence. The calibration of this apparatus is on-going, and in particular it will be taken into account the polarisation dependent influences and fibre connector losses. The target relative standard uncertainty is 2 %.
b) The set-up for the calibration of the detection efficiency of a free-running fiber-coupled InGaAs SPAD detector. The light source used in this setup was a sub-ns laser source based on a distributed-feedback laser diode operating at a wavelength of 1550 nm. The uncertainty evaluation was performed following the GUM guidelines. For this purpose, a new evaluation model developed in this project (reported below in bibliography). The relative uncertainty achieved was less than 2 %. These measurement capabilities have been implemented in a calibration facility for the characterisation of (single-mode) fiber-coupled single photon detector operating at telecom wavelenths (around 1550 nm). This facility represents an exploitable result oft he project.
c) The development of the fast-gated detector based on an InGaAs/InP SPAD sinusoidally-gated at more than 1 GHz has been completed and the experimental measurements showed good results in terms of count rate (up to 650 Mcps) and afterpulsing probability. An optical fibre receptacle has been developed and mounted in front of the detector for facilitating its use in the following activities with SMF 28 fibres.

Outcomes from both these reported and future results are potentially useful to update the current stable draft version of ETSI DGS/QKD 010 and DGS/QKD 013 documents.

Impact

The outputs from this project are contributing 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. At this stage, the project contributed to: 5 open access peer-reviewed; 28 conference presentations and 19 other dissemination activities; 2 early uptakes in collaboration with external companies, and related to 2 facilities now completed, operational and already included in the platform of facilities and services that the EMN-Q will provide to users and stakeholders; 3 exploitable results. Representatives of the consortium regularly attended the meeting of 3 unique standardisation committees, providing 71 inputs to the relative working groups and in particular provided 4 stable drafts of relevant ETSI ISG-QKD documents.

It is worth to notice that MeTISQ partners actively contributed also to the standardisation activities of ISO/IEC and CEN CENELEC. In the specific, contributions were provided to drafting the documents: “Security requirements, test and evaluation methods for quantum key distribution”, ISO/IEC 23837-1 and 23837-2. On the other side, thanks also to the tight synergy with EMN-Q, outcomes of the project were provided in particular

to the Quantum Communication Working Group (and to the Quantum Metrology, Sensing and Enhanced Imaging WG) of the CEN CENELEC FGQT (operational in the period: May 2020-February 2023), that recently published a review paper on EPJ-QT (listed in the bibliography below) and the documents *CEN CENELEC FGQT Q04 Standardization Roadmap on Quantum Technologies (Release 1)* and *Q05 Quantum Technologies Use Cases (Release 1*), thanks to which the CEN and CENELEC BTs established the CEN-CENELEC/JTC 22 on Quantum Technologies (kickoff in March 2023).

Moreover, the consortium engaged with more than 45 Stakeholders, and it is worth to mention that it is now collaborating with relevant Stakeholders to provide metrological and standardisation support to studies for the deployment of European Quantum Communication Infrastructure (EuroQCI), coordinated by the EU Commission, that aims to build a secure quantum communication infrastructure that will span the whole EU, and related National Deployment of Quantum Communication Networks.

Impact on industrial and other user communities

There is now a critical mass of European industries developing QKD systems and 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, together with a representative of the Quantum Industry Consortium (QuIC) in the Stakeholder Advisory Board, 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. The developed methods are directly supporting relevant user communities, on the basis of their specific needs, and 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 EU 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 is used by this project to guide any re-adjustment of this project's work-plan to meet evolving requirements. The relationship with EMN-Q is providing a link to EU Quantum Flagship and Quantum Community Network.

Impact on relevant standards

The MeTISQ consortium is deploying within this project all its resources to support the leading role of Europe in the development of measurement-related QKD standards, appropriate to European and global market needs. The work carried out in the project is closely aligned with the work-plan of 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 are now supporting 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 is strategic to aid the development of the quantum communication ecosystem and achieving the projected growth in market value of QKD technologies, paving the way to the EuroQCI initiative and related National Quantum Communication Networks (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 videoconferences and secure data transfer of important documents, thereby reducing need to travel to Face to face meetings).*

List of publications

H. Georgieva, A. Meda, S. M. F. Raupach, H. Hofer, M. Gramegna, I. P. Degiovanni, M. Genovese, M. López, and S. Kück, Detection of ultra-weak laser pulses by free-running single-photon detectors: Modeling dead time and dark counts effects, Applied Physics Letters 118, 174002 (2021)
https://doi.org/10.1063/5.0046014

C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, M. Lucamarini, I. P. Degiovanni & D. Calonico, Coherent phase transfer for real-world twin-field quantum key distribution. Nature Communications 13, 157 (2022).
https://doi.org/10.1038/s41467-021-27808-1

S. M. F. Raupach, I. P. Degiovanni, H. Georgieva, A. Meda, H. Hofer, M. Gramegna, M. Genovese, S. Kück, and M. López, Unexpected detection rate dependence of the intrinsic detection efficiency in single-photon detectors based on avalanche diodes. Physical Review A 105, 042615 (2022).
https://doi.org/10.1103/PhysRevA.105.042615

O. van Deventer, N. Spethmann, M. Loeffler, M. Amoretti, R. van den Brink, N. Bruno, P. Comi, N. Farrugia, M. Gramegna, A. Jenet, B. Kassenberg, W. Kozlowski, T. Länger, T. Lindstrom, V. Martin, N. Neumann, H. Papadopoulos, S. Pascazio, M. Peev, R. Pitwon, M. A. Rol, P. Traina, P. Venderbosch, F. K. Wilhelm-Mauchl. Towards European standards for quantum technologies. EPJ Quantum Technologies 9, 33 (2022).
https://doi.org/10.1140/epjqt/s40507-022-00150-1

S. Virzì, A. Avella, F. Piacentini, M. Gramegna, T. Opatrný, A. G. Kofman, G. Kurizki, S. Gherardini, F. Caruso, I. P. Degiovanni, M. Genovese, Quantum Zeno and Anti-Zeno Probes of Noise Correlations in Photon Polarization, Phys. Rev. Lett. 129, 030401 (2022).
https://doi.org/10.1103/PhysRevLett.129.030401

This list is also available here: https://www.euramet.org/repository/research-publications-repository-link/

Project start date and duration:	1 September 2020, 42 Months	
Coordinator: Marco Gramegna, INRIM Tel: +390113919245 E-mail: m.gramegna@inrim.it Project website addresses: www.euramet.org/project-19nrm06 http://empir.npl.co.uk/metisq/		
Chief Stakeholder Organisation: European Telecommunications Standards Institute	Chief Stakeholder Contact: Hakim Mkinsi	
Internal Funded Partners: 1. INRIM, Italy 2. Aalto, Finland 3. CMI, Czech Republic 4. DFM, Denmark 5. Metrosert, Estonia 6. NPL, United Kingdom 7. PTB, Germany	External Funded Partners: 8. IDQ, Switzerland 9. MPD, Italy 10. PoliMi, Italy 11. TEUR, United Kingdom	Unfunded Partners: -
RMG: -		