Gramegna, M.; Ruo Berchera, I.; Kueck, S.; Porrovecchio, G.; Chunnilall, C. J.; Degiovanni, I. P.; Lopez, M.; Kirkwood, R. A.; Kübarsepp, T.; Pokatilov, A.; Castagna, N.; Morel, J.; Manoocheri, F.; Vaigu, A.

European coordinated metrological effort for quantum cryptography

Published in:
Quantum Technologies 2018

DOI:
10.1117/12.2307841

Published: 01/01/2018

Document Version
Publisher's PDF, also known as Version of record

European coordinated metrological effort for quantum cryptography

M. Gramegna, I. Ruo Berchera, S. Kueck, G. Porrovecchio, C. J. Chunnilall, et al.

M. Gramegna, I. Ruo Berchera, S. Kueck, G. Porrovecchio, C. J. Chunnilall, I. P. Degiovanni, M. Lopez, R. A. Kirkwood, T. Kübarsepp, A. Pokatilov, N. Castagna, J. Morel, F. Manoocheri , A. Vaigu, "European coordinated metrological effort for quantum cryptography," Proc. SPIE 10674, Quantum Technologies 2018, 106741K (21 May 2018); doi: 10.1117/12.2307841

SPIE.

Event: SPIE Photonics Europe, 2018, Strasbourg, France

European Coordinated Metrological Effort for Quantum-Cryptography

M. Gramegna*[a], I. Ruo Berchera [a], S. Kueck[b], G. Porrovecchio[c], C. J. Chunnilall[d], I. P. Degiovanni[a], M. Lopez[b], R. A. Kirkwood[d], T. Kübarsepp[e], A. Pokatilov[e], N. Castagna[f], J. Morel[f], F. Manoocheri[g], A. Vaigu[h]

[a]INRIM, Strada delle Cacce 91, I-10135 Torino, Italy; [b]Physikalisch-Technische Bundesanstalt (PTB), Bundesallee 100, 38116 Braunschweig, Germany ; [c]Cesky Metrologicky Institut (CMI), Praha, Czech Republic; [d]National Physical Laboratory, Hampton Road, Teddington TW11 0LW, UK; [e]AS Metrosert, Teaduspargi 8, 12618, Tallinn, Estonia; [f]METAS, Lindenweg 50, 3003 Bern-Wabern, Switzerland; [g]Aalto University, Maarintie 8, FI-00076, Espoo, Finland; [h]VTT, P.O. Box 1000, 02044 VTT, Finland

ABSTRACT

Quantum Key Distribution, a fundamental component of quantum secure communication that exploits quantum states and resources for communication protocols, can future-proof the security of digital communications, when if advanced quantum computing systems and mathematical advances render current algorithmic cryptography insecure.

A QKD system relies on the integration of quantum physical devices, as quantum sources, quantum channels and quantum detectors, in order to generate a true random (unconditionally secure) cryptographic key between two remote parties connected through a quantum channel. The gap between QKD implemented with ideal and real devices can be exploited to attack real systems, unless appropriate countermeasures are implemented. Characterization of real devices and countermeasure is necessary to guarantee security. Free-space QKD systems can provide secure communication to remote parties of the globe, while QKD systems based on entanglement are intrinsically less vulnerable to attack. Metrology to characterize the optical components of these systems is required.

Actually, the "Optical metrology for quantum-enhanced secure telecommunication" Project (MIQC2) is steering the metrological effort for Quantum Cryptography in the European region in order to accelerate the development and commercial uptake of Quantum Key Distribution (QKD) technologies. Aim of the project is the development of traceable measurement techniques, apparatus, and protocols that will underpin the characterisation and validation of the performance and quantum-safe security of such systems, essential steps towards standardization and certification of practical implementations of quantum-based technologies.

Keywords: Metrology, Quantum Key Distribution, Quantum Communication, Single-Photon Sources

1. INTRODUCTION

Quantum Key Distribution (QKD) relies on the generation of unconditionally secure random keys shared between two parties connected by an open quantum channel [1]. QKD is today no longer confined to laboratories. Practical QKD networks have been realised in the metropolitan area in all five continents [1] and commercial products or industrial prototypes for point-to-point QKD are available from SMEs and large companies. With increasing amounts of data being transmitted and stored online, there is an increasing need to secure that data. Researchers in the field consider QKD as the only truly secure key distribution technology (except secret courier) since it is secured by the laws of physics.

*m.gramegna@inrim.it; phone +39 011 39 19 251; fax +39 011 39 19 259; www.inrim.it ; empir.npl.co.uk/miqc2/

Quantum Technologies 2018, edited by Jürgen Stuhler, Andrew J. Shields, Miles J. Padgett, Proc. of SPIE Vol. 10674, 106741K · © 2018 SPIE
CCC code: 0277-786X/18/$18 · doi: 10.1117/12.2307841

Interestingly, conventional asymmetrical cryptography, which is almost exclusively used for key distribution today, could be rendered insecure by the advent of extremely powerful computers, including quantum computers, or new mathematical insights.
Moreover, fibre and free-space QKD systems use real devices, which do not have the ideal characteristics envisaged by the initial QKD concept. This means that those practical systems can be vulnerable to one or more of the many quantum hacking attacks proposed and/or demonstrated. Counter-measures against these attacks have already been identified, but their effectiveness should be ensured by rigorous characterisation of the optical components – this will be addressed by the project.
Another approach against these attacks is represented by entanglement-based QKD techniques e.g. device independent (DI) QKD, measurement-device-independent (MDI) QKD, etc. The development of entanglement characterisation and quantification techniques is essential in order to provide the metrological framework for next-generation (entanglement-based) QKD systems.

Despite this strong industrial interest in QKD, the standardisation process of QKD systems is still in its initial phase, as is the development of a measurement framework for the characterisation of the physical (optical) components inside QKD system. Specifically, European National Metrological Institutions under the EURAMET research programmes EMRP and EMPIR (by means of the funded project EMRP IND06 "MIQC" [2-3] and EMPIR 14IND05 "MIQC2" [4]) are pushing the development of a metrology framework to foster a market take-up of quantum communication technologies, in order to achieve the maximum impact for the European industry in this area.

In the framework of the EMRP IND06 "MIQC" project, measurement techniques for the characterisation of QKD quantum optical components were developed [3, 32]. The activities in the project were mainly focused on pseudo-single-photon sources and single-photon detectors.

Following the lines of the good results achieved by MIQC, and in order to sustain advances of the metrology for quantum technologies, a follow-up project, namely EMPIR 14IND05 "MIQC2", was then conceived, funded and is actually ongoing. In summary, the aim of this work is to provide an overview of this European Effort for the development of the Metrology needed for the standardisation of the QKD.

2. METROLOGY FRAMEWORK FOR QUANTUM COMMUNICATION TECHNOLOGIES

The "Optical metrology for quantum-enhanced secure telecommunication" Project (EMPIR 14IND05 "MIQC2) [4] focuses on aspects of primary importance as outlined in the following. Firstly, four pilot-comparisons in photon counting regime will be carried out in the context of this project: two on single-photon sources and two on single-photon detectors.

The second covered topic takes into consideration the fact that fibre and free-space Quantum Key Distribution (QKD) systems use real devices, which do not have the ideal characteristics envisaged by the initial QKD concept. This means that practical systems can be vulnerable to one or more of the many quantum hacking attacks proposed and/or demonstrated. Counter-measures against these attacks have already been identified, but their effectiveness should be ensured by rigorous characterisation of the optical components. The 14IND05 "MIQC2" has already started the work to assess and fix these issues.

In parallel and synergy with all these aspects, it is worth noting that some of the National Metrological Institutions and industrial partners of the EMPIR 14IND05 "MIQC2" project actively participate in the standardisation effort in the context of the ETSI Industry Specification Group for QKD [22].

The aim of MIQC2 project is to accelerate the development and commercial success of QKD technologies. This presents a number of metrological challenges, which result from the current and predicted development and deployment trajectories of QKD technologies, and that takes advantage and goes further the results obtained in the context of EMRP JRP IND06-MIQC project, mainly focused in development of techniques to characterise specific quantum-layer optical

components of fibre-based QKD systems, e.g. pseudo-single-photon sources based on attenuated lasers, and commercial single-photon detectors based on avalanche photodiodes operating in Geiger mode.

Following the considerations above, the key objectives addressed in this project are the following:

(1) The development of efficient measurement techniques for characterisation of counter-measures to side-channel and Trojan-horse attacks in fibre-based QKD systems, and the realisation of pilot measurement comparisons to validate the techniques;

(2) The development of dedicated calibration techniques for new high-speed (sine-gated) single-photon detectors for fibre-based QKD;

(3) The development of measurement techniques for the characterisation of the components of free-space QKD systems for ground-air communication, and the realisation of pilot measurement comparisons to validate techniques developed;

(4) The development of measurement techniques for characterising quantum states;

(5) To provide two Best-Practice Guides: (i) one on characterisation of counter-measures to side-channel and Trojan-horse attacks; and (ii) one on characterisation of components of free-space QKD systems;

(6) Contribute to impact - via contributions to international guidelines/standards and showcase examples of early uptake by end users.

It is worth to mention that interesting results appear immediately exploitable by manufacturers. Regarding Objective 1, the first result [5] concerns the security analysis of a typical "Prepare & Measure" (P&M) QKD transmitter, together with the extended security model. Specifically, a quantitative evaluation of fibre-based QKD system security with active and passive counter-measures against Trojan-horse attacks caused by injecting bright laser light into a QKD transmitter and receiver has been carried out. The second [14] is related to the identification and characterisation of the back-flash light emitted by an InGaAs/InP SPAD (single-photon avalanche photodiode). This investigation showed that the back-flashes can be exploited in Trojan-horse attacks, providing a substantial information leakage to an unauthorized party (in the absence of counter-measures). Furthermore, studies were carried out to describe the creation of backdoors which can be created for hackers through the use of intense laser pulses [11], and the limitations of an earlier counter-measure to an attack to take control of the detectors in QKD systems [13].

These four results are important for the practical security of QKD systems and for this reason they can be considered as early uptakes. On one side QKD manufacturers should take account of these results in designing their new devices, and on the other side the NMIs should develop measurement services necessary for testing the protection strategies implemented.

The fifth result consists in the development of techniques for characterizing specific "passive" optical components for fibre-based QKD systems (such as a MEMS attenuator, a polarization-maintaining circulator and interference filters) to test their behaviour and their effectiveness as potential counter-measures against quantum hacking based on Trojan-horse or side-channel attacks. It showed interesting and unexpected results in terms of potential weaknesses QKD manufacturers should be aware of. In this perspective, a new services for the calibration of the spectral properties of optical fiber components in the 700 nm to 1800 nm range has been realised by METAS.

In the context of Objective 2, new electronic circuit solutions were developed, and a first prototype of an InGaAs SPAD sine-gated at frequencies greater than 1 GHz has been successfully realized. This device is designed to be tunable over a wide range (900-1400 MHz) for synchronization with different external laser systems and for selecting the best trade-off between after-pulsing and detection efficiency. The excess bias is adjustable for optimizing the main SPAD parameters, like photon detection efficiency, dark count rate, afterpulsing, timing jitter. The system can be controlled remotely from a PC and has already demonstrated proved long-term stability.

One key result for Objective 3 is the establishment of the technical protocol for a pilot study on the detection efficiency measurement of silicon SPADs This pilot study is being performed worldwide (including outside the consortium) and within the Consultative Committee for Photometry and Radiometry (CCPR). 11 NMIs will participate, of which 6 are

within this JRP. The pilot comparison has been started and measurements are under way. Furthermore, activities to provide traceability of measurements at single-photon level by developing detectors and amplifiers to provide linkage to conventional radiometric standards are in progress, as well as the experimental setup for their characterisation.

Techniques for characterising components of free-space QKD systems for ground-air communication have been organized and are ready for use. High-quality single-photon sources have been realised and characterised [15,16,19,20]. The free-space-QKD transmitter module (based on passive optical components, such as (non-)polarising beam splitter and waveplates) exploiting polarization as the encoding degree of freedom has been realised and it is under characterisation. The measurement apparatus is essentially a single-photon polarimeter operating in the NIR-VIS.

Concerning with Objective 4, optimal estimators have been developed for measuring the amount of entanglement and the geometric discord with low uncertainty level. Experimental set-ups encoding information in several spatial degrees of freedom (Hilbert space larger than 2) exploiting multi-core fibres have been realized. 2-dimension and 4-dimension entanglement has been generated and analysed by quantum state tomography [17]. Experimental realisation of weak measurements and weak values estimation has been performed, allowing the properties of quantum systems to be measured, without, to some extent, the wave-function collapse. This has provided some important returns not only in the field of quantum metrology [7,12, 21]. Realization of a first version of a new source (folded-sandwich configuration) of polarization entangled photon pairs, highly tunable in frequency [5]. This source is particularly useful as an interface for quantum hybrid systems. A high rate, long distance detector-device independent (DDI-QKD) scheme has been realized using two degrees of freedom of the same photons; the security analysis has been carried out [10]. This represents a first step towards a more feasible approach to MDI-QKD.

3. IMPACT ON STANDARDS AND METROLOGY, INDUSTRIAL AND SCIENTIFIC COMMUNITIES

The aim of MIQC2 project is to ensure that the results achieved [5-21, 23-30] are provided to the stakeholders and end-user community in a timely and appropriate manner. The primary beneficiaries of the outputs of this project will be the QKD community, but the wider community exploiting single-photon states [32] will also derive significant benefits from the methods, devices, calibration facilities and measurement protocols developed.

Some partners of the MIQC2 consortium are active in the context of the ETSI ISG-QKD QKD, and contribute to the drafting of pre-standards and standards concerned with characterisation, validation, and certification of the optical layer of QKD systems and networks. The ETSI Group Specification document "ETSI QKD GS 011 – Component characterisation: characterising optical components for QKD systems"– was published by ETSI in May 2016 [22]. This document took about 2 years to compose, and the work on the initial drafts was supported by EMRP projects IND06-MIQC and EXL02-SIQUTE [31] before EMPIR14IND05 MIQC2. This document is, to our knowledge, the first measurement (pre-) standard for a quantum 2.0 technology. Since it is focussed on the characterisation of attenuated laser sources and gated single-photon detectors, it is also relevant to all quantum optical technologies utilizing these devices. Three other documents currently in draft receive support from this project, in particular: (i) "ETSI GS QKD 010: Implementation Security - Protection against Trojan horse attacks in one-way QKD systems"; (ii) "ETSI GS QKD 003Ed2: Components and internal interfaces - revision of published document" ; (iii) "ETSI GS QKD 013: Characterisation of QKD transmitter modules".

In the project consortium [4] there are two key European QKD manufacturers, as well as single-photon detector manufacturers, and having as collaborators (members of the stakeholder advisory board) an organisation working in the field of information security, and of single photon detector . These ensure that the work is aligned with and will impact on the industrial requirements during the lifetime of the project, as demonstrated for example in the investigation on backflashes from single-photon [14]. Moreover, it should be noted that the published security analyses, derived inside this consortium to improve the protection of the QKD apparatus from quantum-hacking attacks, can lead to: (i) exploitation of the results by QKD manufacturers (impact on industry); and (ii) a required measurement standard and service for establishing whether the required optical isolation is achieved (impact on metrology).

Finally, it is worth to noticing that eight members of the project are also members of the Consulting Committee on Photometry and Radiometry (CCPR) [34], and have been working to incorporate photon-based quantities into its strategic planning. Furthermore, seven members of the project are members of the EURAMET Technical Committee for Photometry and Radiometry ensuring that CCPR and EURAMET are kept informed about the progress of the project and that CCPR & EURAMET roadmaps address the needs of the single-photon and QKD communities.

It should be mentioned that this project triggered the establishment of a task group on "Single-Photon Radiometry" [35] within the working group "Strategic Planning" of the Consultative Committee for Photometry and Radiometry. In a worldwide effort, 11 NMIs (6 are partners of this project), agreed on a technical protocol and will carry out the first pilot study on the detection efficiency of Si-SPADs (coordinated by PTB, the pilot comparison started in May 2016 and measurements are actually on track).

ACKNOWLEDGMENTS

This work has received funding from the European Union's Horizon 2020 and the EMPIR Participating States in the context of the project EMPIR-14IND05 'MIQC2'.

REFERENCES

[1] Lo H.-K., Curty, M., Tamaki, K., "Secure QKD," Nature Photonics 8, 595–604 (2014).

[2] http://projects.npl.co.uk/MIQC/ and publications therein.

[3] Rastello, M. L., *et al.*, "Metrology for industrial quantum communications: the MIQC project," Metrologia 51, S267 (2014).

[4] http://empir.npl.co.uk/miqc2/ and publications therein.

[5] Dietz, O., *et al.*, "A folded-sandwich polarization-entangled two-color photon pair source with large tuning capability for applications in hybrid quantum systems," Applied Physics B 122, 33, (2016).

[6] Piacentini, F., *et al.*, "Towards joint reconstruction of noise and losses in quantum channels," Quantum Meas. Quantum Metrol. 3, 27–31 (2016).

[7] Piacentini, F., *et al.*, "Experiment investigating the connection between weak values and contextuality," Phys. Rev. Lett. 116, 180401 (2016).

[8] Avella, A., *et al.*, "Detecting spatial quantum correlation by a EMCCD camera: a radiometric link between photon counting and analog regime," Optics Letters 41, 1841 (2016).

[9] Tamaki, K.,*et al.*, , "Decoy-state quantum key distribution with a leaky source," New J. Phys. 18, 065008 (2016).

[10] Boaron, A., *et al.*, "Detector-device-independent quantum key distribution: Security analysis and fast implementation," J. Appl. Phys. 120, 063101 (2016).

[11] Makarov, V.,*et al.*, "Creation of backdoors in quantum communications via laser damage," Phys. Rev. A 94, 030302(R) (2016).

[12] Piacentini, F., *et al.*, “Measuring incompatible observables of a single photon,” Phys. Rev. Lett. 117, 170402 (2016).

[13] Huang, A., *et al.*, "Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption,” IEEE Journal of Quantum Electronics 52 (11), 1-11 (2016).

[14] Meda, A., *et al.*, “Quantifying the backflash radiation to prevent zero-error attacks in quantum key distribution,” Light: Science & Applications 6, e16261 (2017).

[15] Heindel, T., *et al.*, “A bright triggered twin-photon source in the solid state,” Nature Communications 8, 14870 (2017).

[16] Fischbach, S., *et al.*, “Single Quantum Dot with Microlens and 3D-Printed Micro-objective as Integrated Bright Single-Photon Source,” ACS Photonics 4, 1327-1332 (2017).

[17] Lee, H. J., *et al.*, "Experimental Demonstration of Four-Dimensional Photonic Spatial Entanglement between Multi-core Optical Fibres,” Scientific Reports 7, 4302 (2017).

[18] Forneris, J., *et al.*, “Creation and Characterization of He-related color centers in diamond,” Journal of Luminescence 179, 59 (2016).

[19] Jakubczyk, T., *et al.*, “Impact of Phonons on Dephasing of Individual Excitons in Deterministic Quantum Dot Microlenses,” ACS Photonics 3, 2461–2466 (2016).

[20] Fischbach, S., *et al.*, “Efficient single-photon source based on a deterministically fabricated single quantum dot - microstructure with backside gold mirror,” Applied Physics Letters 111, 011106 (2017).

[21] Piacentini, F., *et al.*, “Determining the quantum expectation value by measuring a single photon,” Nature Physics 13, 1191-1194 (2017).

[22] http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution

[23] Piacentini, F., “Metrology for Quantum Communication,” Proceedings of IEEE Globecom 2015- IEEE Globecom Workshops, Doi: 10.1109/GLOCOMW.2015.7413960 (2015).

[24] Gramegna, M., *et al.*, “Measuring Non-Commuting Observables of a Single Photon via Sequential Weak Values Evaluation,” Frontiers in Optics 2016 OSA Technical Digest, paper FW3F.4 (2016).

[25] Moreva, E., *et al.*, “Exploring Quantum Correlations from Discord to Entanglement,” Advanced Science, Engineering and Medicine, 9, 46 (2017).

[26] Genovese, M., “A few reflections on protective measurements and more,” Journal of Physics: Conf. Series 880, 012012 (2017).

[27] Huang, A., *et al.*, “Gaps between industrial and academic solutions to implementation loopholes in QKD: testing random-detector-efficiency countermeasure in a commercial system,” IEEE Journal of Quantum Electronics 52 (11), 1-11 (2016).

[28] Forneris, J., “Creation and characterization of He-related color centers in diamond,” Journal of Luminescence 179, 59 (2016).

[29] Schlottmann, E., “Exploring the Photon-Number Distribution of Bimodal Microlasers,” https://arxiv.org/abs/1709.04312

[30] Jakubczyk, T., " Impact of Phonons on Dephasing of Individual Excitons in Deterministic Quantum Dot Microlenses," ACS Photonics 3, 2461–2466 (2016)

[31] http://www.ptb.de/emrp/siqute-home.html

[32] Chunnilall, C. J., et al., "Metrology of single-photon sources and detectors: a review," Opt. Eng. 53(8), 081910 (2014).

[33] G. Brida , et al., "An extremely low-noise heralded single-photon source: A breakthrough for quantum technologies, " Appl. Phys. Lett. 101, 221112 (2012).

[34] https://www.bipm.org/en/committees/cc/ccpr/

[35] https://www.bipm.org/en/committees/cc/wg/ccpr-tg-spr.html