The European Coordinated Effort to develop the Metrology for Quantum-Cryptography

I. P. Degiovanni[1], S. Kueck[2], G. Porrovecchio[3], I. Ruo Berchera[1], C. J. Chunnilall[4], M. Gramegna[1], T. Kübarsepp[5], A. Pokatilov[5], F. Manoocheri[6], A. Vaigu[6]

1 INRIM, Strada delle Cacce 91, I-10135 Torino, Italy
2 Physikalisch-Technische Bundesanstalt (PTB), Bundesallee 100, 38116 Braunschweig, Germany
3 Cesky Metrologicky Institut (CMI), Praha, Czech Republic
4 National Physical Laboratory, Hampton Road, Teddington TW11 0LW, UK
5 AS Metrosert, Teaduspargi 8, 12618, Tallinn, Estonia,
6 Aalto University, Maarintie 8, FI-00076, Espoo, Finland
** corresponding author: i.degiovanni@inrim.it*

Quantum Key Distribution (QKD) is essentially the generation of perfectly secure random keys shared between two parties that communicate by an open quantum channel. This enables the parties to establish a secret key from short pre-shared secret and public exchanges, something which has never been shown to be possible by classical, i.e. non-quantum, means. 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. 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 [1-3].

QKD is today no longer confined to laboratories. Practical QKD networks have been realised in the metropolitan area in all five continents [4], e.g. in Vienna Austria (SECOQC), in Tokyo Japan (UQCC), in Switzerland, in USA, in China. A quantum network is under construction in the UK [5]. Of particular note is the current 560 M RMB (approx. 75 M€) project by China to build a 2000 km fibre QKD network from Shanghai to Beijing, supplemented by ground-to-satellite QKD to reach more distant parts of China such as Ulumuqi [6].

Nowadays, commercial products or industrial prototypes for point-to-point QKD are available from SMEs and large companies, e.g. ID Quantique SA (Suisse), Toshiba Research Europe (UK), Selex ES Leonardo-Finmeccanica (Italy), QuintessenceLabs (Australia). Several other companies have active research programmes on QKD.

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” [7] and EMPIR 14IND05 “MIQC2” [8]) 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.

It should be noted that, irrespective of the underlying technologies, there are quantum devices that appear in most QKD systems, namely sources and detectors. The characteristics of these quantum optical components are crucial for security analysis at the quantum optical level. The identification of relevant parameters, standardisation and the development of appropriate measurement techniques for their metrological characterisation are therefore necessary to enable the efficient specification of generic security requirements for QKD systems. In this sense, the above-mentioned EMRP IND06 “MIQC” project (ended in September 2014), whose aim was the development of techniques to characterise specific optical components of fibre-based QKD systems, had been the first answer of the metrological community to these needs. In fact, although characterisation of classical communication parameters is a well-established metrological activity (even if research and optimisation are still necessary), the implementation of practical quantum communication protocols

requires further developments of these 'classical' measurement techniques, in order to cover parameter ranges that are beyond the interests of classical communication. In the framework of the EMRP IND06 “MIQC” project, measurement techniques for the characterisation of QKD quantum optical components in the telecom regime (around 1.55 µm) were developed. The activities in the project were mainly focused on pseudo-single-photon sources and single-photon detectors, but also attention was paid to the characterisation of quantum random number generators (QRNG). This aspect was technically challenging since measurement standards did not exist before MIQC for photon-counting technologies at telecom wavelengths. Indeed, where standards were present, they operated in the regime of microwatts or above, and were cumbersome to use for measurements at the single photon level.

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 14IND06 “MIQC2”, was then conceived, funded and is actually ongoing. It focuses on aspects of primary importance as outlined in the following. Firstly, since measurement comparisons between NMIs are fundamental to ensure the consistencies of the calibration results performed in different countries, two pilot-comparisons in photon counting regime will be carried out in the context of this project: one on single-photon sources and the other on single-photon detectors.

The second covered topic takes into consideration the fact that fibre and free-space Quantum Key Distribution (QKD) systems [9] 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 EMPIR 14IND06 “MIQC2” has already started the work to assess and fix these issues [10-13].

MIQC2 is also tackling the development of metrological techniques to characterise the optical components and devices for free-space QKD systems, providing traceability (relying on results of the IMERA Plus JRP qu-Candela [14]) to the measurement in the photon-counting regime at wavelengths in the visible spectral range. Other strategic activities of the project are aimed at advances beyond the state of the art. In particular, we can list the following quests: the requirement of new calibration techniques for novel detector technology for fibre-based QKD, together with devices to enable networking and higher data rates; the development of suitable techniques for characterisation of entangled states, entanglement quantification and/or witnessing, and estimation of the entangling-process efficiency relevant to the needs of QKD. The latter will benefit from extensive research by the quantum optical community, where several interesting results have been already demonstrated. However, the development of these techniques represents completely new tasks for metrology, and it will be carried out within this on-going project.

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 (ISG-QKD) [15]. Specifically, they are providing metrology leadership for the drafting of pre-standards and standards concerned with characterisation, validation, and certification of the optical layer of QKD systems and networks. In the specific, two industrial partners (Toshiba, idQuantique) and three NMIs (INRIM, NPL, PTB) are in fact members of the ETSI ISG-QKD, the chair of which is currently held by Toshiba. This ISG has so far published 5 Group Specification documents. One of the current documents “DGS/QKD-011 Component characterisation: characterising optical components for QKD systems” [16] benefits directly from the results of EMRP IND06 MIQC. The current ETSI programme of drafting a series of Group Specification documents concerned with implementation security against hacking attacks will directly benefit from input from this project, as well as specifications concerned with characterisation of assembled modules, and updates of existing documents.

In summary, the aim of this talk is to provide an overview of this European Effort for the development of the Metrology needed for the standardisation of the QKD.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301 (2009).

[3] ETSI White Paper (Quantum Safe Cryptography V1.0.0, October 2014): Quantum Safe Cryptography and Security;An introduction, benefits, enablers and challenges, ISBN 979-10-92620-03-0.

[4] H.-K. Lo, M. Curty, K. Tamaki, Secure quantum key distribution, Nature Photonics 8, 595–604 (2014)

[5] https://www.quantumcommshub.net/about-us/

[6] https://docbox.etsi.org/workshop/2014/201410_crypto/s01_setting_the_scene/s01_gisin.pdf

[7] http://projects.npl.co.uk/MIQC/

[8] http://empir.npl.co.uk/miqc2/

[9] E. Gibney, Chinese satellite is one giant step for the quantum internet, Nature 535, 478–479 (2016)

[10] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, V. Makarov, "Gaps between industrial and academic solutions to implementation loopholes in QKD: testing random-detector-efficiency countermeasure in a commercial system", Submitted (Preprint available at http://arxiv.org/abs/1601.00993v1).

[11] K. Tamaki, M. Curty, M. Lucamarini, "Decoy-state quantum key distribution with a leaky source", New J. Phys. 18, 065008 (2016).

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

[13] A. Meda, et al., "Quantifying the backflash radiation to prevent zero-error attacks in quantum key distribution", Light: Science & Applications, Accepted for publication (preprint available: http://aap.nature-lsa.cn:8080/cms/accessory/files/AAP-lsa2016261.pdf)

[14] http://www.quantumcandela.org/

[15] http://www.etsi.org/index.php/technologies-clusters/technologies/quantum-key-distribution

[16] http://www.etsi.org/deliver/etsi_gs/QKD/001_099/011/01.01.01_60/gs_QKD011v010101p.pdf