Worldwide Standardization Activity for Quantum Key Distribution

Romain Alléaume
Institut Mines-Telecom/Telecom ParisTech
Paris, France
romain.alleaume@telecom-paristech.fr

Thomas E. Chapuran
Applied Communication Sciences
Basking Ridge, NJ, USA
tchapuran@appcomsci.com

Christopher J. Chunnilall
National Physical Laboratory
Teddington, UK
christopher.chunnilall@npl.co.uk

Ivo P. Degiovanni
INRIM
Torino, Italy
i.degiovanni@inrim.it

Norbert Lutkenhaus
University of Waterloo
Ontario, Canada
nlutkenhaus@uwaterloo.ca

Vincente Martin
Universidad Politécnica de Madrid
Madrid, Spain
vicente@fi.upm.es

Alan Mink
NIST
Gaithersburg, MD, USA
amink@nist.gov

Momtchil Peev
AIT
Vienna, Austria
momtchil.peev@ait.ac.at

Marco Lucamarini, Martin Ward, Andrew Shields
Toshiba Research Europe
Cambridge, UK
<marco.lucamarin>, <martin.ward>, <andrew.shields>
@crl.toshiba.co.uk

***Abstract*—We discuss the on-going worldwide activity to develop forward looking standards for quantum key distribution (QKD) in the European Telecommunications Standards Institute (ETSI) QKD industry specification group (ISG). The long term goal is to develop a certification methodology that bridges the gap between theoretical proofs and practical implementations with imperfect devices. Current efforts are focused on the handling of side channels and characterization of the most relevant components.**

Keywords—industry security standards; quantum key distribution; quantum cryptography; quantum communications; optical and electro-optical components

I. Introduction

Quantum key distribution (QKD) [2][10] is a unique security primitive that builds on quantum physics, telecommunications and information theory. It employs a multi-stage protocol over an insecure quantum channel and a public authenticated and integrity protected classical channel to generate information theoretically secure cryptographic key between two parties (usually called "Alice" and "Bob"), even in the presence of an unconstrained eavesdropper (Eve). The requirement of authenticity of the classical channel can be dropped if Alice and Bob initially share a short secret. This allows enforcing channel integrity but reduces the scheme to key expansion. The expansion rate depends on the physical characteristics of the given quantum channel. The resulting key can then be used in symmetric ciphers like the advanced-encryption standard (AES) or the provably information theoretically secure One-Time-Pad .

The main advantage of QKD is that it is information theoretically secure [24] rather than based on computational complexity assumptions, as are existing key distribution algorithms employing public-key cryptography methods. Moreover, it provides composable security so that the security level of the key expansion protocol may be changed by choosing appropriate epsilon deviations from perfect security [22]. This key expansion primitive can be combined with any other composable primitives to again yield composable epsilon secure results (the new epsilon being the sum of the components'). The security of QKD is based on the laws of quantum physics and specifically on a model of the physical layer of the system. In this framework it is proven that the quantum bit error rate (QBER) bounds the information attainable over the quantum channel by an eavesdropper, even though the errors are normally caused by the non-ideal behavior of system components. Security risks connected to real-world implementations can be present in all key distribution systems [15]. In QKD security can be breached if the model used to prove security deviates from the actual implementation of the physical layer, opening so called "side channels" [24]. It is natural to try to extend the ideal of bounding risks to such imperfections that may be present in an implementation. The specification of how this should be done for particular implementation issues and the practical requirements that are necessary to enable the underlying security are some of the current challenges in the field.

A world-wide effort to develop standards for QKD systems has been formed through ETSI [7][13], the QKD Industry Specification Group (ISG). Its focus is to combine the QKD security analysis with details of practical implementations to develop standards that could be used by companies developing QKD products. The ultimate goal is to develop a certification framework that bridges the gap between theoretical security proofs and practical implementations with imperfect devices. In some cases, this has stimulated further theoretical research, in order to make the theoretical assumptions easier to meet in

We would like to acknowledge funding from project MIQC (contract IND06) of the European Metrology Research Programme (EMRP). The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union.

978-1-4799-7470-2/14/$31.00 ©2014 IEEE

practice. In other cases, it consists of defining the best engineering practice to approach existing theoretical assumptions. This framework is considered a "forward looking standard". Most standards are based on a number of existing methods already in commercial use. Forward looking standards anticipate the emerging technology and attempt to provide the needed operational guidance, testing methods and verification to help advance new technology towards broad commercial adoption [8].

Another important aspect of the QKD technology is its integration into existing optical networks. An increasing number of QKD quantum networks and field trials from all over the world have been reported recently [20][4][5] showing the feasibility of QKD architectures that are far more complex than the original point-to-point dark fiber connection. The QKD ISG aims to assist the integration process by defining relevant standards for such efforts.

Standardization is fundamental to promoting broad commercialization of QKD by building trust and consistency leading to certification. The standardization process is also highlighting areas of QKD research needed to support the development of these standards. A well-established set of standards would be beneficial both to potential QKD users, as it provides definition to what they might consider buying, and to QKD vendors, as it provides a framework for requirements and how to specify them.

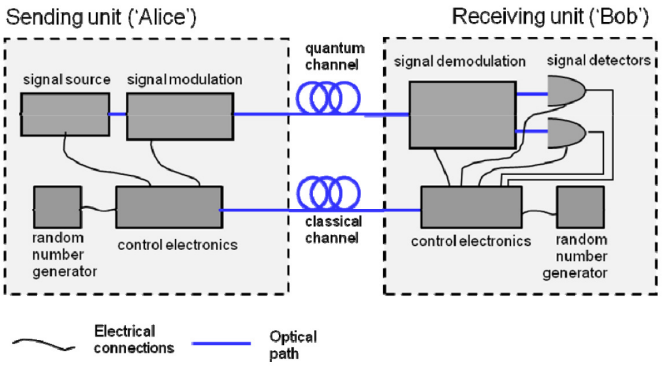
In the following, after a brief overview of the QKD technology, we provide a description of some of the ongoing standardization work in the ETSI ISG-QKD. A final discussion summarizes the work done and the questions to be addressed in the near future.

II. QKD Overview

There are four stages to the QKD protocol. In stage 1 quantum signals are generated (e.g., polarization of single photons), transmitted over the lossy quantum channel and measured. In stage 2, sifting, Alice and Bob exchange information over the classical channel to agree upon a common sequence of valid quantum measurements to work with. But within that sequence the bit values in Bob's copy may be not be identical to Alice's, i.e. errors might exist. In stage 3, reconciliation, Alice and Bob exchange information over the classical channel to correct errors between the two versions of their common bit sequence without exposing the value of their bits. In stage 4 Alice and Bob perform privacy amplification on their now identical bit sequences (e.g. through the application of a 2-universal hash function, which they select at random and that does not require any further communication), yielding a shared secret between Alice and Bob. There are several important differences between QKD and conventional communications. Information is transmitted over the lossy quantum channel and error correction is sent over the reliable (e.g., TCP/IP) classical channel. The quantum information can not be re-transmitted and QKD requires efficient error correction, (code rates greater than 1/2 and operating close to the Shannon limit), to enable extraction of some amount of secret bits while dealing with a high QBER (up to 11%). As a consequence, some variations on the error correction code configuration are possible that result in additional efficiency. Unlike the case of conventional communications, losses on the quantum channel (photons never received) do not affect the outcome of the protocol since the data is random, but only reduce the key generation rate. Measurement errors on the photons received over the quantum channel (i.e., the QBER) are a concern since they bound the level of eavesdropping that may have occurred, and limit the amount of secure key that can be extracted, if any.

A typical QKD system based on the BB84 protocol using weak coherent pulses and decoy states is illustrated in Fig. 1. Any system parts or any signals leaking out of the security perimeters, i.e. the dashed line boxes, (e.g., the channels, reflected light, electromagnetic emissions, etc.) can provide potential information to the eavesdropper (Eve). QKD is a technology that uses light pulses at a level where a quantum mechanical description is required and the bulk of the photonic components in a QKD system are optical or electro-optical ones. The sending unit consists of an attenuated laser, for the photonic signal source, and a source of randomness, to encode the outgoing photons. The receiving unit consists of a component for signal demodulation (i.e., using a source of randomness to select the measurement basis) as well as one or more signal detectors. The source of randomness can be either an active random number generator or a passive random selection component, such as a non-polarizing beam splitter. Control electronics (e.g., FPGAs and other special chips) manage the generation, transmission, reception and capture of the raw shared key. Additional control electronics and a computer (not shown in Fig 1) implement the remainder of the protocol and storage of the secure key.

Fig. 1. Diagram of a generic QKD system based on the BB84 protocol using weak coherent pulses and decoy states.



Photons are the typical quantum carriers (as massive particles are easily absorbed). A quantum channel must then be an end-to-end optically transparent medium, like an optical fiber or free space. Transmission through an absorptive medium implies a limit to the maximum distance that a signal can travel. In QKD, a Gb/s transmission rate often results in Mb/s secure key rates over a 50 km optical fiber. However, at the quantum level (i.e. extremely low light power levels), the main factor limiting QKD distance is the noise (dark count rate) of the light detectors employed. At long distances, this can impact considerably on QBER and reduce to zero the final secure key rate distilled by the system. In practical terms, this

means a maximum reach of about 250 km with current or foreseeable technology

The classical channel is a conventional communication channel and is used in QKD for the classical portion of the protocol, which includes sifting, error correction, privacy amplification and authentication. It can be optical or electrical and except for application requirements, does not require tight time constraints. In some cases a control channel (a second classical channel) may support the quantum channel by providing synchronization and time alignment between Bob and Alice, and thus would have timing constraints.

III. QKD Deployment

Another important challenge for QKD lies in its compatibility with existing and future optical network infrastructures.

The ETSI QKD group is working to provide a practical framework for exchanging information between a QKD user and a telecom operator. Where a QKD user can include a QKD manufacturer and a telecom operator can include the person in charge of managing the network resources. In particular the optical links that will be used to connect the two QKD devices (Alice and Bob). Facilitating the exchange of information between QKD manufacturers and telecom operators can be a major driver to promote the deployment of QKD on existing optical networks. It can also help to identify how QKD should evolve to fit with the trends of future optical networks.

Current QKD deployments rely on dark fibers. A crucial challenge for the integration of QKD into existing optical infrastructure is how to optimize QKD as one component of an optical architecture, taking cost versus performance trade-offs into accounts. In that perspective, deploying QKD with existing optical traffic, using multiplexing techniques and in particular wavelength division multiplexing (WDM) is a major technical objective that has been pursued over the past years [4][19][6].

From the standardization viewpoint, our first objective will be to support QKD manufacturers and network operators by providing guidelines on how to jointly express the important information they need to share in the context of QKD deployments, and in particular their system requirements. In addition, QKD manufacturers will also be able to express how their QKD system can perform, as a function of the communication resources provided by the telecom operator.

This analysis can be made relatively systematic by distinguishing the main architectural scenarios in a QKD deployment, depending on how the telecom channels are operated. Once this architecture is fixed, among a finite number of possibilities, (e.g., the quantum channel wavelength-multiplexed with the bidirectional classical channel) then the requirements can address different elements such as:

- quantum channel characteristics (maximum attenuation, maximum tolerated impairments),
- available wavelengths,
- stability requirements on some parameters (for example polarization),
- maximum tolerable external noise (and available filtering),
- rate and latency for the classical channel.

By standardizing how this information should be specified, it will also allow QKD manufacturers to state a guaranteed level of service (secret key rate mean value as well as fluctuations), provided a specific list of requirements is met.

We can expect standardization of QKD from the viewpoint of optical networking to help both QKD users and network operators plan QKD deployments. It could also serve as a basis for cost optimization, helping quantify the impact and the expected performances associated with the integration of QKD in a network infrastructure.

IV. Standardization Framework

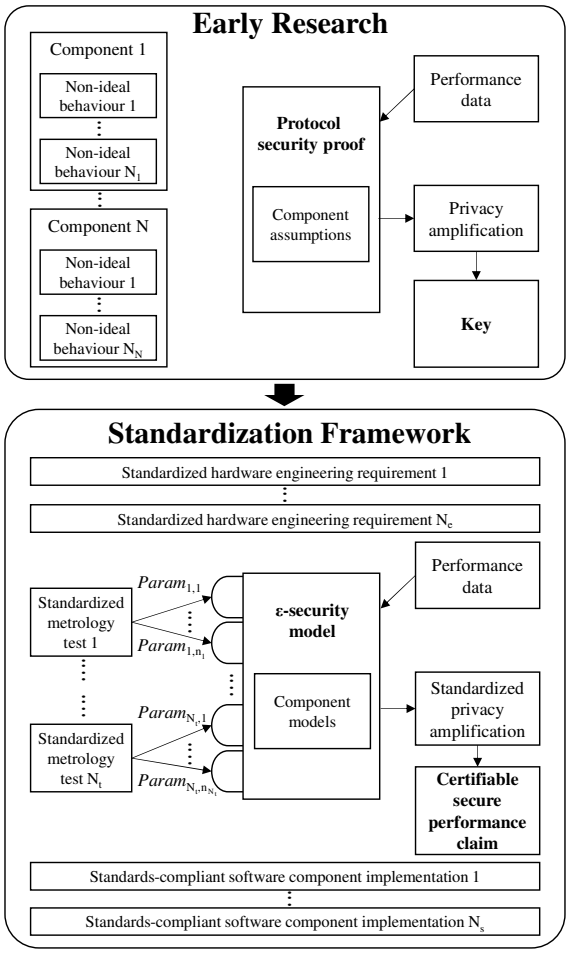
For QKD, information theoretic security proofs exist for a number of different protocols. However a standardization and certification framework for QKD needs to consider aspects of the system beyond the underlying protocol and to look more widely at the implementation of complete systems. In order to evolve a solid set of standards for QKD it is necessary to examine the assumptions that are made in such protocol security proofs and to study the manner in which they may vary in the implementation. In some cases, such as the substitution of weak coherent states for the single photons initially assumed in many protocols, it was already known how to extend asymptotic security proofs to accommodate specific non-ideal behaviors exhibited by real components. “Epsilon (ε) security” models [22] based on a quantifiable failure probability, ε, are the basis for much theoretic work and continue to be an important area of active research to support the standardization process. One of the challenges is to extend such ε-security models to other non-ideal behaviors of components that might otherwise introduce loopholes.

However, the standardization framework can be even wider than this and should also consider how the parameters required as inputs to the security models can be accurately measured. It should also consider the engineering requirements necessary to ensure that best-practice is followed in terms of the design and operation of systems. Some design requirements may be imposed to eliminate potential risks while others may be introduced to simplify the security models that may be necessary.

Standards will also take the ε-security model for a system and use this to specify how privacy amplification should be implemented based on performance data from the system in order to make a claim of secure performance. An overview of an approach to developing a standardization framework from early QKD research is shown in Fig. 2. The top part of the figure shows the situation that existed during early research phases. A security proof for the idealized system that includes a number of assumptions about the components in the system is used to determine privacy amplification requirements, but details of the non-ideal behavior of the real components are not necessarily included in the security analysis. In the lower

part of the figure we give an overview of approaches to a standardization framework for a QKD system. A more sophisticated, epsilon-security model is introduced that includes parameterized models of key components of the system. In many cases putting forward such models is not straight-forward and open research problems remain. The parameters that are inputs to the security model are derived from standardized metrology tests, where each test may provide multiple parameters to the security model. Arrows can be taken to indicate flows of actual values for a specific system but the model may also take into account the existence of engineering requirements (hardware and software), which may serve to reduce the complexity of the model. The requirements for privacy amplification are specified based on the security model resulting in a certifiably secure performance claim.

Fig. 2. Overview of the approach to develop a standardization framework (bottom) from early QKD research (top).



In terms of developing well-defined methods to characterize the parameters of the major QKD components the Metrology for Industrial Quantum Communications (MIQC) project [17] was established by the EU. This enabled the metrology experience of National Measurement Institutes such as INRIM [11], NPL [18] and PTB [21] to be focused on the development of pre-standards to characterize QKD components and systems.

Multiple approaches have been adopted to identify the most important non-ideal behaviors to address. Analysis of each of the components typically included in QKD systems and investigation of known side-channel attacks have both proved valuable. Side-channels usually refer to situations where differences between engineered components and those assumed in a security proof may directly provide information or allow control not specified in the protocol.

The above framework highlights the multiple areas in which standards are needed. Standards for the software components that implement the classical algorithms used in QKD stages 2 thru 4 will also be needed. At present the ETSI QKD group is focusing on the initial quantum stage for which a number of open questions need to be addressed. Five specification documents have been produced [7]. Current activities include standards for the characterization of key components including single photon sources and detectors. This will ensure that important details are tested and will also enable data sheets for components to be generated in a consistent manner, including pertinent parameters and performance figures to allow comparison between different vendors and manufacturers. This will include measurements needed to determine if appropriate countermeasures to side-channel attacks are employed, how effective they are (i.e., the potential for information leakage) and, if possible, how to compensate for that leakage. Standards considering how to specify good practice in combining components to produce a system that implements QKD functions safely, and guidelines for networking QKD systems, will follow.

V. Source and Detector Characterization

A major contribution of this effort is the characterization of the main optical QKD sub-systems, initially single-photon sources and detectors. This activity will have an impact on the quantum community beyond that of QKD. This will provide a list of parameters for specifying the performance of optical QKD components and the development of appropriate, traceable measurement techniques for their metrological characterization. Such characterization is necessary to enable the efficient specification of generic security requirements for QKD systems and will shape a validation and certification framework for wider implementation of this technology. Engagement with manufacturers has highlighted the importance of characterizing the physical performance of QKD sub-systems in order to assure both suppliers and customers that the devices are operating as intended.

Although characterization of classical communication parameters is a well-established metrological activity (even if research and optimization are still necessary), for quantum communication further development of these "classical" measurement techniques is necessary to cover parameter ranges that are beyond the interests of classical communication. These are, for example, optical power and detector characterization at very weak intensities — including down to the single-photon level — at telecom wavelengths. This is technically challenging, since no measurement standards are established for photon counting technologies in this spectral range. Indeed, where standards are present, they

operate at microwatt or higher power levels, and are cumbersome to use for measurements at the quantum level.

For example, a QKD source is specified by its power (mean number of photons per pulse) as well as its photon number statistics (a property peculiar to the description of quantum light). This is of prime importance for QKD security. In this respect, the quantification of parameters like the mean and variance of the number of photons per pulse are fundamental in guaranteeing the correct implementation of a QKD system. The complexity of such a measurement is due to the fact that this parameter is probabilistic and not deterministic. Additional complications occur because current test instrumentation cannot measure every possible photonic emission.

The current metrological work has developed a measurement framework for characterizing the following devices in the 1.55 µm band:

- attenuated-laser weak coherent pulse sources approximating single-photon ones;
- gated InGaAs non photon-number-resolving single-photon detectors.

Traceable measurements for quantifying most QKD-relevant parameters of these devices were developed and implemented.

However, this is just the beginning of the metrological effort for QKD. As new sources and new detectors, based on different physical phenomena, appear in the market, the metrology community needs to determine suitable parameters and develop measurement techniques for them.

QKD utilizing satellites is also under active consideration as a solution for implementing QKD over global distances. Despite the fact that some metrological work has been performed to provide traceability for photon-counting regimes at wavelengths in the visible spectral range, the metrology community should develop characterization, validation, and calibration methods for single-photon sources, detectors and other relevant optical components (e.g. polarization controllers, intensity modulators, etc.) used in free-space visible-light QKD.

Entanglement, as in entangled states or entangling measurements, is expected to have a central role in the next generation of QKD technologies. This ranges from the development of quantum repeaters and quantum networks, to the practical application of (measurement-) device-independent QKD [1][14]. Accurate characterization of entangled states, development of measurement techniques for entanglement quantification and/or witnessing, and for estimating the entangling-process efficiency are required.

VI. Side Channels

QKD theory provides an information theoretical secure framework for the distribution of cryptographic keys but the practical security of real-world implementations crucially depends on how the system-models assumed in the theory are realized in the implementation. For example, if Alice were to shout out the bit values as she encoded them onto single photons, she would have released the information audibly without there being any imperfections in the optical model of the QKD device. As discussed, deviations of system model assumptions and implementations lead to side channels that are common to all cryptographic systems. In QKD, however, these are particularly relevant since the security of QKD is solely based on the functionality of the quantum physical layer and is not prone to algorithmic attacks, leaving side channels as the primary adversarial target. Widely known side channels are those related to the losses of the quantum channel and to imperfections of the photon source or the single-photon detectors. Each of these side channels leads to one or more ways to attack the QKD system, e.g., the beam-splitting attack [25] for the quantum channel losses, the photon number splitting attack [3] for imperfect sources and the light back-flash attack [12] for imperfect detectors.

It should be emphasized that side channels are not a violation of quantum physics, nor a demonstration that QKD can be broken. They are ways to get around the intrinsic protection offered by QKD using potential imperfections in the implementation. On the other hand, it is not trivial to guarantee that an implementation is free from such imperfections and the QKD ISG is working to address this difficult aspect. Proper countermeasures against these side-channel attacks must be implemented. Metrology is needed to prove a countermeasure is effective, or that the relevant devices (e.g., the detectors) are unaffected by attempts to manipulate them [16].

The approach has been to accumulate a list of known side channels. For each side channel determine if it is applicable to a given implementation. If applicable, develop appropriate measurements to determine the effectiveness of the countermeasure. In some cases this could result in a need to redesign the countermeasure to reduce or eliminate the leakage. In other cases, it may only result in the need for extended security analysis, and ultimately, an adjustment to the final amount of secure key that can be extracted.

The QKD ISG is focusing on the quantum channel since the data on the classical channel does not need to be encrypted, and conventional (but information theoretically secure) integrity protection must be used to prevent tampering. In the most basic case the eavesdropper is passive and simply reads information that might have been inappropriately sent out of the channel along with the intended quantum signal. For example, if the source sometimes emits a light pulse that contains more than 1 photon, Eve could read the extra photon and learn the information without introducing a disturbance to the quantum channel. It can be seen that in this case Alice herself copied the same informative bit onto several photons thus providing Eve with a way to circumvent the no-copying (or no-cloning) theorem of quantum physics [27]. Another passive side channel would be if the detectors were to emit some light upon detecting an incoming photon. In this case too, Eve might simply record the emitted light and associate it with an information bit without being detected by Alice or Bob. Again this clearly does not violate any quantum principle but must be avoided through proper system design.

Eve is not obliged to be passive. She could try, for instance, to inject light into Alice's and Bob's systems in

order to modify the usual behavior of the components or to learn about the internal status of their components (e.g., by detecting reflections from within the systems). On Alice's side, one main example of such an eavesdropping strategy is the so-called "Trojan-horse attack". Eve injects light into the system. If this light can reach a signal modulator and if it is subsequently reflected back to the eavesdropper it could carry information about the internal status of the modulator [26]. Modulator values are classical and independently reading their values would not mean a disturbance of the quantum channel. The Trojan horse attack is not due to a failure of QKD but is made possible where good engineering design is not in place to protect internal active components from such attacks.

It should be noted that many side-channel attacks require specific actions by an attacker during the transmission of the key material itself. From the point of view of forward-security this is advantageous over conventional key distribution schemes where a copy of the classical data can be trivially stored for subsequent crypto-analysis. If a QKD side channel were to be discovered this would present a risk of data loss from that point forward but information exchanged before such a discovery would usually remain secure. By contrast all historic classical data protected by public key cryptography would become readable on the exposure of the private key, the discovery of a fast way to break the algorithmic security primitive or a defect in its implementation.

VII. Conclusion

If quantum computers become a reality, the key distribution algorithms that are currently in use will be broken and thus research is on-going in the area of quantum resistant key distribution algorithms [8][9]. QKD is one of those candidate algorithms. As an emerging technology, QKD stands out because of its information theoretic security. A vital concern for market place penetration is standards and certification methods. We have outlined a work-in-progress certification model along with a brief discussion of the need for characterization of QKD devices that operate at quantum power levels. Such characterization includes the side channel concerns that emanate from engineered components that attempt to approximate the theoretical models of components assumed in the security proofs. As we pointed out, the needed characterization is well under way at a number of the European National Measurement Institutes, while researchers are busy trying to close the gap between imperfect real devices and the security proofs. This standardization process is highlighting areas of QKD research needed to complete the development of these standards.

References

[1] J. Barrett, L. Hardy and A. Kent, "No signaling and quantum key distribution", Phys. Rev. Lett. **95**, 010503 (2005).

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", Proc. of the IEEE Int. Conf. on Comp. Syst. and Sign. Process., Bangalore, India, 1984.

[3] G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Limitations on practical quantum cryptography", Phys. Rev. Lett. **85**, 1330 (2000).

[4] T. E. Chapuran, P. Toliver, N. A. Peters *et al.*, "Optical networking for quantum key distribution and quantum communications," New J. Phys. **11**, 105001 (2009).

[5] I. Choi, *et al.*, "Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber", Opt. Expr. **22**, 23121 (2014).

[6] A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden and V. Martín, "Quantum metropolitan optical network based on wavelength division multiplexing", Opt. Expr. **22**, 1576 (2014).

[7] ETSI QKD-ISG, <http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution>

[8] ETSI Quantum-Safe-Crypto Workshop, Sophia Antipolis, France, Sep. 2013 <http://www.etsi.org/news-events/past-events/648-crypto-workshop2013>

[9] ETSI 2nd Quantum-Safe Crypto Workshop, Ottawa, Canada, Oct. 2015. <http://www.etsi.org/news-events/events/770-etsi-crypto-workshop-2014>

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

[11] INRIM - Istituto Nazionale di Ricerca Metrologica, Torino, Italy <http://www.inrim.it/>

[12] C. Kurtsiefer, P. Zarda, S. Mayer and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes - backdoor for eavesdropper attacks?", J. Mod. Opt. **48**, 2039 (2001).

[13] T. Langer and G. Lenhart "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD", New J. Phys. **11**, 055051 (2009).

[14] H. Lo, M. Curty and B. Qi, "Measurement-device-independent quantum key distribution", Phys. Rev. Lett. **108**, 130503 (2012).

[15] H-K. Lo, M. Curty and K. Tamaki, "Secure quantum key distribution", Nat. Phot. **8**, 595-604 (2014)

[16] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination", Nat. Phot. **4**, 686 (2010); Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the blinding attack in QKD", Nat. Phot. **4**, 800 (2010).

[17] MIQC - Metrology for Industrial Quantum Communications project <http://projects.npl.co.uk/MIQC/>

[18] NPL - National Physical Laboratory, Teddington, UK <http://www.npl.co.uk/>

[19] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Pent, and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber", Phys. Rev. X **2**, 041010 (2012).

[20] M. Peev, *et al.*, "The SECOQC quantum key distribution network in Vienna", New J. Phys. **11**, 075001 (2009).

[21] PTB – Physikalisch-Technische Bundesanstalt, Braunschweig, Germany, WG 4.13 <http://www.ptb.de/index_en.html>

[22] R. Renner and R. Konig, "Universally composable privacy amplification against quantum adversaries", Lect. Notes in Comp. Sci., vol. 3378, pp. 407-425 (2005).

[23] M. Sasaki, *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," Opt. Expr. **19**, 10387 (2011).

[24] 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).

[25] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems", arXiv:0906.4547 (2012).

[26] A. Vakhitov, V. Makarov and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography", J. Mod. Opt. **48**, 2023 (2001).

[27] W. Wootters and W. Zurek, "A Single Quantum Cannot be Cloned", Nature **299**, 802 (1982).