Quantum communication technology

N. Gisin and R.T. Thew

Quantum communication is built on a set of disruptive concepts and technologies. It is driven by fascinating physics and by promising applications. It requires a new mix of competencies, from telecom engineering to theoretical physics, from theoretical computer science to mechanical and electronic engineering. First applications have already found their way into niche markets, and university labs are working on futuristic quantum networks, but most of the surprises are still ahead of us. Quantum communication, and more generally quantum information science and technologies, are here to stay and will have a profound impact on the 21st century.

Introduction: Quantum communication enjoys an enviable position in physics, in between fundamental quantum mechanics and applied quantum optics [1]. For most physicists, quantum communication is merely a playground to explore fascinating topics like entanglement, superposition of large objects and, more generally, to look for places where quantum physics may fail, that is, to explore the limits of quantum physics. This playground requires new technologies and concepts. Usually, new technologies are driven by applications and quantum communication is no exception: the emerging and future technologies are driven by the need for

1. Fast quantum random number generators (QRNG): from cryptography to internet lotteries and gaming.
2. Reliable fibre-based quantum key distribution (QKD): for today's cryptography applications.
3. Quantum repeaters: for future continental scale fibre-optic quantum communication.
4. Earth to satellite links: for free space quantum communication.

The first two are already commercially available [2] and have also found small niche markets, while the latter two are still at an early stage.

Conceptual revolution: The basic idea of quantum communication is to take advantage of the oddities of quantum physics, like the uncertainty relation, the superposition principle and randomness. Note the conceptual revolution: instead of being afraid of quantum peculiarities and trying to avoid their detrimental effects for standard technologies, the new generation of quantum engineers aim at exploiting the new physics. In particular, they fully admit quantum physics as it stands and want to find original uses for its most counter-intuitive features. It is somewhat surprising, and disappointing, that it took six or seven decades before realising that this new physics ought to produce new technology. One might argue that the laser, semiconductors, superconductivity, among others, are technologies based on quantum physics. However, the big difference with quantum communication–and more generally with quantum information science and technology–is that it exploits quantum physics at the level of individual quanta.

The simplest example is the QRNG. Since the detection of a single photon after one of the two output ports of a beam splitter is an intrinsically random event, it offers a valuable source of randomness, see Fig. 1. Moreover, according to today's physics, such a source of randomness is unique: no device based on classical physics will ever produce true randomness, only at best 'pretty good' pseudo-random numbers, or noise, the origin of which is hard to fully identify. Yet, engineering a photon source, beam splitter and two CMOS-based single-photon detectors is not that complex: the existing commercial QRNG is about the size of a matchbox.

Another example, the basic principle of which is rather straightforward, is QKD [3]. Every first year quantum physics student knows that measurements tend to unavoidably disturb the quantum state of the system under investigation. This has puzzled generations of students and professors. Now, if this 'negative fact' is applied to an adversary, like a spy on a communication channel where the bits are carried by quantum systems, like photons, then it is the spy who cannot measure the bits without unavoidably leaving a trace of her intrusion under the form of some disturbance. Again, the reasoning is so simple that one wonders why no student came across that idea long ago (or did their professor tell them to shut up and compute?). Thus, while QRNGs generate randomness, QKD provides a means of distributing private (secure) randomness.

Further discussion of what quantum communication is and how it relates to entanglement and other quantum oddities can be found, e.g., in [1]. In the following we concentrate on future technology challenges.

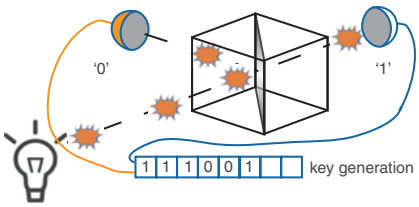

Fig. 1 *Quantum random number generation*

One single photon at a time is sent to a 50/50 beam splitter and can only exit in one of the output modes. This process is fundamentally random and the photon's detection is used to the generate truly random bit strings

Near-future technologies: The most advanced applications of quantum communication are clearly QRNG and QKD. The first was initially developed as a component of the second. It was originally thought that QRNG would also find applications in classical cryptography and in Monte-Carlo numerical simulations. QRNG did find some application in classical cryptography (e.g. the state of Geneva uses QRNG to produce the pin-codes used for Internet voting), but by far the largest application came as a surprise: Internet gambling for which it has now been certified by Metas [4]. This is a good example that applications of new technologies are hard to predict (physicists are especially bad at predicting good commercial applications!).

QRNG development is a timely topic, but any approach should concentrate on three key requirements:

1. Origin of randomness easily identifiable. One should be able to quantify how much randomness is truly quantum and how much is 'technological noise', e.g. thermal noise, detector noise etc.
2. Reliability, size and price. There is no fundamental reason for a QRNG not to be as small and cheap as a standard electronic chip.
3. Fast, in particular faster than classical, physical, RNG. The minimal rate of future QRNG should be in the range of hundreds of Mbit/s to Gbit/s.

Present QKD systems are mostly based on the historical BB84 protocol [5] (with some improvements like SARG [6] and Decoy-state [7–10]). However, better protocols have been invented in the context of fibre networks [11, 12]. It should be understood that BB84 originally was described using polarisation encoding, which is intuitively easy to understand, though in practice most real systems use some type of phase encoding that is more compatible with fibre optical systems. Despite these advances, the best QKD protocols have probably not yet been discovered. In any case, the protocol should use telecom photons (i.e. around 1550 nm), be compatible with standard optical fibre networks, and combine them with the necessary quantum features to guarantee 'quantum security'. This requires synergy between telecom engineers and quantum theorists.

Most technology developments on QKD concentrate on single-photon sources and on detectors [13]. However, somewhat surprisingly, single photons are not required for QKD: it is much easier to use so-called pseudo single-photon sources, i.e. strongly attenuated pulsed lasers. These are cheap, very reliable and fast (GHz rates). Note however, that single-photon sources could find their application in quantum repeaters [14], see below. Improving single-photon detectors, on the contrary, is a real must. The best detectors in terms of efficiency are superconductor bolometers, though these are prohibitively slow and operate at a few milliKelvin [15]. QKD applications need cheap, compact, electronically cooled detectors. Today this is achieved with semiconductor detectors (InGaAs APDs) though their performance and functionality needs to greatly improve. The APDs need to have lower dark count rates and 'afterpulsing' [16], which can introduce errors on the key. Furthermore, one of the most important characteristics of single-photon detectors, which is too often neglected, is the maximum count rate; future QKD systems will need to generate several Mbit/s of secure keys.

Some physicists speculate that QKD systems using not-so-weak laser pulses and homodyne detection, continuous variable (CV) QKD [17], will outperform single-photon schemes. They argue that, contrary to

single-photon schemes, homodyne detection always produces a result. This is correct, though the results are necessarily very noisy. We expect that it is more efficient to let nature select the cases with low noise, i.e. the cases where a single-photon is detected, rather than to always have a noisy result, where the noise has then to be removed by sophisticated error correction algorithms. Furthermore, for long distances the not-so-weak laser pulses tend to become pseudo-single-photon and the difference between the two systems vanishes. But, admittedly, the future will show us the truth with possibly both systems finding their niches.

An increasingly important requirement for future QKD schemes is that they run on the same fibre as the classical channels (both the classical processing and encrypted data channels). This is a serious challenge as the intensity difference is huge: 8 to 9 orders of magnitude. Hence, Raman scattering and other nonlinear effects have to be taken into account: even microwatts can produce enough photons to impair the quantum communication; recent efforts suggest that multiplexing quantum and classical channels in a fibre is limited to around 50 km [18] with current technology.

A serious push towards network compatibility can also be witnessed by the number of QKD testbeds running or planned worldwide. In 2008 in Vienna, the European consortium SECOQC demonstrated a mix of different QKD systems running in a complex network [19]. A triangular network has been running continuously in Geneva (data available in real-time at www.swissquantum.com) since April 2009. In Durban, South Africa, yet another network runs continuously carrying real data, and in October 2010 a large network will commence operation in Tokyo, while others have been announced for Madrid and China.

Another sign of the maturing of QKD is the appearance of quantum hackers. They do not attack the principle on which QKD relies, as this is provably secure, but take advantage of implementation weaknesses [20–22]. The latter can, and have to be, tested and strengthened, rendering QKD more and more reliable.

The rate of future development of QKD systems will be such that true Mbit/s one-time pad encryption should be possible over metropolitan networks. This is including all the real-time classical processing, communication and network overheads. It will thus be the result of an interdisciplinary team of engineers.

Future technologies and applications: This approach to fibre-based QKD is ultimately limited in distance to a few hundred kilometers. Indeed, for 1000 km, even with a perfect 10 GHz single-photon source, ideal detectors and 0.2 dB/km fibre losses one would detect only 0.3 photon on average per century! Consequently, futuristic continental scale quantum communication requires completely different technologies from today's QKD systems, mere improvements will not do. There are two main paths: satellite-based and quantum repeaters.

Satellite-based quantum communication is conceptually similar to fibre-based QKD, except that instead of fibres one sends the photons through free space between satellites and earth-based stations, both equipped with telescopes. Since no fibres are used, the choice of wavelength is compatible with silicon APDs. The technological requirements are not so much set by quantum optics, but are defined by the stringent specifications imposed by space agencies. Currently, ESA is investigating this possibility [23] and the USA and China also have programmes in place. We would not be surprised if China is the first to demonstrate a QKD link between earth and a satellite.

The alternative to satellites for continental distance quantum communication exploits a beautiful idea: quantum repeaters. Repeaters for classical optical communication, e.g. based on erbium fibre amplifiers, are well known, but unusable for quantum communication as any stimulated emission process necessarily brings with it spontaneous emission. At the single-photon level this noise is as strong as the signal, hence standard repeaters do not work in the quantum regime (this is a form of the quantum no-cloning theorem that follows from the linearity of Schrödinger's equation). The basic idea of quantum repeaters is to first establish entanglement between a series of stations, and next to use quantum physics [24] to teleport a 'photon' (more precisely, the quantum state carried by a photon) from one station to the next. As fascinating as this is, the technological challenge is huge. First, contrary to point-to-point QKD, quantum repeaters require entanglement, i.e. the ingredient necessary for quantum teleportation. Hence, mere attenuated laser pulses will never suffice. Next, it is crucial that one distributes entanglement between neighbour stations in parallel and stores it until two neighbouring stations are entangled. This required quantum memories [25], i.e. the capacity to store photons, or more precisely their quantum state, in a reversible way without losing any of their quantum features; in particular quantum memories ought to preserve entanglement. Furthermore, it has recently be shown that 'reasonable' rates ($\geq$ 1 bit/s over 1000 km) are possible only if the quantum memories are vastly multimode, i.e. able to store hundreds of quantum bits simultaneously.

Each of the necessary ingredients for a quantum repeater have been individually demonstrated in various labs, but not always with compatible technology and not with sufficiently high specifications. However, there are good reasons to be optimistic. First, as the challenges are truly fascinating, some of the best students are doing their PhDs on quantum repeaters. Furthermore, Europe and several national funding agencies have realised the potential and are thus supporting the research [26, 27].

Conclusions: Quantum communication technologies involve diverse disciplines, ranging from pure engineering problems (integrate a QRNG, optimise QKD systems), to fascinating basic physics (quantum memories and teleportation), via theoretical physics (design more efficient and secure QKD protocols) and computer science (design and implement the necessary processing for the raw data delivered by QKD) and lots of electronic, telecom and software engineering (the real work). The market is still small, but burgeoning, the physics fascinating, the challenges mind-boggling. Only one thing is certain: there will be surprises.

Acknowledgments: This work has been supported by the EU projects QuReP, Q-ESSENCE and QUIE^{2}T and by the Swiss NCCR-QP.

4 June 2010
doi: 10.1049/el.2010.1626
One or more of the Figures in this Letter are available in colour online.

N. Gisin and R.T. Thew (*Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland*)

E-mail: Robert.Thew@unige.ch

References

1 Gisin, N., and Thew, R.: 'Quantum communication', *Nature Photonics*, 2007, **1**, pp. 165–171
2 www.idQuantique.com
3 Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H.: 'Quantum cryptography', *Rev. Mod. Phys.*, 2002, **74**, (1), pp. 145–195
4 Swiss national metrology institute, http://www.metas.ch
5 Bennett, Ch.H., and Brassard, G.: 'Quantum cryptography: public key distribution and coin tossing'. Int. conf. Computers, Systems & Signal Processing, Bangalore, India, 1984, Vol. 10–12, pp. 175–179
6 Scarani, V., Acin, A., Ribordy, G., and Gisin, N.: 'Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations', *Phys. Rev. Lett.*, 2004, **92**, p. 057901
7 Hwang, W.-Y.: 'Quantum key distribution with high loss: toward global secure communication', *Phys. Rev. Lett.*, 2003, **91**, p. 057901
8 Wang, X.-B.: 'Beating the photon-number-splitting attack in practical quantum cryptography', *Phys. Rev. Lett.*, 2005, **94**, p. 230503
9 Lo, H.-K., Ma, X., and Chen, K.: 'Decoy state quantum key distribution', *Phys. Rev. Lett.*, 2005, **94**, p. 230504
10 Harrington, J.W., Ettinger, J.M., Hugues, R.J., and Nordholt, J.R.: 'Enhancing practical security of quantum key distribution with a few decoy states', *quant-ph/0503002, Los Alamos report LA-UR-05-1156*, 2005
11 Inoue, K., Waks, E., and Yamamoto, Y.: 'Differential-phase-shift quantum key distribution using coherent light', *Phys. Rev. A*, 2003, **68**, p. 022317
12 Stucki, D., Brunner, N., Gisin, N., Scarani, V., and Zbinden, H.: 'Fast and simple one-way quantum key distribution', *App. Phys. Lett.*, 2005, **87**, p. 194108
13 Hadfield, R.H.: 'Single-photon detectors for optical quantum information applications', *Nature Photonics*, **3**, p. 696
14 Sangouard, N., Simon, C., Minar, J., Zbinden, H., de Riedmatten, H., and Gisin, N.: , *Phys. Rev. A*, 2007, **76**, p. 050301
15 Lita, A.E., Miller, A.J., and Nam, S.W.: 'Counting near-infrared single-photons with 95% efficiency', *Opt. Exp.*, 2008, **16**, p. 3032

16 An afterpulse is caused by trapped charges in the APD being released when the detector is reset causing another avalanche resulting in a false detection event
17 Grosshan, F., and Grangier, Ph.: 'Continuous Variable Quantum Cryptography Using Coherent States', *Phys. Rev. Lett.*, 2002, **88**, p. 057902
18 Eraerds, P., Walenta, N., Legre, M., Gisin, N., and Zbinden, H.: 'Quantum key distribution and 1 Gbit/s data encryption over a single fibre', *J. Lightwave Technol.*, 2010, **28**, p. 952
19 Peev, M., *et al.*: 'The SECOQC quantum key distribution network in Vienna', *New J. Phys.*, 2009, **11**, p. 075001
20 Gisin, N., Fasel, S., Kraus, B., Zbinden, H., and Ribordy, G.: 'Trojan-horse attacks on quantum-key-distribution systems', *Phys. Rev. A*, 2006, **73**, p. 022320
21 Makarov, V., Anisimov, A., and Skaar, J.: 'Effects of detector efficiency mismatch on security of quantum cryptosystems', *Phys. Rev. A*, 2006, **74**, p. 022313
22 Qi, B., Fung, C.-H.F., Lo, H.-K., and Ma, X.: 'Time-shift attack in practical quantum cryptosystems', *Quantum Inf. Comput.*, 2007, **7**, p. 43
23 Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W., and Zeilinger, A.: 'Long distance quantum communications with entangled photons using satellites', *IEEE J. Sel. Top. Quantum Electron.*, 2005, **9**, p. 1541 (see also the Space Quest programme at http://www.quantum.at/quest)
24 Bennett, Ch.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W.K.: 'Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels', *Phys. Rev. Lett.*, 1993, **70**, p. 1895
25 Simon, C., *et al.*: 'Quantum memories: A review based on the European integrated project Qubit Applications (QAP)', *Eur. Phys. J. D*, 2010, **58**, p. 1
26 See the websites for QuRePP at http://quantumrepeaters.eu and Q-ESSENCE: http://qurope.eu/projects
27 For example in Switzerland, the NCCR – quantum photonics programme http://nccr-qp.epfl.ch