Quantum communication

Quantum communication, and indeed quantum information in general, has changed the way we think about quantum physics. In 1984 and 1991, the first protocol for quantum cryptography and the first application of quantum non-locality, respectively, attracted interest from a diverse field of researchers in theoretical and experimental physics, mathematics and computer science. Since then we have seen a fundamental shift in how we understand information when it is encoded in quantum systems. We review the current state of research and future directions in this field of science with special emphasis on quantum key distribution and quantum networks.

NICOLAS GISIN* AND ROB THEW

Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland.
***e-mail: Nicolas.Gisin@physics.unige.ch**

Quantum communication is the art of transferring a quantum state from one place to another. Traditionally, the sender is named Alice and the receiver Bob. The basic motivation is that quantum states code quantum information — called qubits in the case of two-dimensional Hilbert spaces — and that quantum information allows tasks to be performed that could only be achieved far less efficiently, if at all, using classical information. The best known example is quantum key distribution (QKD)[1–3]. In fact, there is another motivation, at least equally important to most physicists, namely the close connection between quantum communication and quantum non-locality[4,5], as illustrated by the fascinating process of quantum teleportation[6].

Quantum-communication theory is a broad field, including for example, communication complexity[7] and quantum bit-string commitment[8] . In this review we restrict ourselves to its most promising application, QKD, both point to point and in futuristic networks.

There are several ways to realize quantum communication. We list them below from the simplest to the more involved. As 'flying qubits' are naturally realized by photons, we often use 'photon' to mean 'quantum system', although in principle, any other quantum system could do the job.

The basic procedure is as follows. Alice encodes the state she wants to communicate into a quantum system and sends it to Bob. Entanglement is exploited to prepare the desired quantum state at a distance. The quantum state is then teleported from Alice to Bob and the entanglement is also teleported — entanglement swapping.

In this review, a more intuitive perspective of quantum communication, overlooking this complexity, will be considered first, starting from the basic ingredient, namely entanglement and its non-locality, continuing with weak-laser-pulse QKD and its security, before discussing quantum teleportation. Finally, a review of quantum relays as well as repeaters that require quantum memories will be given. Future challenges will be underlined throughout.

ENTANGLEMENT AND NON-LOCALITY

Entanglement is the essence of quantum physics. To understand this statement already stressed by Schrödinger[9] in 1935, it is worth presenting it in modern terms inspired by quantum-information theory. In science in general, all experimental evidence takes the form of conditional probabilities: if observer A_i performs the experiment labelled x_i, she observes a_i and in general the probability for all of the possible results is written $P(a_1 \ldots a_n | x_1 \ldots x_n)$. Such conditional probabilities are often called correlations. For simplicity, we restrict the discussion here to the bipartite case, denoting their correlation $P(a,b|x,y)$.

The correlations $P(a,b|x,y)$ carry a lot of structure. Apart from being non-negative and normalized, the local marginals are independent of the experiment performed by independent observers: $\sum_a P(a,b|x,y) = P(b|y)$, is independent of the experiment x performed by Alice. As a trivial example of independent observers, imagine two physicists performing different experiments in labs in distant countries, in which case the independence of the marginals is obvious. There is, however, another more interesting situation. Suppose the two parties perform similar experiments, but at two space-like separated locations, thus preventing any communication, as is the case in Fig. 1. It is therefore natural to assume that the local probabilities depend only on the local state of affairs and, as the local state of affairs may be unknown, one merely denotes them by a generic symbol, λ. Note that the local state of affairs at Alice's site and at Bob's site may still be correlated. This is why computer scientists call λ shared randomness. Given the local state of affairs, the correlations factorize to local correlations, $P(a,b|x,y,\lambda) = P(a|x,\lambda) \cdot P(b|y,\lambda)$, which necessarily satisfy some (infinite) set of inequalities, known as Bell inequalities[5,10]. Let us emphasize that there is no need to assume predetermined values to derive Bell inequalities, it suffices to assume that the probabilities of results of local experiments depend only on local variables.

Almost all correlations between independent observers known in science are local. The only exceptions are some correlations predicted by quantum physics, when the two observers perform measurements on two (or more) entangled systems. This implies that in some cases, a quantum experiment performed at two distant locations can't be completely described by the local state of affairs[5], a very surprising prediction of quantum physics indeed.

Einstein, among others, was so surprised by this that he concluded that it 'proves' the incompleteness of quantum mechanics[11]. Following Bohr's reply to the famous EPR (Einstein, Podolsky and Rosen) paper, the debate became philosophical. John Bell resolved this with the introduction of the experimental question of Bell inequalities[5,10,12] and remarkably, by 1991 it had become applied physics[2]. Indeed, it was realized that the

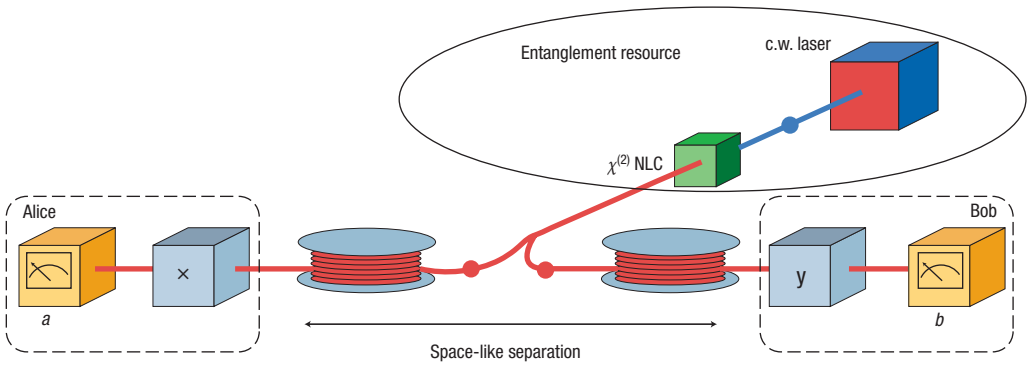

Figure 1 Revealing non-locality. Alice and Bob independently perform experiments x and y, on an entangled state at space-like separated locations, and study the correlations for the results *a* and *b*.

non-existence of a local state of affairs guarantees that Alice's and Bob's data have no duplicate anywhere else in the world, in particular not in any adversary's hands. The intuition is clear: as there is no λ, no one can hold a copy of λ, hence no one can compute the probabilities for Alice's and Bob's data, $P(a|x,\lambda)$ and $P(b|y,\lambda)$. Consequently, Alice's and Bob's data have some secrecy. This is the essence of QKD, but clearly, this intuition needs elaboration (see below).

Let us conclude this section with a brief review of the experimental and theoretical status of quantum non-locality. Today, no serious physicist doubts that nature exhibits quantum non-locality. Despite the depth of such a conclusion (whose revolutionary aspect is often not fully appreciated), it has turned out to be exceedingly difficult to realize an experiment between space-like separated parties with detection efficiencies high enough to avoid the detection loophole[13]. Although the detection loophole was closed in an ion-trap experiment, the close proximity of the ions meant that these were not space-like separated[14]. Only a few experiments have managed to perform space-like separated tests with entanglement[15] distributed over ten kilometres both in fibre[16–18] and free space[19], without closing the detection loophole. Also with respect to theory, it is surprisingly poorly understood why the most well-known Bell inequality, the CHSH-inequality, named after its discoverers John Clauser, Michael Horne, Abner Simony and Richard Holt[12], seems the most efficient despite the existence of infinitely many other Bell inequalities (see ref. 10). In particular, we still have no practical way to tell whether a given quantum state is able to exhibit non-locality or not. This limited understanding is especially frustrating given that the experimental violation of a Bell inequality is the only direct evidence for the presence of entanglement. Indeed, all the other entanglement witnesses require that the dimension of the relevant Hilbert space[20] is known.

QUANTUM KEY DISTRIBUTION

One simple way to think about entanglement for the non-specialist is that some composite systems, such as pairs of photons, are able to provide the same random answer when asked the same question. Let us emphasize that the answer (measurement result) is random, but it is precisely the same randomness that manifests itself at two distant locations, provided that Alice and Bob perform the same experiment (or experiments related by a simple transformation). It then suffices that Alice and Bob independently choose to perform a series of experiments, drawn from a pre-established list of possible experiments, and, after recording all their data, they post-select those corresponding to the cases in which they happened, by chance, to have chosen to perform the same experiment. In these cases, they asked the same question and thus obtained the same random answer. This provides them with a cryptographic key. The secrecy of such keys will be analysed below. In this section the focus is on practical ways to implement QKD.

The first choice that the quantum-telecom engineer has to face is that of the wavelength. Although most quantum-optics experiments since the invention of the laser have used silicon-based detectors, limited to wavelengths below 1 μm, for long-distance quantum communication, wavelengths suitable for fibre-optic communication, 1.3 μm and 1.5 μm, should be considered. (Although space communication to satellites is a serious and fascinating alternative[21], it is beyond the scope of this review). Nowadays, there are several options for detectors compatible with optical fibres, ranging from detectors based on superconduction transitions to commercially available avalanche photodiodes.

The second choice concerns the degree of freedom in which to encode the qubits. An obvious first choice is the state of polarization, but polarization is unstable in standard fibres, especially in aerial fibre cables. In 1989, Jim Franson proposed the use of energy–time entanglement[22], with the initial objective to test a Bell inequality, though later adapted to quantum communication. Figure 2 illustrates Franson's idea, consisting of a continuous-wave (c.w.) laser that pumps a $\chi^{(2)}$ (where χ refers to the crystal susceptibility) nonlinear crystal (NLC), for which each photon from the pump laser has a probability of, at best, 10^{-6} of being down-converted into a pair of photons, depending on the crystal[23]. Each of the two photons has an uncertain energy (that is, an uncertain wavelength), where 'uncertain' should be understood in the quantum-mechanical sense. However, through energy conservation, the sum of the energy of the two photons equals the well-defined energy of the pump-laser photon. Moreover, both photons are created at the same time (again through energy conservation), but this time is 'quantum-uncertain' within the long coherence time of the pump laser. We see a nice analogy with the case presented by EPR: the energy and the age of each photon are uncertain, but the sum of the energies and the difference between their ages are both sharply defined. Look now at the two unbalanced interferometers and detectors on both sides of Fig. 2, which have replaced our abstract operations and measurements from Fig. 1, and consider the cases where both photons hit a detector simultaneously. Recalling that the photons were produced simultaneously, this can happen in two ways: both photons propagate through the short arm of their interferometers; or both take the long arms.

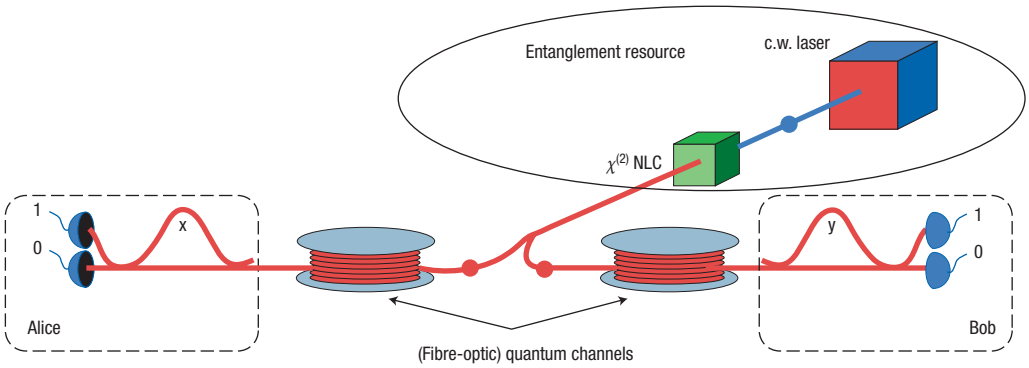

Figure 2 The Franson interferometer for testing the energy–time entanglement of the entanglement resource. The correlations between each of Alice's and Bob's results 0 or 1 depends on both the phase measurement settings x and y.

If the imbalances of both interferometers are alike and much smaller than the pump-laser coherence length, then these two paths are indistinguishable. According to quantum physics, one should thus add the probability amplitudes and expect interference effects. These are two-photon interferences and have been used to violate the Bell CHSH inequality[16,24,25]. This configuration is thus suitable for QKD, but it is not practical using today's technology — hence it can be simplified[26].

First, let's move the source from the centre towards Alice, as in Fig. 3a, thus limiting the number of sites from three to two. Now the photons don't arrive simultaneously at their detectors but, for an appropriate difference of arrival times, the same reasoning as above applies: there are still interferences between the short–short and the long–long two-photon paths. The second simplification consists of moving the source to the left of Alice's interferometers, Fig. 3b. Now the two interfering paths are the short–long and long–short paths. As before, they are indistinguishable and thus lead to interferences, though now one of the two photons is not really used (except possibly as a herald). This leads to the third and major simplification: replace this two-photon source with a simple weak laser pulse, Fig. 3c. The story about the interfering paths remains the same, but the source is now very simple and reliable — a standard telecom laser diode with enough attenuation. A 60- to 100-dB attenuation (requiring a well-calibrated attenuator) ensures that only a very small fraction of the laser pulses contain more than one photon. It is essential to understand that, provided this fraction of multi-photon pulses is known, the security of such a weak-laser-pulse QKD system is in no way compromised[27,28]. Moreover, using the recent idea of decoy states, weak-laser-pulse QKD obeys the same scaling law as ideal single-photon QKD[50–52].

Today, all practical QKD systems use this simplification[29–43] and the major challenge for QKD (besides the distance, discussed below) is the secret-bit rate. Given that the source is not an issue, there remains two ways to improve this. First, we can make technical improvements, for example to the detectors, whose maximal count rates are severely limited by dark counts and after-pulses[44,45], by using better InGaAs avalanche photodiodes, up-conversion detection schemes[43,46] or superconducting detectors[47,48]. Second, the historical protocols, like BB84 and Ekert91 (refs 1 and 2), were invented for the sake of presenting a beautifully simple idea, but today's many new protocols have been designed with the aim of optimizing their implementation using weak laser pulses[38,41,49–53] or mesoscopic systems[54]. It is probable that more efficient protocols are yet to be discovered by teams combining telecom engineers and quantum physicists.

SECURITY OF QKD

The intuition as to why QKD provides perfectly secret bits is quite straightforward (as has been discussed above). However, the details of the proofs are very involved and many questions remain open, especially concerning optimality[28,55,56].

It is, however, helpful to highlight just a few key concepts. We can characterize bounds on the security by comparing the Shannon mutual information[57] for Alice and Bob $I(A{:}B)$ and for Alice and an adversary, traditionally called Eve, $I(A{:}E)$. It is intuitive (and can be proven[58,59]) that if Bob has more information than Eve on Alice's data, $I(A{:}B) > I(A{:}E)$, then Alice and Bob can distil a secret key out of their data. This first intuition is, however, incomplete. Eve's information should be treated as quantum information: there is no way to know whether she performed measurements on her quantum systems (resulting in classical information) before the key is used. As our goal is to provide a secret key, whose security does not rely on assumptions about Eve's technology, whether it is classical computer power or quantum technology, this remark has to be taken seriously. Fortunately, the quantum analogue of Shannon mutual information[60] and its consequences, have recently been resolved[55].

A second limitation to the above intuitive idea is the so-called man-in-the-middle attack: how can Alice and Bob be sure they really talk to each other? The answer is known and requires that they start from an initial short common secret, so as to be able to recognize each other. It has been shown that QKD provides much more secret key than it consumes. In this sense, QKD should be called quantum key expansion.

A third, less-studied difficulty is side-channels: how can Alice be sure she doesn't inadvertently code more than one degree of freedom? For example, it might be that her phase modulator introduces a measurable distortion to the pulse envelope, in which case Eve could measure the encoded bit indirectly and remain undetected. Related dangers are the Trojan horse attacks, in which Eve actively profits from the quantum channel (that is, the optical fibre) to probe inside either or both of Alice's and Bob's systems. Not too much is known how to counter such attacks, except by emphasizing that real systems should be well characterized (see for example, refs 61 and 62).

Before we end here, let us briefly elaborate on the widely used terminology 'unconditionally secure'. Note that there is nothing like this: security proofs rely on assumptions and some assumptions are difficult to check in realistic systems. The historical reason for that terminology comes from classical cryptography where computer scientists use it to mean 'not conditioned on assumptions about the adversary's classical computation power', a meaning quite foreign to quantum physics.

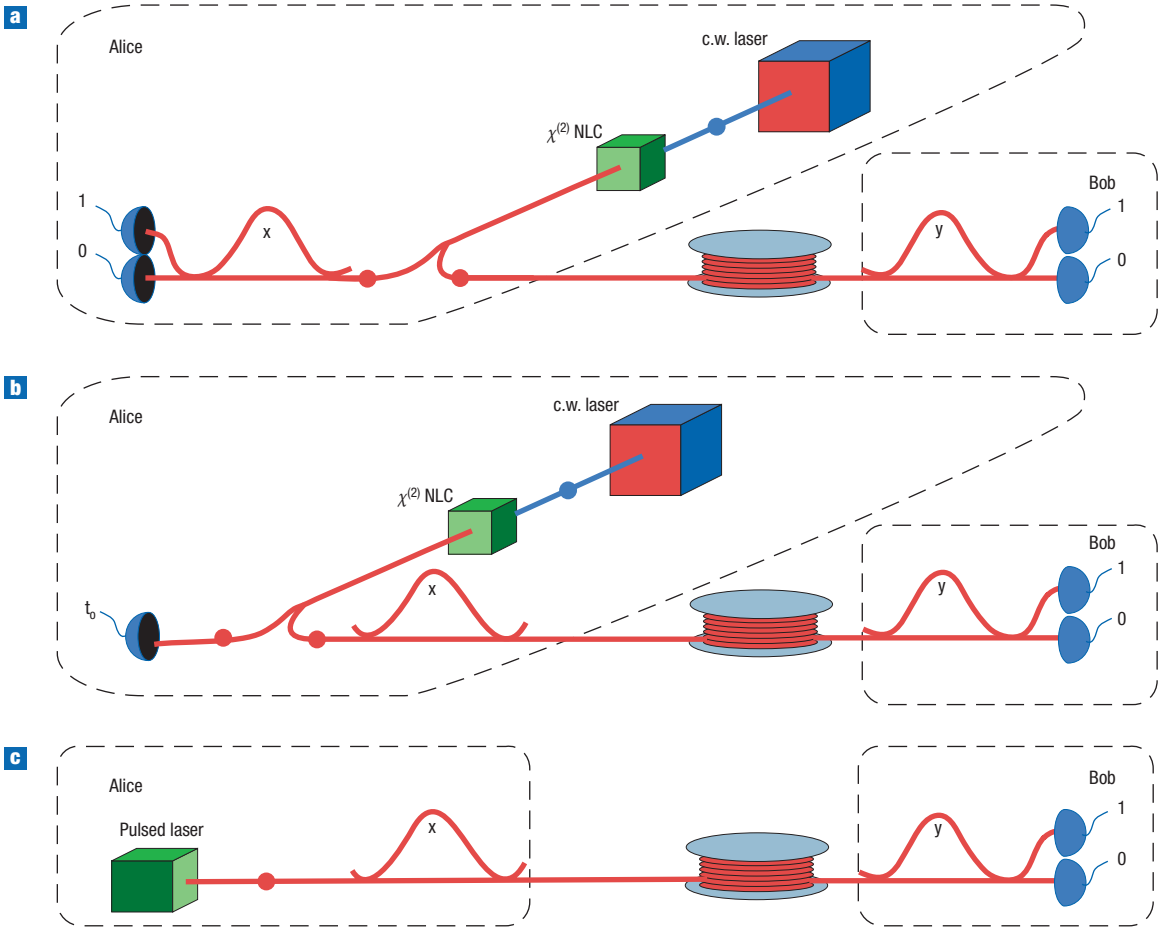

Figure 3 Simplifying the Franson scheme. **a**, The entanglement resource from Fig. 2 is moved to Alice's side. **b**, The entanglement resource is placed before Alice's interferometer — the interfering paths are different, but we don't need the extra photon except as a herald. **c**, Remove the entanglement resource and replace with a single heralded photon with attenuated pulsed diode laser.

QUANTUM TELEPORTATION

Quantum teleportation is the most fascinating manifestation of quantum non-locality: an 'object' dissolves at one point and reappears at a distance[6]. Well, not the entire object, 'only' its quantum state, that is, its ultimate structure, is transferred from here to there without ever existing at any intermediate location. The energy–matter must already be present at the receiver side and must be entangled with the transceiver. Quantum teleportation attracts a lot of attention from physicists and journalists, and rightly so. Mathematically, quantum teleportation is very simple, but understanding it requires clarifying some often confused concepts concerning quantum non-locality.

The entire process requires three steps. Consider Fig. 4 where first there is the distribution of entanglement, usually photon pairs sent through optical fibres (for ions see refs 63 and 64). The 'quantum-teleportation channel' is then established and, in principle, the fibres could be removed. Next, the sender performs a so-called Bell-state measurement (BSM) between his photon from the entangled pair and the qubit photon that carries the quantum state to be teleported[65,66]. Technically, this is the most difficult step and usually only a partial BSM is realized (see, however, refs 67 and 68). The BSM provides no information at all about the teleported state, but tells us something about the relationship between the two photons[69].

This ability to acquire information only about the relationship between two quantum systems is typical of quantum physics: it is another manifestation of entanglement, but in this case it is not present between the incoming photons to be measured. The entanglement lies in the eigenvectors of the operator representing the BSM. Hence, entanglement plays a dual role in teleportation. Finally, the third step consists of Alice informing Bob of the result of her BSM and Bob performing a result-dependent unitary rotation on his system. Only after this operation is the teleportation process finished. Note that the size of the classical information sent by Alice to Bob is infinitely smaller than the information required to give a classical description of the teleported quantum state, but it is the need for this message that ensures that the teleportation process is slower than the speed of light.

The BSM provides a fundamental limit to these experiments. It has been proven that no BSM with an efficiency greater than 50% is achievable with linear optics[70]. To perform these partial BSMs, the two photons should arrive on a beam splitter simultaneously within their coherence time. As single-photon detectors have a large timing jitter, the timing has so far always been set by bulky and expensive femtosecond lasers. Moreover, the length of the optical fibres needs to be stabilized within the coherence length of the photons, typically a few tens of micrometres, an unrealistic

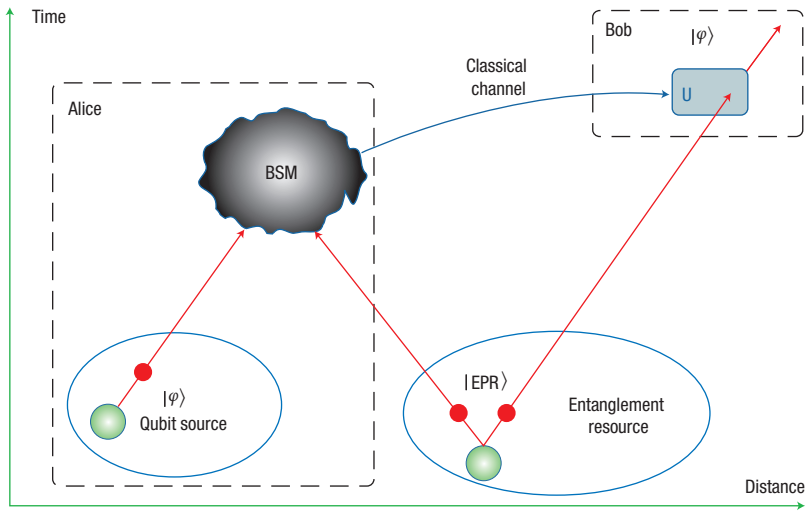

Figure 4 Quantum teleportation. Alice performs a BSM, a joint measurement, on the unknown qubit $|\varphi\rangle$ and one photon from the entangled state $|EPR\rangle$. The result does not reveal the state of the qubit, but is sent to Bob, who performs a result-dependent operation U to complete the teleportation.

requirement over tens of kilometres. Consequently, some of the next steps will require detectors with improved jitter[43,71] as well as compact sources of entangled photons with significantly increased single-photon coherence. Alternatively, this limitation has been overcome in some experiments by using continuous variables[72,73] or hyperentanglement[74], whereas others have used generalized quantum measurements to probabilistically distinguish three out of the four Bell states[75] (it is an open question whether all four could be distinguished using passive linear optics). The intense interest in the BSM is due to the key role it plays not only in teleportation, but more importantly its role in long-distance quantum communication and specifically entanglement swapping.

ENTANGLEMENT SWAPPING, RELAYS AND QUANTUM REPEATERS

What happens if one photon from an entangled pair is teleported, that is, if entanglement itself is teleported? This process, known as entanglement swapping, allows one to entangle photons that have no common past[76]. The general idea consists of first establishing entanglement between not-too-distant nodes, then teleporting the entanglement from one node to the next. This is called a quantum relay[77] and the general principle is illustrated in Fig. 5a. So far only very few groups have demonstrated this process[78–80], but this is an active field of research as it has the potential to increase the distance for QKD.

However, the distances achievable with quantum relays are still limited. The reason is that in order to be able to swap the entanglement of pair A–B and of pair B–C to A–C, the entanglement between the pairs A–B and B–C has to be established first. However, the probability that all photons propagate between A and B and between B and C is precisely the same probability that a photon propagates from A directly to C. Hence, there is no hope that entanglement swapping by itself helps to increase the bit rate. Still, quantum relays may be useful for some intermediate distances, because in principle they allow the detrimental effects of detector dark counts to be mitigated[77,81,82].

To efficiently overcome the distance limitation, quantum repeaters are needed, which require both quantum relays and quantum memories[83,84]. The basic idea is that if the entanglement distribution has succeeded between nodes A and B, but failed between B and C, the A–B entanglement can be stored in a quantum memory and the B–C entanglement distribution can be restarted. One can imagine concatenating entangled systems to further increase this distance (see Fig. 5b). Ideally, one would also like the quantum memories to contain a rudimentary (few qubit) quantum computer, able to realize the 2-qubit gates for purification or distillation techniques[85,86] to concentrate the entanglement contained in each of two pairs of qubits into a single highly entangled qubit pair. In practice, we are a long way from here, but have started to think about interim possibilities. In the first instance, there is the possibility of having a quantum memory without knowing whether it is loaded. In this case the sources could be placed closer to one of the quantum memories in each chaining element of Fig. 5b. The motivation behind the asymmetric sources is that if one photon is directly absorbed by the quantum memory, it is more certain that it is loaded than if it had been transmitted, and possibly absorbed or lost in the fibre. This thinking is reminiscent of the simplifications that were made with respect to Fig. 2 and the evolution from Franson's intereferometer to weak-pulse-encoded QKD.

The development of a fully operational quantum repeater and a realistic quantum-network architecture are grand challenges for quantum communication. Despite some claims, nothing like this has been demonstrated so far and one should not expect any real-world demonstration for another five to ten years.

QUANTUM MEMORIES

If quantum repeaters are to be built successfully, then a quantum memory that is able to store a qubit for a period sufficient to allow several rounds of communication between the nearby nodes (typically several milliseconds) is required. In Fig. 5B we denote the quantum memory by some absorbing medium, but more importantly, also with a heralding mechanism so we know when it is loaded. Furthermore, it should either be possible to perform a BSM between two stored qubits or to trigger the release of photons carrying the qubits with a jitter small enough to achieve this, and all of this at wavelengths and bandwidths compatible with existing fibre-optic networks. Today, the best quantum memory by far is a simple fibre loop (though it does not have all the specifications mentioned above). Storing qubits in some atoms, either in traps or

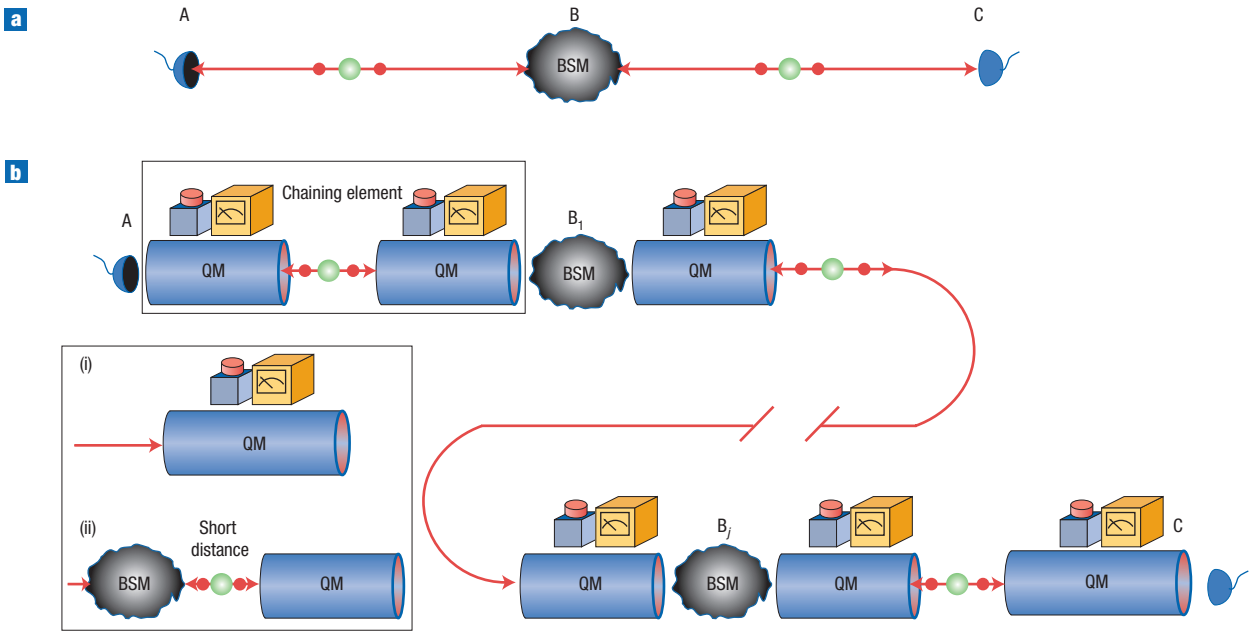

Figure 5 Quantum networks. **a**, Quantum relay. Entanglement resources and quantum channels joined by means of a BSM, where the entanglement of photons A–B and B–C is swapped to A–C. **b**, Quantum repeater. An entanglement resource and quantum memories (QM) provide a chaining element that can be concatenated for longer quantum-communication distances, where B_1 and B_j denote the connecting BSM links in the repeater chain. The inset illustrates the difference between a 'heralded QM', (i), and a possible modification for a QM without heralding, (ii).

in some solid-state devices, is a huge challenge. But the potential applications, both for fundamental experiments (for example, long-distance loophole-free Bell tests) and for a worldwide quantum web, motivates many physicists. Moreover, it is probable that the successful techniques will also find applications in other types of quantum-information processors.

At present there is an increasing number of groups working towards quantum memories from a range of different perspectives. The different approaches have so far been motivated by the degree of freedom chosen to encode the quantum state. We have already seen some progress: continuous-variable systems in atomic vapour[87]; atomic ensembles[88–90]; polarization of atom–photon systems[91]; others are using nitrogen-vacancy centres in diamonds[92]; as well as rare-earth ions in fibres and crystals[93,94]. Indeed this last case is interesting, as most proposals have focused on storing a single mode, or single quantum state, whereas the rare-earth systems offer the possibility of storing several modes and many quantum states, which could have significant practical implications. These and many more approaches are now being actively pursued within national and international collaborative programmes around the world[95–98].

FUTURE OUTLOOK

The field of quantum communication has established itself over recent years thanks to its driving force, QKD, and to the fascinating process of quantum teleportation, not to mention continuous-variable[99] and satellite quantum communication[21] and linear-optics quantum computation[100]. It will be an important part of physics in the decades to come, with great challenges in quantum memories and repeaters for worldwide applications. It is an ideal teaching tool and is attracting bright young physicists who are learning to build the bridge between quantum physics and communication technologies.

doi: 10.1038/nphoton.2007.22

References

1. Bennett, C. H. & Brassard, G. in *Int. Conf. Computers, Systems & Signal Processing, Bangalore* 175–179 (1984).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
4. Popescu, S. & Rohrlich, D. *Introduction to Quantum Computation and Information: The Joy of Entanglement* (eds Lo, H.-K., Popescu, S. & Spiller, T.) (World Scientific, 1998).
5. Bell, J. S. *Collected Papers on Quantum Philosophy: Speakable and Unspeakable in Quantum Mechanics* (Cambridge Univ. Press, Cambridge, 1987).
6. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895 (1993).
7. Brassard, G. Quantum communication complexity. *Found. Phys.* **33,** 1593–1616 (2003).
8. Buhrman, H., Christandl, M., Hayden, P., Lo, H.-K. & Wehner, S. On the (im)possibility of quantum string commitment. *Phys. Rev. Lett.* (in the press); preprint at <http://arxiv.org/abs/quant-ph/0504078> (2005).
9. Schrödinger, E. Probability relations between separated systems. *Proc. Cambridge Phil. Soc.* **32,** 446 (1935).
10. Collins, D. & Gisin, N. A relevant two qubit Bell inequality inequivalent to the CHSH inequality. *J. Phys. A* **37,** 1775–1787 (2004).
11. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47,** 777–780 (1935).
12. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880 (1969).
13. Gisin, B. & Gisin, N. A local hidden variable model of quantum correlation exploiting the detection loophole. *Phys. Lett. A* **260,** 323–327 (1999).
14. Rowe, M. A. *et al.* Experimental violation of a Bell's inequality with efficient detection. *Nature* **409,** 791–794 (2001).
15. Aspect, A., Dalibard, J. & Roger, G. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.* **49,** 1804 (1982).
16. Tittel, W., Brendel, J., Zbinden, H. & Gisin, N. Violation of Bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.* **81,** 3563–3566 (1998).
17. Weihs, G., Jennewein, T., Simon, C., Weinfurter, H. & Zeilinger, A. Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.* **81,** 5039–5043 (1998).
18. Zbinden, H., Gisin, N., Brendel, J. & Tittel, W. Experimental test of nonlocal quantum correlation in relativistic configurations. *Phys. Rev. A* **63,** 022111 (2001).
19. Peng, C. *et al.* Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. *Phys. Rev. Lett.* **94,** 150501 (2005).
20. Acin, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97,** 120405 (2006).
21. Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. & Zeilinger, A. Long distance quantum communications with entangled photons using satellites. *IEEE J. Sel. Top. Quant. Electron.* **9,** 1541–1551 (2003).
22. Franson, J. D. Bell inequality for position and time. *Phys. Rev. Lett.* **62,** 2205–2208 (1989).

23. Tanzilli, S. *et al.* Highly efficient photon-pair source using a periodically poled lithium niobate waveguide. *Electron. Lett.* **37,** 26–28 (2001).
24. Brendel, J., Mohler, E. & Martienssen, W. Experimental test of Bell's Inequality for energy and time. *Europhys. Lett.* **20,** 575–580 (1992).
25. Kwiat, P. G., Steinberg, A. M. & Chiao, R. Y. High-visibility interference in a Bell-inequality experiment for energy and time. *Phys. Rev. A* **47,** R2472–R2475 (1993).
26. Gisin, N. & Brunner, N. in *Proc. Les Houches Summer School 2003* (eds Esteve, D., Raimond, J. M. & Dalibard, J.) 295–314 (Elsevier, Amsterdam, 2003).
27. Inamori, H., Lütkenhaus, N. & Mayers, D. Unconditional security of practical key distribution. *European Phys. J. D* (in the press); preprint at <http://lanl.arxiv.org/abs/quant-ph/0107017> (2001).
28. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **4,** 325–360 (2004).
29. www.idQuantique.com
30. www.magiqtech.com
31. www.smartquantum.com
32. Townsend, P., Rarity, J. G. & Tapster, P. R. Single photon interference in a 10 km long optical fiber interferometer. *Electron. Lett.* **29,** 634–639 (1993).
33. Muller, A., Zbinden H. & Gisin, N. Underwater quantum coding. *Nature* **378,** 449 (1995).
34. Bourennane, M. *et al.* Experiments on long wavelength (1550nm) 'plug and play' quantum cryptography systems. *Opt. Express* **4,** 383–387 (1999).
35. Hughes, R., Morgan, G. & Peterson, C. Quantum key distribution over a 48km optical fibre network. *J. Mod. Opt.* **47,** 533–547 (2000).
36. Bethune, D. & Risk, W. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *IEEE J. Quantum Electron.* **36,** 340–347 (2000).
37. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. Quantum key distribution over 67 km with a plug & play system. *New J. Phys.* **4,** 41 (2002).
38. Inoue, K., Waks, E. & Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A* **68,** 022317 (2003).
39. Gobby, C., Yuan, Z. L. & Shields, A. J. Unconditionally secure quantum key distribution over 50km of standard telecom fibre. *Electron. Lett.* **40,** 1603–1604 (2004).
40. Elliott, C. *et al.* Current status of the DARPA Quantum Network. Preprint at <http://arxiv.org/abs/quant-ph/0503058> (2005).
41. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87,** 194108 (2005).
42. Takesue, H. *et al.* Differential phase shift quantum key distribution experiment over 105 km fibre. *New. J. Phys.* **7,** 232 (2005).
43. Thew, R. T. *et al.* Low jitter up-conversion detectors for telecom wavelength GHz QKD. *New J. Phys.* **8,** 32 (2006).
44. Ribordy, G. *et al.* Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: Current performance. *J. Mod. Opt.* **51,** 1381–1398 (2004).
45. Pellegrini, S. *et al.* Design and performance of an InGaAs-InP single-photon avalanche diode detector. *IEEE J. Quant. Electron.* **42,** 397–403 (2006).
46. Langrock, C. *et al.* Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled $LiNbO_3$ waveguides. *Opt. Lett.* **30,** 1725–1727 (2005).
47. Gol'tsman, G. N. *et al.* Picosecond superconducting single-photon optical detector. *Appl. Phys. Lett.* **79,** 705 (2001).
48. Miller, A. J., Nam, S. W., Martinis, J. M. & Sergienko, A. V. Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination. *Appl. Phys. Lett.* **83,** 791–793 (2003).
49. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Phys. Rev. Lett.* **92,** 057901 (2004).
50. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
51. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
52. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
53. Harrington, J. W., Ettinger, J. M., Hugues, R. J. & Nordholt, J. R. Enhancing practical security of quantum key distribution with a few decoy states. Los Alamos report LA-UR-05–1156; preprint at <http://arxiv.org/abs/quant-ph/0503002> (2005).
54. Grosshan, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88,** 057902 (2002).
55. Kraus, B., Gisin, N. & Renner, R. Lower and upper bounds on the secret key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **95,** 080501 (2005).
56. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
57. Cover, T. M & Thomas, J. A. *Elements of Information Theory* (Wiley, New York, 1991).
58. Csiszár, I. & Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theor.* **IT-24,** 339–348 (1978).
59. Maurer, U. M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theor.* **39,** 733–742 (1993).
60. Renner, R. & Wolf, S. in *Proc. 2004 IEEE Int. Symp. Inf. Theor.* 233 (ISIT, 2004).
61. Makarov, V, Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74,** 022313 (2006).
62. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73,** 022320 (2006).
63. Barrett, M. D. *et al.* Deterministic quantum teleportation of atomic qubits. *Nature* **429,** 737–739 (2004).
64. Riebe, M. *et al.* Deterministic quantum teleportation with atoms. *Nature* **429,** 734–737 (2004).
65. Bouwmeester, D. *et al.* Experimental quantum teleportation. *Nature* **390,** 575–579 (1997).
66. Weinfurter, H. Experimental Bell-state analysis. *Europhys. Lett.* **25,** 559 (1994).
67. Boschi, D., Branca, S., De Martini, F., Hardy, L. & Popescu, S. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **80,** 1121–1125 (1998).
68. Kim, Y.-H., Kulik, S. P. & Shih, Y. Quantum teleportation of a polarization state with a complete Bell state measurement. *Phys. Rev. Lett.* **86,** 1370–1373 (2001).
69. Gisin, N. & Iblisdir, S. Quantum relative states. *Euro. Phys. J. D* **39,** 321 (2006).
70. Lütkenhaus, N., Calsamiglia, J. & Suominen, K. A. Bell measurements for teleportation. *Phys. Rev. Lett.* **59,** 003295 (1999).
71. Diamanti, E., Takesue, H., Langrock, C., Fejer, M. M. & Yamamoto, Y. 100 km secure differential phase shift quantum key distribution with low jitter up-conversion detectors. *Opt. Exp.* **14,** 13073 (2006).
72. Braunstein, S. L. & Kimble, H. J. Teleportation of continuous quantum variables. *Phys. Rev. Lett.* **80,** 869–872 (1998).
73. Furusawa, A. *et al.* Unconditional quantum teleportation. *Science* **282,** 706–709 (1998).
74. Schuck, C., Huber, G., Kurtsiefer, C. & Weinfurter, H. Complete deterministic linear optics Bell state analysis. *Phys. Rev. Lett.* **96,** 190501 (2006).
75. Van Houwelingen, J., Brunner, N., Beveratos, B., Zbinden, H. & Gisin, N. Quantum teleportation with a three-Bell-state analyzer. *Phys. Rev. Lett.* **96,** 130502 (2006).
76. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71,** 4287–4290 (1993).
77. Jacobs, B. C., Pittman, T. B. & Franson, J. D. Quantum relays and noise suppression using linear optics. *Phys. Rev. A* **66,** 052307 (2002).
78. Pan, J.-W., Bouwmeester, D. & Zeilinger, A. Experimental entanglement swapping: Entangling photons that never interacted. *Phys. Rev. Lett.* **80,** 3891 (1998).
79. Jennewein, T., Weihs, G., Pan, J.-W., Weinfurter, H. & Zeilinger, A. Experimental nonlocality proof of quantum teleportation and entanglement swapping. *Phys. Rev. Lett.* **88,** 017903 (2002).
80. de Riedmatten, H. *et al.* Long-distance entanglement swapping with photons from separated sources. *Phys. Rev. A* **71,** 05302 (2005).
81. Waks, E., Zeevi, A. & Yamamoto, Y. Security of quantum key distribution with entangled photons against individual attacks. *Phys. Rev. A* **65,** 052310 (2002).
82. Collins, D., Gisin N. & de Riedmatten, H. Quantum relays for long distance quantum cryptography. *J. Mod. Opt.* **52,** 735–753 (2005).
83. Briegel, H. J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81,** 5932–5935 (1998).
84. Duan, L. M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414,** 413–418 (2001).
85. Bennett, C. H. *et al.* Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76,** 722 (1996).
86. Deutsch, D. *et al.* Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77,** 002818 (1996).
87. Julsgaard, B., Sherson, J., Cirac, J. I., Fiurasek, J. & Polzik, E. S. Experimental demonstration of quantum memory for light. *Nature* **432,** 482 (2004).
88. Chou, C. W. *et al.* Measurement-induced entanglement for excitation stored in remote atomic ensembles. *Nature* **438,** 828–832 (2005).
89. Chanelière, T. *et al.* Storage and retrieval of single photons transmitted between remote quantum memories. *Nature* **438,** 833–836 (2005).
90. Eisaman, M. D. *et al.* Electromagnetically induced transparency with tunable single-photon pulses *Nature* **438,** 837–841 (2005).
91. Volz, J. *et al.* Observation of entanglement of a single photon with a trapped atom. *Phys. Rev. Lett.* **96,** 030404 (2006).
92. Tamarat, P. *et al.* Stark shift control of single optical centers in diamond. *Phys. Rev. Lett.* **97,** 083002 (2006).
93. Kraus, B. *et al.* Quantum memory for nonstationary light fields based on controlled reversible inhomogeneous broadening. *Phys. Rev. A* **73,** 020302R (2006).
94. Alexander, A. L., Longdell, J. J., Sellars, M. J. & Manson, N. B. Photon echoes produced by switching electric fields. *Phys. Rev. Lett.* **96,** 043602 (2006).
95. http://www.qubitapplications.com
96. http//:www.scala-ip.org
97. http://www.qist.ect.it
98. http://www.qist.lanl.gov
99. Braunstein. S. L. & van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77,** 513–577 (2005).
100. Myers, C. R. & Laflamme, R. Linear optics quantum computation: An overview. Preprint at <http://arxiv.org/abs/quant-ph/0512104> (2005).

Acknowledgements

This work was supported by the EC under projects QAP (contract no. IST-015848) and SECOQC (contract no. IST-2002-506813) and by the Swiss NCCR Quantum Photonics.