Beckman Center, Stanford University, Stanford,
California 94305-5329, USA.
e-mail: rnusse@stanford.edu

1. Zeng, X. *et al. Nature* **438,** 873–877 (2005).
2. Davidson, G. *et al. Nature* **438,** 867–872 (2005).
3. Logan, C. & Nusse, R. *Annu. Rev. Cell Dev. Biol.* **20,** 781–810 (2004).
4. Cong, F., Schweizer, L. & Varmus, H. *Development* **131,** 5103–5115 (2004).
5. Mao, J. *et al. Mol. Cell* **7,** 801–809 (2001).
6. Tolwinski, N. S. *et al. Dev. Cell* **4,** 407–418 (2003).
7. Tamai, K. *et al. Mol. Cell* **13,** 149–156 (2004).
8. He, X., Semenov, M., Tamai, K. & Zeng, X. *Development* **131,** 1663–1677 (2004).
9. Lee, E., Salic, A., Kruger, R., Heinrich, R. & Kirschner, M. W. *PLoS Biol.* **1,** E10 (2003).

QUANTUM INFORMATION

Remember that photon

Philippe Grangier

Storing single photons in atomic memories, and releasing them at a later time, is a required step on the way to quantum repeaters and long-distance quantum cryptography networks. This step has now been taken.

The basic unit of quantum information, the quantum bit or qubit, can be encoded in various physical quantities, such as the polarization states of photons, or the spin states of atomic nuclei. To make qubits practically useful, random coupling of them with the external world — an effect known as decoherence — must at all costs be avoided or corrected. This makes photons (the quanta of light) particularly suitable for qubit transmission, as they can travel over very long distances with very little decoherence. For qubit storage, encoders such as atoms come into their own: they can be kept in 'traps' for long periods, again avoiding deleterious decoherence effects from outside.

In experiments detailed in two papers in this issue, Chanelière *et al.* (page 833)[1] and Eisaman *et al.* (page 837)[2] contrive to combine the two crucial aspects of transport and storage: they generate a single photon on demand, catch it and store it in a remote atomic memory, and release it some time later. The advance is potentially highly significant for the field of quantum cryptography, also known as quantum key distribution (QKD). This emerging technology promises absolutely secure transmission of the key codes that are essential to decipher any encrypted message (Box 1).

Previous advances in quantum key distribution have owed much to the fact that photons that are used to encode the keys are very good qubit carriers: apart from maintaining a robust quantum state throughout transmission, they can be detected efficiently and with low levels of noise. But light signals cannot — whether viewed classically or quantum-mechanically — propagate over infinite distances in optical fibres. They are in fact dampened exponentially with distance: by a factor of two over 15 kilometres, and by a factor of a hundred over 100 kilometres. In classical optical telecommunications, this problem is solved by using simple, readily available devices known as repeaters, which can amplify and reshape the transmitted signal. But a good classical repeater is no use in the quantum regime: it is much too noisy, and creates so many errors that any quantum key being transmitted would not survive. To put the problem in more quantum-mechanical terms, a classical repeater breaks down quantum entanglement. This delicate phenomenon is associated with very strong, non-classical correlations between the states of two widely separated qubits, and is a crucial element of all quantum communication schemes: in effect, it allows any useful qubit to be 'teleported' directly to its destination, avoiding transmission losses[3].

So quantum communication must reinvent the repeater concept, using quantum hardware that preserves coherence. This is feasible in principle[4]: a quantum repeater would be nothing more than a small quantum processor. The exact number of qubits that would have to be stored and processed in such a repeater to ensure high-fidelity quantum communication over thousands of kilometres is an open issue. But it is likely to be in the range of tens or hundreds — much lower than the number required for a fully fledged quantum computer. The proposal in 2001 of the so-called DLCZ quantum information protocol[5], in which an ensemble of many atoms stores just one qubit, was a significant step towards a functioning quantum repeater. This protocol uses a process known as spontaneous Raman scattering, in which an incident photon is scattered inelastically (that is, with a change in its frequency) between two atomic ground states.

Chanelière *et al.*[1] and Eisaman *et al.*[2] exploit the DLCZ protocol to set up a controllable single-photon source for further experimentation. After initially preparing all the atoms of an ensemble in one ground state, a weak laser pulse (which nevertheless contains many photons) is used to induce a Raman transition of just one atom within the ensemble. As a consequence, a single spontaneous Raman photon is scattered, and its detection heralds the creation of a collective, delocalized, single-atom excitation of the ensemble. This excitation can be stored for as long as all the atomic levels in the sample maintain a constant phase relationship (a period known as the coherence time of the ensemble). This excitation can be converted back into a single-photon light field of controllable direction, intensity and frequency using another pump pulse (for a review of recent experimental work in this area, see ref. 6).

Once a single photon has been generated, the second stage is to catch it, and then release it again, in a second, remote atomic ensemble. The trick here is to use a second atomic ensemble that is opaque to the photon — absorbing rather than transmitting it — and that can only be made transparent by using an extra laser beam. This transparency arises through a neat and extensively studied interference phenomenon, electromagnetically induced transparency (EIT). If the EIT laser

Box 1 | Key codes: classical versus quantum cryptography

The purpose of quantum key distribution is to share a secret key among legitimate users that allows them and only them to decode messages. Some sort of key that allows a message to be deciphered is essential to all forms of encryption. Common, classical schemes used in electronic commerce can set up a key by relying on computationally difficult problems, such as the splitting of a very large number into two prime-number factors, that are in fact — given unlimited patience and computational power — breakable.

The only totally secure classical encryption system is the 'one-time pad', which uses a key that is as long as the message itself and that may be used only once. This solution leads to what is known as the key distribution problem: as the key must be transmitted between sender and recipient, it is itself susceptible to interception by an eavesdropper. In the classical world, someone can listen in on such a signal passively without changing the bits that make it up at all, so neither sender nor recipient need ever know that their communication has been intercepted.

Not so in the world of quantum communication. Qubits do not possess definite values such as the 0 or 1 of classical bits; rather, they represent a so-called coherent superposition of physical states such as the polarizations of a photon. A fundamental feature of quantum mechanics is that the mere act of observing such a superposition will cause it to 'collapse' into a definite state. This means any attempt by an eavesdropper to intercept a key made of qubits can be easily spotted by sender and recipient. Given this knowledge, and as long as the errors created by the eavesdropper (or any other perturbation) are not too large, it should be possible to build up an errorless and perfectly secure key. **P.G.**

beam is turned off, the medium becomes opaque once again, and any photon inside it is trapped, converting into another atomic excitation (known as a dark-state polariton). The photon can be regenerated at any time within the coherence time of the ensemble, simply by turning the EIT laser beam on again.

Throughout this sequence of events, it is clearly essential to check that the photon maintains its quantum, particle-like properties. One way to do this is to put a beam-splitter in the photon's way, and verify that photon counts on the two paths after the beam-splitter are anticorrelated. Correlated counts would indicate that the incoming beam splits in two, a clear sign of classical, wave-like behaviour. The degree of photon splitting can be conveniently characterized[7] by a parameter α, with an ideal single photon (exhibiting a purely quantum behaviour) having $\alpha = 0$, and a classical source having $\alpha > 1$. A value of α between 0 and 1 thus corresponds to a light beam showing a mixture of quantum and classical behaviours, or in other words, to an imperfect single photon. Chanelière and colleagues[1] obtain a value for α of 0.36 after a storage time of 500 nanoseconds, whereas Eisaman and colleagues[2] find a value of 0.51 under EIT conditions, but without storage (they also observe storage, but without evidence that α is less than 1).

Obviously, the 'quantum memories' (the ability to 'regenerate' a photon stored in an ensemble after a delay) described in these articles[1,2] are not the end of the story. First, what has to be stored and released is not a photon, but a qubit — the quantum information encoded on a photon. In the context of the DLCZ proposal, how to store and release a qubit is known in principle, and preliminary results have been obtained[8]. Another crucial issue is that it should be possible to create some entanglement between distant atomic ensembles[9], as discussed also by Chou *et al.* in this issue (page 828)[10]. The next key step will be to gradually increase the entanglement between the two remote memories — the process of 'entanglement distillation', which would be the fundamental duty of a quantum repeater[3,4]. This is a long-term goal, as many features have to be improved: counting rates (presently much too low), storage times (presently much too short), and the fidelity of the successive transfer processes in the ensembles. Although this looks more like mountain climbing than highway driving, new ways upwards keep on opening, as the present research[1,2] shows. The summit may seem far off, but it is not out of reach. ■

Philippe Grangier is at the Laboratoire
Charles Fabry de l'Institut d'Optique,
91403 Orsay Cedex, France.
e-mail: philippe.grangier@iota.u-psud.fr

1. Chanelière, T. *et al. Nature* **438,** 833–836 (2005).
2. Eisaman, M. D. *et al. Nature* **438,** 837–841 (2005).
3. Bennett, C. H. *et al. Phys. Rev. Lett.* **70,** 1895 (1993).
4. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. *Phys. Rev. Lett.* **81,** 5932–5935 (1998).
5. Duan, L.-M., Lukin, M., Cirac, J. I. & Zoller, P. *Nature* **414,** 413–418 (2001).
6. Felinto, D. *et al. Phys. Rev. A* **72,** 053809 (2005).
7. Grangier, P., Roger, G. & Aspect, A. *Europhys. Lett.* **1,** 173–179 (1986).
8. Matsukevich, D. N. *et al. Phys. Rev. Lett.* **95,** 040405 (2005).
9. Matsukevich, D. N. *et al.* preprint available at www.arxiv.org/quant-ph/0511012 (2005).
10. Chou, C. W. *et al. Nature* **438,** 828–832 (2005).

---

50 & 100 YEARS AGO

50 YEARS AGO

Over the past twenty years I have been interested in the possibility of using X-ray crystallographic methods to find the arrangement of the atoms in protein molecules and particularly in insulin. One of many possible approaches to solving this problem seems to be the crystallographic study of naturally occurring peptides such as the gramicidins and tyrocidine... These all have molecules much smaller in size than even the smallest protein molecules; some indeed are smaller than vitamin B_{12}, of which we have already found it possible to obtain the kind of information we require... We already have evidence that there may be a connexion between the way the peptide chain is folded in gramicidin *S* and the way it is folded in part of the molecule of insulin. But even if later we find that the connexion in chain configuration is less close than we at present suppose, we think that the atomic arrangement in these peptide molecules is itself of great interest and some importance.

Dorothy Crowfoot Hodgkin

From *Nature* 10 December 1955.

100 YEARS AGO

The death-knell of the atom[1]

Old Time is a-flying; the atoms are dying;
Come list to their parting oration:—
"We'll soon disappear to a heavenly sphere
On account of our disintegration.

"Our action's spontaneous in atoms uranious
Or radious, actinious or thorious:
But for others, the gleam of a heaven-sent beam
Must encourage their efforts laborious.

"For many a day we've been slipping away
While the savants still dozed in their slumbers;
Till at last came a man with gold-leaf and tin can
And detected our infinite numbers."

[1] Sung at the Chemical Laboratory dinner at University College, November 17.

From *Nature* 7 December 1905.

CANCER BIOLOGY

Emissaries set up new sites

Patricia S. Steeg

The capacity of tumours to spread to other organs is one of their most dangerous attributes. A study of how cancer cells settle in new places shows that they send out envoys to prepare the ground for them.

During the process of metastasis, tumour cells move from the primary tumour to colonize another organ. But why do these mobile cells put down roots only in particular organs, or only at specific sites within an organ? The lungs and liver, for example, seem particularly popular secondary targets for tumour cells. Some studies imply that this 'preference' might occur because, as they branch out within those organs, the blood vessels become very narrow, and the blood-borne tumour cells are trapped when they enter the fine capillary beds[1]. Other work has identified proteins that are specific to the cells lining the capillaries of certain tissues as possibly promoting metastasis formation[2]. A report from Kaplan *et al.* (page 820 of this issue)[3] provides another explanation. The authors show that tumour cells can mobilize normal bone-marrow cells, causing them to migrate to particular regions and change the local environment so as to attract and support a developing metastasis.

Metastasis is a sequential process, contingent on tumour cells breaking off from the primary tumour, travelling through the bloodstream, and stopping at a distant site. At the new site, the cells establish a blood supply and can grow to form a life-threatening mass. Both stimulatory and inhibitory molecular pathways within the tumour cell regulate this