Underwater quantum coding

SIR — Quantum mechanics is often presented as a limitation on achieving certain tasks, such as the simultaneous determination of position and momentum. Recently, the idea of using Heisenberg's uncertainty relations for secure communications has been explored, both theoretically (see, for example, ref. 1) and experimentally (for example, refs 2, 3). Here we report a cryptographic channel using a 23-km optical cable below Lake Geneva.

The idea is that whenever a third party taps into a quantum communication channel, this action necessarily perturbs the signal, provided that the bits of the key are represented by incompatible quantum states. This unavoidable perturbation can then be detected by controlling the correlation between the transmitted and the received signals. No information is transmitted; only a coding key is established. Once the secrecy of the key has been checked, it can safely be used to encode the message using standard cryptography[4]. The future of quantum cryptography depends on the possibility of using standard telecommunications fibres over some tens of kilometres[5,6], and on the evolution of current public key cryptosystems whose safety is still not proven mathematically[7].

In our experiment, the quantum channel was one of 40 fibres installed in a cable operated by Swiss PTT at 2.5 Gbit s^{-1} between Nyon and Geneva. Most of the cable is under water; its attenuation is 8.2 dB and its length 22.7 km. We also performed tests in the laboratory with a 26-km-long fibre coil. A 1,300-nm pulsed laser with 1 ns pulse width and 1.1 MHz pulse rate was used. The key was encoded using the polarization of light pulses manually selected by a rotating polarizer placed after a $\lambda/4$ wave plate. A polarization controller, compensating the polarization modification due to the fibre link, was used to align the emission and measurement axis.

The bit error rate (BER), the ratio of the number of wrong detections to the total number of detections, is the sum of the detector noise and the optical noise. We obtained a BER of 4.3% in the laboratory and 3.4% in the field, with an error of 0.3% (see figure), using low-intensity pulses. The optical noise consists of depolarization due to polarization-mode dispersion and polarization fluctuation due to birefringence and topological effects (see refs 2, 8–10 for details). A polarization separation of 23 dB has been obtained using an intense continuous-wave light source, both in the laboratory and in the field. This corresponds to a BER_{opt} of 0.5%. The stability of the polarization alignment was excellent for most of the time. When not stable, a fast polarization controller could overcome larger fluctuations.

The detector noise (BER_{det}) can be evaluated as follows:

$$BER_{det} = (D\delta\tau)/(D\delta\tau)+(p_{inj}L\eta)$$

where $\delta\tau$ is the detection time window, D is the number of counts per unit time not due to incoming photons (700 c s^{-1}), p_{inj} is the number of photons per pulse at the transmitter output (0.12 per pulse), L is the sum of the losses in the transmission cable and in the receiver's polarization splitter ($\sim$10 dB), and η is the overall quantum efficiency of the detector (0.2%). This corresponds to a BER_{det} of around 3%. Thus, the BER is mostly caused by the detector and is low enough for standard algorithm of errors correction and privacy

amplification to be applied, and to guarantee the privacy of the key.

We have thus demonstrated the feasibility of a quantum cryptographic system using polarization coding in the second telecommunications window around 1,300 nm on installed optical cables. The measured bit error rate (3.4%, before any error correction) is low enough to guarantee the privacy of the quantum communication channel. Consequently, the issue is no longer whether the quantum technology works, but whether it can be made robust and practical enough for use over an optical network.

A. Muller, H. Zbinden
N. Gisin
Group of Applied Physics,
University of Geneva,
1211 Geneva 4, Switzerland

1. Ekert, A. *Nature* **358**, 14–15 (1992).
2. Muller, A., Breguet, J. & Gisin, N. *Europhys. Lett.* **23**, 383–388 (1993).
3. Franson, J. D. & Jacobs, B. C. *Electron. Lett.* **31**, 232–234 (1995).
4. Shannon, C. E. *Bell Syst. tech. J.* **28**, 656 (1949).
5. Hughes, R. J., Luther, G. G., Morgan, G. L. & Simmons, C. *Proc. 7th Rochester Conf. Coherence and Quantum Optics* (1995).
6. Marand, C. & Townsend, P. D. *Opt. Lett.* **20**, 1695–1697 (1995).
7. Grollman, J. & Selman, A. L. *SIAM J. Computing* **17**, 309–335 (1988).
8. Gisin, N. & Pellaux, J. P. *Opt. Commun.* **89**, 316–323 (1992).
9. Tomita, A. & Chiao, R. Y. *Phys. Rev. Lett.* **57**, 937–940 (1986).
10. De Angelis, C., Galtarossa, A., Gianello, G., Matera, F. & Schiano, M. *J. Lightwave Technol.* **10**, 552–555 (1992).
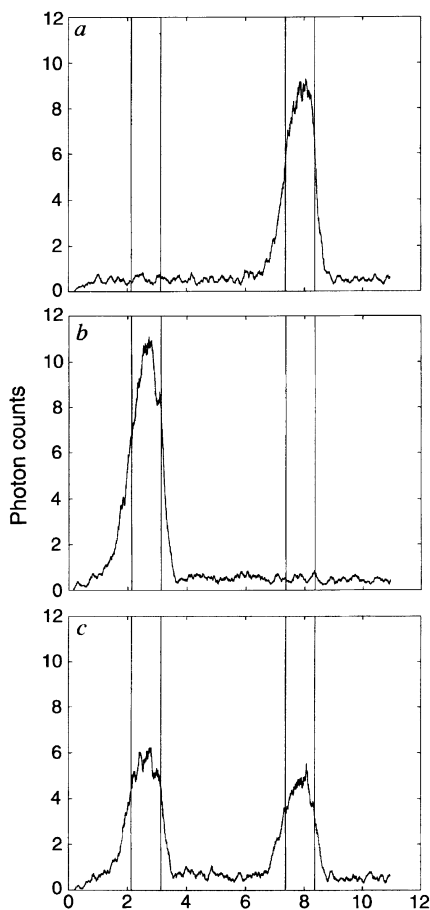
Time histogram of the detected photons in three different configurations. The horizontal scale gives the time in nanoseconds and the vertical scale the corresponding number of detected photons. Photons are 90° polarized (*a*), 0° polarized (*b*) and 45° polarized (*c*), in order to simulate the selection of a wrong detection basis or the effect of an eavesdropper. The number of wrong counts is very small in *a* and *b*, in contrast to *c*, where the incoming photons are found to be distributed equally.

Ambient ozone and loblolly pines

SIR — McLaughlin and Downing[1], studying loblolly pine (*Pinus taeda* L.) trees, conclude that "ozone exposures at >40 nl l^{-1} interacted with low soil moisture and high air temperatures to reduce short-term rates of stem expansion. Annual growth was also inversely related to seasonal ozone exposure and soil moisture stress." We suspect that most of the within-year (short-term) variation in stem growth is accounted for by the growth trend term (slope against time) in their model, leaving relatively little to be explained by ozone or other environmen-
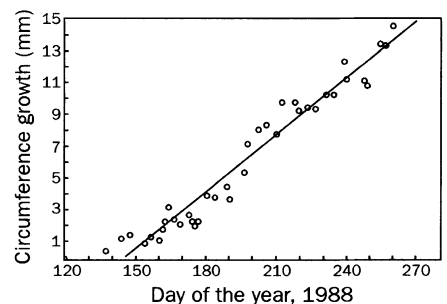

FIG. 1 Plot of simple linear regression against observed values (circles) for tree 23. Transcribed from McLaughlin and Downing's Fig. 2.

449