http://www.who.int/fsf/
4. European Commission Scientific Committee on Food (SCF) *Opinion of the Scientific Committee on Food on New Findings Regarding the Presence of Acrylamide in Food* (SCF/CS/CNTM/CONT/4 Final, 3 July 2002) http://europa.eu.int/comm/food/fs/scf/index_en.html
5. Ledl, F. & Schleicher, E. *Angew. Chem. Int. Ed. Engl.* **29,** 565–594 (1990).
6. Paulsen, H. & Pflughaupt, H. in *The Carbohydrates — Chemistry and Biochemistry* (eds Pigman, W. & Hortin, D.) Vol. 1B, 881–927 (Academic, New York, 1980).
7. Von Euler, H. & Brunius, E. *Chem. Ber.* **59,** 1581–1585 (1926).
8. Chen, J., Pill, T. & Beck, W. *Z. Naturforsch. B* **44,** 459–464 (1989).

Competing financial interests: declared none.

Quantum cryptography

A step towards global key distribution

Large random bit-strings known as 'keys' are used to encode and decode sensitive data, and the secure distribution of these keys is essential to secure communications across the globe[1]. Absolutely secure key exchange[2] between two sites has now been demonstrated over fibre[3] and free-space[4–6] optical links. Here we describe the secure exchange of keys over a free-space path of 23.4 kilometres between two mountains. This marks a step towards accomplishing key exchange with a near-Earth orbiting satellite and hence a global key-distribution system.

The security of our key-exchange system is guaranteed by encoding single photons using two sets of orthogonal polarizations. Our transmitter module (Alice; Fig. 1) incorporates a miniature source of polarization-coded faint pulses (approximating single photons; C.K., P.Z., M.H. and H.W., unpublished results), where 0° or 45° polarization encode binary zero, and 90° or 135° code binary one. These light pulses are expanded and collimated in a simple telescope to a beam of about 50 mm and then accurately aligned on the receiver (Bob; Fig. 1), a 25-cm-diameter commercial telescope. Light is collected and focused onto a compact four-detector photon-counting module (Fig. 1). A detection in any one detector then has an associated bit value, measurement basis (0° or 45°) and detection time. The bit values then form a raw key string. Valid bits are measured in the same basis as that in which they were encoded.

Alice and Bob use a standard communications channel, such as a mobile telephone, to ascertain which bits arrived (many are lost) and which measurement basis was used, then they both discard the invalid bits — which leaves them with nearly identical random bit-strings, the sifted key. Eavesdropping measurements on the single photons disturb the encoding and introduce errors of up to 25%, so Alice and Bob test for errors in a short section of sifted key to verify the security of the channel. Low error rates due to background light detection and polarization settings are securely eliminated by using classical error-correcting codes sent over the mobile-telephone link.

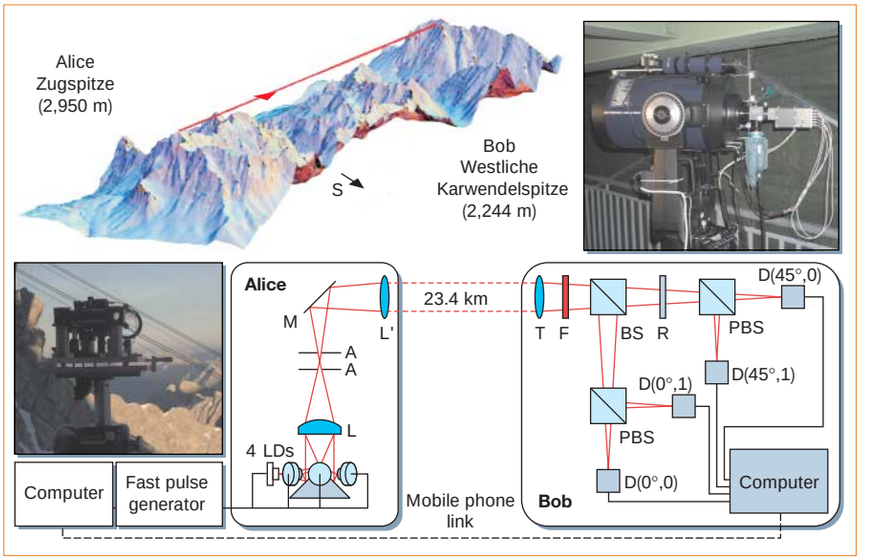

Figure 1 Overview of the experiment against a relief map of the trial site. In the Alice module, four separate lasers (LDs) encode the four polarizations based on a random bit-string fed from the Alice computer. They are combined in a spatial filter (A,A) using a conical mirror (M) and a lens (L). The beam expands to 50 mm and is collimated in an output lens (L8). In the Bob module, a telescope (T) collects the light, which is filtered (F) and then spilt in a polarization-insensitive beam-splitter (BS), passing on to polarizing beam-splitters (PBS) and four photon-counting detectors (D). One polarizing beam-splitter is preceded by a 45° polarization rotator (R). A click in one of the photon-counting detectors D(u, *B*) sets the bit value *B* and the measurement basis u.

In the long-range experiment, Alice was located at a small experimental facility on the summit of Zugspitze in southern Germany, and Bob was on the neighbouring mountain of Karwendelspitze, 23.4 km away. At this distance, the transmitted beam was 1–2 m in diameter and was only weakly broadened by air-turbulence effects at this altitude. Lumped optical losses of about 18–20 decibels were measured and, using faint pulses containing 0.1 photons per bit, the detected bit rate at Bob was 1.5–2 kilobits per second (receiver efficiency of 15%).

Operating at night with filters of 10-nm bandwidth reduced the background counts, and errors appeared in less than 5% of key bits. After sifting and error correction, net key exchange rates were hundreds of bits per second. In a series of experiments, several hundreds of kilobits of identical key string were generated at Alice and Bob.

In associated experiments in poorer visibility, we showed that key exchange could be carried out when transmission losses were up to 27 decibels, but improvements in receiver efficiency and background counts should take us beyond 33 decibels. With this performance, key exchange to near-Earth orbit (500–1,000 km range) should become possible.

Until now, the principal method of high-security key exchange has been the 'trusted courier' carrying a long random bit-string, the key, from one location to the other. Our experiment paves the way for the development of a secure global key-distribution network based on optical links to low-Earth-orbit satellites. We note that a 10-kilometre key-exchange experiment has recently been announced[7].

C. Kurtsiefer*, P. Zarda*, M. Halder*, H. Weinfurter*, P. M. Gorman†, P. R. Tapster †, J. G. Rarity†

**Ludwig-Maximilian University, 80799 Munich, Germany*

†Photonics Department, QinetiQ, Malvern , Worcestershire WR14 3PS, UK

e-mail: jgrarity@qinetiq.com

1. Singh, S. *The Code Book* (Anchor, New York, 1999).
2. Bennett, C. H. *et al. J. Cryptol.* **5,** 3–28 (1992).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. *Rev. Mod. Phys.* **74,** 145–196 (2002).
4. Buttler, W. T. *et al. Phys. Rev. Lett.* **84,** 5652–5655 (2000).
5. Rarity, J. G., Gorman, P. M. & Tapster, P. R. *Electron. Lett.* **37,** 512–514 (2001).
6. Rarity, J. G., Gorman, P. M. & Tapster, P. R. *J. Mod. Opt.* **48,** 1887–1901 (2001).
7. Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G. *New J. Phys.* **4,** 43.1–43.14 (2002).

Competing financial interests: declared none.

erratum

Cognitive change and the *APOE* ε4 allele

I. J. Deary, M. C. Whiteman, A. Pattie, J. M. Starr, C. Hayward, A. F. Wright, A. Carothers, L. J. Whalley

Nature **418,** 932 (2002)

In the second sentence of the seventh paragraph of this communication, the MMSE scores are incorrectly specified as less than or equal to 28; these should read as greater than or equal to 28.