Royal Society for the Protection of Birds, †The Lodge, Sandy, Bedfordshire SG19 2DL, UK, and
§Dunedin House, Edinburgh EH4 3TP, UK
‡School of Biological Sciences, University of Wales, Swansea, Singleton Park, Swansea SA2 8PP, UK

1. Krebs, J. R., Wilson, J. D., Bradbury, R. B. & Siriwardena, G. M. *Nature* **400,** 611–612 (1999).
2. Gregory, R. D. *et al. The State of the UK's Birds 2000* (RSPB, BTO and WWT, Sandy, UK, 2001).
3. Summers-Smith, J. D. *The Sparrows* (Poyser, Calton, 1988).
4. Cornuet, J. M. & Luikart, G. *Genetics* **144,** 2001–2014 (1996).
5. Crochet, P. A. *Mol. Ecol.* **9,** 1463–1469 (2000).
6. Wernham, C. V. *et al. The Migration Atlas: Movements of the Birds of Britain and Ireland* (Poyser, London, in the press).
7. Chamberlain, D. E., Fuller, R. J., Bunce, R. G. H., Duckworth, J. C. & Shrubb, M. *J. Appl. Ecol.* **37,** 771–788 (2000).
8. Robinson, R. A. & Sutherland, W. J. *J. Appl. Ecol.* **39,** 157–176 (2002).
9. Hanski, I. *Nature* **396,** 41–49 (1998).

Competing financial interests: declared none.

Ageing

Cognitive change and the *APOE* ε4 allele

There is a marked variation in whether people retain sufficient cognitive function to maintain their quality of life and independence in old age, even among those without dementia, so it would be valuable to identify the determinants of normal age-related cognitive change[1,2]. We have retested non-demented 80-year-olds who were participants in the Scottish Mental Survey of 1932, and find that the variation in their non-pathological cognitive change from age 11 to 80 is related to their apolipoprotein E (*APOE*) genotype. This effect of the *APOE* ε4 allele on normal cognitive ageing may be mediated by a mechanism that is at least partly independent of its predisposing effect towards Alzheimer's disease.

The Scottish Mental Survey of 1932 tested cognitive ability in almost everyone attending school in Scotland in June 1932 and who was born in 1921 ($n = 87{,}498$; ref. 3). From the Lothian birth cohort of 1921, 491 surviving participants (206 men) of the 1932 survey had their Moray House Test (MHT) score at age 11 traced. All lived independently in the community. Disease history and current medication were established at interview.

Subjects with Mini-Mental State Examination (MMSE) scores that were suggestive of dementia (score <24; 4 men, 4 women), or with any history of dementia-related illness (3 men, 2 women), were omitted from the study. There were 466 subjects (190 men) for whom we had Moray House Test scores at both age 11 and age 80, and whose *APOE* genotype we were able to determine.

The MHT takes 45 minutes and comprises 71 verbal and non-verbal reasoning questions. It has criterion validity in youth and old age[4]. Up to 50% of the variation between subjects in the MHT remains stable from age 11 to about 80 (ref. 4). Subjects took the test in 1932 and again in 1999–2001. Scores at each age were controlled for age (in days) and were converted to IQ-type scores (mean, 100; s.d., 15). Subjects were classified according to the presence ($n = 121$) or absence ($n = 345$) of one or more *APOE* ε4 allele(s)[5].

At age 11, MHT scores (mean, s.d.) were similar ($t = 0.91$, $P = 0.36$) for those with the ε4 allele (99.4, 15.2) and for those without it (100.8, 14.4). But at age about 80, MHT scores were significantly different ($t = 2.64$, $P = 0.009$) between the two groups (with the ε4 allele, 97.0, 15.7; without the ε4 allele, 101.1, 14.2).

We used analysis of covariance to examine the significance and effect sizes of contributors to cognitive change from age 11 to 80. Effects of age-11 MHT score ($F_{1,461} = 334.8$, $P < 0.001$, $\eta^2 = 0.42$; Pearson's correlation between MHT at age 11 and at age 80, 0.65, $P < 0.001$), sex ($F_{1,461} = 8.7$, $P = 0.003$, $\eta^2 = 0.018$) and presence of the ε4 allele ($F_{1,461} = 5.2$, $P = 0.02$, $\eta^2 = 0.011$) were significant; sex and ε4 status did not interact. Cardiovascular disease history was not significantly associated with cognitive function. People with and without the *APOE* ε4 allele did not differ in the number and type of medications that they took.

We reran these models to investigate the possibility that the effects of ε4 might be caused by incipient dementia in some *APOE* $\varepsilon4^+$ individuals. Including only those subjects with MMSE scores of ≤ 28 resulted in an increased effect of ε4 ($F_{1,342} = 8.4$, $P = 0.004$, $\eta^2 = 0.024$). The effect was also evident after excluding those subjects whose IQ decrement from age 11 to 80 was greater than two standard deviations ($F_{1,459} = 5.1$, $P = 0.02$, $\eta^2 = 0.011$).

This study has the advantage of examining the same individuals with the same cognitive test in childhood and in old age. Individual differences in childhood IQ are the most reliable predictor of late-life cognitive performance (accounting for at least 42% of variance). Possession of *APOE* ε4 is unrelated to differences in mental ability in youth, but is significantly associated with mental ability in old age and the change in ability score from youth.

Incipient dementia may have been more common in our *APOE* ε4-positive individuals and so could account for part of the effect we have observed. But we contend that this is not the only possible explanation, because the effect of *APOE* ε4 increases when the MMSE threshold is raised to include only near-perfect scorers, and remains similar after excluding those whose IQ decrement from age 11 to 80 was greater than 2 s.d. Moreover, the number of incipient cases expected in this age group[6,7], and the effect size of *APOE* on Alzheimer's disease[8], mean that each case would require a massive cognitive decline to account for the observed effects, and no such skewing or bimodal distribution was seen in either ε4 subgroup. The results do not seem to be due to selective attrition, because the proportion of people with ε4 alleles is similar to that in other, younger groups from Scotland[9].

Further clinical and pathological investigation is required to determine whether Alzheimer's disease or other changes could be responsible for the differences we observe. APOE isoforms show differences in their binding to receptors, lipoproteins and amyloid-β, in atherosclerosis, neurite extension, neuroprotection and repair[10]. These various interactions could influence cognitive ageing independently of those that operate in Alzheimer's disease, which remain uncertain[10].

Identifying a factor that influences non-pathological, lifetime cognitive change has large public-health implications because, in the absence of a sharp risk threshold, most adverse events — and most of the personal and economic burdens that these bring — occur to old people who are within the 'normal' part of the distribution[11].

Ian J. Deary*, Martha C. Whiteman*, Alison Pattie*, John M. Starr†, Caroline Hayward‡, Alan F. Wright‡, Andrew Carothers‡, Lawrence J. Whalley§
*Department of Psychology, University of Edinburgh, 7 George Square, Edinburgh EH8 9JZ, UK
e-mail: i.deary@ed.ac.uk
†Department of Geriatric Medicine, Royal Victoria Hospital, Craigleith Road, Edinburgh EH4 2DN, UK
‡Medical Research Council Human Genetics Unit, Western General Hospital, Crewe Road, Edinburgh EH4 2XU, UK
§Department of Mental Health, University of Aberdeen, Clinical Research Centre, Royal Cornhill Hospital, Cornhill Road, Aberdeen AB25 2ZH, UK

1. US National Research Council *The Aging Mind* (Natl Acad. Press, Washington DC, 2000).
2. Anstey, K. & Christensen, H. *Gerontology* **46,** 163–177 (2000).
3. Scottish Council for Research in Education *The Intelligence of Scottish Children: A National Survey of an Age Group* (Univ. London Press, 1933).
4. Deary, I. J., Whalley, L. J., Lemmon, H., Crawford, J. R. & Starr, J. M. *Intelligence* **28,** 49–55 (2000).
5. Wenham, P. R., Price, W. P. & Blundell, G. *Lancet* **33,** 1158–1159 (1991).
6. Breitner, J. C. *et al. Neurology* **55,** 161–162 (2000).
7. Corder, E. H. *et al. Nature Genet.* **7,** 180–184 (1994).
8. Slooter, A. J. *et al. Arch. Neurol.* **55,** 964–968 (1998).
9. Robertson, F. W. & Cumming, A. M. *Arteriosclerosis* **5,** 283–292 (1985).
10. Mahley, R. W. & Rall, S. C. Jr *Annu. Rev. Genom. Hum. Genet.* **1,** 507–537 (2000).
11. Rose, G. *The Strategy of Preventive Medicine* (Oxford Univ. Press, 1992).

Competing financial interests: declared none.

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.

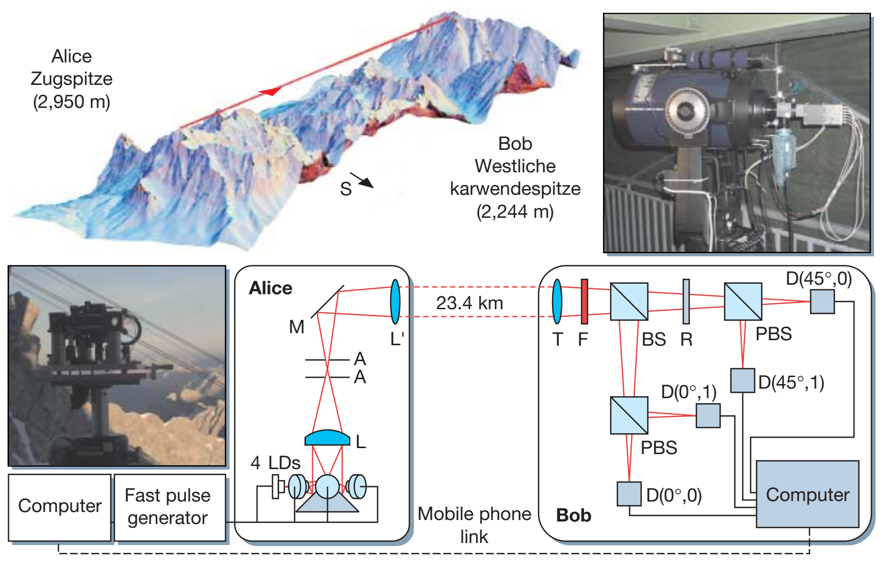

Figure 1 Overview of the experiment against a relief map of the trial site. In the Alice module, four separate lasers (LDs) encode the four polarizations based on a random bit-string fed from the Alice computer. They are combined in a spatial filter (A,A) using a conical mirror (M) and a lens (L). The 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* ;4 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.