sensors and body temperature, derived from analysis of present-day (extant) species.

To establish whether their prediction system is valid, the authors determined the TMI of more than 200 extant species. They did this using sophisticated analyses of data such as semicircular canal dimensions and body mass to generate a mathematical model relating the TMI to the known body temperatures of these animals. Fossils reveal only the bony dimensions of the canals; however, the dimensions of the canals' membranes are crucial for determining the TMI, and these were estimated using regression models. Although the accuracy of predicting body temperature was relatively poor at the species level, for species grouped into clades, the estimation was fairly good, explaining more than 80% of the variability in the data.

The observed relationship was then used to estimate body-temperature distributions from the TMIs using fossil records of more than 60 extinct species. According to this analysis, the threshold for reaching endothermy, tentatively marked by a 'sudden' increase in the TMI, occurred approximately 230 million years ago. This was in the Late Triassic period during what is known as the Carnian pluvial episode, a period of a large-scale climate change consisting of global warming and increased humidity. The first vertebrates to have thermoregulatory capacity were probably early members of the clade Mammaliamorpha, animals similar in shape to large rodents, and these presumed common ancestors of all extant mammals appeared around the same time as the first dinosaurs[6].

The work by Araújo *et al.* also provides other insights. In extant species, the TMI increased disproportionately more with body temperature than would be expected from just temperature-driven changes in viscosity, thus effectively increasing the sensor's functional limits. The authors interpreted this result as further evidence for the aerobic-capacity model of the evolution of endothermy — a higher body temperature enables increased physical activity, which, in turn, requires motion sensors that can cope with faster movements. In other words, you can only run as fast as your motion sensor can detect the movement.

The evidence pointing to an onset of mammalian endothermy in the Late Triassic is not entirely surprising, given predictions made by other studies using different methods, but the exact timing of this emergence is not undisputed. For example, a study[6] that compiled evidence from various sources, such as the development of hair, signs of nocturnal activity and aspects of bone structure, suggested that mammalian endothermy developed about 20 million years earlier, at the transition between the Permian and Triassic periods.

Although Araújo and colleagues demonstrate systematic changes in the semicircular canals' properties that are related to increases in body temperature, there are limitations to inferring the evolution of endothermy from the bony encasements of a motion sensor. Fossil remains cannot capture the functionally relevant dimensions of the membranous inner ear labyrinth structure, nor the endolymph viscosity or its molecular composition. Araújo *et al.* assumed that the composition of the endolymph remained unchanged during mammalian evolution. By contrast, the viscosity of the endolymph in another group of endothermic animals, birds, is much higher[7], leading Araújo *et al.* to assume that birds and perhaps their dinosaur ancestors compensated for a rise in body temperature in part by changing the biochemical composition of their endolymph.

The most notable caveat regarding determination of the time window for the onset of endothermy is the fact that only three samples of non-mammalian species called probainognathians were included, which, according to Araújo and colleagues' study, were our closest non-endothermic relatives. Although the authors took great care in carrying out extensive mathematical and statistical calculations to show that the observed shift in TMI was probably not a sampling artefact, it is still possible that the estimated onset is off by some tens of millions of years. Given the large variation between TMI and body temperature in extant species, some of the few extinct sample species might have been outliers. Nevertheless, by considering the sensory requirements that accompany movement agility in early mammals, this study offers a refreshing alternative viewpoint that will certainly fuel the discussion[6] about the onset of mammalian endothermy.

Stefan Glasauer is at the Institute of Medical Technology, Brandenburg University of Technology Cottbus-Senftenberg, 03046 Cottbus, Germany. **Hans Straka** is in the Faculty of Biology, Ludwig-Maximilians-Universität München, 82152 Planegg, Germany.
e-mails: stefan.glasauer@b-tu.de; straka@lmu.de

1. Ruben, J. *Annu. Rev. Physiol.* **57**, 69–95 (1995).
2. Araújo, R. *et al. Nature* **607**, 726–731 (2022).
3. Bennett, A. F. & Ruben, J. A. *Science* **206**, 649–654 (1979).
4. Muller, M. *J. Theor. Biol.* **198**, 405–437 (1999).
5. Rabbitt, R. D., Damiano, E. R. & Grant, J. W. in *The Vestibular System* (eds Highstein, S. M., Fay, R. R. & Popper, A. N.) 153–201 (Springer, 2004).
6. Benton, M. J. *Gondwana Res.* **100**, 261–289 (2021).
7. Money, K. E. *et al. Am. J. Physiol.* **220**, 140–147 (1971).

The authors declare no competing interests.
This article was published online on 20 July 2022.

Quantum information

Entanglement provides a key to improved security

Krister Shalm

A cryptographic scheme offers a secure way of exchanging data using a phenomenon called quantum entanglement. The approach relies on special quantum correlations between particles that help to prevent tampering. **See p.682 & p.687**

Every time you buy something online, sensitive information such as your credit-card number is sent to a merchant. To prevent this information from being obtained by a hacker, it is necessary to 'lock' it before sending it. Then, if the merchant has a 'key' corresponding to the one that was used to lock your information, they can unlock it. But how can these keys be distributed in a secure way, so that only you and the merchant have them? In two papers in this issue, Nadlinger *et al.*[1] (page 682) and Zhang *et al.*[2] (page 687) report on a method for using a special property of quantum particles — known as quantum entanglement — to share a secret key without needing to trust the 'courier' that performs the exchange.

In any cryptographic system, each component that needs to be trusted is a possible doorway through which a hacker can enter. And, just as a room with 100 doors is more difficult to guard than a room with only one door, the number of components that need to be trusted determines how challenging it is to protect a cryptographic system from intrusions. Reducing the amount of trust required in such a system is therefore one of the main goals of cryptography.

The oldest method of sharing keys is through a courier, but this requires some assurance that the courier has not been bribed or compromised, and that the keys they carry have not been intercepted in transit. Using couriers for processes such as

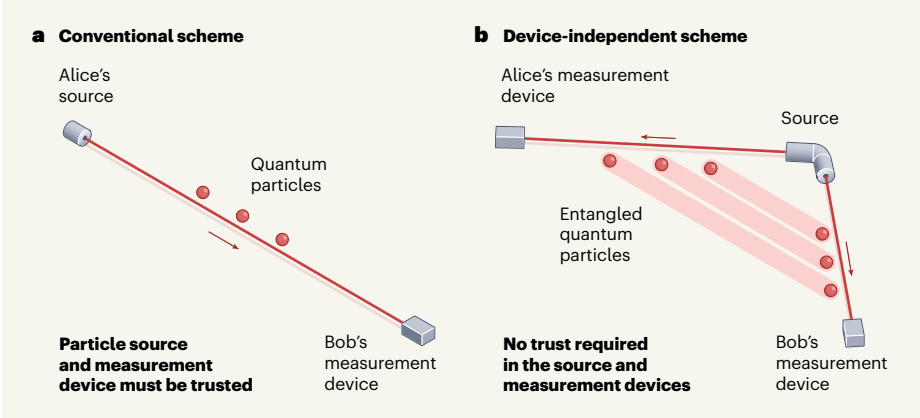

Figure 1 | Schemes for distributing secret keys using quantum mechanics. Quantum particles can be used to deliver a key for encrypting sensitive information, because quantum mechanics dictates that anyone who intercepts the particles will inadvertently disturb them in a way that can be detected. **a**, In conventional schemes, two parties (labelled Alice and Bob) can create a key to encrypt and decrypt secret messages, but this method assumes that the particle source and measurement devices have not been compromised. **b**, Nadlinger *et al.*[1] and Zhang *et al.*[2] used quantum entanglement — through which pairs of quantum particles are correlated over long distances — to implement a scheme that does not require a trustworthy source or measurement devices. Alice and Bob can perform a test on their entangled particles under a strict set of conditions to detect whether the source has been compromised, so they need only safeguard their measurement results by sealing their laboratories.

online credit-card transactions is not practical: imagine hiring someone to carry a secret key to an online store every time you wanted to buy something. Instead, mathematical problems that are difficult to solve — such as calculating the factors of very large numbers — can be used to encrypt information in such a way that only the intended recipient can easily decrypt it. It would be too difficult, and would take too long, for a hacker to perform the decryption calculation using modern computers.

However, hackers can still intercept encrypted messages — and then wait, either until more-powerful computers are available, or until weaknesses in the encryption schemes are discovered, allowing the information to be decrypted[3]. Of particular concern is the expected arrival of quantum computers that will be able to solve these difficult mathematical problems in a fraction of the time it takes conventional computers to do so. Such computers would compromise the functions that form the basis of current cryptographic schemes.

But quantum mechanics can solve this conundrum, by offering an alternative way of distributing keys — using quantum particles, such as photons, as couriers. Two people who wish to create a secret key prepare, send and measure photons. The information encoded in the photon cannot be perfectly copied — any measurement of the system will disturb it. A hacker who is trying to intercept the information encoded in a photon will have to measure it in some way, and will therefore introduce anomalies into the system that the sender and receiver can detect. Once the key is created, the sender and receiver can use it to encrypt and share secret information[4] (Fig. 1a).

Because this quantum encryption process does not depend on mathematical functions, a hacker intercepting messages will not be able to decrypt them in the future when improved technology becomes available. For this reason, quantum-key distribution technology is advancing rapidly, with commercial systems already in use. However, the photons cannot be used to detect all possible types of tampering. This method still requires that the photon sources and detectors be trusted, and it is possible for a hacker to exploit this trust to tamper with the system and discover the key[5]. It would be like hiring a trustworthy courier to carry a secret key in a briefcase locked to their wrist, only to discover that the briefcase itself is bugged.

Luckily, quantum systems have yet another property that can help to overcome the problems associated with trusting devices. And that's the phenomenon known as quantum entanglement. Entangled particles share strong correlations that have no classical analogue — one interpretation is that measurements or actions on one particle can seem to influence the other particle, even over long distances. These correlations, which Albert Einstein termed spooky actions at a distance, have an element of randomness that prevents information from being transmitted instantaneously. But in cryptography, this randomness can be used to create a shared secret key that isn't vulnerable to untrustworthy devices[6].

Nadlinger and colleagues and Zhang and colleagues used quantum entanglement to implement a next-generation quantum-key distribution method that does not require any trust in the devices used to create and detect the quantum particles. In the authors'

From the archive

How to design an academic library in the digital era, and a celebration of London's Bloomsbury neighbourhood.

50 years ago

The Making of a Library: The Academic Library in Transition. By Robert S. Taylor — The author, who has been called a meta-librarian, believes that those who plan a modern academic library should first examine its objectives, and what it could do to become a productive participant in the learning process and in the community it serves. The place of the library in relation to the newer media for transference of information, its inter-relation with educational technology, and its function as a teaching instrument are currently matters of fierce debate ... Clearly the time has come to recognize the extent of common concern in the library, computer, graphics and communications fields and to solve the problems involved in their proper integration. The ideal is to create a social institution, which will raise the probability of effective use of data, information, knowledge and artistic form in all media in support of education, leisure enjoyment, research and decision making.

From *Nature* 28 July 1972

100 years ago

Bloomsbury, originally Lomosbury, was in ancient days a retired village, renowned for its wholesome and pleasant air ... The British Museum forms the natural centre of the district ... The museum was opened in 1759, and ever since has been available for "studious and curious persons," to quote the official regulations ... The next most important building in Bloomsbury is undoubtedly University College in Gower Street, founded in 1826 to afford "literary and scientific education at a moderate expense."... Bloomsbury has many interesting associations, as the plaques fixed to its houses testify ... At the Bedford Square end of Gower Street is the house where Cavendish, the chemist and philosopher, lived for some years. The house became packed with books and apparatus, and another in Dean Street, Soho, was taken as a library.

From *Nature* 29 July 1922

experiments, two parties (called Alice and Bob, following a convention often used in cryptography) use pairs of entangled particles instead of single photons to exchange the key (Fig. 1b). Alice and Bob measure their particles independently under a strict set of experimental conditions. Some of the measurements are used to create a key, whereas others are used to perform a test that has been shown to rigorously detect entanglement[7–11]. Passing the test guarantees that a hacker has not tampered with the entangled particles in any way that would allow them to predict or control Alice's and Bob's measurements. In our courier example, the hacker could provide the briefcase used to transport the keys, and any tampering would still be detected.

This method eliminates one of the biggest security risks from the system. Because there is no need to trust the devices that create and distribute the entangled particles, these schemes are said to be device independent. Alice and Bob need worry only about protecting the devices that choose their measurements from being tampered with, and isolating their labs to keep information about their results or the key from leaking out.

Nadlinger and co-workers performed measurements on entangled ions that were trapped by an oscillating electromagnetic field. Their measurements were taken over a period of nearly 8 hours, creating a shared key that was 95,884 bits long. This is the first complete implementation of a device-independent protocol for generating a key. But in this case, the stations were separated by only 2 metres — about the minimum distance needed for Alice and Bob to carry out a secure conversation while practising social distancing during a pandemic. Moving the stations farther apart, to more realistic distances, is not trivial.

In Zhang and colleagues' experiment, measurements were made on entangled atoms, trapped by laser beams, and the two systems were much farther apart, at a separation of 400 m. The researchers were able to prove that the system met the rigorous requirements for device-independent key distribution. But the rate at which entanglement was generated was so low that a key could not be created in a reasonable amount of time.

In both experiments, the rate at which particles at the two stations can be entangled decreases markedly as the distance between them increases. For device-independent quantum-key distribution to become practical, the obstacle of low rates at long distances must be overcome. Still, both demonstrations represent major advances in quantum-communications technology.

Several efforts are under way around the world to build the kinds of entangled quantum network that will eventually support these device-independent cryptographic protocols[12]. Because the requirements for these protocols are so demanding, they serve as a useful benchmark — any quantum network that can meet them is able to exceed a crucial operational threshold. Consequently, I expect that our most advanced future quantum networks will have these device-independent cryptographic capabilities built in, enabling widespread adoption of innovative ways of keeping our most sensitive secrets safe.

Krister Shalm is in the Department of Physics, University of Colorado at Boulder, Boulder, Colorado 80309, USA.
e-mail: lynden.shalm@colorado.edu

1. Nadlinger, D. P. *et al. Nature* **607**, 682–686 (2022).
2. Zhang, W. *et al. Nature* **607**, 687–691 (2022).
3. Singh, S. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography* (Doubleday, 1999).
4. Bennett, C. H. & Brassard, G. *Theor. Comput. Sci.* **560**, 7–11 (2014).
5. Gerhardt, I. *et al. Nature Commun.* **2**, 349 (2011).
6. Acín, A. *et al. Phys. Rev. Lett.* **98**, 230501 (2007).
7. Hensen, B. *et al. Nature* **526**, 682–686 (2015).
8. Shalm, L. K. *et al. Phys. Rev. Lett.* **115**, 250402 (2015).
9. Giustina, M. *et al. Phys. Rev. Lett.* **115**, 250401 (2015).
10. Rosenfeld, W. *et al. Phys. Rev. Lett.* **119**, 10402 (2017).
11. Li, M.-H. *et al. Phys. Rev. Lett.* **121**, 80404 (2018).
12. Wehner, S., Elkouss, D. & Hanson, R. *Science* **362**, eaam9288 (2018).

The author declares no competing interests.

Developmental biology

A self-defence strategy for long-lived eggs

Deepak Adhikari & John Carroll

Egg cells need to stay out of harm's way to keep the next generation healthy and free of unwanted mutations. A mechanism by which eggs avoid the ravages caused by harmful reactive oxygen species has now been discovered. **See p.756**

In what seems to be a high-risk evolutionary strategy, female mammals are born with a finite reserve of immature eggs. These eggs need to be capable of avoiding harm until the end of an organism's reproductive life — for more than 40 years in people — to remain capable of producing healthy offspring. Writing on page 756, Rodríguez-Nuevo *et al.*[1] have now found an adaptation that might explain how eggs stay safe for so long, related to how they produce energy.

Cellular energy is stored in ATP molecules. Most ATP is made in organelles called mitochondria by a process known as oxidative phosphorylation, which involves five protein complexes in the inner mitochondrial membrane. Complexes I to IV comprise an electron transport chain (ETC), which begins with oxidation of the molecule NADH to NAD^+ by complex I. Oxidation releases electrons, which are passed from complex to complex, coupled to the pumping of hydrogen ions that generates an electrical potential across the mitochondrial membrane. This mitochondrial membrane potential (MMP) ultimately drives ATP synthesis by complex V (Fig. 1a). Complexes I–V are highly evolutionarily conserved across most of the animal kingdom, except in a few unicellular organisms[2] and parasitic plants[3].

Unfortunately, oxidative phosphorylation comes with some collateral damage. Inevitably, some electrons leak from the ETC, and are received by oxygen to generate reactive oxygen species (ROS) — highly reactive molecules that wreak havoc in cells by inducing damage to essential biomolecules such as RNA, proteins and lipids. In eggs, this type of damage could prevent proper egg development or embryo formation. Furthermore, ROS-induced damage to nuclear or mitochondrial DNA can lead to genetic mutations that could propagate across generations. It makes sense, then, to take extreme, even unique, measures to protect eggs from ROS. And this is exactly what Rodríguez-Nuevo *et al.* have discovered.

The authors noted that something was different about the mitochondria in eggs compared with those of their neighbouring support cells: the organelles had a much-reduced MMP. They examined early-stage eggs (called primordial oocytes, which remain quiescent in the ovary for most of the lifespan) from humans and the frog species *Xenopus laevis*. This revealed that primordial oocytes lack any detectable ROS signals. Furthermore, when the researchers induced ROS artificially, eggs degenerated rapidly, suggesting that they are particularly prone to ROS-mediated damage — perhaps indicating poorly developed protective mechanisms.

These data point to primordial oocytes having relatively low mitochondrial activity

Correction

The original version of this article incorrectly said that the reason a key could not be created in Zhang and colleagues' experiment was because the distance between the atomic systems reduced the rate at which entangled particles could be generated.