arising from oncometabolite accumulation, given that we now have a clearer picture of how such cancer cells are vulnerable if DNA-repair processes are targeted.

Lei-Lei Chen and **Yue Xiong** are in the Department of Biochemistry and Biophysics, and at the Lineberger Comprehensive Cancer Center, University of North Carolina at Chapel Hill, North Carolina 27516, USA.
e-mail: yxiong@email.unc.edu

1. Sulkowski, P. L. *et al. Nature* **582**, 586–591 (2020).
2. King, A., Selak, M. A. & Gottlieb, E. *Oncogene* **25**, 4675–4682 (2006).
3. Ye, D., Guan, K.-L. & Xiong, Y. *Trends Cancer* **4**, 151–165 (2018).
4. Rose, N. R., McDonough, M. A., King, O. N. F., Kawamura, A. & Schofield, C. J. *Chem. Soc. Rev.* **40**, 4364–4397 (2011).
5. Chowdhury, R. *et al. EMBO Rep.* **12**, 463–469 (2011).
6. Xu, W. *et al. Cancer Cell* **19**, 17–30 (2011).
7. Xiao, M. *et al. Genes Dev.* **26**, 1326–1338 (2012).
8. Sun, Y. *et al. Nature Cell Biol.* **11**, 1376–1382 (2009).
9. Cairncross, J. G. *et al. J. Clin. Oncol.* **32**, 783–790 (2014).
10. Knijnenburg, T. A. *et al. Cell Rep.* **23**, 239–254.e6 (2018).
11. Sulkowski, P. L. *et al. Sci. Transl. Med.* **9**, eaal2463 (2017).
12. Inoue, S. *et al. Cancer Cell* **30**, 337–348 (2016).

Quantum physics

A step closer to secure global communication

Eleni Diamanti

Quantum key distribution is a cryptographic method that can guarantee secure communication. A satellite-based experiment has shown that this technique can be applied over long distances without the need for trusted relays. **See p.501**

Modern society is driven by the large-scale exchange of information. As a result, secure communication of sensitive data around the world is an increasingly valuable asset. The mathematical toolbox that is widely used for this task can be complemented by applying the principles of quantum physics to enhance the security of the communication link. This approach has highly desirable features, such as protection of the encrypted information from threats that might arise as a consequence of future advances in computational power. However, it also comes with substantial technological challenges in terms of the range of communication possible and the degree of trust in the devices used. Yin *et al.*[1] demonstrate on page 501 that such cryptographic solutions can be deployed over distances exceeding 1,000 kilometres, without compromising the security promised by the underlying quantum technology.

The flagship application of quantum communication is known as quantum key distribution (QKD). This process enables two parties located at a distance from each other to share a secret string of bits (units of information) called a key, which they can use to encrypt and decrypt secret messages, without making assumptions about the computational power of a potential eavesdropper. Although the principle of such absolute security is based solidly on fundamental laws of nature, practical implementations come in different configurations[2].

For example, it is possible for one of the two parties to prepare quantum states of light — the natural physical carrier of information in quantum communication — and to send them to the second party, who measures them. By processing these data using standard classical communication, the two parties can then extract the secret key. QKD in this setting has been demonstrated over 400 km in a low-loss optical fibre[3] and over 1,200 km using a satellite-to-ground communication link[4].

Although impressive, these demonstrations require the two parties' devices to be fully characterized and trusted. Furthermore, losses in the optical-transmission medium eventually become prohibitive. As a result, the networks that need to be established to distribute keys securely between parties contain nodes, which also need to be trusted[5,6]. This constraint might be undesirable for some applications.

If, instead, one could use the distribution of 'entangled' states of light produced by a source, the need for trust would be greatly alleviated. Entangled states embody the peculiar nature of quantum physics and exhibit correlations not found in classical physics. Such correlations can be routed through devices called quantum repeaters, so that remote physical systems can become entangled. The past few years have seen major progress in this direction[7]. But, so far, the longest distances for entanglement distribution have been achieved by transmitting the states directly. These distances are approximately 100 km in an optical fibre[8,9] and 1,200 km using satellite links[10].

Ideally for QKD, the security of the key generated would be confirmed just by detecting these non-classical correlations experimentally, through statistical properties known as Bell inequalities, without having to trust the devices used by the two parties[11]. However, in practice, achieving this level of security places stringent requirements on the experimental devices that cannot be satisfied by currently available technologies. A way forward is to implement entanglement-based QKD that has weaker requirements, whereby, although the parties' devices must be trusted, the source of the entangled states can remain untrusted[12].

Yin *et al.* have performed a complete, long-distance implementation of QKD with these restrictions (Fig. 1). A key way to

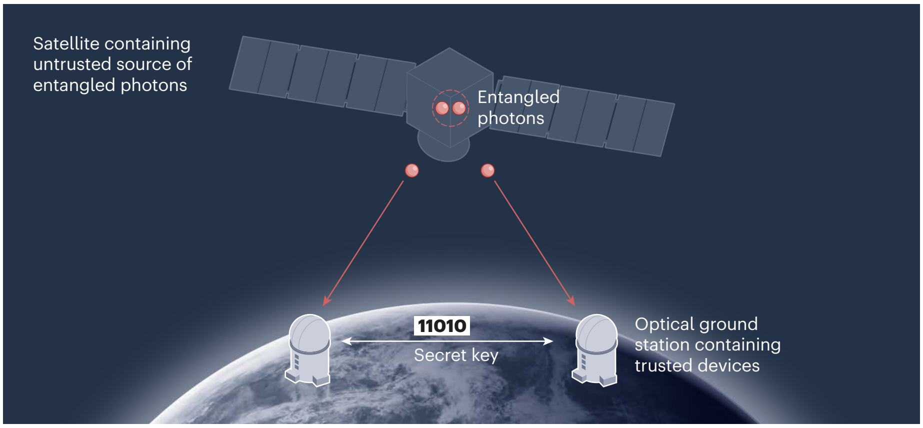

Figure 1 | Entanglement-based quantum cryptography. Yin *et al.*[1] report an experiment in which pairs of entangled photons (photons that are correlated in a non-classical way) are produced on board the satellite Micius. The photons in each pair are then sent to two optical ground stations that are separated by a distance of 1,120 kilometres. This process enables parties at the two stations to share a secret string of bits called a key, which they can use to encrypt and decrypt secret messages with absolute security. In the authors' set-up, the devices used by the two parties must be trusted, but the source of the entangled photons is allowed to be untrusted.

understand their result is to observe how it was achieved, starting from previous work[10] by some of the current authors and their colleagues in 2017. In that paper, the researchers demonstrated the distribution of entangled states generated on board the satellite Micius and sent through two communication links to optical ground stations in China separated by 1,200 km.

Although that work was a milestone for the field, the transmission efficiency achieved was too low for QKD to be carried out in practical conditions. In particular, because only a finite number of states can be transmitted during a short data-collection window, the many errors involved prevented a secret key from being extracted. Taking into account the use of a finite number of transmitted states is crucial for achieving security, especially in the case of a satellite-based experiment, in which data are collected only during the brief time the satellite is visible from the ground stations.

Yin *et al.* remedied this problem by implementing major technological enhancements. These included installing highly efficient telescopes at the ground stations and optimizing equipment components at all stages of the optical path. The authors' meticulous optimization also involved cutting-edge signal acquisition, pointing and tracking systems and synchronization techniques for both the satellite and the ground stations. Their efforts led to a fourfold increase in transmission efficiency compared with the previous experiment and, consequently, produced low enough error rates for a secret key to be extracted. The authors also verified the stability and reliability of their findings over multiple satellite orbits.

From a security perspective, this demonstration does not remove the need for trust in the receiving stations. Therefore, assumptions must be made about the internal workings of the devices in these stations. Yin *et al.* did two things to minimize the risk that these assumptions would not hold in practice. First, they used a systematic approach to tackling imperfections that might inadvertently leak information to a potential eavesdropper. Second, they used a range of solutions to actively control the properties of the photonic information carriers. Combined with security from this quantum approach that should be guaranteed against all possible attacks, this makes the authors' result the most advanced QKD demonstration so far.

However, several shortcomings will need to be overcome for these findings to become relevant for truly practical high-security applications. For instance, the experiment produced keys at extremely low rates. Also, the experiment was carried out only at night, and using a wavelength that is incompatible with the optical-fibre networks used for telecommunication that would interface with space-based networks in infrastructures for global quantum communication. Moreover, QKD can be achieved only between ground stations that are visible simultaneously from the satellite.

Progress in all these areas requires the development of high-performance devices operating at a longer wavelength than that used in this work, the use of satellites in higher orbits than that of Micius and — in the long term — integration of the demonstrated technology with quantum repeaters and other promising architectures allowing for untrusted nodes[13]. Such advances would then unlock the full potential of quantum technologies for executing cryptographic tasks at a global scale.

Eleni Diamanti is at the National Centre for Scientific Research (CNRS), Sorbonne University, 75005 Paris, France.
e-mail: eleni.diamanti@lip6.fr

1. Yin, J. *et al. Nature* **582**, 501–505 (2020).
2. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. *npj Quantum Inf.* **2**, 16025 (2016).
3. Boaron, A. *et al. Phys. Rev. Lett.* **121**, 190502 (2018).
4. Liao, S.-K. *et al. Nature* **549**, 43–47 (2017).
5. Peev, M. *et al. N. J. Phys.* **11**, 075001 (2009).
6. Liao, S.-K. *et al. Phys. Rev. Lett.* **120**, 030501 (2018).
7. Bhaskar, M. K. *et al. Nature* **580**, 60–64 (2020).
8. Aktas, D. *et al. Laser Photon. Rev.* **10**, 451–457 (2016).
9. Wengerowsky, S. *et al. Proc. Natl Acad. Sci. USA* **116**, 6684–6688 (2019).
10. Yin, J. *et al. Science* **356**, 1140–1144 (2017).
11. Ekert, A. K. *Phys. Rev. Lett.* **67**, 661–663 (1991).
12. Bennett, C. H., Brassard, G. & Mermin, N. D. *Phys. Rev. Lett.* **68**, 557–559 (1992).
13. Lo, H.-K., Curty, M. & Qi, B. *Phys. Rev. Lett.* **108**, 130503 (2012).

Ecology

Model system might reveal how coral cells evict algae

Alejandro Sánchez Alvarado

Global warming is threatening the survival of coral reefs. A laboratory model system has now been developed that should aid efforts to understand reef biology and the processes that underlie harmful bleaching events. **See p.534**

From the late Precambrian era (around 650 million years ago) to the present day, a singular, carbon-based 'economy' has been operating between corals and algae that has fuelled the building of untold expanses of barrier reefs in oceans around the globe. On page 534, Hu *et al.*[1] now set the stage for efforts to gain a deeper understanding of how corals and algae interact in coral reefs.

Corals — multicellular marine invertebrates belonging to the class Anthozoa of the phylum Cnidaria — usually live in compact colonies composed of individual structures called polyps. Most reef-building corals harbour algae in their cells in a specialized, membrane-bound compartment called a symbiosome. As its name implies, this specialized structure is home to one of nature's most remarkable, mutually beneficial, endosymbiotic relationships. Corals provide specific species of alga with a protected environment and with compounds needed to carry out photosynthesis. In return, the algae supply the coral with the products of photosynthesis: oxygen, glucose, glycerol and amino acids. This biomolecular bounty is then transformed by the corals into proteins, fats, carbohydrates and a calcium carbonate skeleton.

> **"The authors confirmed that they had correctly identified the coral cells that host algae."**

Around 90% of the organic material produced by these algal endosymbionts is ultimately transferred to the coral host[2], underpinning the quiet yet unceasing growth and productivity of coral reefs[3]. It has been estimated that this endosymbiotic relationship is responsible for an area of nearly 250,000 square kilometres of the most spectacular and crucial ecosystems on our planet, supporting some 2 million or more species[4]. However, the current rise in ocean temperatures is causing disruption, because exposure to prolonged heat causes corals to evict their symbiotic algae, resulting in a phenomenon known as coral bleaching — loss of the colourful algae leaves the coral white in appearance. Severe coral bleaching threatens to cause a marine calamity of global proportions. Unfortunately, we know little about the molecular basis that underlies how coral cells orchestrate algal expulsion, nor about how corals recognize, take up and maintain their algal endosymbionts.

Hu and colleagues' work heralds a new