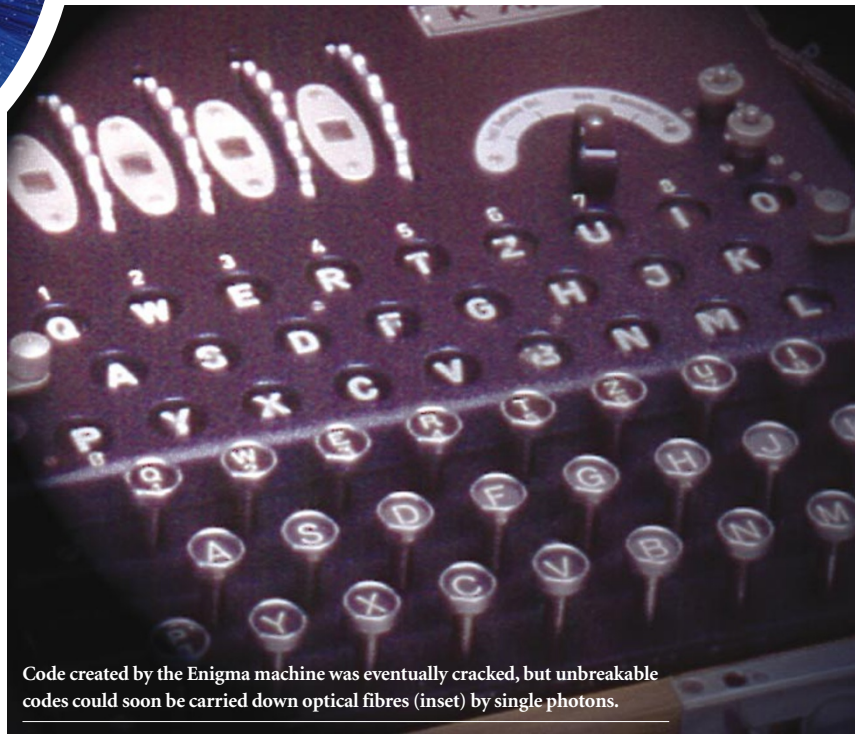
Can you keep a secret?

A. HART-DAVIS/SPL

Practical products are about to emerge from the weird world of quantum mechanics. Erica Klarreich finds out how quantum cryptography made it from the lab to the marketplace.



SCIENCE MUSEUM/SCIENCE & SOCIETY PICTURE LIBRARY

Code created by the Enigma machine was eventually cracked, but unbreakable codes could soon be carried down optical fibres (inset) by single photons.

The Enigma code machine, used by the German military during the Second World War, was a masterpiece of complexity. Each letter of the alphabet was encoded by a system of wheels that could be set in an almost endless array of configurations, creating a seemingly unbreakable cipher. But Enigma had a chink in its armour.

Messages could not be decoded unless the receiver knew which wheel settings the sender had used. Users exchanged this information, known as a key, at the beginning of the message and encoded it using another, prearranged, key. But security for this second key was not perfect. Enigma users changed it only once a day. After cracking a few messages by focusing on commonly used words, code-breakers could tease out the second key and decipher all of the day's transmissions.

More then half a century later, secret messages are still only as secure as the keys used to encrypt them. Sensitive data are exchanged every day, yet no one has developed a system that ensures that the keys to these messages are absolutely secure.

This may soon change. Companies are close to marketing cryptographic systems that use quantum mechanics to offer absolute security — guaranteed by the laws of physics. Devices that can securely transmit keys through fibre-optic cables may soon be available. And it might eventually be possible to transmit quantum keys using satellites, allowing users across the world to form secure connections.

The keys used to encrypt most messages, such as those used to exchange credit-card information over the Internet, are themselves encrypted before being sent. The schemes used to disguise keys are thought to be secure, because cracking them would take too long for even the fastest computers. The widely used RSA algorithm is one example. Anyone wanting to receive a message publishes two numbers, one of which is the product of two very large prime numbers. Senders convert their message into a series of digits, and perform a simple mathematical calculation on the series using the publicly available numbers. Messages are deciphered by reversing the calculation.

Prime movers

This is easy to do if you know the values of the prime numbers, which are not published. An eavesdropper can, in principle, work them out, but for big enough numbers this would take millions of years with the computing power available today.

The future performance of such systems depends on estimates about the speed of future computers, and such guesses have proved wrong is the past. In 1977, for example, *Scientific American* challenged computer scientists to decode a message encrypted using a 129-digit number[1]. Ron Rivest, a computer scientist at the Massachusetts Institute of Technology and one of RSA's creators, estimated that it would take 4×10^{16} years to factor such a number. But in 1994, a team of computer scientists and amateur volunteers managed to decipher the message by applying 1,600 computers to the problem over a period of eight months[2].

In the same year, computer scientist Peter Shor of AT&T Labs in Florham Park, New Jersey, described a new kind of threat. Shor was interested in quantum computers — hypothetical machines that should be able to carry out a large number of calculations simultaneously. He showed that if such a computer is ever built, it will be able to factor large numbers rapidly, and could quickly crack all the commonly used public key systems[3].

A quantum computer or new factoring technique might not come along for decades. But some secrets encrypted today, such as the design of nuclear weapons, will still be important then. "We have to assume that any information encrypted today is probably being recorded by eavesdroppers in the hope that it will be of value 10 or 20 years into the future," says Richard Hughes, a physicist at Los Alamos National Laboratory in New

Mexico who works on quantum cryptography. "If they have quantum computers, they'll be able to look at information encrypted today and learn useful things from it."

But while quantum computers remain no more than an interesting possibility, another quantum technology could soon be ensuring total security. In quantum mechanics the act of measurement changes the properties of the very thing being measured. This is a boon to cryptologists, because it means that eavesdroppers cannot listen to certain types of information without leaving an unmistakable disturbance.

Polarized opinion

The details of a quantum cryptography system were first described in 1984 by theoretical physicists Gilles Brassard of the University of Montreal in Canada and Charles Bennett of IBM's Thomas J. Watson Research Center in Yorktown Heights, New York[4]. In their scheme, Alice sends Bob a series of ones and zeros, which are used to generate the key. Each 'bit' is represented by a photon of light with one of four possible polarizations: horizontal, vertical or one of the two diagonals. Alice and Bob agree that a horizontal polarization corresponds to a zero and a vertical polarization corresponds to a one, and make a similar decision for the two diagonal polarizations.

Quantum mechanics says that Bob can either look to see whether the photon is horizontally or vertically polarized, or which of the diagonal polarizations it has, but he cannot do both. When a photon arrives at Bob's end, he randomly chooses which of the two types of orientation to test for. If Alice has sent a vertically polarized photon and Bob makes a horizontal–vertical measurement, he will discover the polarization correctly and read off a one.

But if Bob makes a diagonal measurement, the vertical polarization of the photon lies exactly midway between the orientations he is looking for. The photon will instantly switch to one of the diagonal polarizations, each with the same probability, and Bob has an equal chance of recording a one or a zero. Bob will also get a random result if he makes a horizontal–vertical measurement on a diagonally polarized photon.

At the end of the transmission, Bob knows he has correctly measured the polarizations of about half of the photons, but doesn't know which ones. So Bob contacts Alice on a channel that doesn't have to be secure, and tells her which type of measurement he made for each photon, but not the outcome of those measurements. Alice tells him which measurements were correct. They discard the incorrectly measured photons, and keep the rest for their key.

To make sure that a third party, Eve, hasn't listened in to their original exchange, Alice and Bob next sacrifice a small amount of their key and check it over the public channel for errors. If Eve has been assessing the polarization of the photons somewhere between Alice and Bob, she will have changed the polarization of about half of them. This makes about one in every four entries in Bob's key different from those that Alice sent — a clear indication that Eve has been snooping. And there is no way consistent with the laws of physics for Eve to cover her tracks.

In reality, noise in the channel through which the photons pass introduces a small number of errors into the transmission. So a clever eavesdropper could gain some information about the key by measuring such a small number of photons that Alice and Bob cannot distinguish the errors this introduces from those caused by noise. Alice's single-photon generator could also cause problems by occasionally sending out two photons instead of one. Eve can divert and measure one of the photons, while allowing the other to proceed to Bob. But in each case, Bob and Alice can generate a new key by applying an algorithm to their existing key. Eve, who is missing the bulk of the original key, cannot hope to predict the outcome of this algorithm.

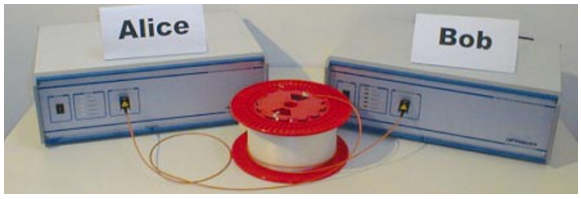
In 1989, a team led by Bennett and Brassard built a working device, and sent photons through the air to a receiver about 30 centimetres away[5]. By the mid-1990s, other groups were sending encrypted keys through tens of kilometres of optical fibre. And over the past few years, the first steps towards commercializing such systems have been taken. "Quantum cryptography is very much a reality," says Brassard.

Gone in a flash

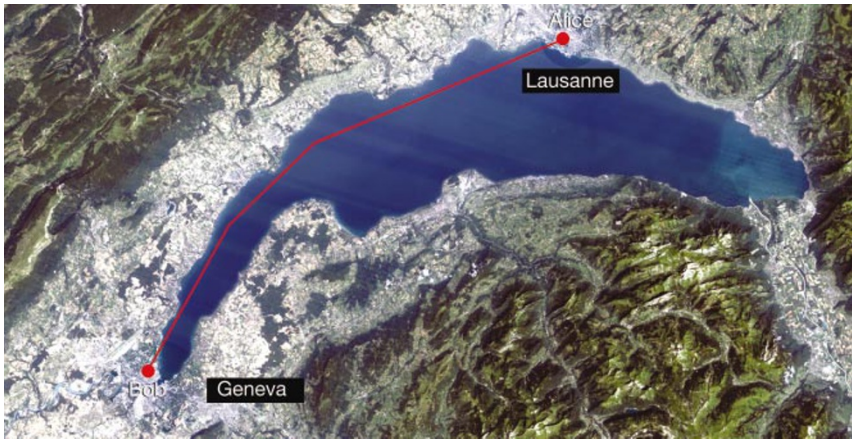
Last October, a group of physicists at the University of Geneva in Switzerland launched a company called id Quantique, which will supply a system integrating the cryptography hardware — photon sources and detectors, and fibre-optic connections — needed to exchange keys. In March this year, they used the system to send single photons through 67-km telecommunication cables running under Lake Geneva[6]. "The system is very stable, and has the potential to be very fast," says Nicolas Gisin, a member of the team.

MagiQ Technologies, a New York firm that specializes in quantum technologies, is trying to a build a system in which the discussion about which photons have been received correctly is streamlined and integrated with the photon generators, detectors and fibre-optics. The firm hopes to market a full quantum-cryptography system by early next year.

MagiQ and id Quantique's systems are designed to connect users who are linked by a single dedicated fibre, but other groups are working on systems that can support a network of users. Last September, BBN Technologies, an information-technology company based in Cambridge, Massachusetts, began a five-year collaboration with teams at Boston and Harvard universities to build



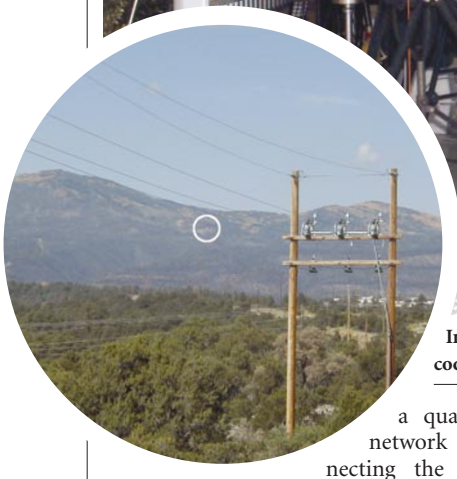
Light work: keys encoded using polarized photons have been sent between Alice and Bob (left) through 67 km of fibre-optic cable under Lake Geneva.



Gilles Brassard (left) and Charles Bennett laid the foundations of quantum cryptography.

G. FROIDEVAUX/UNIV. GENEVA

LANL



In the air: Richard Hughes has sent a photon-encrypted code from a laser source (circled, inset) to a receiver.

a quantum network connecting the three institutions. Photons will be routed round the network using mirrors. "The mirrors send the photon along without measuring it, so they don't create the kind of disturbance an eavesdropper would," explains Chip Elliott, an engineer at BBN.

Working devices may soon be on the market, but that does not mean that the engineers involved can rest on their laurels. Reliable single-photon generators, for example, are not yet commercially available. Today's systems, such as those developed by id Quantique, instead use lasers that generate pulses so weak that they almost never contain more than one photon. But at such low intensities, nine out ten attempts to fire a photon fail.

Current photon detectors also present some problems. To spot a single photon, the detectors must be so sensitive that they will sometimes register photons that are not there. Even then, they will typically miss 90% of the transmitted photons. What's more, many photons are absorbed by the optical fibre and never make it to the receiver. "We send five million bits per second, but by the time we get done with all the detectors and the specialized protocols that shorten the key during the public discussion, we get somewhere between 100 and 1,000 bits per second," says Elliott.

But this is enough for cryptographic uses. The Advanced Encryption Standard, the encryption algorithm used by the US government, uses a key with a maximum of 256 bits. A key distribution that sends 500 bits per second would allow users to change the key roughly twice per second, more than ample for most purposes.

The distance that the key can be transmitted is a more important technical limitation. Most experts agree that the Geneva group's 67-km transmission is close to the maximum that can be achieved with current technology. Beyond about 80 km of cable, too few photons make it from Alice to Bob. Both id Quantique and MagiQ are reluctant to discuss who is interested in their products, but this limitation means that the first users are likely to be organizations that want to transfer highly secret material within a single city, such as government offices, banks and businesses.

Long-range forecast

The range could be extended by devices that strengthen the signal as it passes by, like those used to send telephone conversations over long distances. But unlike telephone repeaters, quantum versions would have to bolster the signal without measuring the photons. "A repeater that doesn't measure was thought to be impossible in the early 1980s, but since then scientists have shown that it is feasible in principle," Brassard says. "But we're nowhere near the technology to build one."

Satellites could provide an alternative means of achieving long-distance transmission. Hughes' team at Los Alamos is developing a key-distribution system that sends single photons through open air. So that the photons can be distinguished from all the others bombarding the detector, the team uses various techniques to filter the incoming light. The detector only accepts photons within a narrow range of wavelengths — about 0.1 nanometres — and ignores photons that arrive from angles outside a window of about a hundredth of a degree. A bright pulse of light is also sent 100 nanoseconds ahead of each photon, cueing the detector to expect the next signal.

"When we threw in these three filters, we could get the amount of light down to the level where we could detect the photons we wanted, even if the Sun was shining directly on the receiver," says Hughes. In a paper published this month[7], Hughes and his colleagues describe how they sent keys over a distance of 10 km with rates similar to those achieved using optical fibres.

Ten kilometres is still a long way short of the hundreds of kilometres between the Earth's surface and satellites. But because air turbulence, the factor that most disrupts the photons, occurs predominately in the lower two kilometres of the atmosphere, Hughes believes his system should be able to send signals to satellites. "I don't see any showstoppers at all to doing this from ground to satellite," he says. The team is now trying to make the receiver light and sturdy enough to fit in a satellite and survive a rocket launch.

Combined with optical fibres, satellites could eventually form part of a long-distance transmission system. In the shorter term, the technology might help to protect the security of satellite television broadcasts. In one embarrassing breach, a hacker known as Captain Midnight interrupted a 1986 broadcast by US company Home Box Office and sent over half of the company's customers a five-minute broadcast of a message complaining about the firm's new subscription charges.

Quantum cryptography may soon be helping to prevent similar lapses, and to protect sensitive transmissions. Within the next few months, such systems could start encrypting some of the most valuable secrets of government and industry. Cryptography is about to lose its Achilles' heel. ■

Erica Klarreich is journalist in residence at the Mathematical Sciences Research Institute in California.

1. Gardner, M. *Sci. Am.* **237,** 120–124 (1977).
2. Atkins, D., Graff, M., Lenstra, A. K. & Leyland, P. C. in *Advances in Cryptology — ASIACRYPT '94* (eds Pieprzyk, J. & Safavi-Naini, R.) 263–277 (Springer, Heidelberg, 1995).
3. Shor, P. W. in *Proc. 35th Annu. Symp Foundations Comp. Sci.* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, Los Alamitos, California, 1994).
4. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conference on Computers, Systems & Signal Processing* 175–179 (IEEE Press, Los Alamitos, California, 1984).
5. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. *J. Cryptol.* **5,** 3–28 (1992).
6. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. *New J. Phys.* **4,** 41 (2002).
7. Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G. *New J. Phys.* **4,** 43 (2002).

www.idquantique.com
www.magiqtech.com
www.bbn.com