

The unbreakable code: Is this the lock?

Use of quantum properties ensures unauthorised attempts to access encoded information do not go undetected

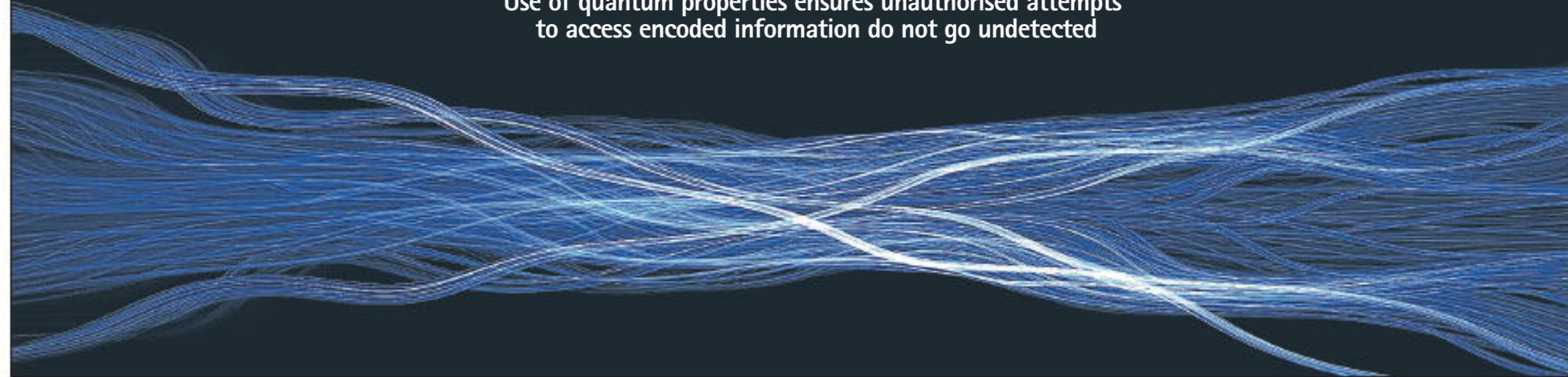


PHOTO: ISTOCKPHOTO

ULTIMATE SECURITY?: Entangled photons may be harnessed to keep information secure – no matter how complex and subtle the advanced technology and computing power available to the eavesdropper.

BY ARTUR EKERT

ACCORDING to a popular story, when the Mongols ruled China in the 14th century, the success of an uprising against them hinged on secret messages hidden in mooncakes.

The successful revolution depended on keeping the method of communication secret.

Not such a good idea. No matter how creative we are in hiding messages, our tricks will be found out sooner or later.

Can we reveal our methods of secret communication without compromising secrecy? Yes. Modern methods of secret communication can be described as sending messages in locked boxes.

The sender locks his message in a box and sends it to his ally, who unlocks the box and reads it.

Everybody knows how the boxes are constructed but only the sender and recipient hold the keys. If an eavesdropper got hold of the key, he could open the boxes in transit and read the messages undetected. The legitimate users know about this risk, and try to change their keys frequently because the security relies entirely on keeping them secret.

Here, boxes are mathematical methods of disguising messages. Locking a box is called encryption, and real cryptographic keys are secret sequences of numbers used by senders and recipients to

encrypt and decrypt their messages. Ultimate security is possible, but only if each message is encrypted with its own unique key that is truly random and never reused. This method is known as the one-time pad and requires as many keys as messages.

The snag is, users may be miles apart, so how do they exchange keys? The problem of getting the key from sender to recipient without an eavesdropper intercepting it – the “key distribution problem” – has become an expensive logistical issue for banks, governments and the military.

If the same key is used for too long, encryption can be broken in many ingenious ways.

Physicists relate the key distribution problem to eavesdropping abilities. Suppose an eavesdropper is tapping a telephone line used for key distribution. Any measurement on the signal in the line may disturb it and leave traces. However, any eavesdropper with superior technology can escape detection.

The way around this problem involves quantum physics – physics that describes the world of elementary particles such as photons and atoms.

If, for example, some quantum properties of photons are used to carry the information, then, according to quantum principles, one cannot pick up all the encoded information and go undetected. No matter how complex and

subtle the advanced technology and computing power available to the eavesdropper, the “quantum noise” caused will expose each attempt to gain even partial information about the key. This is the basic idea behind quantum key distribution.

One approach, which I proposed in 1991 during my student days in Oxford, involves entanglement, a quantum property which implies that two separated objects behave as if they were two parts of the same entity.

That this behaviour has not

FOILING EAVESDROPPERS

Any eavesdropper with superior technology can escape detection. The way around this problem involves quantum physics – physics that describes the world of elementary particles such as photons and atoms.

been “pre-programmed” is one of the most surprising and profound things we have learnt about the physical reality in the past few decades.

This is also what protects the entanglement-based key distribution. With no pre-determined outcome of a measurement, no eavesdropper may know the outcome.

Convincing the world of academia was easy, but it took a

bit longer for quantum entanglement to enter the banking sector. In 2004, Bank Austria Creditanstalt finally put some trust into quantum theory by allowing Austrian researchers to carry out the first demonstration of a bank transfer protected by entangled photons.

Singapore is not lagging behind; on the contrary, many of the most advanced quantum experiments have been performed here, on our small “Quantum Island”.

Research in quantum technology here goes back to 1998, when

A few years later, support from A*Star’s consolidated research efforts in the field and the National University of Singapore faculty appointments of professors Berge Englert, Christian Kurtsiefer, and Antia Lamas Linares strengthened the group. The last two deserve a special mention – over the past four years they managed to put Singapore at the frontiers of experimental research in quantum technologies.

It was their team of local young researchers that developed excellent sources of entangled photons and demonstrated very stable free-space quantum key distribution between buildings on the NUS campus. These and many other exciting experiments are now carried out at the Centre for Quantum Technologies (CQT), which is the first Research Centre of Excellence here, funded jointly by the National Research Foundation and Ministry of Education, and hosted by NUS.

One truly remarkable feature of the entanglement-based key distribution is that there is no need for sender or recipient to control the source of entangled photons.

It does not have to be protected at all.

One can imagine sources of entangled photons in public places such as rooftops, to which any two parties willing to establish cryptographic keys can just tune in.

Indeed, a team of European researchers, with the European

Space Agency, is working on the possibility of distributing quantum keys worldwide by satellite.

An even more puzzling feature of entanglement-based quantum cryptography was recently demonstrated here. CQT’s Valerio Scarani, together with European colleagues, showed that the entanglement-based key distribution scheme is far more general and much more powerful than I originally anticipated; it works even with devices of dubious provenance.

This means that you and your friend may purchase cryptographic equipment from any company, even from your competitors or enemies, and still be able to establish a secret key.

This amazing feat has just been demonstrated by CQT’s quantum optics group. The experiment opens a new chapter of modern cryptography.

Quantum information technology is a fundamentally new way of harnessing nature. It is too early to say how important this will eventually be, but we can reasonably speculate about its impact on data security – the future of secure military and commercial communication will probably go quantum.

The writer is the director of the Centre for Quantum Technologies at the National University of Singapore, the first Research Centre of Excellence here. He is one of the inventors of quantum cryptography and has made a number of contributions to quantum information science.