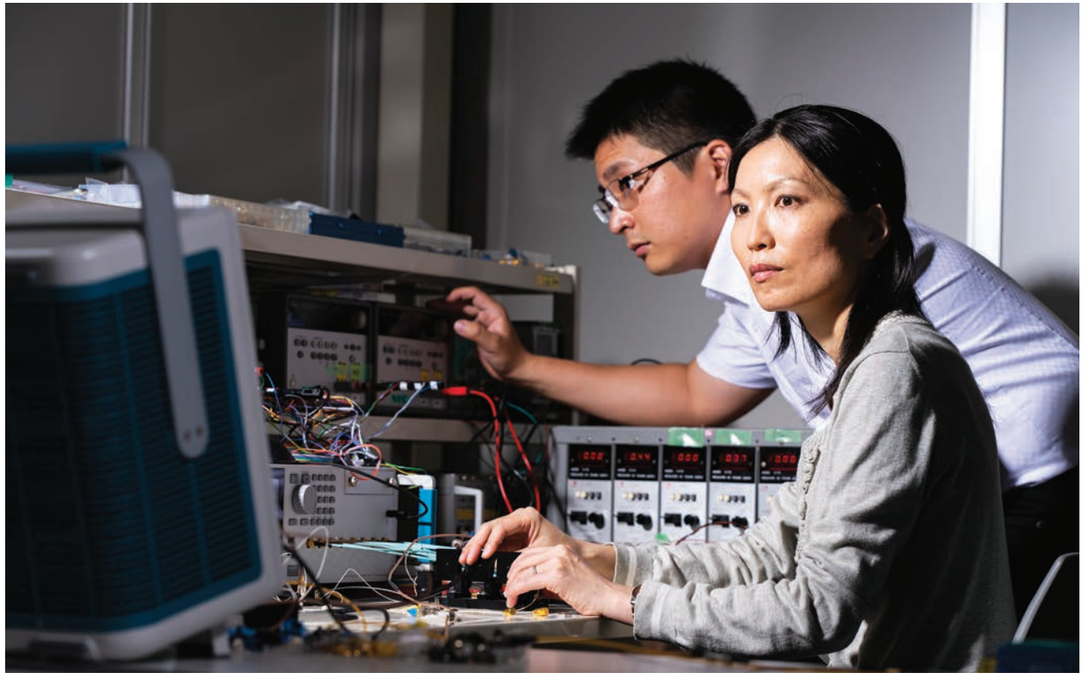


HOW TO TAKE QUANTUM CRYPTOGRAPHY MAINSTREAM

New systems promise widespread secure quantum communication by using COST-EFFECTIVE DETECTORS that monitor for telltale noise in properties of optical signals sent along standard communication fibres.

Quantum computers will eventually pose a problem to standard encryption, warns Wakako Maeda, a manager in the quantum cryptography team at NEC Corporation in Tokyo, Japan. As far back as 1994, it was calculated that a quantum computer with just over 4,000 quantum bits — or qubits — could crack the security codes that keep banking details, internet transactions and communications safe from hackers, all in a matter of seconds[1].

▲ **Wakako Maeda (front) works at NEC Corporation in Tokyo. NEC are pioneering continuous variable quantum key distribution systems.**

The danger is not immediate, but it is real, she says. Teams across the globe are painstakingly striving to build a working quantum computer. So far, IBM leads with its Eagle computer that strings together only a modest 127 qubits. But progress has been accelerating in recent years.

Quantum physicist, Takuya Hirano, of Tokyo's Gakushuin University, and his team, have also warned of the risk of 'store now, decrypt later' attacks, in which a hacker undetectably wiretaps a link and holds on to the encrypted information, waiting until a quantum computer exists to decrypt it.

Online communication today is protected by algorithms that scramble our data, explains Maeda. The receiver is able to decode the message using a secret private key. This technique is so effective that even the world's best supercomputers typically can't hack these keys — without taking a period equivalent to the age of the universe to do so. But "if quantum computers, which promise to be exponentially more powerful, become common and widely used, these keys could be decrypted," says Maeda. "This could be very disruptive to critical systems, such as those protecting national security."

A handful of companies located in China, Switzerland and Japan, already sell small-scale quantum encryption devices, but they are prohibitively expensive. None are commercially used in Japan — however, the Japanese government is heavily investing in research and development, and has suggested it will offer tax credits to companies that introduce quantum encryption.

Since 2018, NEC, a leader in IT and network technologies, with headquarters in Tokyo, Japan, has been developing a new range of more affordable, ultra-secure quantum communication systems that partly exploit a different set of quantum features than previous cryptography systems. NEC is predicting these will be commercially available in the next few years.

LESS EXPENSIVE DETECTORS

In collaboration with Gakushuin University physicists, including Hirano, NEC are pioneering continuous variable quantum key distribution (or CV-QKD) systems[2]. These harness a less-studied, but potentially much more cost-effective, security breach detection technique.

Quantum cryptographic systems not only encrypt information, they alert legitimate users to hacking activity. The idea is that a secret key is encoded in the quantum properties of optical signals that are transmitted between sender and receiver. The laws of quantum physics are such that a hacker measuring a quantum property to read a secret key signal irrevocably disturbs it. So, an eavesdropper can't surreptitiously detect a key without interfering with the signal in a noticeable way, setting off an alarm.

Currently available quantum cryptographic systems all use a technique called discrete variable quantum key distribution (or DV-QKD), in which the secret key is encoded as a series of 0s and 1s in the properties of a string of single particles of light, or photons. These photons are individually detected by the receiver using photon detectors, which make a clicking sound when they're hit by a photon, with a click of one detector corresponding to a '1' and a click of another detector corresponding to a '0'. If a hacker tries to intercept that signal, it introduces an error in the transmission of the string, explains Hirano. The method is extremely successful, but the receiving unit needs very high sensitivity, thus is expensive, says Maeda.

The NEC/Gakushuin University quantum cryptographic systems are based on CV-QKD, where, rather than monitoring the discrete clicks of incoming photons, the receiver's detector continually measures aspects of the light's electric field, such as its amplitude. Here "eavesdroppers are detected by an increase in excess noise" in the signal picked up by the receiver, explains Hirano. A major advantage of CV-QKD is that the detectors do not need to be as sensitive, and are much cheaper.

METROPOLITAN USES

The optical components used in CV-QKD are found in existing commercial optical transport equipment, which reduces installation costs. In existing fibre-optic communication systems, a single optical fibre carries multiple signals simultaneously, each encoded in laser light of different wavelengths. These data signals are amplified along the way, a process that generates some noise in the fibre, but usually not enough to disrupt the signals.

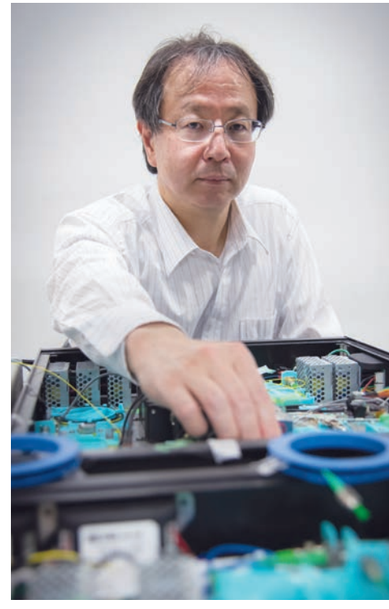
Things are not so simple when a quantum signal is sent down the same line, however, because quantum signals are more sensitive to noise disruption. There is also the risk that the presence of the quantum signal would interfere with the other data travelling through the channel, causing cross-talk. To overcome this, Hirano and his colleagues fine-tuned transmission wavelength filters and developed a detection method that also works as a filter, damping cross-talk and allowing the true quantum data signals to be interpreted.

In 2017, they confirmed that information can be communicated through standard optical fibres[2] and in 2019, they demonstrated the fastest ever data transmission with 100 channels of normal data coexisting with secure CV-QKD in a single fibre[3]. "We showed that CV-QKD can work in real conditions, using commercially available technology," explains Hirano.

This more economical alternative could make large-scale secure communication networks vastly more viable, he says. The technology can work in very noisy environments, over a range of about 20 kilometers, potentially covering a metropolitan area. "DV-QKD has been more mainstream, and more work has been done on it, so it has been somewhat surprising to be able to realize secure key distribution with CV-QKD using coherent optical communication technology," says Maeda.

But she emphasizes that CV-QKD will not replace DV-QKD, but should be considered as a complement to it. NEC began research on DV-QKD in 1999, and DV-QKD still has certain advantages over CV-QKD. In particular, it can support a longer transmission distance of around 50 km. NEC have been working on CV-QKD with Hirano and his colleagues since 2018, building on work that Gakushuin University began in 1998.

NEC is continuing research and development of both kinds of systems, in tandem. "We want the systems to meet the needs of different customers," says Maeda. She believes that a secure, global quantum communication network will probably require a mix of both systems. NEC intends to commercialize its DV-QKD technologies in 2023, and its CV-QKD systems around 2024, she says, adding: "I think a combination of the two will be possible after that." ■



▲ **Takuya Hirano, from Gakushuin University, researches cryptographic systems that measure aspects of light's electric field.**

REFERENCES

1. Shor, P. W. Proc. *35th Annu. Symp. Found. Comput. Sci.* 124–134 (1994)
2. Hirano, T. *et al. Quantum Sci. Technol.* **2,** 024010 (2017)
3. Eriksson, T. *et al. Commun. Phys.* **2,** 9 (2019)

Advertiser retains sole responsibility for content