# BUILDING A FORTRESS WITH CONVENTIONAL AND QUANTUM CRYPTOGRAPHY

Quantum cryptography needs to be carefully INTEGRATED WITH SECURE DATA STORAGE SYSTEMS and conventional cryptography to create truly unhackable information infrastructure.

**A Japanese programme aims to be among the first** to create a national, integrated, quantum-enabled and quantum-resistant cybersecurity system for communications and information processing.

While currently only in their infancy, the powerful processing of future quantum computers poses a major threat to global long-term data security, explains Mikio Fujiwara, director of the Quantum ICT Laboratory at the National Institute of Information and Communications Technology (NICT).

If a large enough quantum computer is created, today's public key cryptography — based on the mathematical complexity of prime number factorization or discrete logarithm problems — could be instantly deciphered.

"The Japanese government is actively addressing this challenge through a programme called 'Photonics and Quantum Technology for Society 5.0'," says Fujiwara.

The core technologies that will underpin the project's 'Quantum Secure Cloud' system use quantum properties to create cryptographic keys, known as quantum key distribution devices, explains Masahide Sasaki, who, as sub-programme director, is in charge of leading the project's standardization activities.

Every part of the system must be as resistant as possible to quantum attack, he adds. "It's most important that the technologies are fully integrated into a single secure platform, otherwise the security of the whole system can't be assured," he says. "A hacker will just attack the weakest point in the system." The most vulnerable points probably won't be quantum-protected channels, he adds, but part of an existing, conventional layer.

**JAPAN HAS BEEN THE FIRST TO IMPLEMENT A COMPREHENSIVE AND INTEGRATED QUANTUM AND CONVENTIONAL SYSTEM.**

Fujiwara agrees. "We consider eavesdropping on quantum communications to be nearly impossible. On the other hand, it is difficult to completely eliminate the possibility of hacking the node where the quantum key distribution device is installed, so it's important to distribute data that is indecipherable on its own across multiple storage systems." NICT are also working on incorporating a highly secure conventional system to protect nodes, he says.

## MEDICAL-RECORD TEST

The NICT and a consortium of academic and industrial partners have developed a quantum-cryptography integrated system that has recently been tested on a hospital database of 10,000 sensitive medical records.

The new system, called LINCOS (Long-term Integrity and Confidentiality Protection System), uses a distributed storage technique called 'secret sharing', in which the data are split into pieces for storage and a number of pieces must be gathered for reconstruction. This, says Fujiwara, provides 'information theoretic security', meaning that even if attackers could collect some pieces of the data, unless a threshold is reached, they cannot decipher its meaning, regardless of computing power.

LINCOS exchanges data using a dedicated optical fibre network with end-to-end encryption protected by quantum key distribution technology.

Quantum key distribution devices allow a sender and receiver to produce a shared key using properties of quantum mechanics. Any attempt to read these keys disturbs the properties and alerts users.

In a hacking or disaster scenario, provided that there is a limited number of compromised storage servers, the data is exchanged through private channels and remains secure.

In 2019, the group tested their system by establishing a LINCOS between several hospitals in Japan connected by an optical network that extends from Tokyo to the city of Kochi, on the island of Shikoku in the country's south.

"We demonstrated secure sharing and distribution of 10,000 medical records totalling 90 gigabytes of data across more than 800 kilometres," says Sasaki. Over 20 trials of this system, the group confirmed that the average time between entering a patient ID and displaying their medical record on a viewer screen was a workable 7.4 seconds, and that the average time from clicking the prescription record selection button to displaying the contents was 7.1 seconds. That's about 10 times longer than a typical system, but is manageable in a real setting, says Sasaki.

The system has also been built with the ability to restore data from a backup via a satellite link during disasters or outages, says Fujiwara. "In Japan, where there are many large earthquakes, there is a real possibility that hospitals that store electronic medical record data will be damaged."

In one test that assumed disaster at a data storage point, prescription records and allergy information were displayed on a screen roughly nine seconds after a query, using a system supplemented by satellite.

## FAST FINANCES

In 2020, NICT assessed whether part of the Tokyo QKD Network, a quantum key distribution test network managed between a number of industry partners, could protect the data of a fast-moving, large volume financial system. A simulation of a Japanese stock market was created for this purpose by financial holding and securities companies, Nomura Holdings and Nomura Securities.

For this test, NICT used quantum key distribution devices developed by Japanese electronics companies Toshiba and NEC, based on NICT research, explains Fujiwara. Because financial data is delicate and fast moving, NICT incorporated an extra layer of very secure conventional cryptography that included the one-time pad method, advanced encryption standard method, and a low-latency network encryptor that is being developed by NEC.

These additional layers support highly confidential communication, particularly the low-latency one-time pad encryption, which is not currently hackable, explains Fujiwara. But the one-off nature of one-time pad systems do increase the risks of running out of encryption keys in very fast-moving, high-volume systems, so a variety of methods were combined, he adds.

"In the trial, we succeeded in sending dummy financial data that exceeds the amount of data per day used by Japan's stock market in less than 200 µsec without running out of keys," says Fujiwara. The result, he says, suggested that their quantum protected system could more or less maintain the speeds of a conventional stock market system.

## SETTING STANDARDS

Standardization is the next major hurdle with the rollout of a Quantum Secure Cloud and quantum key distribution network in Japan. With many major jurisdictions around the world working on their own implementation, setting standards for the fundamental aspects of a future global quantum cryptography architecture is vital.

"Japan has been the first to develop and implement a comprehensive and integrated quantum-conventional system comprising all of the components and layers needed for real applications," Fujiwara says. "So, the NICT has been working very hard in the international arena on standardization for the hardware, such as the quantum-key distribution modules, but also the application software and conventional elements."

Through collaboration with hospitals, banks, universities and industry, they will continue, he says, to test new applications "based on actual need, and keep Japan at the forefront of quantum secure networking globally". ■

Yuichiro Chino/Getty

▲ Japanese researchers are testing a quantum-conventional system in which data are split into indecipherable, encrypted pieces for storage.

NICT

www.nict.go.jp/en