Source: *The Straits Times,* pA40
Date: 17 June 2017

Communications privacy in the quantum era

Alexander Ling

For The Straits Times

China's satellite Micius is making news for connecting two ground stations 1,200km apart at a rate of one signal per second. That won't sound impressive – it's a lot slower than broadband – but this satellite is transmitting an extraordinary signal. It's a harbinger of the future for cyber security.

On Thursday in the journal Science, the Micius team reported that the 600kg satellite, orbiting 500km above Earth, has distributed pairs of light particles to the two receivers. Most satellites beam out bright signals, made up of large numbers of light particles (known as photons), to make sure their messages reach the ground. This satellite sends out individual photons. Moreover, the satellite sends out pairs of photons that share a special correlation called quantum entanglement. This property is a vital ingredient in emerging technologies for computing and encryption.

There has long been a scientific consensus that entanglement distribution from satellites should be possible. My team at the Centre of Quantum Technologies had demonstrated, in December 2015, a source of photon pairs in space on board the 2kg Galassia spacecraft built by the National University of Singapore (NUS). Galassia was not equipped with telescopes to distribute photons, and so the recent report is the first demonstration of photon pair distribution from space to ground. It's a great technological feat – and it's encouraging for groups around the world working on entanglement-based technology.

In the long term, we may look to quantum satellites to connect a global network of quantum computers. In the near term, we may need them to protect our privacy from such machines.

China's satellite Micius blasting off from a launch centre in Gansu province last year. Micius is now able to send out pairs of photons that share a special correlation called quantum entanglement. PHOTO: AGENCE FRANCE-PRESSE

The past few years have seen dramatic progress in the development of quantum computers. These machines accelerate problem-solving for some types of mathematical sequences by exploiting phenomena such as entanglement. Very basic quantum computers are already available on the cloud – IBM launched one last year to the public, which it upgraded last month to have 16 quantum bits. Other big industry players such as Google, Microsoft and Intel, and aggressive deep-technology start-ups, are also readying the technology for commercial applications.

Quantum computers should bring benefits in areas such as optimisation and drug simulation, but it is also an established fact that they can crack today's common encryption systems. Concern is growing that malicious actors may be recording encrypted data in anticipation of quantum computers. This is a particular challenge for those tasked with maintaining long-term data privacy, from government communications to personal health data.

This has spurred interest in encryption techniques that are "quantum-safe". There are two approaches – a search for mathematical problems that will remain difficult for a quantum computer, and the more novel approach of developing quantum hardware for encryption. Scientists and mathematicians in Singapore are working on both, engaged in the worldwide effort to develop the encryption eco-system of the future.

The search for problems that can resist a quantum computer is a tricky proposition since the technology is still maturing. It is likely that we have not yet uncovered the full potential of quantum computing. Nevertheless, some of my colleagues at NUS are working in this area and they are not alone. The National Institute of Standards and Technology in the United States is organising a competition to identify quantum-resistant problems.

The second approach uses hardware to enhance an encryption scheme we already know to be immune to quantum computers, in which the communicating parties lock and unlock their data using the same key. The key is simply a string of random numbers. The key lacks mathematical structure for the quantum computers to analyse, blunting their advantage. The challenge is to distribute the keys. In today's crypto environment, we use complex mathematical sequences that are vulnerable to quantum computers.

Quantum Key Distribution (QKD) offers an alternative. In QKD, the communicating parties share photons that are encoded with randomness. An advanced form of QKD achieves this with quantum entanglement. Any eavesdropping attempt on the photon stream disturbs the encoding, giving rise to detectable errors. QKD is a peerless technology in forcing an eavesdropper to leave behind tell-tale signs.

Singapore has deep expertise in entanglement technology. Researchers at the Centre for Quantum Technologies pioneered the development of entanglement-based key distribution. Scientists from the centre are collaborating with the NUS-Singtel Cyber Security Research & Development Laboratory to prepare local optical fibre for QKD technology, aimed at securing critical infrastructure and sensitive communications. Singapore's size and rich fibre connections make it an ideal environment for this project.

The situation changes if we need to connect distant parts of the globe, for example Singapore to New York. If we use optical fibres, the photons would have to travel through thousands of kilometres of glass, and will ultimately be lost. That's when we look to satellites.

My team is focused on making instruments that fit on small spacecraft such as Galassia. These smaller satellites are commercially attractive, and could enable a constellation of spacecraft to enhance service quality. This is a community effort. We are working with the University of New South Wales-Canberra to investigate inter-satellite QKD and are engaging with university and industry teams around the world to improve the technology. By working together, we will be able to ensure continued communications privacy even when the technology landscape changes rapidly.

stopinion@sph.com.sg

• Alexander Ling is a principal investigator at the Centre for Quantum Technologies, associate professor at the National University of Singapore, and also a theme leader at the NUS-Singtel Cyber Security Research & Development Laboratory.