Source: *The Straits Times,* pB1
Date: 18 February 2022

S'pore a step closer to unhackable Internet

15 organisations involved in initiative to test quantum security software and hardware

Dominic Low

Singapore is a step closer to building an unhackable Internet for safeguarding citizens and customers' data with the setting up of the nation's first test bed for quantum cryptography.

Quantum cryptography uses the quantum properties of light particles to create an unbreakable cryptographic algorithm to secure satellite or fibre broadband communications.

Yesterday the National Research Foundation (NRF) announced the creation of the test-bed initiative, dubbed the National Quantum-Safe Network.

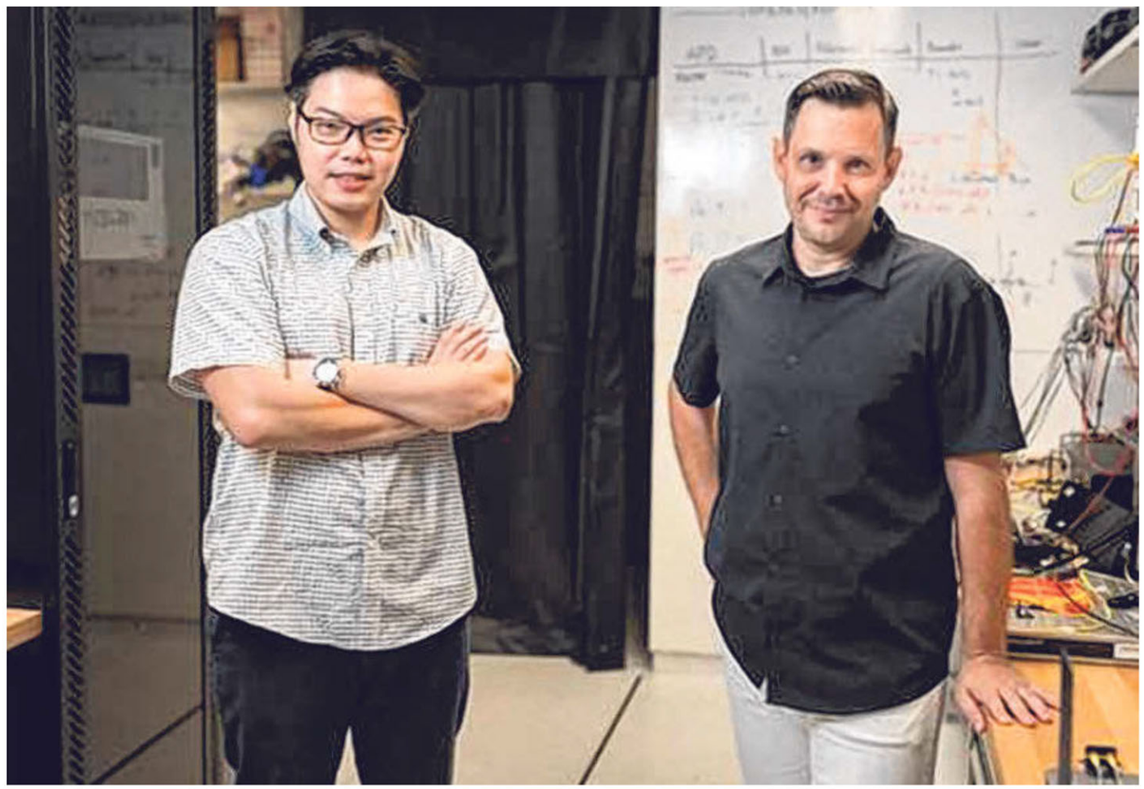
The aim of the initiative is to test quantum security software and hardware that are already commercially available today. These tests simulate day-to-day operations in the hope of deploying them one day to securely process sensitive functions, including the operation of energy grids and e-banking transactions. Target users include those in the medical, finance and military sectors.

"Today's encryption methods are unlikely to withstand future attacks based on quantum computing technology," said Assistant Professor Charles Lim, who is the lead principal investigator for the project.

The network will be financed by NRF's Quantum Engineering Programme, with a funding of $8.5 million over three years. The test bed is expected to be up and running by the end of this year.

Quantum computers rely on theoretical particle physics and run on subatomic particles such as electrons in sub-zero temperatures.

Unlike conventional computers – which store information in a binary "0" or "1" format called bits – quantum computers use "qubits" that can represent both a "0" and a "1" simultaneously. This is said to allow them to process information significantly faster than ordinary computers, and therefore crack encrypted data more easily.



NUS Assistant Professor Charles Lim, lead principal investigator for the project, with Mr Michael Kasper, department director for cyber and information security at Fraunhofer Singapore, which is part of the initiative, dubbed the National Quantum-Safe Network. PHOTO: CENTRE FOR QUANTUM TECHNOLOGIES, NATIONAL UNIVERSITY OF SINGAPORE

For example, Japan's first prototype quantum computer, unveiled in 2017, could make complex calculations 100 times faster than a conventional supercomputer.

In 2019, Google created a quantum computer that could perform in 200 seconds a computation that would take the world's fastest supercomputers about 10,000 years.

Prof Lim, who works at the Centre for Quantum Technologies at the National University of Singapore (NUS), said quantum cryptography requires the use of specialised hardware such as quantum key distribution systems.

Quantum key distribution is a process where secret keys are exchanged between intended users of encrypted data. Such keys are used to unlock the algorithm securing the data, so that it can be read.

If unauthorised parties intercept the data stream, the intended users will be notified to delete the stolen key, rendering the data unreadable to the hacker.

These systems can be deployed over existing fibre-optic networks, which already blanket homes and offices in Singapore providing fibre broadband connections.

Quantum key distribution systems can also be deployed over satellite systems, but the project will focus on fibre broadband connections for now.

So far, 15 organisations – including NUS, Amazon Web Services, the Cyber Security Agency of Singapore and the Infocomm Media Development Authority – are involved in the National Quantum-Safe Network.

The setting up of secure links to locations that cannot be connected to fibre or may even be moving, such as boats, will also be explored under the initiative. A new quantum security lab will also be set up to conduct research on quantum security vulnerabilities and designs, as well as host workshops for potential end-users to better understand quantum technologies.

domlow@sph.com.sg