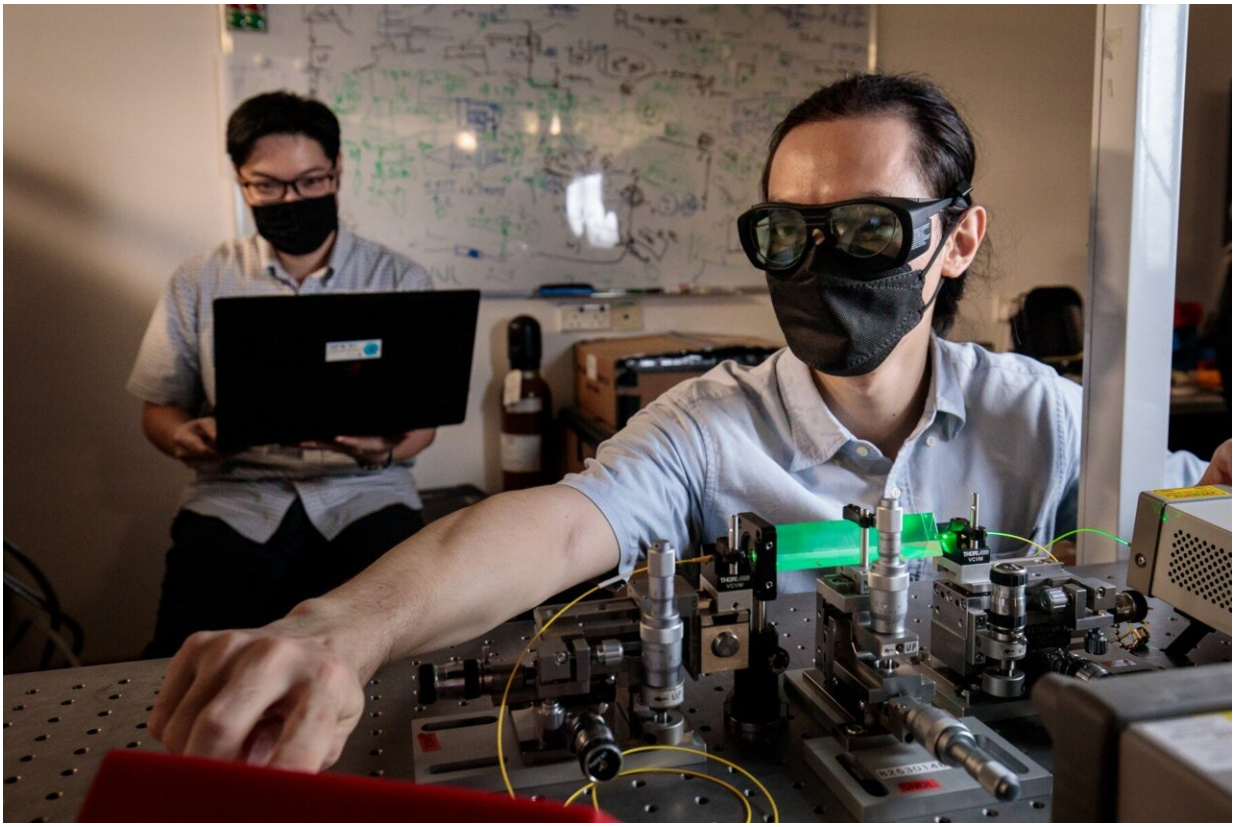
Researchers bring attack-proof quantum communication two steps forward

July 8 2021



Assistant Professor Charles Lim (back) and Dr Zhang Gong (front) with their team's first-of-its-kind quantum power limiter device. Credit: National University of Singapore

Quantum key distribution (QKD) is a method for secure communication

that uses quantum mechanics to encrypt information. While the security of QKD is unbreakable in principle, if it is incorrectly implemented, vital information could still be stolen by attackers. These are known as side-channel attacks, where the attackers exploit weaknesses in the setup of the information system to eavesdrop on the exchange of secret keys.

Researchers from the National University of Singapore (NUS) have developed two methods, one theoretical and one experimental, to ensure that QKD communications cannot be attacked in this way. The first is an ultra-secure cryptography protocol that can be deployed in any communication network that needs long-term security. The second is a first-of-its-kind device that defends QKD systems against bright light pulse attacks by creating a power threshold.

"Rapid advances in quantum computing and algorithmic research mean we can no longer take today's toughest security software for granted. Our two new approaches hold promise to ensuring that the information systems which we use for banking, health and other critical infrastructure and data storage can hold up any potential future attacks," said Assistant Professor Charles Lim, from the NUS Department of Electrical and Computer Engineering and Centre for Quantum Technologies, who led the two research projects.

Future-proof quantum communication protocol

Typically, in QKD, two measurement settings are used—one to generate the key and the other to test the integrity of the channel. In a paper published in the journal *Nature Communications* on 17 May 2021, the NUS team showed that with their new protocol, users can independently test the other party's encryption device by generating a secret key from two randomly chosen key generation settings instead of one. The researchers demonstrated that introducing an extra set of key-generating measurements for the users makes it harder for the eavesdropper to steal

information.

"It's a simple variation of the original protocol that started this field, but it can only be tackled now thanks to significant developments in mathematical tools," said Professor Valerio Scarani, who was one of the inventors of this type of method and is a co-author of the paper. He is from the NUS Department of Physics and Centre for Quantum Technologies.

Compared to the original 'device-independent' QKD protocol, the new protocol is easier to set up, and is more tolerant to noise and loss. It also gives users the highest level of security allowable by quantum communications and empowers them to independently verify their own key generation devices.

With the team's setup, all information systems built with 'device-independent' QKD would be free from misconfiguration and mis-implementation. "Our method allows data to be safe against attackers even if they have unlimited quantum computing power. This approach could lead to a truly secure information system, eliminating all side-channel attacks and allowing end-users to monitor its implementation security easily and with confidence," explained Asst Prof Lim.

A first-of-its-kind quantum power limiter device

Quantum cryptography, in practice, uses optical pulses with very low light intensity to exchange data over untrusted networks. Leveraging quantum effects can securely distribute secret keys, generate truly random numbers, and even create banknotes that are mathematically unforgeable.

However, experiments have shown that it is possible to inject bright light pulses into the quantum cryptosystem to break its security. This side-

channel attack strategy exploits the way injected bright light is reflected to the outside environment, to reveal the secrets being kept in the quantum cryptosystem.

In a new paper published in *PRX Quantum* on 7 July 2021, the NUS researchers reported their development of the first optical device to address the issue. It is based on thermo-optical defocusing effects to limit the energy of the incoming light. The researchers use the fact that the energy of the bright light changes the refractive index of the transparent plastic material embedded in the device, thus it sends a fraction of the light out of the quantum channel. This enforces a power limiting threshold.

The NUS team's power limiter can be seen as an optical equivalent of an electric fuse, except that it is reversible and does not burn when the energy threshold is breached. It is highly cost-effective, and can be easily manufactured with off-the-shelf components. It also does not require any power, so it can be easily added to any quantum cryptography system to strengthen its implementation security.

Asst Prof Lim added, "It is imperative to close the gap between the theory and practice of quantum secure communications if we are to use it for the future Quantum Internet. We do this holistically—on one hand, we design more practical quantum protocols, and on the other hand, we engineer quantum devices that conform closely with the mathematical models assumed by the protocols. In doing so, we can significantly narrow the gap."

More information: René Schwonnek et al, Device-independent quantum key distribution with random key basis, *Nature Communications* (2021). DOI: 10.1038/s41467-021-23147-3

Provided by National University of Singapore