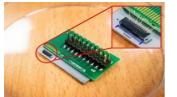# Tiny Quantum Chip For Enhanced Security In Data Communication

November 4, 2019

Quantum technology to provide a much better communication security and create the next-generation of secure digital communication devices

In a breakthrough achievement in chip designing, researchers at the Nanyang Technological University, Singapore have developed an extremely small quantum chip that offers excellent quantum communication as compared to the current quantum chips.

The present security standards are not equipped with enough security measures for communication to prevent the theft of information from online transactions and digital communication.

How it works

However, despite small size (approximately 3mm), the tiny chip's quantum communication algorithms is capable of providing a much enhanced security. While sending information, a password is integrated within that information to form what is called as 'quantum key'. As soon as the information is received, the password along with the quantum key is destroyed, thus making the entire communication extremely secure.

All Internet-based email and messaging platforms make use of passwords, whether in the form text, numbers or biometric data. While these act as a good security measure, a security risk is however always present. In contrast, quantum communication effectively eliminates this risk by integrating security password right into the encrypted information. Is each password is different, any risk of information being intercepted is nullified.

Compact and low cost

Other benefits of the chip includes compact space and low cost. At 1,000 times less space required than current quantum communication chips, this quantum chip that can be easily placed in devices such as smartphones, tablets and smart watches. It uses standard industry material such as silicon for easy and widescale manufacture, which in turn is beneficial for bringing down costs.

Liu Ai Qun, professor at School of Electrical and Electronic Engineering, NTU, said, "In today's world, cyber security is very important as so much of our data are stored and communicated digitally. Almost all digital platforms and repositories require users to input their passwords and biometric data, and as long as this is the case, it could be eavesdropped on or deciphered. Quantum technology eliminates this as both the password and information are integrated within the message being sent, forming a 'quantum key'."

Kwek Leong Chuan, associate professor at School of Electrical and Electronic Engineering, NTU states that random encryption used by quantum communication can only be accessed by the intended recipient with the correct 'key'. There is no need for additional passwords or biometric data.

He said, "It is like sending a secured letter. Imagine that the person who wrote the letter locked the message in an envelope with its 'key' also inside it. The recipient needs the same 'key' to open

it. Quantum technology ensures that the key distribution is secure, preventing any tampering to the 'key'."