
NTU Singapore researchers create quantum chip 1,000 times smaller than current setups

October 30, 2019

Researchers at Nanyang Technological University, Singapore (NTU Singapore) have developed a quantum communication chip that is 1,000 times smaller than current quantum setups, but offers the same superior security quantum technology is known for.

Most leading security standards used in secure communication methods - from withdrawing cash from the ATM to purchasing goods online on the smartphone - does not leverage quantum technology. The electronic transmission of the personal identification number (PIN) or password can be intercepted, posing a security risk.

Roughly 3mm in size, the tiny chip developed by NTU scientists uses quantum communication algorithms to provide enhanced security compared to existing standards. It does this by integrating passwords within the information that is being delivered, forming a secure 'quantum key'. After the information is received, it is destroyed along with the key, making it an extremely secure form of communication.

It also needs 1,000 times less space than current quantum communication setups that can be as big as a refrigerator or even take up the space of an entire room or office floor. This opens doors for more secure communication technologies that can be deployed in compact devices such as smartphones, tablets and smart watches. It also lays the foundation for better encryption methods for online transactions and electronic communication.

Led by NTU Professor Liu Ai Qun, and Associate Professor Kwek Leong Chuan, the team's findings were published in a leading peer-reviewed journal, *Nature Photonics*.

Prof Liu, who is from NTU's School of Electrical and Electronic Engineering, 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'."

Assoc Prof Kwek explains that quantum communication works by using randomised strings of code to encrypt the information, which can only be opened by the intended recipient with the correct 'key'. There is no need for additional passwords or biometric data to be transmitted, which is the standard practice in current forms of communication.

"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'", said Assoc Prof Kwek, a physicist at NTU's National Institute of Education.

Military-grade communication tech, made cost-effective

The world's biggest tech companies such as Google and IBM are racing to develop quantum supercomputers that would revolutionise computing at speeds now inconceivable.

One highly anticipated strength of quantum technology lies in cryptography, the art of secret communication.

With the proliferation of Internet services, emails and messaging platforms such as WhatsApp, Facebook, Skype, Snapchat, Telegram etc., have created their own secured channels for communication - what is known as "classical channels".

In contrast, "quantum channels" that carry information have security protocols that are integrated into the encrypted data. Each channel is uniquely different from each other, reducing or even eliminating the risk of information being intercepted or leaked during transmission.

Simply put, quantum technology does not require additional transmissions of passwords or biometric data that is necessary in "classical channels". This eliminates the risk of interception or information being leaked, creating an almost unbreakable encryption.

The quantum communication chip developed by the NTU researchers will be cost effective as it uses standard industry materials such as silicon, which also makes it easy to manufacture.

Prof Liu said, "This is the future of communication security and our research brings us closer to quantum computing and communication. It will help spark the creation of next-generation communication devices, as well as enhance digital services such as online financial portals of banks, and digital government services."

The NTU team is now looking to develop a hybrid network of traditional optical communication systems and quantum communication systems. This will improve the compatibility of quantum technologies that can be used in a wider range of applications such as internet connectivity.