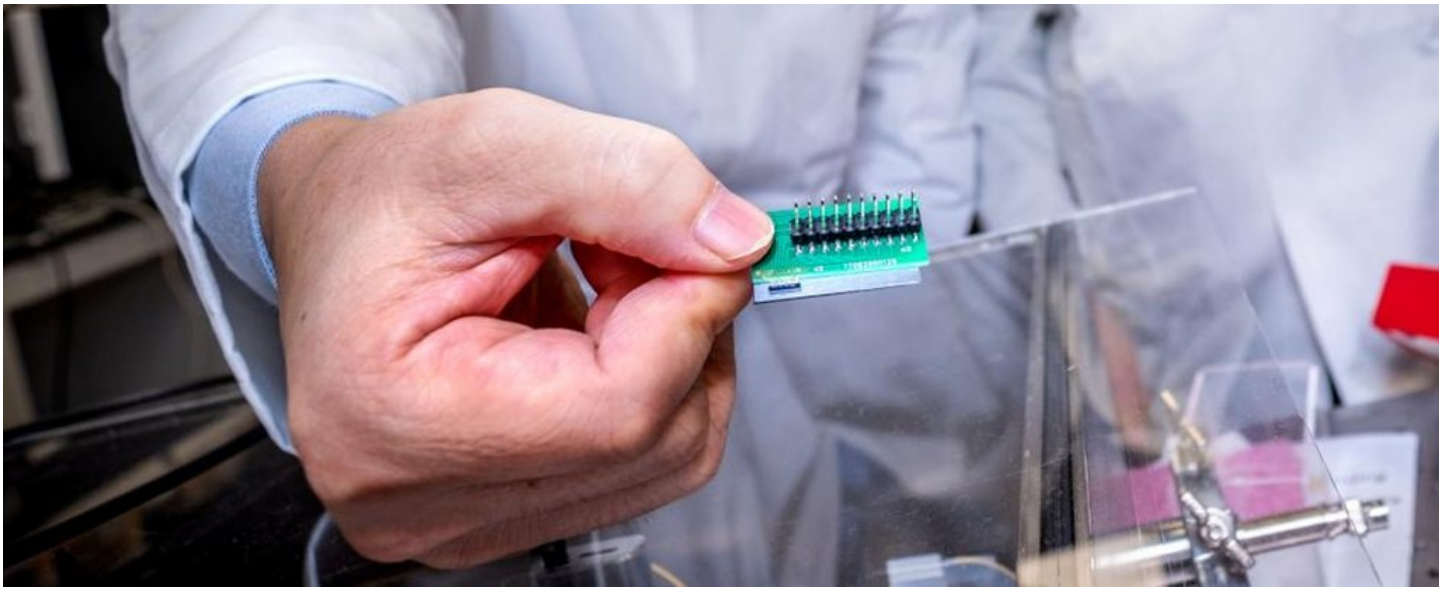


PHYSICS

Scientists Have Made a Quantum Encryptor 1,000 Times Smaller Than What Came Before

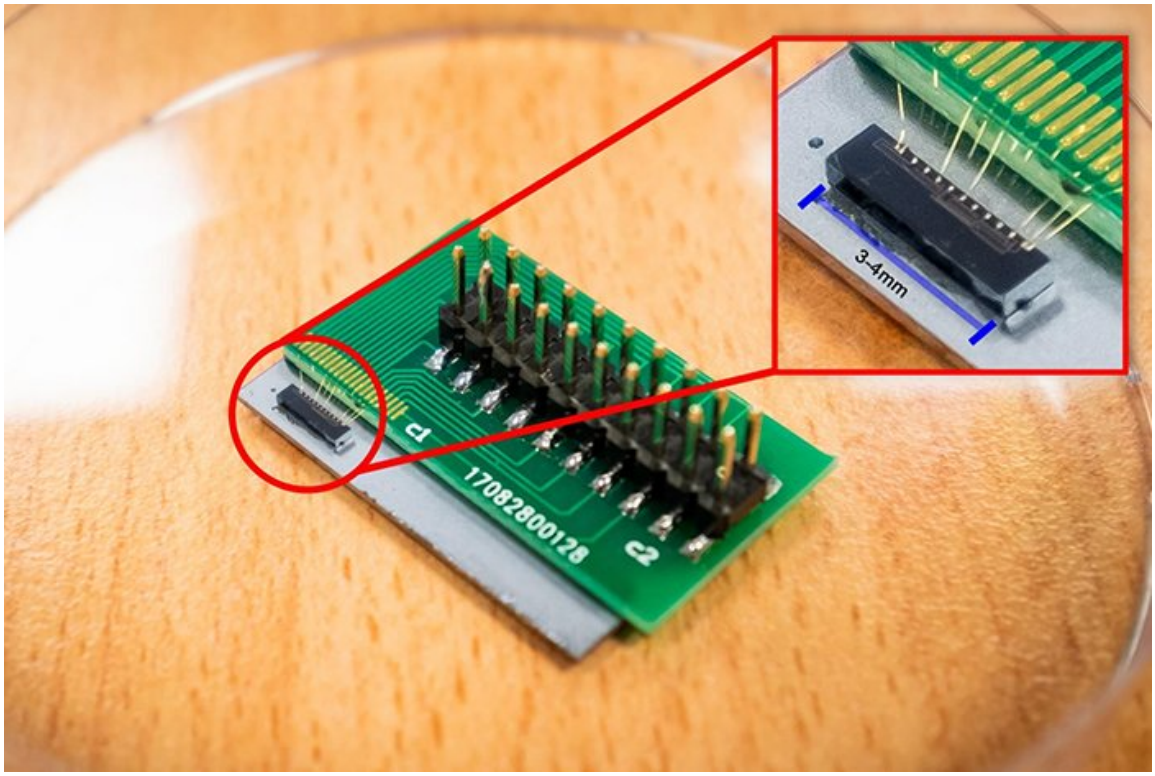
DAVID NIELD 3 NOV 2019

One of the ways in which quantum technology promises to revolutionise computing is through quantum key distribution (QKD) – a quantum device that lets people securely encrypt and decrypt communications.

Now, scientists have been able to seriously shrink down the amount of space needed to create one.

Researchers have developed a QKD chip just 3 millimetres (0.12 inches) in size – an impressive feat considering similar quantum computing setups can be as large as a fridge or even take up an entire office floor.

That opens up all kinds of new possibilities for this type of quantum tech. A chip just 3 mm in size can be built into a smartwatch or fitness tracker, for example, but going around with a fridge strapped to your wrist is less practical.



(NTU Singapore)

So why is QKD so important? Right now, when we encrypt data we generally use passwords or biometric data, which can be hacked or leaked.

Quantum technology, however, allows us to encrypt the key within the message. Only the person with the exact same key as the one inside the message can open it.

"It is like sending a secured letter," says physicist Kwek Leong Chuan, from Nanyang Technological University (NTU) in Singapore. "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."

It's hoped that further down the line this highly secure form of communication could be used everywhere from cash machines to online shopping sites. It's dangerous to brand any technology as "unhackable", but QKD gets close.

The technology takes the classic Schrödinger's cat paradox often associated with quantum mechanics, and applies it to messaging—as soon as the cat is observed we know whether it's alive or dead, in

the traditional puzzle. In QKD, as soon as the message is observed by someone without the key, it becomes unreadable.

"In today's world, cyber security is very important as so much of our data is stored and communicated digitally," says physicist Liu Ai Qun from NTU.

"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."

We're still waiting for quantum computing in its full form to become a reality, but QKD systems have been around for several years. The challenge for scientists is to make the technology smaller and more practical – which is where this new chip comes in.

The new solution developed by the scientists at NTU should be relatively easy and cheap to produce, as it uses standard industry materials like silicon, that are already widely used in computer manufacturing.

For now though, this is still just a "proof-of-principle" chip – it shows what can be done, but it's not ready for widespread production or use just yet.

That should come, in time. To begin with, like a lot of similar innovations, we might see this quantum computing tech used alongside systems based on classical computing, while it gets established and refined.

Despite the huge technological challenge of developing quantum computing systems, scientists continue to edge closer to making true quantum computing a reality. When it does arrive, it should mean our data is a lot more secure.

"This is the future of communication security and our research brings us closer to quantum computing and communication," says Liu.

"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 research has been published in *Nature Photonics*.