

How quantum mechanics is working to protect security online

Press release issued: 6 March 2017

Scrambled and indecipherable messages are the back bone of the internet as we know it.

Complex cryptography protects our bank accounts and identities from fraud, allowing us to safely buy and sell online without ever leaving the comfort of our living rooms.

But the potential introduction of ultra-powerful quantum computers renders our personal information vulnerable to direct attack.

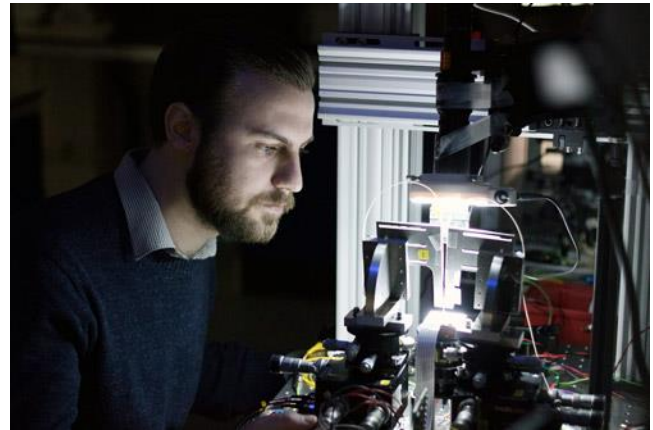
Now researchers at the University of Bristol's [Quantum Engineering Technology Labs \(QETLabs\)](#) have developed tiny microchip circuits which exploit the strange world of quantum mechanics and provide a level of security enhanced by the laws of quantum physics.

These devices distribute cryptographic keys using the quantum properties of entanglement, superposition and the absolute randomness provided by quantum behaviour, which is reproducible by no other means.

Principal investigator [Professor Mark Thompson](#) said: "The system we have developed allows information to be exchanged using single photons of light in a quantum state.

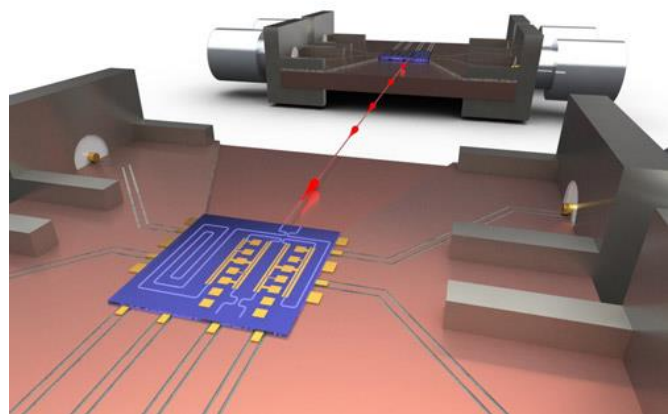
"If an eavesdropper hacks your transmission, they will collapse the fragile quantum states and the system will immediately alert you to their presence and terminate the transmission."

This work, published in the February issue of [Nature Communications](#), has demonstrated the world's first chip-to-chip



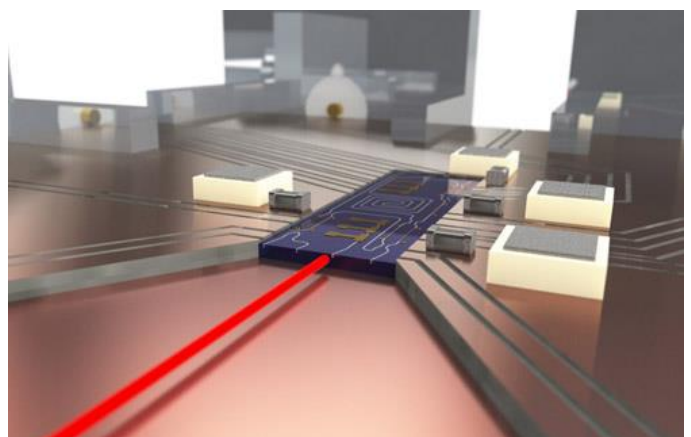
Lead author, Phil Sibson in the lab

Image Credit: University of Bristol



Silicon render - Quantum Key Distribution between silicon chips

Image Credit: University of Bristol



Chip based render - Indium Phosphide QKD transmitter

Image Credit: University of Bristol

quantum secured communication system, using microchip circuits just a few millimetres in size.

This international collaboration, including researchers from Bristol, Glasgow and NiCT in Japan, used commercial semiconductor chip manufacturers to make their devices - in much the same way as Intel pattern silicon to make the latest central processing units (CPUs).

However, instead of using electricity these miniaturised devices used light to encode information at the single photon level, providing encryption keys with an unlimited lifetime.

Lead author [Philip Sibson](#), added: "Our research opens the way to many applications that have, until now, been infeasible.

"The technology is miniaturised for handheld devices, has enhanced functionality for telecommunications networks, and employs cost-effective manufacturing to feasibly deploy quantum key distribution technology in the home."

The Bristol team has continued developing this technology, demonstrating an innovative design that allows the same functionality in a complementary metal-oxide-semiconductor (CMOS) compatible process, appearing in the February issue of [Optica](#).

While the first devices used a more expensive and complex manufacturing approach, these next generation devices are fabricated in standard silicon, paving the way for direct integration with microelectronic circuits.

This will ultimately lead to integration in every day electrical devices, such as laptops and mobile phones.

[Dr Chris Erven](#) explained: "As part of the [UK Quantum Communications](#) Hub, we are in the process of deploying these devices throughout the heart of the Bristol City fibre-optic network, allowing us to test out these ultra-secure communications systems in real-world scenarios."

This work has been supported by the [UK Quantum Communication Hub](#), part of the [National Network of Quantum Technology hubs](#), demonstrating the next generation of quantum technologies.

Through the University of Bristol [Quantum Technology Enterprise Centre](#) (QTEC), the commercial potential of this technology is being explored by [KETS Quantum Security Ltd](#).

Further information

Video:

<https://youtu.be/EV6xXvF5i2Q>

Papers:

[‘Chip-based Quantum Key Distribution’](#) by P. Sibson *et al.* in Nature Communications

[‘Integrated silicon photonics for high-speed quantum key distribution’](#) by P. Sibson *et al.* in
Optica