Game changing invention to revolutionise cybersecurity

July 2 2018

Random numbers underlie cryptocurrencies like Bitcoin. Credit: Lancaster University

Cyberattacks may become impossible with the creation of the first practical quantum random number generator.

Patented by Quantum Base and Lancaster University, it will provide 100% provable quantum security for authentication and communication when integrated in microelectronic products.

Chosen for inclusion in the prestigious Royal Society Summer Exhibition 2018, this device overcomes the weaknesses of current QRNGS which are typically slow, expensive or large.

The Quantum Base QRNG can be embedded within any electronic device without increasing cost or complexity and with a very high maximum speed.

Phillip Speed, CEO of Quantum Base said: "We have created a small, low power device that produces pure random numbers. It can be incorporated into any electronic product with little or no incremental cost once volume production is achieved."

With the number of smart devices expected to reach up to 50bn by 2020, security is of vital importance.

Globally, the bill for cybercrime will reach $6 trillion by 2021 while the bill for ransomware attacks – like the Wannacry attack on the NHS in 2017- could reach $11.5bn by 2019.

Hackers have been able to exploit weaknesses in the generation method of the 'pseudo' random numbers that are commonly used to underpin digital network device security.

One ingenious attempt even involved hackers trying to steal data from a casino using an internet connected fishtank.

A Vital Defence: the role of "True" Random Numbers

Random numbers underpin the algorithms which lie behind every electronic communication. Many current applications rely on what is

termed 'pseudo' random number generators, but information security requires 'true' random numbers for everything from online shopping and banking to vehicle electronics, gaming and smart household appliances.

By harnessing the innate randomness of quantum mechanics, the team has developed an ell-electronic nanoscale, simple quantum true random number generator that can be embedded within a semiconductor chip like those found in billions of our everyday smartphones, laptops and home IoT smart devices such as Alexa.

Professor Rob Young, Director of Lancaster University's Quantum Technology Centre, said: "Flaws in the way current electronic devices produce random numbers weakens their security and makes them less efficient. Our solution fixes this, but it's also incredibly small and efficient, which is very important."

With the lowest power requirements and high scalability due to the simple semiconductor structure – a resonant tunnelling diode (RTD) - it is hoped that this innovation will play a pivotal role in protecting both consumers and businesses across the globe in their digital futures.

More information: Ramón Bernardo-Gavito et al. Extracting random numbers from quantum tunnelling through a single diode, *Scientific Reports* (2017). DOI: 10.1038/s41598-017-18161-9

Provided by Lancaster University