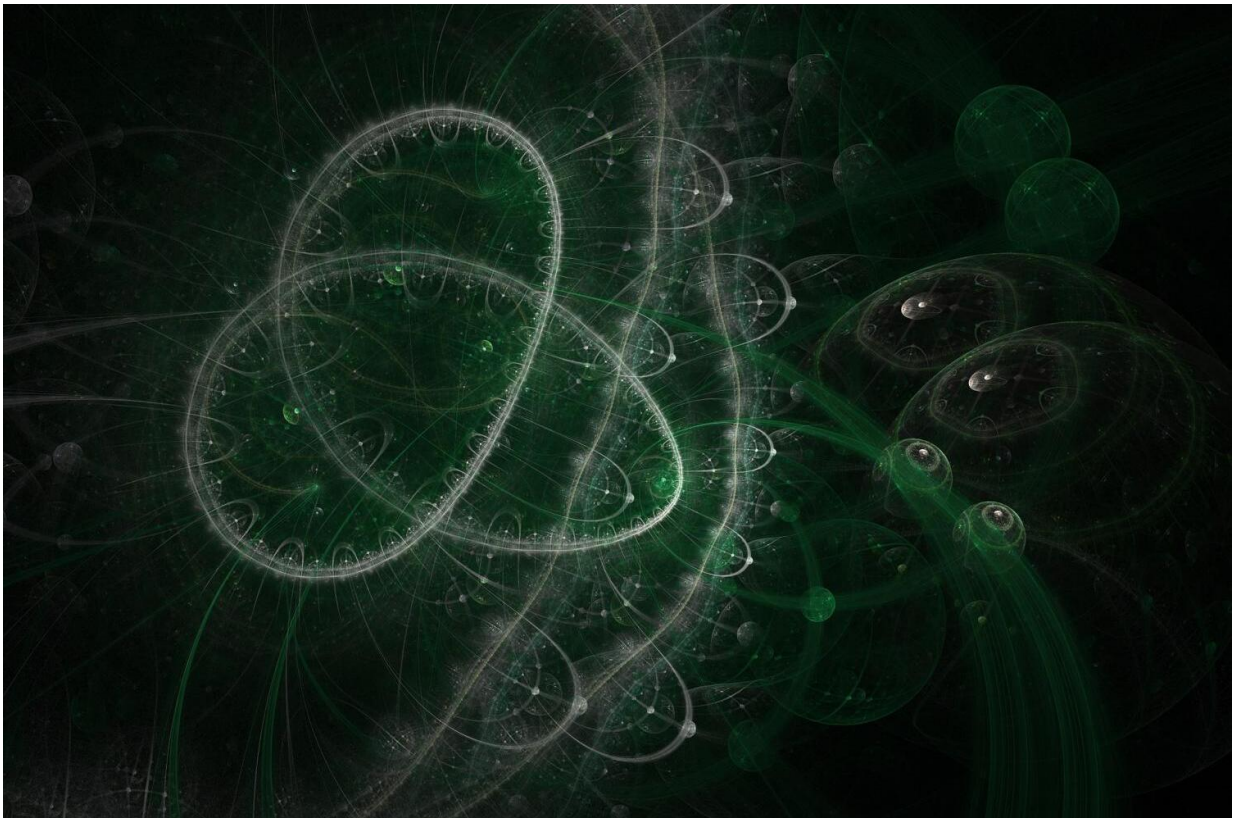
Developing a secure, un-hackable net

January 11 2018



Credit: CC0 Public Domain

A method of securely communicating between multiple quantum devices has been developed by a UCL-led team of scientists, bringing forward the reality of a large-scale, un- hackable quantum network.

To date, communicating via quantum networks has only been possible

between two devices of known provenance that have been built securely.

With the EU and UK committing €1 billion and £270 million respectively into funding quantum technology research, a race is on to develop the first truly secure, large-scale network between cities that works for any quantum device.

"We're in a technology arms race of sorts. When quantum computers are fully developed, they will break much of today's encryption whose security is only based on mathematical assumptions. To pre-emptively solve this, we are working on new ways of communicating through large networks that don't rely on assumptions, but instead use the quantum laws of physics to ensure security, which would need to be broken to hack the encryption," explained lead author, Dr Ciarán Lee (UCL Physics & Astronomy).

Published in *Physical Review Letters* and funded by the Engineering and Physical Sciences Research Council, the study by UCL, the University of Oxford and the University of Edinburgh scientists details a new way of communicating securely between three or more quantum devices, irrespective of who built them.

"Our approach works for a general network where you don't need to trust the manufacturer of the device or network for secrecy to be guaranteed. Our method works by using the network's structure to limit what an eavesdropper can learn," said Dr Matty Hoban (University of Oxford, previously University of Edinburgh).

The approach bridges the gap between the theoretical promise of perfect security guaranteed by the laws of quantum physics and the practical implementation of such security in large networks.

It tests the security of the quantum devices prior to engaging in

communications with the whole network. It does this by checking if the correlations between devices in the network are intrinsically quantum and cannot have been created by another means.

These correlations are used to establish secret keys which can be used to encrypt any desired communication. Security is ensured by the unique property that quantum correlations can only be shared between the devices that created them, ensuring no hacker can ever come to learn the key.

The team used two methods - machine learning and causal inference - to develop the test for the un-hackable communications system. This approach distributes secret keys in a way that cannot be effectively intercepted, because through quantum mechanics their secrecy can be tested and guaranteed.

"Our work can be thought of as creating the software that will run on hardware currently being built to realise the potential of quantum communications. In future work, we'd like to work with partners in the UK national quantum technologies programme to develop this further. We hope to trial our quantum network approach over the next few years," concluded Dr Lee.

The team acknowledge that an un-hackable network could be abused in the same way that current networks are, but highlight that there is also a clear benefit to ensuring privacy too.

More information: Ciarán M. Lee et al, Towards Device-Independent Information Processing on General Quantum Networks, *Physical Review Letters* (2018). DOI: 10.1103/PhysRevLett.120.020504

Provided by University College London