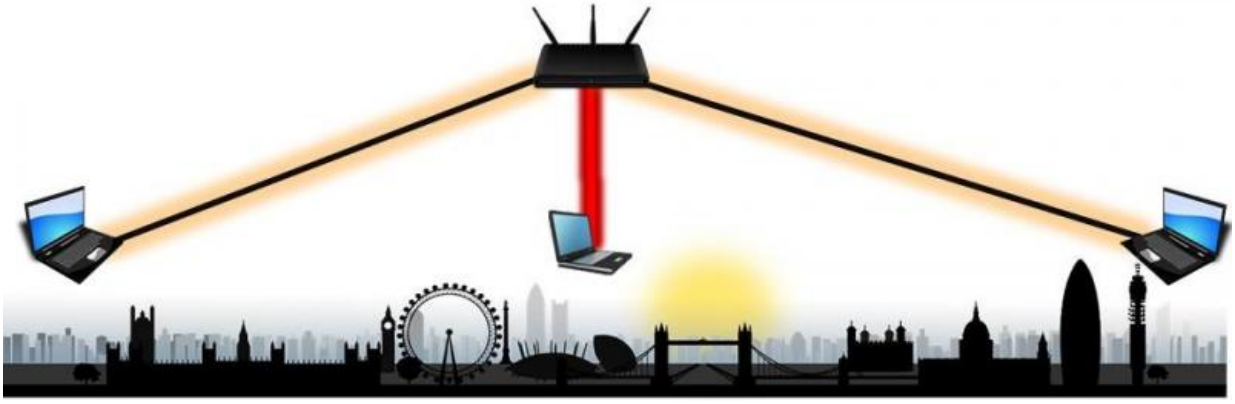
Team finds the 'key' to quantum network solution

May 25 2015



Credit: University of York

Scientists at the University of York's Centre for Quantum Technology have made an important step in establishing scalable and secure high rate quantum networks.

Working with colleagues at the Technical University of Denmark (DTU), Massachusetts Institute of Technology (MIT), and the University of Toronto, they have developed a protocol to achieve key-rates at metropolitan distances at three orders-of-magnitude higher than previously.

Standard protocols of Quantum Key Distribution (QKD) exploit random sequences of quantum bits (qubits) to distribute secret keys in a completely secure fashion. Once these keys are shared by two remote parties, they can communicate confidentially by encrypting and decrypting binary messages. The security of the scheme relies on one of the most fundamental laws of quantum physics, the uncertainty principle.

Today's classical communications by email or phone are vulnerable to eavesdroppers but quantum communications based on single particle levels (photons) can easily detect eavesdroppers because they invariably disrupt or perturb a quantum signal. By making quantum measurements, two remote parties can estimate how much information an eavesdropper is stealing from the channel and can apply suitable protocols of privacy amplification to negate the effects of the information loss.

However, the problem with QKD protocols based on simple quantum systems, such as single-photon qubits, is their low key-rate, despite their effectiveness in working over long distances. This makes them unsuitable for adaptation for use in metropolitan networks.

The team, led by Dr Stefano Pirandola, of the Department of Computer Science at York, overcame this problem, both theoretically and experimentally, using continuous-variable quantum systems. These allow the parallel transmission of many qubits of information while retaining the quantum capability of detecting and defeating eavesdroppers. The research is published in *Nature Photonics*.

Dr Pirandola said: "You want a high rate and a fast connection particularly for systems that serve a metropolitan area. You have to transmit a lot of information in the fastest possible way; essentially you need a quantum equivalent of broadband.

"Continuous-variable systems can use many more photons but are still quantum based. Our system reaches extremely high speeds by three orders of magnitude higher than ever before over a distance of 25 kilometres. Its effectiveness above that distance decreases rapidly however.

"Nevertheless, our protocol could be used to build high-rate quantum networks where devices securely connect to nearby access points or proxy servers."

More information: High-rate measurement-device-independent quantum cryptography, *Nature Photonics*, DOI: 10.1038/nphoton.2015.83

Provided by University of York