Researchers confirm ‘realistic’ answer to quantum network puzzle

Posted on 19 November 2015

Scientists at the University of York’s Centre for Quantum Technology have discovered new evidence to support the development of scalable and secure high rate quantum networks.

Earlier research with colleagues at the Technical University of Denmark (DTU), Massachusetts Institute of Technology (MIT), and the University of Toronto, saw the development of a protocol that used continuous-variable quantum systems to achieve key-rates at metropolitan distances at three orders-of-magnitude higher than previously.

In a new study published in *Nature Photonics*, the researchers, led by Dr Stefano Pirandola, of the Department of Computer Science at York, say that a potential alternative using cryogenic devices and standard Quantum Key Distribution (QKD) is unlikely to approach the high rates achieved both theoretically and experimentally using a continuous variable quantum system.

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 option of using continuous-variable quantum systems allows the parallel transmission of many qubits of information while retaining the quantum capability of detecting and defeating eavesdroppers.

Dr Pirandola said: “We have compared the state of the art in continuous variable systems (optical modes) with the standard discrete variable systems (qubits). If you want to build a metropolitan network based on quantum cryptography you need a high-rate super-fast connection otherwise you can’t compete with the classical communication infrastructure. Continuous variable systems offer the best and cheapest technology for reaching high rates over metropolitan distances and they can work at room temperature.

“On the other hand, the cryogenic devices needed to improve the bit rate on a system using standard qubit-based QKD would require a built-in facility that operated at temperatures close to zero kelvin (minus 273 degrees Celsius). This would be unrealistic from a cost perspective and would still not approach the rate of continuous-variable systems.”

Dr Pirandola was funded by the Engineering and Physical Sciences Research Council (EPSRC).

The University of York leads a unique collaboration to exploit fundamental laws of quantum physics for the development of secure communication technologies and services for consumer, commercial and government markets.

The Quantum Communications Hub is one of the EPSRC's new £155m National Network of Quantum Technology Hubs.

Further information:

• The paper 'MDI-QKD: Continuous- versus discrete-variables at metropolitan distances' by Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L Braunstein, Seth Lloyd, Tobias Gehring, Christian S Jacobsen and Ulrik L Andersen is available on the public arXiv (http://arxiv.org/abs/1506.06748) and published as a Correspondence to Nature Photonics.

• For more information about the Department of Computer Science at the University of York, please visit http://www.cs.york.ac.uk/