Establishing the boundaries of quantum secure communications

April 26 2017, by Alistair Keely

Credit: quantumcommshub.net

Scientists at the University of York's Centre for Quantum Technology have made an important breakthrough in the theory of quantum secure communications.

Today's classical communications, such as email or phone, are

potentially vulnerable to eavesdroppers as conventional data encryption is based on the factorisation of large integers, an operation which is computationally hard on a classical computer but easily solvable on a quantum computer.

Recently, Google said that large quantum computers are only five years from commercial exploitability, therefore setting a deadline to current classical methods for private communication. Scientists say the solution comes from the field of quantum key distribution (QKD).

QKD uses particles, such as photons, to enable two remote parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt confidential messages. The security is not computational but based on a fundamental law of nature, the uncertainty principle.

Maximum rates

Based on this idea, secure quantum networks are being built on a large scale in the UK and other countries, with China playing an important role and also leading the exploration of quantum satellite communication.

In such a scenario it is crucial to understand the ultimate limits of QKD, in terms of maximum rates, or capacities, at which two parties can distribute secret keys in a point-to-point connection.

In a paper published in *Nature Communications*, scientists have established these capacities through the most important communication lines, including optical fibres.

Protocols

Professor Stefano Pirandola of the University's Department of Computer Science said: "This is a breakthrough result because it establishes the ultimate performance that any point-to-point protocol of QKD cannot surpass.

"Setting these limits is extremely important for both theoreticians and experimentalists, because they provide benchmarking for new theoretical protocols and actual experimental implementations."

The study was funded by the EPSRC via the UK quantum communication hub.

More information: Stefano Pirandola et al. Fundamental limits of repeaterless quantum communications, *Nature Communications* (2017). DOI: 10.1038/ncomms15043

Provided by University of York