Establishing the ultimate limits of quantum communication networks

Posted on 31 May 2019

Scientists say they have established the ultimate limits of quantum communication networks.

At the moment, sensitive data is typically encrypted and then sent across fibre-optic cables and other channels together with the digital “keys” needed to decode the information. However, the data can be vulnerable to hackers.

Quantum communication takes advantage of the laws of quantum physics to protect data. These laws allow particles—typically photons of light —to transmit the data using quantum bits, or qubits.

Superior capabilities

Multinational corporations, such as IBM and Google, are now building intermediate-size quantum computers with increasing number of quantum units or qubits.

Once they scaled up to larger sizes, these devices will have far-superior capabilities than current classical computers. For instance, they may process extremely large numbers in just a few seconds, speed-up many fundamental mathematical operations, and perfectly simulate molecular and biological processes.

One challenge will be to connect quantum computers together, in order to create a quantum-version of the Internet or "quantum Internet".

However, an important but unanswered question remains: what is the ultimate rate at which one can transmit secret messages or quantum systems from one remote quantum computer to another?

Notoriously difficult

Writing in the journal *Communications Physics*, Professor Stefano Pirandola, from the University of York's Department of Computer Science, said scientists have answered the question.

Prof Pirandola studied the optimal working mechanism of a future quantum Internet, and also provided the ultimate secret-key capacities that can potentially be achieved.

He said: "Studying quantum networks is notoriously difficult, but recent mathematical tools developed in quantum information theory have allowed us to completely simplify the analysis.

Qubits

"An outstanding question was to compute the maximum number of elementary quantum systems (known as qubits) that could be reliably transmitted from one user of the network to another, or similarly, the maximum number of completely secret bits that these remote users could share.

"This number has now a precise analytical formula."

Furthermore, the study reveals that the classical-inspired strategy of simultaneously sending qubits through multiple routes of the network can remarkably boost the rate, i.e., the speed of the quantum communication between any two remote users.

Further information:

The study sponsors are:

- EPSRC Quantum Communications hub: https://www.quantumcommshub.net/
- EU project: "Continuous Variable Quantum Communications" CiViQ: http://civiquantum.eu/