# Physicists add amplifier to quantum communication toolbox

June 1 2017

Quantum encryption using single photons is a promising technique for boosting the security of communication systems and data networks, but there are challenges in applying the method over large distances due to transmission losses. Using conventional optical amplification doesn't help as this disrupts the quantum link between sender and receiver, but physicists in Europe have found a solution – heralded photon amplification – and put it to the test.

The team, which includes researchers from the University of Geneva and Delft University of Technology, has demonstrated the technique over a simulated distance of 50 km, reporting its results in the journal *Quantum Science and Technology*. The work is published as part of a focus issue on the theme of quantum cryptography and quantum networking.

"In classical communication, amplifiers are used to regenerate the signal. However, in the quantum regime this adds too much noise and destroys the coherence of the quantum states," explained Robert Thew, who co-leads the Quantum Technologies Group at the University of Geneva. "In our experiments, we overcome this limitation by exploiting a teleportation-based approach, which can be thought of as a lossless channel."

Today, when we send sensitive information over the internet, we rely on hard-to-solve mathematical expressions to protect our data from eavesdroppers. However, this approach is vulnerable to attack in the future as computers become more capable of finding answers to these

numerical problems.

To get around the issue, physicists have been busy developing alternative schemes for secure key generation based not on mathematical expressions, but on the quantum behaviour of single particles of light – photons. What's more, not only are these techniques impossible to crack through conventional means, they also warn of eavesdropping. These are so-called quantum keys.

As the researchers highlight, one of the major applications of heralded photon amplification is for so-called device-independent quantum key distribution – an approach aimed at certifying the security of a connection with minimal assumptions about the system itself and the technology that is exploited.

At the heart of the approach is the conceptually simple idea of sending a single photon on a 50/50 beam-splitter to generate entanglement. Repeating the process in succession and monitoring the output from single photon detectors provides the building blocks for studying quantum communication protocols.

Taking this a step further, it's possible to distribute the entanglement between two locations, generating a unique key for encrypting data transmission.

"The single photon, or path entangled, scheme we are using is also closely connected to quantum repeaters in terms of how entanglement is distributed in these long distance and fully-quantum network solutions," commented Thew. "Our next step is to develop compact and more efficient heralded photon sources that can be more easily deployed, allowing us to push these sorts of experiments into real-world networks."

**More information:** F Monteiro et al. Heralded amplification of path

entangled quantum states, *Quantum Science and Technology* (2017). DOI: 10.1088/2058-9565/aa70ad