

# Quantum cryptography conquers noise problem

Encoded photons sent a record distance along busy optical fibres.

**Zeeya Merali**

20 November 2012

It's hard to stand out from the crowd — particularly if you are a single photon in a sea of millions in an optical fibre. Because of that, ultra-secure quantum-encryption systems that encode signals into a series of single photons have so far been unable to piggyback on existing telecommunications lines. But now, physicists using a technique for detecting dim light signals have transmitted a quantum key along 90 kilometres of noisy optical fibre<sup>1</sup>. The feat could see quantum cryptography finally enter the mainstream.

You cannot measure a quantum system without noticeably disrupting it. That means that two people can encode an encryption key — for bank transfers, for instance — into a series of photons and share it, safe in the knowledge that any eavesdropper will trip the system's alarms. But such systems have not been able to transmit keys along telecommunications lines, because other data traffic swamps the encoded signal. As a result, quantum cryptography has had only niche applications, such as connecting offices to nearby back-up sites using expensive 'dark' fibres that carry no other signals. "This is really the bottleneck for quantum cryptography," says physicist Nicolas Gisin, a scientific adviser at quantum-cryptography company ID Quantique in Geneva, Switzerland.

Physicists have attempted to solve the problem by sending photons through a shared fibre along a 'quantum channel' at one characteristic wavelength. The trouble is that the fibre scatters light from the normal data traffic into that wavelength, polluting the quantum channel with stray photons. Andrew Shields, a physicist at the Toshiba Cambridge Research Laboratory, UK, and his colleagues have now developed a detector that picks out photons from this channel only if they strike it at a precise instant, calculated on the basis of when the encoded photons were sent. The team publishes its results in *Physics Review X*.

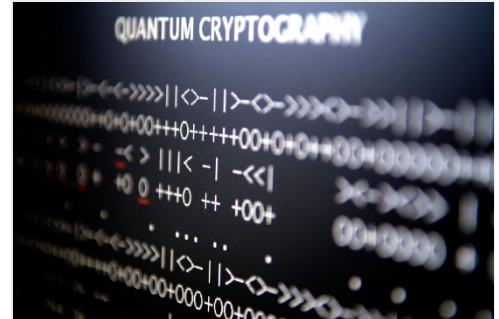
## Just in time

Designing a detector with such a sharp time focus was tough, explains Shields. Standard detectors use semiconducting devices that create an avalanche of electrical charge when struck by a single photon. But it usually takes more than one nanosecond ( $10^{-9}$  seconds) for the avalanche to grow large enough to stand out against the detector's internal electrical hiss — much longer than the narrow window of 100 picoseconds ( $10^{-10}$  seconds) needed to filter a single photon from a crowd.

The team's 'self-differentiating' detector activates for 100 picoseconds, every nanosecond. The weak charge triggered by a photon strike in this short interval would not normally stand out, but the detector measures the difference between the signal recorded during one operational cycle and the signal from the preceding cycle — when no matching photon was likely to be detected. This cancels out the background hum. Using this device, the team has transmitted a quantum key along a 90-kilometre fibre, which also carried noisy data at 1 billion bits per second in both directions — a rate typical of a telecommunications fibre. The team now intends to test the technique on a real telecommunications line.

Gisin's team has independently developed a photon detector with a similar time window, which they presented at the QCrypt 2012 meeting at the Centre for Quantum Technologies in Singapore in September. However, Gisin has calculated that such a technique cannot be used to transmit quantum signals beyond the range of a large city of 100 kilometres<sup>2</sup>. Scattering accumulates over distance, so there would eventually be so many stray photons that it would be impossible to filter them out, even with a precisely timed detector.

Still, 90 kilometres is a "world record that is a big step forward in demonstrating the applicability of quantum cryptography in real-world telecommunications infrastructures", says Vicente Martín, a physicist at the Technical University of Madrid.



N. Gregory/Alamy

Quantum cryptography could keep messages ultra-secure — if the right detector can be developed.

## References

---

1. Patel, K. A. *et al. Phys. Rev. X* **2**, 041010 (2012).
2. Eraerds, P., Walenta, N., Legré, M., Gisin, N. & Zbinden, H. *N. J. Phys.* **12**, 063027 (2010).