# Quantum cryptography goes maintream

December 5 2012

(Phys.org)—Researchers from Toshiba and the Department of Engineering have perfected a technique that offers a less expensive way to ensure the security of high-speed fibre-optic cables, protecting communication networks from unauthorized snooping.

The Cambridge Research Laboratory of Toshiba Research Europe Ltd, working in collaboration with Professor Richard Penty and his team in the Department, has succeeded in extracting the very weak signals used for quantum cryptography from ordinary telecom fibres transmitting

data traffic. This means that existing telecom networks can now be secured with this ultimate form of encryption.

Quantum cryptography can be used to distribute the secret digital keys important for protecting our personal data, such as bank statements, health records, and digital identity. Its security relies upon encoding each bit of the digital key upon a single photon (particle of light). If a hacker intercepts the single photons, they will unavoidably disturb their encoding in a way that can be detected. This allows eavesdropping on the network to be directly monitored.

Up until now it has been necessary to send the single photons through a dedicated fibre that is distinct from the fibres carrying the ordinary data signals in the network. The data signals are much more intense than the single photon signals used for quantum cryptography: in fact one bit of data is carried by over 1 million photons. The disparity in the intensity of the signals means that scattered light caused by the data signals would contaminate and overwhelm the single photon signals if sent along the same fibre.

Dr Andrew Shields, of Toshiba Research Europe Ltd, explained: "The requirement of separate fibres has greatly restricted the applications of quantum cryptography in the past, as unused fibres are not always available for sending the single photons, and even when they are, can be prohibitively expensive. Now we have shown that the single photon and data signals can be sent using different wavelengths on the same fibre."

The Cambridge team achieved this using a detector that is sensitive only for a very brief window (100 millionths of a micro-second) at the expected arrival time of the single photons. The detector thereby responds largely to just the single photon signals and is insensitive to the scattered light caused by the data signals. This allows the weak single photon signals to be recovered from the fibre.

Using this technique the Cambridge researchers have successfully implemented quantum cryptography on ordinary telecom fibres while simultaneously transmitting data at 1 Gbit/s in both directions. They demonstrated a secure key rate over 500kbit/sec for 50km of fibre, about 50000 times higher than the previous best value for this fibre length. This work is reported in the scientific journal, *Physical Review X*.

**More information:** physics.aps.org/synopsis-for/1 … 03/PhysRevX.2.041010

For further information on Department of Engineering's photonic systems research click here.

Provided by University of Cambridge