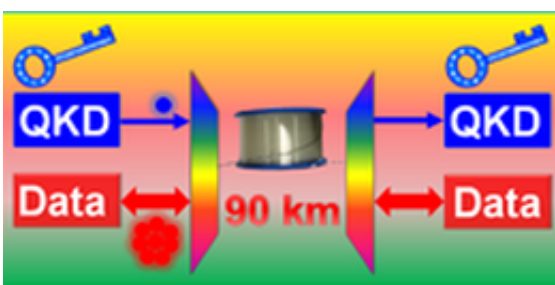


Researchers devise method of sending quantum encryption keys over shared fiber cable

November 21 2012, by Bob Yirka



(Phys.org)—Researchers from Toshiba and Cambridge University working together in Britain have developed a technique for sending quantum encryption keys over a shared fiber cable. As they describe in their paper published in *Physics Review X*, their technique involves employing a super sensitive photon detector capable of detecting the photons that make up a quantum key at the precise moment they arrive.

Up till now, the problem with trying to send [quantum encryption](#) keys over a shared fiber cable was finding the photons that make up the quantum key among the millions of others that serve as data as they arrived at the other end. Recent efforts have sidestepped the problem by using a secondary dedicated cable for just the encrypted keys, but that obviously drives up network costs. The use of quantum keys is desirable

because they have the built in advantage of producing errors if someone else observes or measures them as they move from one end of the cable to the other.

In this new research, the team reasoned that if a system could be devised that would allow for keeping precise track of the time single photons that make up the key left the source and calculate their arrival time at the destination, it would be possible to focus only on them, and thus, see the key and use it for its designed purpose. The problem with this approach was that there didn't exist a photon detector that could open and close quickly enough to suit the needs of detecting photons in a stream of others in a fiber cable. Their only choice was to make one themselves, and that's exactly what they did. Their new [photon detector](#) snaps open and closed like the shutter on a camera, capturing only what is arriving at a precise moment in time. In this case, the "[shutter](#)" activates for just 100 picoseconds, every [nanosecond](#). Fast enough to capture just the [photons](#) from the encrypted key, and nothing else. At a [test facility](#) the team demonstrated that such a system could work by sending encrypted quantum keys over a shared fiber cable for a distance of 90 kilometers (56 miles). The next step will be to test the system on a real world cable.

The researchers believe their new technique will allow for metropolitan wide distribution of encrypted keys which will be useful for military and financial communications. In the long term, they suggest the new technology may be modified to one day include the entire Internet infrastructure.

More information: Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber, *Phys. Rev. X* 2, 041010 (2012)
[DOI: 10.1103/PhysRevX.2.041010](https://doi.org/10.1103/PhysRevX.2.041010)

Abstract

Quantum key distribution (QKD) uniquely allows the distribution of

cryptographic keys with security verified by quantum mechanical limits. Both protocol execution and subsequent applications require the assistance of classical data communication channels. While using separate fibers is one option, it is economically more viable if data and quantum signals are simultaneously transmitted through a single fiber. However, noise-photon contamination arising from the intense data signal has severely restricted both the QKD distances and secure key rates. Here, we exploit a novel temporal-filtering effect for noise-photon rejection. This allows high-bit-rate QKD over fibers up to 90 km in length and populated with error-free bidirectional Gb/s data communications. With a high-bit rate and range sufficient for important information infrastructures, such as smart cities and 10-Gbit Ethernet, QKD is a significant step closer toward wide-scale deployment in fiber networks.

[Physics Synopsis](#)

© 2012 Phys.org

Citation: Researchers devise method of sending quantum encryption keys over shared fiber cable (2012, November 21) retrieved 26 April 2024 from <https://phys.org/news/2012-11-method-quantum-encryption-keys-fiber.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--