

# New quantum key system combines speed, distance

June 9 2007

---



Detection stage of the NIST prototype quantum key distribution system: Photons are "up-converted" from 1310 to 710 nm by one of the two NIST-designed converters at right, then sent to one of two commercial silicon avalanche photo diode units to the left. Credit: NIST

Researchers at NIST have built a prototype high-speed quantum key distribution system, based on a new detector system that achieves dramatically lower noise levels than similar systems.

Researchers at the National Institute of Standards and Technology have built a prototype high-speed quantum key distribution (QKD) system, based on a new detector system that achieves dramatically lower noise levels than similar systems. The new system, they say, can perform a theoretically unbreakable "one-time pad" encryption, transmission and

decryption of a video signal in real-time over a distance of at least 10 kilometers.

Key distribution—the problem of ensuring that both the sender and receiver of an encrypted message (and no one else) share the same long string of random digits (the so-called “key”) used to encode and decode the message—has always been one of the most important challenges in cryptography. Since the 1980’s it’s been recognized that the unique properties of quantum mechanics—the fact that certain measurements cannot be made without altering the thing measured—offered the possibility of a system that could transmit as long a key as desired between two parties with no chance that it could be copied undetectably by a third party.

Since then the race has been on to build a fast, practical and reliable QKD system. One important requirement for any candidate system is that it be compatible with existing fiber-optic telecom networks that transmit at wavelengths of either 1550 or 1310 nanometers (nm) to reach the greatest distance. Another requirement is a highly efficient photon detector that can detect single photons reliably without introducing significant amounts of “noise.” One of the best low-noise detectors, a silicon-based avalanche photo diode (Si-APD), does not function at the telecom wavelengths. Instead, it operates best at much shorter wavelengths around 700 nm. To take advantage of the Si-APD, the NIST group designed a sub-system to “up-convert” single photons from a transmission wavelength of 1310 nm to 710 nm for high-efficiency detection.

Their QKD system that incorporates this up-conversion technique, described in a recent paper, generates and transmits secure keys at a rate of over half a million bits per second over 10 km of optical fiber, fast enough to encrypt streaming digital video using one-time pad in real time. The group also has transmitted secure keys at rates near 10 kilobits

per second at five times that distance. The same team last year set a speed record for transmission of secure keys over a kilometer of fiber (see [www.physorg.com/news64589539.html](http://www.physorg.com/news64589539.html)). This work improves the distance by at least 10 times.

Advantages of the new system, according to the research team, include high speed, high efficiency, low noise and convenience of operation. The fact that it uses a 1310 nm transmission wavelength somewhat limits the propagation distance but adds the advantage that the parallel “classical-quantum” communication, which is needed for a full QKD system, can be realized in a single fiber without significant interference.

Details of NIST’s up-conversion QKD research are available at <http://w3.antd.nist.gov/quinn.shtml>.

Citation: H. Xu, L. Ma, A. Mink, B. Hershman and X. Tang. 1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm. *Optics Express*, Vol. 15, Issue 12, pp. 7247-7260.

Source: National Institute of Standards and Technology

Citation: New quantum key system combines speed, distance (2007, June 9) retrieved 27 April 2024 from <https://phys.org/news/2007-06-quantum-key-combines-distance.html>

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.