

# LANL/NIST Team Sends Quantum Encryption 'Keys' Over Record Distances

**Using an innovative sensor for detecting single photons, the smallest particles of light, scientists from Los Alamos National Laboratory (LANL), the National Institute of Standards and Technology (NIST) and Albion College (Albion, Mich.) have set two significant distance records for distributing “keys” (or codes) for quantum encryption, the most secure method known for protecting the privacy of information.**

As described in the September issue of *New Journal of Physics*, the team generated and transmitted secret quantum keys over 184.6 kilometers (km) of fiber-optic cable, the longest distance ever recorded for quantum key distribution (QKD). The previous record was 122 km. Secret quantum key is a code for encrypting data that not only have been transmitted and detected successfully, but also processed to correct for errors and enhance privacy, steps considered essential for practical applications. The keys are then used to encrypt ordinary digital data for transmission over conventional communications channels.

“This work extends the potential range of one link of a quantum communications system,” says Sae Woo Nam, the NIST physicist who designed the photon detectors. “Experiments like this are interesting because they establish new thresholds for the distance between repeaters,” or devices that re-send and boost fading signals between links in far-reaching networks.

LANL and NIST are among a number of laboratories and companies around the world developing QKD systems, which are expected to provide the next generation of data security. A variety of threats as well as advances in code-breaking create continuous pressure to improve encryption systems, which have been used widely for many years to ensure the security of electronic financial transactions, military operations, and commercially valuable or confidential data.

QKD systems produce keys using single photons transmitted with their electric fields in different orientations to represent the values 1 and 0 used in digital communications. Under the laws of quantum physics, nature’s instruction book for the smallest particles of matter and light, a photon cannot be intercepted without changing its quantum state (including orientation), changes that can be detected to reveal eavesdropping. Thus, unlike today’s best encryption methods, which depend on mathematical complexity and could be broken with sufficient time and computing power, quantum encryption is “unbreakable”—as long as the QKD system is properly designed.

A weakness in typical QKD systems is the current lack of reliable commercial single-photon sources. Very weak laser pulses are used instead, and they often produce more than one photon per pulse, all with the same orientation and bit value (0 or 1). This introduces vulnerability: An eavesdropper could intercept a photon and “read” it accurately without its loss being detected by the intended receiver, because the same laser pulse may still contain another photon.

The LANL/NIST absolute distance record of 184.6 km is secure against reasonable attacks, that is, the laser adjustments used in this case have only a moderate probability of generating more than one photon per pulse. The team also used slightly different adjustments to set other QKD distance records, including absolutely secure transmission of secret keys over 67.5 km, surpassing the previous record of 50.6 km. This method generated so few multi-photon pulses that some of the photons detected at the receiver must have originated in single-photon pulses, enabling the creation of secret key.

The experiments were performed in LANL laboratories using fiber-optic cables wrapped around several

spools. The photon detectors were designed and built at NIST labs in Boulder, Colo. A detector consists of a small square of thin tungsten film chilled to the transition temperature between normal conductivity and superconductivity. When a photon hits the tungsten, the temperature rises and results in an increase in electrical resistance. The change in temperature is proportional to the photon energy, allowing the sensor to determine the number of photons in a pulse of light.

Compared to commercial photodiodes typically used in QKD systems, the NIST detectors are far more efficient (detecting 65 percent of received photons versus about 20 percent) and have much lower false count rates at telecommunications wavelengths (1310 and 1550 nanometers), advantages that increase transmission distance and enhance security. The NIST detectors also recover much faster (4 microseconds versus tens of microseconds) between detection events, which may increase system speed. (The NIST sensors are capable of even greater efficiency but the rolled fiber-optic cable loses longer-wavelength photons, reducing detection efficiency at 1550 nm from 89 percent to 65 percent.)

Commercial photon detectors still have better timing resolution—capability to synchronize with the timing of photon transmissions—than the NIST sensors (less than 100 picoseconds versus 100 nanoseconds). This so-called timing jitter may cause crosstalk or signal distortion. However, the researchers believe that improvements in detector electronics will reduce this problem, potentially leading to faster transmissions over long distances.

Citation: P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller and J.E. Nordholt. 2006. Long-distance quantum key distribution in optical fibre. *New Journal of Physics*. Posted online Sept. 14.

Source: NIST

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