Scientists demonstrate ultra-secure, long-distance quantum key distribution

December 22 2006

Scientists at Los Alamos National Laboratory and the National Institute of Standards and Technology in Boulder have demonstrated unconditionally secure quantum key distribution (QKD) over a record-setting 107 kilometers of optical fiber. The work is a significant step towards enabling communication with an unprecedented level of security over long distances of optical fiber.

In research published in *Physical Review Letters*, a team of scientists led by Beth Nordholt of Los Alamos describes how they have implemented a decoy-state protocol that enables the creation of secure keys that are immune to certain kinds of interceptions and attacks.

According to Danna Rosenberg, lead author of the *PRL* paper, "in theory, QKD is completely secure, but real QKD systems rely on imperfect devices that can create a security loophole. In particular, most systems use a laser pulse instead of a single photon source. For QKD, it's important that the information be encoded in a single photon, but laser sources put out a distribution of photon numbers, and there is always some probability that there will be more than one photon in the laser pulse. This makes the system vulnerable to certain kinds of attacks that could defeat the encryption system."

These multi-photon pulses could allow an eavesdropper to perform a photon-number-splitting (PNS) attack, a sophisticated type of attack that is not currently feasible but which exploits the fact that only those signals that arise from single photons are secure. One method of

thwarting PNS attacks is to use very weak signals, but this limits the distance that the signal can be transmitted because of signal loss in optical fiber.

According to Jim Harrington, another researcher on the project, "When developing secure communications, it is necessary to consider the worst possible case of an adversary's actions. Conventionally, QKD with laser pulses has been insecure or infeasible at long distances. By following a decoy-state protocol, where the sender randomly varies the laser power level, users can effectively learn what happened to the single-photon versus multi-photon pulses during transmission. This allows them to bound the number of single-photon signals that were detected by the receiver, which they can then use to construct a truly secure key."

The new Los Alamos protocol uses ultra low noise, high-efficiency transition-edge sensor photodetectors, developed at NIST, to generate a secure key by implementing a three-level decoy state protocol. This protocol is similar to one demonstrated by a group of researchers at the University of Toronto, but Los Alamos utilized a one-way QKD system instead of a two-way QKD system, which is more susceptible to an adversary's manipulation. The researchers believe they will be able to extend the system past the current range to distances of 250 kilometers, or more.

In addition to Nordholt, Rosenberg, and Harrington, other members of the team include Pat Rice, Glen Peterson, Phil Hiskett, and Richard Hughes at Los Alamos, and Adriana Lita and Sae Woo Nam of NIST.

Source: Los Alamos National Laboratory

December 22) retrieved 19 April 2024 from https://phys.org/news/2006-12-scientists-ultra-secure-long-distance-quantum-key.html