NIST System Sets Speed Record For Generation of Quantum Keys for 'Unbreakable' Encryption

May 13 2004

Quantum systems - exploiting the laws of quantum mechanics - are expected to provide the next big advance in data encryption. The fastest known cryptographic system based on transmission of single photons - the smallest pulses of light - has been demonstrated by a team at the Commerce Department's National Institute of Standards and Technology (NIST). The NIST "quantum key distribution" system transmits a stream of individual photons to generate a verifiably secret key - a random series of digital bits, each representing 0 or 1, used to encrypt messages -**at a rate of 1 million bits per second (bps)**. This rate is about **100 times faster** than previously reported systems of this type.

Quantum systems—exploiting the laws of quantum mechanics—are expected to provide the next big advance in data encryption. The beauty of quantum key distribution is its sensitivity to measurements made by an eavesdropper. This sensitivity makes it possible to ensure the secrecy of the key and, hence, the encrypted message. The keys are generated by transmitting single photons that are polarized, or oriented, in one of four possible ways. An eavesdropper reading the transmission causes detectable changes at the receiver. When such changes are observed, the associated key is not used for encryption.

Previous works has demonstrated quantum key distribution (QKD) over distances up to 150 km in fiber and 23 km in free space, but the bit rates of these systems have been low and definitely insufficient for network and telecommunications applications of the one-time-pad cipher, or for large numbers of multiple users. NIST researchers report a QKD system that has attained sifted-key rates of up to 1 Mbps over a 730 m free-space link, and identify pathways for increasing the transmission rate by another order of magnitude.

Compared to previously described QKD systems, the major difference in the NIST system is the way it identifies a photon from the sender among a large number of photons from other sources, such as the sun. To make this distinction, scientists time-stamp the QKD photons, then look for them only when one is expected to arrive.

The NIST quantum system uses an infrared laser to generate the photons and telescopes with 8-inch mirrors to send and receive the photons over the air. The data are processed in real time by printed circuit boards designed and built at NIST, so that a computer produces ready-made keys. NIST researchers also developed a high-speed approach to error correction.

See more information about quantum key distribution systems on NIST

website.
Original pressrelease is here.
Technical paper is published in Optics express.