'Dead time' limits quantum cryptography speeds

September 28 2007

Quantum cryptography is potentially the most secure method of sending encrypted information, but does it have a speed limit" According to a new paper by researchers at the National Institute of Standards and Technology and the Joint Quantum Institute, technological and security issues will stall maximum transmission rates at levels comparable to that of a single broadband connection, such as a cable modem, unless researchers reduce “dead times” in the detectors that receive quantum-encrypted messages. The JQI is a research partnership that includes NIST and the University of Maryland.

In quantum cryptography, a sender, usually designated Alice, transmits single photons, or particles of light, encoding 0s and 1s to a recipient, “Bob.” The photons Bob receives and correctly measures make up the secret “key” that is used to decode a subsequent message. Because of the quantum rules, an eavesdropper, “Eve,” cannot listen in on the key transmission without being detected, but she could monitor a more traditional communication (such as a phone call) that must take place between Alice and Bob to complete their communication.

Modern telecommunications hardware easily allows Alice to transmit photons at rates much faster than any Internet connection. But at least 90 percent (and more commonly 99.9 percent) of the photons do not make it to Bob’s detectors, so that he receives only a small fraction of the photons sent by Alice.

Alice can send more photons to Bob by cranking up the speed of her

transmitter, but then, they'll run into problems with the detector's "dead time," the period during which the detector needs to recover after it detects a photon. Commercially available single-photon detectors need about 50-100 nanoseconds to recover before they can detect another photon, much slower than the 1 nanosecond between photons in a 1-Ghz transmission.

Not only does dead time limit the transmission rate of a message, but it also raises security issues for systems that use different detectors for 0s and 1s. In that important "phone call," Bob must report the time of each detection event. If he reports two detections occurring within the dead time of his detectors, then Eve can deduce that they could not have come from the same detector and correspond to opposite bit values.

Sure, Bob can choose not to report the second, closely spaced photon, but this further decreases the key production rate. And for the most secure type of encryption, known as a one-time pad, the key has to have as many bits of information as the message itself.

The speed limit would go up, says NIST physicist Joshua Bienfang, if researchers reduce the dead time in single-photon detectors, something that several groups are trying to do. According to Bienfang, higher speeds also would be useful for wireless cryptography between a ground station and a satellite in low-Earth orbit. Since the two only would be close enough to communicate for a small part of the day, it would be beneficial to send as much information as possible during a short time window.

Citation: D.J. Rogers, J.C. Bienfang, A. Nakassis, H. Xu and C.W. Clark, Detector dead-time effects and paralyzability in high-speed quantum key distribution, *New Journal of Physics* (September 2007); available at www.iop.org/EJ/abstract/-kwd=n … f2/1367-2630/9/9/319 .

Source: National Institute of Standards and Technology