Quantum eavesdropper steals quantum keys

June 20 2011, by Lisa Zyga

(PhysOrg.com) -- In quantum cryptography, scientists use quantum mechanical effects to encrypt and then communicate confidential information. Although quantum cryptography codes are unbreakable in principle, even the best techniques have loopholes in practice that scientists are trying to address. In a recent study, physicists have exposed one of these loopholes by hacking a quantum code, which involved copying a secret quantum key without being detected.

The researchers, Ilja Gerhardt, et al., from the National University of Singapore and the University of Trondheim, have published their study in a recent issue of *Nature Communications*. Although this is not the first experiment to show that quantum cryptography systems are vulnerable and that a quantum key can be secretly copied, it is the first time that someone has actually copied a quantum key.

“This confirms that non-idealities in physical implementations of QKD [quantum key distribution] can be fully practically exploitable, and must be given increased scrutiny if quantum cryptography is to become highly secure,” the scientists wrote in their study.

In the quantum cryptography technique explored here, the secret key is the tool that the sender and receiver (“Alice” and “Bob”) use to encode messages. For instance, Alice can send a key in the form of polarized single photons to Bob. Alice randomly polarizes the photons using either a horizontal-vertical polarizer or a polarizer with two diagonal axes. Bob also randomly uses one of the two different polarizers to detect each photon. Then, Bob asks Alice over an open channel which polarizer she

used for each photon and compares them to his measurements. The measurement results for which Bob used the correct polarizer now become Alice and Bob's secret key.

In order to copy this key and intercept a message, an eavesdropper ("Eve") would have to correctly guess which polarizer to use on every photon that Alice sends Bob. Due to the large number of photons used, it's unlikely that Eve could choose correctly for very long. When Eve uses an incorrect polarizer, the photon's polarization is randomized, which makes Bob's measurement incorrect. This error alerts Bob and Alice to an eavesdropper's presence, which they can confirm by comparing a small subset of the key on an open line.

In the new study, the physicists showed how to steal the quantum key without being detected in an experiment on a 290-meter-long fiber link at the National University of Singapore. First, they intercepted single photons traveling along the fiber, and then re-emitted bright light pulses with the same polarization to "blind" the photodioides that Bob uses to detect photons.

When blinded, Bob's photodiodes cannot detect single photons, but instead they respond to the intensity of incoming light pulses. For this reason, Bob can no longer randomly choose a polarizer for each measurement. In their experiment, the researchers intercepted more than 8 million photons in a five-minute span, and then re-emitted corresponding bright pulses; Bob correctly measured all of these bright pulses in the correct detector. So if Alice and Bob were to compare the subset of the key, there would be no errors, and no hint of an eavesdropper on the line.

Now that they have shown how to steal a quantum key without detection, the scientists are working on preventing these attacks from happening and making quantum cryptography more secure. One possibility is for

Bob to set up a single-photon source in front of his detectors and randomly switch it on just to make sure that his detectors can still register single photons. If not, the detectors may have been “blinded” by an eavesdropper.

More information: Ilja Gerhardt, et al. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system." *Nature Communications*, Volume: 2, Article number: 349, DOI: 10.1038/ncomms1348
via: Physics World