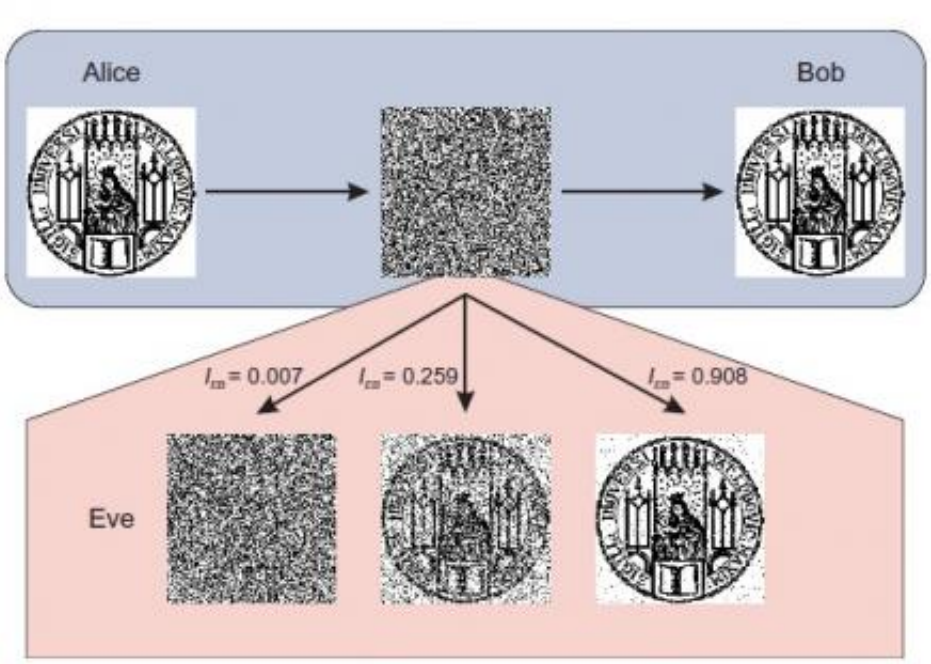
Physicists offer countermeasure to new quantum eavesdropping attack

July 25 2011, by Lisa Zyga



Using the "dead time" attack, Eve can recover Alice and Bob's secret key, the emblem of the University of Munich, without being detected. The figure shows the results of Eve's attacks using low (bottom left), medium (bottom center) and high (bottom right) blinding pulse intensities. Image copyright: Henning Weier, et al. ©2011 IOP Publishing Ltd and Deutsche Physikalische Gesellschaft

(PhysOrg.com) -- As early communications systems using quantum cryptography become commercially available, physicists have been investigating new types of security attacks in an effort to defend against

them. In a recent study, researchers have identified and demonstrated a new, highly effective way to eavesdrop on a quantum key distribution (QKD) system that involves blinding the receiver's detector during the "dead time" of single-photon detectors. For the first time, the eavesdropper does not even have to intercept the quantum channel to compromise the system's security, making this attack technologically very simple.

The physicists, Henning Weier from the Ludwig Maximillians University of Munich and Qutools GmbH in Munich, and coauthors, have published their study on the new quantum eavesdropping attack, along with a countermeasure to prevent it, in a recent issue of the New Journal of Physics.

In QKD systems, two communicating users (Alice and Bob) produce a secret key of qubits, and then use that key to encrypt and decrypt messages. If an eavesdropper (Eve) can uncover this key without being caught, she too can decrypt the messages.

As the physicists explain, theoretical proofs have shown that the ideal QKD protocol is completely secure; that is, the amount of information that an eavesdropper can steal can be quantified and made negligibly small. If Eve were to attack the system, Alice and Bob could detect her presence due to the high error rate, and no secure key will be made. However, when QKD systems are implemented in practice, they can be vulnerable to certain types of attacks, depending on the hardware used.

The attack described here could be used to intercept the key as Alice and Bob are creating it together. This scheme and similar ones work in almost any QKD system since they exploit a feature common to almost all single-photon detectors, which is the dead time. After a detection event, single-photon detectors are rendered inactive for a period of time that can range from less than a nanosecond to a few tens of

microseconds. During this dead time, detectors cannot detect incoming photons.

Taking advantage of this dead time, Eve can send light pulses into the quantum channel to partially blind Bob's (the receiver's) photon detectors. Timing these pulses is critical, since they must be sent shortly before Bob's "time window." As the scientists explained, Bob knows roughly when the photons from Alice should arrive, and accounts for only those photons that come during a narrow time interval around the expected arrival time. The time window allows Bob to filter out background photons (especially during the day) and reduce the error rate significantly. In this case, however, Eve can take advantage of this time window to prevent Bob from noticing her pulses.

In the attack, Eve sends light pulses of one of four polarizations (horizontal, vertical, +45°, or -45°) to blind three of Bob's four detectors, each of which can detect one type of polarization. If a detection event occurs, then Eve knows it had to have happened in the detector that can detect the polarization opposite from that which she used. For example, if she sends out pulses with vertical polarization, the detectors corresponding to vertical, +45°, and -45° will see the light, while the horizontal detector won't. So all detectors except the horizontal one are blind. If a click occurs in Bob's following time window, it can only have happened in the horizontal detector. In this way, Eve can gain information about the key bits being sent to Bob's detectors. By tuning the intensity of the blinding pulses, Eve can tune information about the key.

In experiments, the scientists demonstrated that dim pulses containing only a few photons can determine almost all of the key (in this case, the emblem of the University of Munich). On average, an eavesdropper needs fewer than 20 photons per binding pulse to gather over 98% of the key information. Since the error between Alice and Bob does not

increase during the attack, they are not aware of the eavesdropper's presence.

As simple as this attack is, the scientists explain that a defense against it is even simpler. Bob could monitor the status of his single-photon detectors to ensure that the detection efficiency has not been compromised. When generating their shared key, Alice and Bob would only use detection events in which all detectors were active. So even if Eve had been blinding Bob's detectors and intercepting the key bits, those bits would not end up being used, and the attack would fail.

"In my opinion, actual systems can generally never be proven to be secure," Weier told *PhysOrg.com*. "In this respect, QKD isn't better than its classical counterpart. But scientists are working on bridging the gap between theoretic models and real systems. Ideally one can build a provably secure model that describes the actual QKD system including all (known) implementation imperfections. If the theoretic model gave some bounds with regard to the imperfections, one would get as close to perfect security as possible."

More information: Henning Weier, et al. "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors." *New Journal of Physics* 13 (2011) 073024. DOI: 10.1088/1367-2630/13/7/073024

https://phys.org/news/2011-07-physicists-countermeasure-quantum-eavesdropping.html