Making quantum cryptography truly secure

June 14 2011

Dr. Ilja Gerhardt, professor Antía Lamas-Linares and professor Christian Kurtsiefer set up a quantum cryptography system. Credit: 2009 Vadim Makarov www.vad1.com

Quantum key distribution (QKD) is an advanced tool for secure computer-based interactions, providing confidential communication between two remote parties by enabling them to construct a shared secret key during the course of their conversation.

QKD is perfectly secure in principle, but researchers have long been aware that loopholes may arise when QKD is put into practice. Now, for the first time, a team of researchers at the Centre for Quantum Technologies (CQT) at the National University of Singapore, the Norwegian University of Science and Technology (NTNU) and the University Graduate Center (UNIK) in Norway have created and operated a "perfect eavesdropper" for QKD that exploits just such a

loophole in a typical QKD setup. As reported in the most recent issue of *Nature Communications*, this eavesdropper enabled researchers to obtain an entire shared secret key without alerting either of the legitimate parties that there had been a security breach. The results highlight the importance of identifying imperfections in the implementation of QKD as a first step towards fixing them.

Cryptography has traditionally relied on mathematical conjectures and thus may always be prone to being "cracked" by a clever mathematician who can figure out how to efficiently solve a mathematical puzzle, aided by the continual development of ever-faster computers. Quantum cryptography, however, relies on the laws of physics and should be infinitely more difficult to crack than traditional approaches. While there has been much discussion of the technological vulnerabilities in quantum cryptography that might jeopardize this promise, there have been no successful full field-implemented hacks of QKD security – until now.

"Quantum key distribution has matured into a true competitor to classical key distribution. This attack highlights where we need to pay attention to ensure the security of this technology," says Christian Kurtsiefer, a professor at the Centre for Quantum Technologies at the National University of Singapore.

In the setup that was tested, researchers at the three institutions demonstrated their eavesdropping attack in realistic conditions over a 290-m fibre link between a transmitter called "Alice" and a receiver called "Bob". Alice transmits light to Bob one photon at a time, and the two build up their secret key by measuring properties of the photons. During multiple QKD sessions over a few hours, the perfect eavesdropper "Eve" obtained the same "secret" key as Bob, while the usual parameters monitored in the QKD exchange were not disturbed – meaning that Eve remained undetected.

The researchers were able to circumvent the quantum principles that in theory provide QKD its strong security by making the photon detectors in Bob behave in a classical way. The detectors were blinded, essentially overriding the system's ability to detect a breach of security. Furthermore, this technological imperfection in QKD security was breached using off-the-shelf components.

"This confirms that non-idealities in the physical implementations of QKD can be fully and practically exploitable, and must be given increased scrutiny if quantum cryptography is to become highly secure," says Vadim Makarov, a postdoctoral researcher at the University Graduate Center in Kjeller, Norway. "We can not simply delegate the burden of keeping a secret to the laws of quantum physics; we need to carefully investigate the specific devices involved," says Kurtsiefer.

The open publication of how the "perfect eavesdropper" was built has already enabled this particular loophole in QKD to be closed. "I am sure there are other problems that might show that a theoretical security analysis is not necessarily exactly the same as a real-world situation," says Ilja Gerhardt, currently a visiting scholar at the University of British Columbia in Vancouver, Canada. "But this is the usual game in cryptography – a secure communications system is created and others try to break into it. In the end this makes the different approaches better."

More information: Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Communications* 2, 349 (2011). Article will be available at www.nature.com/ncomms/journal/ … full/ncomms1348.html

A free preprint is available at arxiv.org/abs/1011.0105

Provided by National University of Singapore