More secure communications thanks to quantum physics

March 12 2014

One of the recent revelations by Edward Snowden is that the U.S. National Security Agency is currently developing a quantum computer. Physicists aren't surprised by this news; such a computer could crack the encryption that is commonly used today in no time and would therefore be highly attractive for the NSA.

Professor Thomas Walther of the Institute of Applied Physics at the Technical University of Darmstadt is convinced that "Sooner or later, the quantum computer will arrive". Yet the quantum physicist is not worried. After all, he knows of an antidote: so-called quantum cryptography. This also uses the bizarre rules of quantum physics, but not to decrypt messages at a record pace. Quite the opposite – to encrypt it in a way that can not be cracked by a quantum computer. To do this, a "key" that depends on the laws of quantum mechanics has to be exchanged between the communication partners; this then serves to encrypt the message. Physicists throughout the world are perfecting quantum cryptography to make it suitable for particularly security-sensitive applications, such as for banking transactions or tap-proof communications. Walther's Ph.D. student Sabine Euler is one of them.

As early as the 1980s, physicists Charles Bennett and Gilles Brassard thought about how quantum physics could help transfer keys while avoiding eavesdropping. Something similar to Morse code is used, consisting of a sequence of light signals from individual light particles (photons). The information is in the different polarizations of successive photons. Eavesdropping is impossible due to the quantum nature of

photons. Any eavesdropper will inevitably be discovered because the eavesdropper needs to do measurements on the photons, and these measurements will always be noticed.

"That's the theory" says Walther. However, there are ways to listen without being noticed in practice. This has been demonstrated by hackers who specialize in quantum cryptography based on systems already available on the market. "Commercial systems have always relinquished a little bit of security in the past" says Walther. In order to make the protocol of Bennett and Brassard reality, you need, for example, light sources that are can be controlled so finely that they emit single photons in succession. Usually, a laser that is weakened so much that it emits single photons serves as the light source. "But sometimes two photons can come out simultaneously, which might help a potential eavesdropper to remain unnoticed" says Walther. The eavesdropper could intercept the second photon and transmit the first one.

Therefore, the team led by Sabine Euler uses a light source that transmits a signal when it sends a single photon; this signal can be used to select only the individually transmitted photons for communication. Nevertheless, there are still vulnerabilities. If the system changes the polarization of the light particles during coding, for example, the power consumption varies or the time interval of the pulses changes slightly. "An eavesdropper could tap this information and read the message without the sender and receiver noticing" explains Walther. Sabine Euler and her colleagues at the Institute of Applied Physics are trying to eliminate these vulnerabilities. "They are demonstrating a lot of creativity here" says Walther approvingly. Thanks to such research, it will be harder and harder for hackers to take advantage of vulnerabilities in quantum cryptography systems.

The TU Darmstadt quantum physicists want to make quantum cryptography not only more secure, but more manageable at the same

time. "In a network in which many users wish to communicate securely with each other, the technology must be affordable," he says. Therefore, his team develops its systems in such a manner that they are as simple as possible and can be miniaturized.

The research team is part of the Center for Advanced Security Research Darmstadt (CASED), in which the TU Darmstadt, the Fraunhofer Institute for Secure Information Technology and the University of Darmstadt combine their expertise in current and future IT security issues. Over 200 scientists conduct research in CASED, funded by the State Initiative for Economic and Academic Excellence (LOEWE) of the Hessian Ministry for Science and the Arts. "We also exchange information with computer scientists, which is very exciting," says Walther.

After all, the computer science experts deal with many of the same issues as Walther's quantum physicists. For example, Johannes Buchmann of the department of Computer Science at the TU Darmstadt is also working on encryption methods that theoretically can not be cracked by a quantum computer. However, these are not based on quantum physics phenomena, but rather on an unsolvable math problem.

Therefore, it may well be that the answer to the first code-cracking quantum computer comes from Darmstadt.

Bizarre quantum physics and encryption

A quantum computer could quickly crack current encryptions because it can test very many possibilities simultaneously, in the same way as if you could try all possible variations for a password at once. After all, according to the quantum physics principle of superposition, atoms, electrons or photons can have several states simultaneously; for example, they can rotate clockwise and counterclockwise at the same time.

However, if you were to measure a property of a particle, such as the direction of rotation, the superposition is lost. This phenomenon is useful for quantum cryptography. Eavesdroppers inevitably betray themselves because their measurements of the photon change the photon's characteristics. Moreover, quantum physics forbids them to copy the photon with all its properties. Therefore, they can not siphon off any information to retransmit the uninfluenced photons on to the sender of the message.

Provided by Technische Universitat Darmstadt