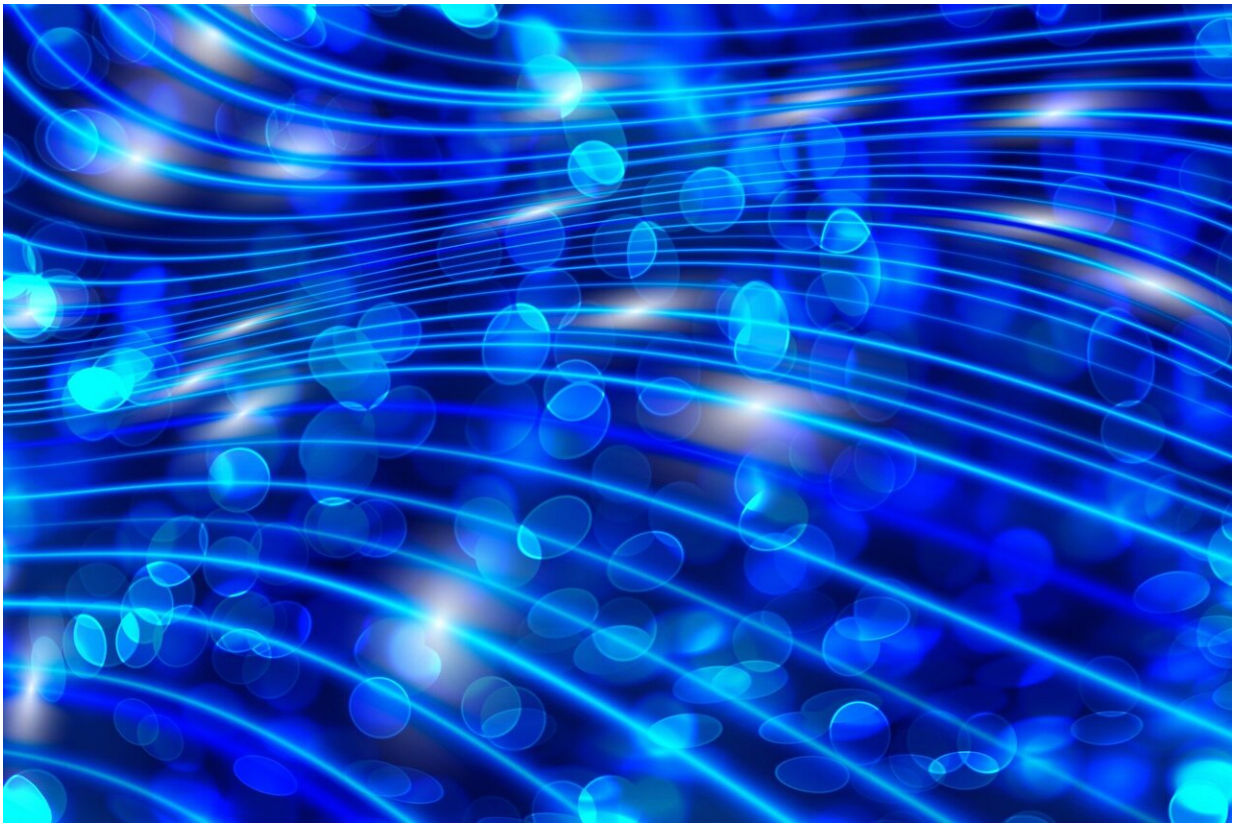
Quantum cryptography: Making hacking futile

July 27 2022



Credit: CC0 Public Domain

The Internet is teeming with highly sensitive information. Sophisticated encryption techniques generally ensure that such content cannot be intercepted and read. But in the future high-performance quantum

computers could crack these keys in a matter of seconds. It is just as well, then, that quantum mechanical techniques not only enable new, much faster algorithms, but also exceedingly effective cryptography.

Quantum key distribution (QKD)—as the jargon has it—is secure against attacks on the communication channel, but not against attacks on or manipulations of the devices themselves. The devices could therefore output a key which the manufacturer had previously saved and might conceivably have forwarded to a hacker. With device- independent QKD (abbreviated to DIQKD), it is a different story. Here, the cryptographic protocol is independent of the device used. Theoretically known since the 1990s, this method has now been experimentally realized for the first time, by an international research group led by LMU physicist Harald Weinfurter and Charles Lim from the National University of Singapore (NUS).

For exchanging quantum mechanical keys, there are different approaches available. Either light signals are sent by the transmitter to the receiver, or entangled quantum systems are used. In the present experiment, the physicists used two quantum mechanically entangled rubidium atoms, situated in two laboratories located 400 meters from each other on the LMU campus. The two locations are connected via a fiber optic cable 700 meters in length, which runs beneath Geschwister Scholl Square in front of the main building.

To create an entanglement, first the scientists excite each of the atoms with a laser pulse. After this, the atoms spontaneously fall back into their ground state, each thereby emitting a photon. Due to the conservation of angular momentum, the spin of the atom is entangled with the polarization of its emitted photon. The two light particles travel along the fiber optic cable to a receiver station, where a joint measurement of the photons indicates an entanglement of the atomic quantum memories.

To exchange a key, Alice und Bob—as the two parties are usually dubbed by cryptographers—measure the quantum states of their respective atom. In each case, this is done randomly in two or four directions. If the directions correspond, the measurement results are identical on account of entanglement and can be used to generate a secret key. With the other measurement results, a so-called Bell inequality can be evaluated. Physicist John Stewart Bell originally developed these inequalities to test whether nature can be described with hidden variables. "It turned out that it cannot," says Weinfurter. In DIQKD, the test is used "specifically to ensure that there are no manipulations at the devices—that is to say, for example, that hidden measurement results have not been saved in the devices beforehand," explains Weinfurter.

In contrast to earlier approaches, the implemented protocol, which was developed by researchers at NUS, uses two measurement settings for key generation instead of one: "By introducing the additional setting for key generation, it becomes more difficult to intercept information, and therefore the protocol can tolerate more noise and generate secret keys even for lower-quality entangled states," says Charles Lim.

With conventional QKD methods, by contrast, security is guaranteed only when the quantum devices used have been characterized sufficiently well. "And so, users of such protocols have to rely on the specifications furnished by the QKD providers and trust that the device will not switch into another operating mode during the key distribution," explains Tim van Leent, one of the four lead authors of the paper alongside Wei Zhang and Kai Redeker. It has been known for at least a decade that older QKD devices could easily be hacked from outside, continues van Leent.

"With our method, we can now generate secret keys with uncharacterized and potentially untrustworthy devices," explains

Weinfurter. In fact, he had his doubts initially whether the experiment would work. But his team proved his misgivings were unfounded and significantly improved the quality of the experiment, as he happily admits. Alongside the cooperation project between LMU and NUS, another research group from the University of Oxford demonstrated the device-independent key distribution. To do this, the researchers used a system comprising two entangled ions in the same laboratory. "These two projects lay the foundation for future quantum networks, in which absolutely secure communication is possible between far distant locations," says Charles Lim.

One of the next goals is to expand the system to incorporate several entangled atom pairs. "This would allow many more entanglement states to be generated, which increases the data rate and ultimately the key security," says van Leent. In addition, the researchers would like to increase the range. In the present set-up, it was limited by the loss of around half the photons in the fiber between the laboratories. In other experiments, the researchers were able to transform the wavelength of the photons into a low-loss region suitable for telecommunications. In this way, for just a little extra noise, they managed to increase the range of the quantum network connection to 33 kilometers.

The research was published in *Nature*.

More information: Charles Lim, A device-independent quantum key distribution system for distant users, *Nature* (2022). DOI: 10.1038/s41586-022-04891-y.
www.nature.com/articles/s41586-022-04891-y

Provided by Ludwig Maximilian University of Munich