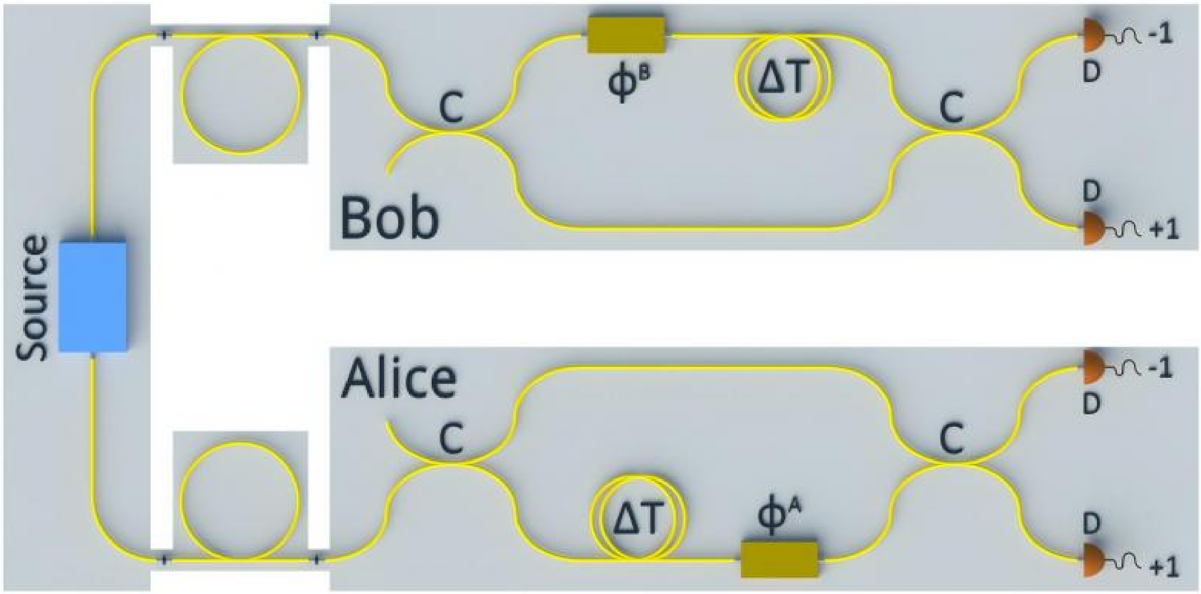
Some quantum cryptography systems vulnerable to hacking, study shows

December 18 2015



An experimental setup of the Franson interferometer. The setup consists of a source, 2 × 2 couplers (C), delay loops (ΔT), phase modulators ΦA and ΦB, and detectors (D). Credit: Jogenfors et al. Sci. Adv. 2015;1:e1500793

Quantum cryptography is considered a fully secure encryption method, but researchers from Linköping University and Stockholm University have discovered that this is not always the case. They found that energy-time entanglement - the method that today forms the basis for many systems of quantum cryptography - is vulnerable to attack. The results of their research have been published in *Science Advances*.

"With this security hole, it's possible to eavesdrop on traffic without being detected. We discovered this in our theoretical calculations, and our colleagues in Stockholm were subsequently able to demonstrate it experimentally," says Jan-Åke Larsson, professor at Linköping University's Division of Information Coding.

Quantum cryptography is considered a completely safe method for information transfer, and theoretically it should be impossible to crack. Many research groups around the world are working to make quantum cryptography resistant to various types of disturbance, and so far it has been possible to handle the disturbance that has been detected. Quantum cryptography technology is commercially available, but there is much doubt as to whether it is actually used.

"It's mostly rumours, I haven't seen any system in use. But I know that some universities have test networks for secure data transfer," says Prof Larsson.

The energy-time entanglement technology for quantum encryption studied here is based on testing the connection at the same time as the encryption key is created. Two photons are sent out at exactly the same time in different directions. At both ends of the connection is an interferometer where a small phase shift is added. This provides the interference that is used to compare similarities in the data from the two stations. If the photon stream is being eavesdropped there will be noise, and this can be revealed using a theorem from quantum mechanics - Bell's inequality.

On the other hand if the connection is secure and free from noise, you can use the remaining data, or photons, as an encryption key to protect your message.

What the LiU researchers Jan-Åke Larsson and his doctoral student Jonathan Jogenfors have revealed about energy-time entanglement is that if the photon source is replaced with a traditional light source, an eavesdropper can identify the key, the code string. Consequently they can also read the message without detection. The security test, which is based on Bell's inequality, does not react - even though an attack is underway.

Physicists at Stockholm University have subsequently been able to demonstrate in practical experiments that it is perfectly possible to replace the light source and thus also eavesdrop on the message.

But this problem can also be solved.

"In the article we propose a number of countermeasures, from simple technical solutions to rebuilding the entire machine," said Jonathan Jogenfors.

More information: Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution, *Science Advances* 18 Dec 2015: Vol. 1, no. 11, e1500793, dx.doi.org/10.1126/sciadv.1500793

Provided by Linköping University

Citation: Some quantum cryptography systems vulnerable to hacking, study shows (2015, December 18) retrieved 26 April 2024 from https://phys.org/news/2015-12-quantum-cryptography-vulnerable-hacking.html