Swiss scientists prove durability of quantum network

December 1 2011

Scientists and engineers have proven the worth of quantum cryptography in telecommunication networks by demonstrating its long-term effectiveness in a real-time network.

Their international network, created in collaboration with ID Quantique and installed in the Geneva metropolitan area and crossing over to the site of CERN in France, ran for more than one-and-a-half years from the end of March 2009 to the beginning of January 2011.

Published in the Institute of Physics and German Physical Society's New Journal of Physics, the researchers' study documents the longest ever deployment of a quantum key distribution (QKD) network and demonstrates its robustness and reliability when coupled with a real-time telecommunications network.

Cryptography—the practice of protecting information from third parties—has long been achieved by encrypting data with a set of complex mathematical algorithms; however, with the power of computers continuing to increase, it is becoming harder to make these algorithms watertight.

Physics has rather conveniently come up with a solution to this ever-growing problem through a process known as quantum key distribution (QKD). QKD is a process that enables two parties to share a secret key before using that key to protect data they want to send over a network.

The key that the two parties share is built up from a stream of photons—the basic unit of light. In a theoretical scenario where Alice and Bob want to protect a piece of information with a quantum key, Alice would send a stream of photons to Bob with each one having a specific orientation, called polarisation: photons can 'spin' vertically, horizontally and diagonally.

Bob would then attempt to measure the photons coming in by randomly choosing which direction to measure them in. Sometimes he will choose the correct orientation, other times he won't. Alice and Bob would then share the measurements using classical communication methods, simply stating if Bob was right or wrong, but not mentioning the actual direction the photons were spinning in.

Alice can then discard all of Bob's wrong measurements and use the correct ones to encrypt their secret data. The beauty of QKD is that if a potential eavesdropper wanted to get hold of this key, they would actually destroy the photons when trying to measure them. As a result, they would need to send their own stream of photons on to Bob to cover their tracks, but this would introduce errors and be discarded during key distillation.

QKD is not a new phenomenon and has already been used for a number of applications: notably by ID Quantique to protect the votes in Geneva's elections and in other commercial installations where high security is needed.

For QKD to become more widespread in the commercial world, its reliability needed to be thoroughly tested as these networks run constantly all year round. Furthermore, the robustness of the network needed to be demonstrated as the systems are being taken out of safeguarded laboratories and placed into more demanding environments.

Co-author of the study Dr Damien Stucki said: "This experiment is a big step in the direction of a wider deployment of QKD in telecommunications networks. From a scientific point of view, the deployment of the quantum layer over a duration of 21 months with high reliability is very significant.

"The SwissQuantum network was very reliable, with the only interruptions coming from external problems, such as power cuts and air conditioning problems, not the QKD layer."

More information: D Stucki et al 2011 *New J. Phys.* 13 123001 doi:10.1088/1367-2630/13/12/123001

Provided by Institute of Physics

Citation: Swiss scientists prove durability of quantum network (2011, December 1) retrieved 26 April 2024 from https://phys.org/news/2011-12-swiss-scientists-durability-quantum-network.html