Researchers unite to distribute quantum keys

July 2 2009

Researchers from across Europe have united to build the largest quantum key distribution network ever built. The efforts of 41 research and industrial organisations were realised as secure, quantum encrypted information was sent over an eight node, mesh network.

With an average link length of 20 to 30 kilometres, and the longest link being 83 kilometres, the researchers from organisations such as the AIT Austrian Institute of Technology (formerly Austrian Research Centers), id Quantique, Toshiba Research in the UK, Université de Genčve, the University of Vienna, CNRS, Thales, LMU Munich, Siemens, and many more have broken all previous records and taken another huge stride towards practical implementation of secure, quantum-encrypted communication networks.

A journal paper, 'The SECOQC Key Distribution Network in Vienna', published as part of IOP Publishing's *New Journal of Physics*' Focus Issue on 'Quantum Cryptography: Theory and Practice', illustrates the operation of the network and gives an initial estimate for transmission capacity (the maximum amount of keys that can be exchanged on a quantum key distribution, QKD, network).

Undertaken in late 2008, using the company internal glass fibre ring of Siemens and 4 of its dependencies across Vienna plus a repeater station, near St. Pölten in Lower Austria, the QKD demonstration involved secure telephone communication and video-conference as well as a rerouting experiment which demonstrated the functionality of the SEcure COmmunication network based on Quantum Cryptography

(SECOQC).

One of the first practical applications to emerge from advances in the sometimes baffling study of quantum mechanics, quantum cryptography has become a soon-to-be reached benchmark in secure communications.

Quantum mechanics describes the fundamental nature of matter at the atomic level and offers very intriguing, often counter-intuitive, explanations to help us understand the building blocks that construct the world around us. Quantum cryptography uses the quantum mechanical behaviour of photons, the fundamental particles of light, to enable highly secure transmission of data beyond that achievable by classical methods.

The photons themselves are used to distribute cryptographic key to access encrypted information, such as a highly sensitive transaction file that, say, a bank wishes to keep completely confidential, which can be sent along practical communication lines, made of fibre optics. Quantum indeterminacy, the quantum mechanics dictum which states that measuring an unknown quantum state will change it, means that the information cannot be accessed by a third party without corrupting it beyond recovery and therefore making the act of hacking futile.

The researchers write, "In our paper we have put forward, for the first time, a systematic design that allows unrestricted scalability and interoperability of QKD technologies."

More information: The SECOQC Quantum Key Distribution Network in Vienna" (Peev M et al 2009 *New J. Phys.* 11 075001, www.iop.org/EJ/volume/1367-2630/11

Source: Institute of Physics (news : web)