Siemens builds a lock made of light: Data transfer using quantum cryptography

August 1 2008

Foto: ARC

(PhysOrg.com) -- Electronic communication is becoming more secure all over the world. Siemens IT Solutions and Services, Austrian Research Centers (ARC) and Graz University of Technology have joined forces to develop the first quantum cryptography chip for commercial use. The chip, which protects data by generating a completely random sequence of numbers from particles of light, replaces the currently used system of key distribution based on mathematical algorithms.

The prototype of the quantum cryptography chip is already available, and the corresponding fiber-optic network for absolutely safe, chip-based data transfer will be presented in October 2008 at Siemens IT

Solutions and Services in Vienna.

This is how it works. Quantum cryptography works with individual light particles known as photons, which are generated and coded by an optical array. The security of the data is guaranteed by laws of nature, as photons generate completely random keys. The mathematical formulae used in the past, which could be decrypted with enough time and effort, will soon be a thing of the past.

Once the optical array has sent the light particles to the recipient via fiber-optic cable, each communication partner uses a detector to measure certain properties of the photons. The values are then compared using a communication protocol via the internet. If they match, the chip takes over the processing and uses the results of the measurements to generate a tap-proof key.

The message is not transferred until this key is in place. Any attempt to listen to a message when generating a key will be registered, as it will cause photons to be changed or destroyed. If the chip registers that someone is trying to listen in, it simply generates a new key. This process is repeated until it is absolutely certain that no one is listening in.

The keys are used immediately in the chip to encrypt or decrypt the data, and then they are deleted. At no time do they leave the chip. Effective though this procedure is, however, it will be another two years before it is ready for series production.

Provided by Siemens

cryptography.html