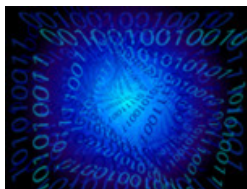




Quantum mechanics enables location-based cryptography

15-07-2010



Research of Serge Fehr of the Centrum Wiskunde & Informatica (CWI) in Amsterdam in collaboration with Nishanth Chandran, Ran Gelles and Rafail Ostrovsky from the University of California, Los Angeles (UCLA) and Vipul Goyal from Microsoft Research India, shows that quantum mechanics makes location-based cryptography possible. This new type of cryptography doesn't need the use of cryptographic keys. The results of the research will be presented in October 2010 at the Symposium on Foundations of Computer Science (FOCS 2010, Las Vegas, Nevada).

The goal of location-based cryptography is to let the geographical position of a person act as the key for accessing secured data and services. This has the important advantage that no cryptographic keys need to be distributed and locally stored, which is often the bottleneck in standard cryptographic solutions and offers additional room for attacks. All previous attempts for location-based cryptography showed inherent security weaknesses. The new approach circumvents these weaknesses by making use of quantum mechanical effects. The leading publication MIT Technology Review and Slashdot have reported on the research results.

An important component for location-based cryptography is secure location verification: a method to verify the geographical position of a person with the guarantee of not being deceived. For years, the wireless security community worked on the development of methods for location verification. It was assumed that the classical approach, based on triangulation offered a secure solution. However, cryptographers demonstrated last year that this approach cannot offer security against a coalition of dishonest persons that actively try to break the scheme.

The new research of Fehr and his colleagues shows that quantum mechanics can provide a secure solution for location verification. The approach is based on quantum bits, e.g. in the form of polarized photon. "Based on the 'no cloning principle' of quantum mechanics, which says that quantum particles cannot be copied, we proved that with this method deception about the location is impossible", says Fehr.

Besides location verification the research focuses on other location-based cryptographic tasks, like location-based secure communication. Fehr explains: "This is a method to communicate a secret message in a way that only the person at a specific location can read the message but an eavesdropper at a different location cannot get any information. In contrast to previous approaches, this method allows for secure communication without the need for distributing cryptographic keys."

The Cryptology group of CWI investigates fundamental cryptographic problems from a broad scientific perspective, especially from mathematics, computer science and physics.