World first for sending data using quantum cryptography

October 8 2008

A Computersimulation done by "Die Drahtwarenhandlung" of the Quantumcryptography-Network. Photo by Austrian Research Centers

(PhysOrg.com) -- For the first time the transmission of data secured by quantum cryptography is demonstrated within a commercial telecommunications network. 41 partners from 12 European countries, including academics from the University of Bristol, have worked on realising this quantum cryptographic network since April 2004.

Today [Wednesday 8 October] the first commercial communication network using unbreakable encryption based on quantum cryptography is demonstrated in Vienna, Austria. In particular the encryption utilises keys that are generated and distributed by means of quantum cryptographic technologies. Potential users of this network, such as government agencies, financial institutions or companies with distributed subsidiaries, can encrypt their confidential communication with the highest level of security using the quantum cryptographically generated keys.

The network consists of six nodes and eight intermediary links with distances between 6km and 82km (seven links utilising commercial standard telecommunication optical fibres and one “free-space”-link along a line of sight between two telescopes). The links employ altogether six different quantum cryptographic technologies for key generation which are integrated into the network over standardised interfaces.

The network is installed in a standard optical fibre communication ring provided by SECOQC partners, Siemens AG Österreich in Vienna. Five subsidiaries of Siemens are connected to the network. The operation of the quantum cryptographic network will be visualised on a screen at the Siemens Forum in Vienna and streamed live over the Internet. The network-wide key generation and distribution will be demonstrated, the different functionalities of the network itself will be presented as well as utilisation of the keys for standard communication applications. A voice-over-iptelephone-application will be secured by the information-theoretically secure "one-time-pad-encryption“ while videoconferencing will be protected by symmetrical AES-encryption with frequent key changes. A low-cost key distributor, with the potential of extending the quantum cryptographic network to the consumer, will also be shown.

Academics at Bristol University led by John Rarity, Professor of Optical Communication Systems in the Department of Electrical & Electronic Engineering, working on the project have developed a low cost free-space quantum cryptography system, complete with purpose-built software that can operate in daylight conditions.

The system is designed to eventually work in applications where a consumer can regularly ‘top up’ a store of secrets for use in a variety of one-time-pad (OTP) and authentication protocols. This system could allow online consumer transactions to be PIN protected for instance. The user would use secret bits shared with the bank to encode his PIN.

In the framework of the project intensive development of existing and novel quantum cryptographic technologies has allowed the production of high performance, stable and mobile quantum cryptographic devices packed into standard 19-inch boxes. Theses devices interoperate seamlessly over standardized interfaces. The technical descriptions of the different quantum cryptographic technologies used in the network can be found on the projects website at: www.secoqc.net/html/technology … blingtechnology.html

Advantages of Quantum Cryptography

Confidential communication needs encryption in order to ensure that no unauthorised party could misuse the content. Quantum cryptography provides long-term security and thus conforms to the requirements of a number of recent legal regulations for protecting information. Quantum cryptographic technologies provide information-theoretically secure keys for encryption.

The basic approach includes sending streams of specially prepared particles of light (photons), their measurement by the legitimate parties and the subsequent post-processing of the measurement data. The output is the cryptographic key consisting of identical random bit strings.

A potential eavesdropper cannot gain any information on this key irrespectively of his resources. This property which has no classical counterpart is due to the fundamental laws of quantum physics which ensure that any measurement leaves indelible traces behind. These traces manifest themselves in an error-rate that can be identified by the legitimate users.

There exists a quantitative relationship between the error-rate and rate of key generation: In case the error is below a certain upper bound, and therefore the eavesdroppers invention was sufficiently weak, the process of generating the cryptographic key is still possible with the same security standard but at a accordingly reduced rate. The latter gets equal to zero if the error-rate exceeds the bound.

Advantages of the quantum cryptographic network

Previous developments in quantum cryptography focused on point-to-point connections between only one sender and one receiver and commercial solutions are already available from several companies (including the SECOQC-Partner id Quantique SA).

Although these solutions are suitable for some applications such as connecting two data-centres in a metropolitan area, they cannot address all scenarios requiring secure communication. These limitations are related to a number of disadvantages of the point-to-point solutions: the maximum distance between sender and receiver is limited due to loss of photons in the optical fibre; the maximal speed of key generation is relatively low – it is comparable to that of a modem from the 1980's – and the communication can be interrupted by simply cutting the fibre or interfering with the line of sight (in case of a free-space application).

In a network, longer distances can be bridged and alternative paths between sender and receiver can automatically be chosen in order to increase key generation throughput or prevent denial-of-service-attacks even if a communication line is interrupted. Furthermore, in a network, more than two partners can simultaneously obtain keys for encrypting confidential communication. This development will open up the possibility for telecom operators to develop novel services and products based on quantum cryptography.

Provided by University of Bristol

Citation: World first for sending data using quantum cryptography (2008, October 8) retrieved 26 April 2024 from https://phys.org/news/2008-10-world-quantum-cryptography.html