SECOQC

Development of a Global Network for Secure
Communication based on Quantum Cryptography

World première in Vienna: Quantum Cryptography Secures Communication in a Commercial Network

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 have worked on realizing this quantum cryptographic network since April 2004. The overall objective is the integration of quantum cryptography into modern business applications. The work has been carried out within the Integrated EU-Project SECOQC (Development of a Global Network for Secure Communication Based on Quantum Cryptography), led by the Austrian Research Centers. The presentation of the quantum-cryptographic network marks the successful completion of the project after four and a half years.

Vienna, October 8, 2008. Today, the first commercial communication network using unbreakable encryption based on quantum cryptography is demonstrated in Vienna, Austria. In particular the encryption utilizes 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 utilizing 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 standardized 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 visualized on a screen at the Siemens Forum in Vienna and streamed live over the Internet (link: www.secoqc.net). The network-wide key generation and distribution will be demonstrated, the different functionalities of the network itself will be presented as well as utilization of the keys for standard communication applications. A voice-over-ip-telephone-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.

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:
http://www.secoqc.net/html/technology/enablingtechnology.html

Advantages of Quantum Cryptography

Confidential communication needs encryption in order to ensure that no unauthorized 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.

Integrating Quantum Cryptography in the business world

In the framework of the Integrated EU-Project SECOQC a „Business-White-Paper" has been prepared. It addresses the business advantages, as well as the limitations, of this provably secure technology in order to facilitate the decision making process on utilizing quantum cryptography for the benefit of public or private organisations. The Business-White-Paper will be presented at the international conference on quantum cryptography that takes place after the demonstration of the quantum cryptographic network. The Business-White-Paper can also be downloaded from the project website at: www.secoqc.net

International Conference on Quantum Cryptography in Vienna

The presentation of the quantum cryptographic network is part of an international conference on quantum cryptography in Vienna, Austria. Renowned experts from Europe, Japan, Singapore and the U.S. will present 35 talks and discuss the global trends of quantum cryptography. A high profile representative of the European Commission will talk on European strategies in this context. Furthermore, technical details of the quantum cryptographic network will be discussed and 45 scientists will present their work during a poster-session. Over 180 delegates from all over the world will participate in the conference.

Kick-off-meeting of the „ETSI Industry Specification Group"

In the framework of the conference the kick-off-meeting of the „Industry Specification Group on Quantum Key Distribution and Quantum Technologies" will take place. Under the direction of the European Telecommunication Standards Institute (ETSI) representatives of industries and future users will start to develop international standards for this new technology. This group is a result of the standardization initiatives started in the framework of the SECOQC – Standardization and Certification Subproject by the Austrian Research Centers and the University of Lausanne.

The Integrated EU-Project SECOQC, led by the Austrian Research Centers

In the Integrated EU-Project SECOQC the results of quantum cryptographic developments were combined with research in cryptography, network-technology, computer-techniques and business applications allowing the development of a fully integrated quantum cryptographic network which is demonstrated on October, 8 in Vienna.

This four and a half year project started in April 2004 and was funded by the EU with 11.4 million Euros.

Project Partners

A total of 41 participants from twelve countries (Austria, Belgium, Canada, Czech Republic, Denmark, France, Germany, Italy, Russia, Sweden, Switzerland and the U.K) were involved in the project.

The total list of the project partners can be found at: http://www.secoqc.net/html/project/partners.html

Pictures from the Event can be downloaded from:
http://www.secoqc.net/html/press/pressmedia.html

Contact: Mag.a Julia Petschinka, for the Austrian Research Centers | Quantum Technologies
Donau-City-Str. 1, 1220 Wien | Phone: +43 (0)699 11902509 | email: julia.petschinka@arcs.ac.at
Web: www.arcs.ac.at | Project website: www.secoqc.net

Supplement:
Key researchers in the SECOQC-Project
The project was divided into eight sub-projects, each of them covering one essential aspect and led by renowned key researchers.

Network Implementation

Momtchil Peev (Austria) | *Austrian Research Centers*

Quantum Information Theory

Norbert Lütkenhaus (Germany and Canada) | *University of Waterloo, Institute for Quantum Computing, Universität Erlangen-Nürnberg*

Quantum Cryptographic Technologies for Key Generation / Quantum Optics

Nicolas Gisin (Switzerland) | *University of Geneva*

Philippe Grangier (France) | *CNRS – Centre National de la Recherche Scientifique*

John Rarity (UK) | *University of Bristol*

Gregoire Ribordy (Switzerland) | *Id Quantique SA*

Andrew Shields (UK) | *Toshiba Research Europe Ltd*

Harald Weinfurter (Germany) | *Ludwig-Maximilian-Universität München*

Anton Zeilinger (Austria) | *Institute for Quantum Optics and Quantum Information IQOQI Vienna, Vienna University*

Development of Quantum Optical Components, i.e. Single-Photon Detectors

Sergio Cova (Italy) | *Politecnico di Milano*

Vincenzo Piazza (Italy) | *Scuola Normale Superiore*

Andrew Shields (UK) | *Toshiba Research Europe Ltd*

Network Architecture, Functionalities and Characteristics

Romain Alleaume (France) | *Telecom ParisTech*

Oliver Maurhart (Austria) | *Austrian Research Centers*

Michel Riguidel (France) | *Telecom ParisTech*

Standardisation and Certification

Solange Ghernaouti-Helie (Switzerland) | *University of Lausanne*

Thomas Länger (Austria) | *Austrian Research Centers*

System Integration

Thomas Lorünser (Austria) | *Austrian Research Centers*

Alexander Marhold (Austria) | *Bearingpoint Infonova*

Management of the project

Christian Monyk (Austria) | Austrian Research Centers

Industrial Partners
Biometrica (Russia), Hewlett Packard (UK), Id Quantique SA (Switzerland), Siemens AG Österreich (Austria), Siemens IT Services and Solutions (Germany), Thales Communications SA (France), Toshiba Research Ltd (UK).

The project website www.secoqc.net features in-depth information and coverage of the event:

- Link to the live-streaming of the presentation
- Business-White-Paper for downloading
- Description of different quantum cryptography-technologies integrated in the network
- Technical description of the network
- Information about the international conference and abstracts of the talks
- Details of the initiative for standardisation
- List of the project partners of SECOQC

SECOQC is an Integrated Project, 6th Framework Program of the European Union (Priority 2).
http://ec.europa.eu/research/fp6/index_en.cfm?p=0