European Scientists against Eavesdropping and Espionage

EU Project aimed at the development of an entirely secure communications network heralds a new era for computer network security

Vienna, 1 April 2004 The security of quantum cryptography is based upon laws of nature. However, asymmetrical encryption techniques that rely on difficult mathematical problems are still in use. Yet the replacement of this out-dated technology is near. Within four years, the cost-effective production of quantum key distribution shall start. A near-to-market prototype for encrypted connections between two points will be developed, as well as a high performance network infrastructure for spanning greater distances.

In order to achieve these ambitious goals, quantum physicists will co-operate with network specialists and experts in the fields of cryptography, electronics, IT security, and software development. The economical applicability and the integration into existing products will be secured by the complementary participation of economic experts and consultants.

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

Starting in April 2004, SECOQC is the first integrated project within the 6th Framework Programme of the EU initiated by an Austrian research centre. The project is managed by its co-ordinator, the business unit *Quantum Technologies* at ARC Seibersdorf Research GmbH.

"We will provide a tool, based on quantum technologies, which will enable economical enterprises to guard their assets against industrial espionage. In the past, significant financial losses due to industrial espionage had to be attributed to activities of the ECHELON communication surveillance and interception network. Our aim is to make a significant contribution to the independence and competitiveness of the European economy", says Dr Christian Monyk, head of the business unit *Quantum Technologies*, and also the initiator of the project.

Quantum Cryptography is the fundament for high-security communication networks

Quantum Cryptography (or, more accurately, the generation of encryption keys by means of quantum physical methods) yields solutions for two major problems of contemporary encryption systems. The first challenge is the generation of entirely random keys; the second is their secure transmission to the intended recipients. Another advantage is the technique's inherent capability to detect eavesdropping already while keys are generated. Therefore, the transmission of keys by an attacker is inhibited. Once a message has been encrypted with quantum generated keys it cannot be decrypted as a matter of principle. This is a tremendous advantage over traditional key distribution and asymmetrical encryption techniques.

SECOQC will lay the cornerstone for a global high-security communications network by advancing experimental quantum technology research and connecting it with cryptography, network technology, and other IT related disciplines

The project has a duration of four years and will be funded by the EU with 11.4 million Euros.

A total of 41 participants from twelve countries (Austria, Belgium, Canada, Czech Republic, Denmark, France, Germany, Italy, Russia, Sweden, Switzerland and the U.K) are involved in the project. This consortium consists of three SMEs, 25 Universities, five national research centres, and eight private enterprises.

Basic Research and Practical Applications join forces

The project is divided into eight sub-projects, each of them covering one essential aspect. After 18 months project duration the different quantum cryptographical methods will be assessed with regards to their technical and economical practicability.

“Both, the economic applicability and the fundamental research contributing to future technologies are equally important goals of the project”, says Dr Christian Monyk.

The business unit *Quantum Technologies* at ARC Seibersdorf’s research division “Information Technologies” was established in 2002 with the objective to accompany emerging future technologies in the field of quantum physics on their way to an economical realisation.

Contact details:

Mag[a] Julia Petschinka
ARC Seibersdorf research GmbH
Geschäftsbereich Informationstechnologien - Arbeitsgruppe Quantentechnologien
Projektkoordination und Öffentlichkeitsarbeit
TechGate Vienna
Donau-City Straße 1
1220 Wien
T: +43-050550-4161
M: +43-(0)664-8251064
E: Julia.Petschinka@arcs.ac.at