



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

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

Integriertes Projekt (IP) im sechsten Rahmenprogramm der EU mit dem Ziel, eine absolute sichere Kommunikationstechnologie zu entwickeln, basierend auf Quantenkryptographie.

Koordination: ARC Seibersdorf research GmbH - INFORMATIONSTECHNOLOGIEN

Globale Hochsicherheitskommunikation

SECOQC legt die Basis für ein hochsicheres, globales Kommunikationsnetzwerk. Im Rahmen des Projektes werden die Ergebnisse der quantenphysikalischen Grundlagenforschung weiterentwickelt und mit Komponenten aus der Kryptographie, Netzwerktechnologie und Computertechnik verbunden werden.

Quantenkryptographie wirtschaftlich einsetzbar machen

Ziel des Projektes ist es, die Quantenkryptographie nach Ablauf von 4 Jahren wirtschaftlich einsetzbar zu machen. Dazu gehört die Entwicklung:

- eines marktreifen Prototypen zur Nachrichtenverschlüsselung
- einer leistungsfähigen Netzwerkinfrastruktur, die den globalen Einsatz der Verschlüsselungsverfahren erlaubt

Quantenkryptographie bietet Lösungen für Probleme der heutigen Verschlüsselung

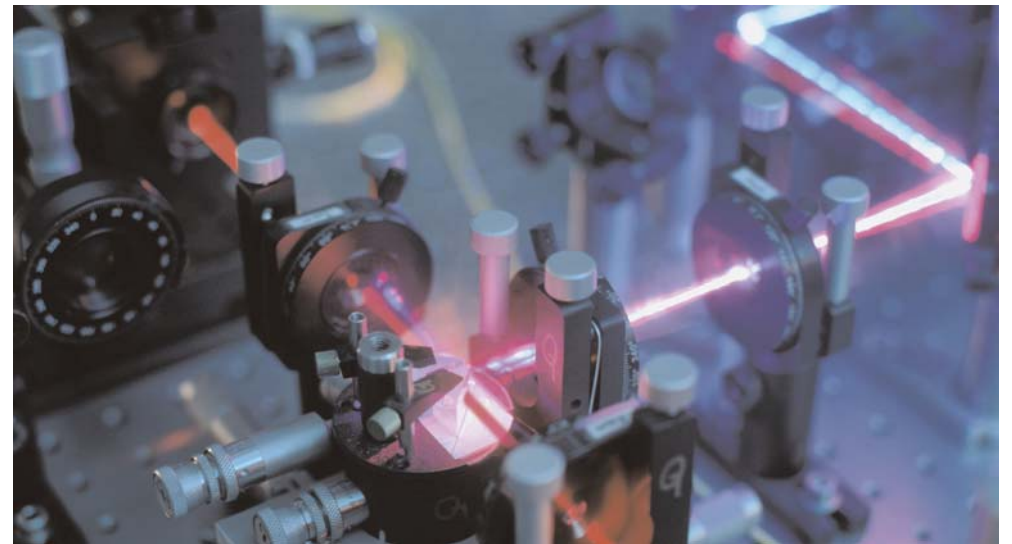
Unter Quantenkryptographie versteht man die Erzeugung eines Datenschlüssels zur Nachrichtenverschlüsselung mittels quantenphysikalischer Methoden. Ihre Sicherheit beruht auf Naturgesetzen und nicht auf schwer lösbaren mathematischen Problemen.

Sie bietet Lösungen für die:

- Erzeugung absolut zufälliger Datenschlüssel
- Übertragung der Schlüssel

Lauschen nicht möglich

Ein weiterer, ausschlaggebender Vorteil: ein möglicher Lauscher verfälscht unweigerlich das Signal und kann daran schon während der Schlüsselübertragung erkannt werden - also noch bevor mit der Übertragung der eigentlichen, verschlüsselten Nachricht begonnen wird.



Ein starkes österreichisches Team

Zusammen mit der Gruppe um Prof. Anton Zeilinger von der Universität Wien arbeitet das Geschäftsfeld Informationstechnologien an der Realisierung eines Quantenkryptographie-Prototypen (im Rahmen des FIT-IT Projektes PRODEQUAC, gefördert durch das BM:VIT).

Am 21. April 2004 wurde diese neue Sicherheitstechnologie eindrucksvoll präsentiert: Die weltweit erste quantenkryptographisch verschlüsselte Banküberweisung wurde zwischen dem Wiener Rathaus und einer Filiale der BA-CA übertragen.

Das herausragende Know-How im Bereich Quantenphysik kam von der Gruppe um Prof. Zeilinger, die Elektronik sowie die Implementierung der Verschlüsselungsprotokolle von ARC Seibersdorf research GmbH.

Factbox SECOQC

Integriertes Projekt im sechsten Rahmenprogramm der Europäischen Union

Kontakt: www.secoqc.net
www.quantenkryptographie.at
Dr. Christian Monyk,
Leiter des Geschäftsfelds "Quantum Technologies",
Kordinator von SECOQC
Christian.Monyk@arcs.ac.at

Start: April 2004

Dauer: 4 Jahre

Förderung: 11,4 Millionen Euro von EU

Koordination: ARC Seibersdorf research GmbH - INFORMATIONSTECHNOLOGIEN

Partner: 41 aus 12 Ländern (Österreich, Belgien, Kanada, Tschechische Republik, Dänemark, Frankreich, Deutschland, Italien, Russland, Schweden, Schweiz und Groß Britannien)
3 KMUs, 25 Universitäten, 5 nationale Forschungszentren, 8 private Firmen.

Unter den Partnern sind: Universität Wien (Prof. Anton Zeilinger), Siemens Austria, Toshiba Research Europe Limited, Ernst & Young sowie Ecole Nationale Supérieure des Télécommunications Paris.