

## **Wirtschaftsspionage ade!**

### **Präsentation eines Prototyps zum absolut sicheren Datenaustausch zwischen Unternehmensstandorten mittels Quantenkryptographie.**

**Wien, 6. Dezember 2004.** Der sichere Datenaustausch zwischen Unternehmensstandorten erfolgt meist über so genannte VPN-Tunnel (VPN steht für „virtual private network“). Dabei handelt es sich um verschlüsselte Verbindungen zwischen privaten und firmeninternen Netzwerken über das öffentliche, und damit unsichere, Internet. Für Hacker und Wirtschaftsspieler ist diese Verbindung eine potentielle und oft genutzte Angriffsfläche.

Der im Rahmen des FIT-IT Projekts PRODEQUAC entwickelte Prototyp bietet gegen Spione die entscheidende Hilfe: Sowohl durch seine Sicherheitsarchitektur als auch durch die neuartige Integration von Quantenkryptographie können nun jegliche Arten von sensiblen Daten bis hin zu IP-Telefongesprächen oder Videokonferenzen zwischen Unternehmensstandorten mit höchster Sicherheit ausgetauscht werden.

### **Das Projekt PRODEQUAC: Prototype Development for Quantum Cryptography**

Das Projekt PRODEQUAC („Prototype Development for Quantum Cryptography“) wurde im Herbst 2002 im Rahmen der Projektklinie „Embedded Systems“ des FIT-IT Programms des bmvit (Bundesministerium für Verkehr, Innovation und Technologie) gestartet.

Ziel des Projekts: die Technologie der Quantenkryptographie mit neuen Hardware- und Softwaresystemen und Sicherheitskonzepten zu verbinden, zu verkleinern und über einfache Schnittstellen den Einbau in bestehende IT-Infrastrukturen von Unternehmen zu ermöglichen.

### **Hardware-Firewall**

Der Prototyp wurde als so genannte Hardware-Firewall realisiert und besteht aus zwei voneinander getrennten Einschubkarten mit jeweils eigenem Betriebssystem. Dadurch ist die Trennung des internen Firmennetzes vom externen Internet auch physisch gewährleistet. Das Konzept verwirklicht die Kombination von neuen Sicherheitstechnologien und bekannten Strukturen in einem eigenen Gerät und erlaubt durch einfache Bedienung eine schnelle Integration in bestehende Systeme.

### **Verschlüsselungssysteme**

Die Quantenkryptographie bietet die Lösung für zwei fundamentale Probleme heutiger Verschlüsselungssysteme: Einerseits die Erzeugung sich niemals wiederholender Schlüssel durch die absolute Zufälligkeit als Grundmerkmal der Quantenphysik. Andererseits deren Verteilung an die beteiligten Partner, da die Schlüssel bei beiden gleichzeitig (in „real time“) erzeugt werden.

Die Schlüssel zur Datencodierung werden mit verschränkten Lichtteilchen erzeugt, wobei die Messung an einem Teilchen die Eigenschaften des zweiten beeinflusst - unabhängig von seiner Entfernung.

### **Datenrate: über 1 Megabit pro Sekunde**

Die quantenkryptographisch erzeugten Bitfolgen, welche zur Verschlüsselung der Daten über den VPN-Tunnel dienen, werden in einem optischen Aufbau erzeugt und im Prototyp gespeichert. Alle Daten, welche z.B. über einen VPN-Tunnel ausgetauscht werden, können automatisch über den PRODEQUAC-Prototypen verschlüsselt und mit einer Geschwindigkeit von mehr als 1 Megabit pro Sekunde übertragen werden. Damit sind IP-Telefonie und Webmeetings mit absoluter Abhörsicherheit und ohne Qualitätsverlust möglich.

## **Österreichische Teams**

Die Gruppe Quantentechnologien (Bereich Informationstechnologien) der ARC Seibersdorf research GmbH übernahm das Hardware- und Softwaredesign, die Implementierung und Entwicklung der Protokolle zur Erzeugung der Schlüssel, das Design der Sicherheitsarchitektur sowie die Projektleitung von PRODEQUAC.

Die Gruppe um Prof. Anton Zeilinger (Institut für Experimentalphysik der Universität Wien) hat ihr herausragendes Know How im Bereich der experimentellen Quantenphysik in die Entwicklung des Geräts eingebracht. Bereits 1998 hat sie zum weltweit ersten Mal die Quantenkryptographie mit verschränkten Lichtteilchen entwickelt und demonstriert.

Die Programm- und Systementwicklung PSE der Siemens AG Österreich zeichnet verantwortlich für das Design der Schnittstellen zwischen dem prototypischen Gerät und der bestehenden IT-Infrastruktur sowie für die Administration und das Management der Schlüssel, des VPN-Tunnels und des Interfaces.

FIT-IT ist eine Initiative des Bundesministeriums für Verkehr, Innovation und Technologie zur Förderung anspruchsvoller IT-Forschung in Österreich. Seit 2001 gibt es die Programmlinie „FIT-IT Embedded Systems“, welche einen Schwerpunkt in einem Bereich setzt, der zu den am stärksten wachsenden in der Informationstechnologie gehört.

PRODEQUAC wird zu Projektabschluss Mitte Dezember von einer internationalen Expertenrunde begutachtet. Der Projektstart war im September 2002, das Projektvolumen betrug etwa 700.000 Euro.

### **Kontakt:**

Mag. Julia Petschinka  
ARC Seibersdorf research GmbH  
Bereich Informationstechnologien – Gruppe Quantentechnologien  
Tech Gate Vienna,  
Donau-City Straße 1, 4.OG,  
1220 Wien

Tel: +43-(0)664 8251064

Mail: [Julia.Petschinka@arcs.ac.at](mailto:Julia.Petschinka@arcs.ac.at)

Web: [www.quantenkryptographie.at](http://www.quantenkryptographie.at)