

Europas Forscher gegen Lauschangriffe

EU-Projekt zur Entwicklung eines absolut sicheren Netzwerks zur Nachrichtenübertragung – basierend auf Quantenkryptographie – läutet neue Ära der Datensicherheit ein.

Wien, 1. April 2004. Die Sicherheit der Quantenkryptographie beruht auf Naturgesetzen und nicht auf schwer lösbaren mathematischen Problemen, wie bei den heute eingesetzten Methoden. Ziel dieses einzigartigen Projekts ist es, das Verfahren der Quantenkryptographie nach Ablauf von vier Jahren wirtschaftlich einsetzbar zu machen. Dazu gehört die Entwicklung eines marktreifen Prototypen zur Nachrichtenverschlüsselung ebenso wie eine leistungsfähige Netzwerk-Infrastruktur, die den globalen Einsatz dieser Verschlüsselungsverfahren erlaubt.

Experten der Quantenphysik arbeiten zusammen mit Netzwerkspezialisten, sowie mit Koryphäen aus den Bereichen Kryptographie, Elektronik, Sicherheitstechnik und Softwareentwicklung. Wirtschaftsexperten ergänzen das Team.

„SECOQC – Development of a Global Network for Secure Communication based on Quantum Cryptography“.

Dieser kryptische Name bedeutet: Entwicklung eines globalen Netzwerkes zur sicheren Kommunikation basierend auf Quantenkryptographie. Das erste integrierte Projekt (IP) im sechsten Rahmenprogramm der EU unter österreichischer Leitung startet heute. Das europäische Forschungs- und Entwicklungsprojekt wird koordiniert von der Arbeitsgruppe Quantentechnologien des Geschäftsbereichs Informationstechnologien der ARC Seibersdorf research GmbH.

„Wir stellen der Wirtschaft ein Werkzeug zur Verfügung, das auf Technologien der Quantenphysik beruht, um sich gegen Spionagetätigkeiten zu schützen. Wirtschaftsspionage wird unter anderem vom weltweiten Überwachungsnetzwerk ECHELON betrieben, das in der Vergangenheit großen Schaden angerichtet hat. Durch das Projekt leisten wir einen wesentlichen Beitrag zur Unabhängigkeit der europäischen Wirtschaft.“ erklärt Dr. Christian Monyk, Leiter der Arbeitsgruppe Quantentechnologien und Initiator des Projekts.

Quantenkryptographie als Basis für ein hochsicheres Kommunikationsnetzwerk

Die Quantenkryptographie, also die Erzeugung von Datenschlüssel zur Nachrichtenverschlüsselung mittels quantenphysikalischer Methoden, bietet Lösungen für zwei Probleme der heute gängigen Verschlüsselungssysteme: Die Erzeugung absolut zufälliger Schlüssel und deren Übermittlung. Ein weiterer Vorteil dieses Verfahrens: Ein Lauscher kann schon während der Schlüsselerzeugung erkannt werden, also noch vor der Übertragung der Nachricht. Somit kann im schlechtesten Fall das Übertragen der Nachricht verhindert werden. Ist die Nachricht aber einmal mit diesem Verfahren verschlüsselt worden, kann der Inhalt von Lauschern prinzipiell nicht mehr ermittelt werden – ein wesentlicher Vorteil gegenüber derzeitigen Verschlüsselungsverfahren.

Durch dieses Projekt wird die Basis für ein hochsicheres Kommunikationsnetzwerk gelegt, in dem Ergebnisse der quantenphysikalischen Grundlagenforschung weiterentwickelt und mit Komponenten aus der Kryptographie, Netzwerktechnologie und Computertechnik verbunden werden.

Österreichs Forscher und Unternehmer beteiligen sich an dem Projekt

Österreich liegt mit seiner Forschung dank der herausragenden Leistung der Gruppe um Prof. Anton Zeilinger (Institut für Experimentalphysik der Universität Wien) im internationalen Spitzenfeld. Gemeinsam mit ihren europäischen Kollegen aus dem Bereich der Quantenphysik ist die Gruppe Zeilinger für die Weiterentwicklung der physikalischen Methoden der Quantenkryptographie im Rahmen des Projekts SECOQC verantwortlich.

Die Siemens AG Österreich (PSE), sowie weitere österreichische Partner, beteiligen sich an dem Projekt mit der Integration der Quantenkryptographie in gängige IT-Infrastrukturen.

Das Projekt hat eine Laufzeit von 4 Jahren und wird von der EU mit 11,4 Millionen Euro gefördert.

Insgesamt beteiligen sich 41 Partner aus 12 Ländern (Österreich, Belgien, Schweiz, Tschechische Republik, Deutschland, Dänemark, Frankreich, Großbritannien, Italien, Russland, Schweden, Kanada), davon 3 KMUs, 25 Universitäten, 5 Forschungseinrichtungen und 8 private Firmen.

Grundlagenforschung und Anwendung unter einem Hut

Das Projekt ist in acht Subprojekte gegliedert, von denen jedes einen wesentlichen Aspekt behandelt. Nach einer Laufzeit von 18 Monaten erfolgt eine Evaluierungsphase, in der die verschiedenen Methoden der Quantenkryptographie auf ihre wirtschaftliche Umsetzbarkeit untersucht werden.

„Der wirtschaftlich verwertbare Anteil der Quantenkryptographie ist gleichwertiges Ziel des Projekts sowie auch die Grundlagenforschung, welche einen wesentlichen Beitrag für zukünftige Technologien leistet.“, so Dr. Christian Monyk.

Die Arbeitsgruppe Quantentechnologien des Bereichs Informationstechnologien von ARC Seibersdorf research GmbH wurde im Jahr 2002 mit dem Ziel gegründet, die Zukunftstechnologien der Quantenphysik auf ihrem Weg zur wirtschaftlichen Umsetzung zu begleiten. Ein erfolgreicher Schritt ist der Start des EU-Projektes SECOQC. Für die Organisation des EU-Projekts hat die Arbeitsgruppe im Dezember 2003 den ersten Preis der ARC-Awards für Forschungsmanagement gewonnen.

Kontakt:

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