

Quantenverschlüsselung im Wiener Siemens-Netz

Die Ergebnisse des europäischen Projekts SECOQC zur Entwicklung eines Quantenkryptographie-Netzes werden 2008 in Wien präsentiert

Wien, 6. Februar 2007. Für die Präsentation des weltweit ersten integrierten Quantenkryptographie-Netzwerks werden Teile der bestehenden Glasfaser-Infrastruktur von Siemens verwendet. Darauf haben sich die Projektpartner des europäischen Projekts SECOQC (Development of a global network for secure communication based on quantum cryptography) bei ihrem Treffen in Genf Mitte Jänner geeinigt. Die Präsentation wird im September 2008 in Wien stattfinden. Das Netzwerk ermöglicht die Erzeugung und Weiterreichung von Schlüsseln und könnte in Zukunft etwa Filialen von großen Firmen mit bisher nicht erreichbarer Sicherheit miteinander verbinden.

Die Arbeit im Projekt SECOQC erfolgt in zwei Teilen, von denen einer die quantenphysikalischen Geräte zur Schlüsselerzeugung abdeckt, der andere das neuartige Design und den Aufbau der Infrastruktur. Darüber hinaus bildet auch die Zertifizierung der Geräte und Infrastrukturen einen wesentlichen Teil des Projekts, das von der Gruppe Quantentechnologien der Austrian Research Centers GmbH – ARC geleitet wird. Projektstart war im April 2004.

Während die Elite der europäischen Quantenforscher an der Erzeugung von Schlüsseln mit Hilfe von Lichtteilchen arbeitet (darunter auch die Gruppe um Prof. Anton Zeilinger von der Universität Wien), erfolgt die Entwicklung des Netzes sowie der Soft- und Hardware durch die Gruppe Quantentechnologien der ARC. Die Programm- und Systementwicklung PSE der Siemens AG Österreich beschäftigt sich mit der Integration der Quantenkryptographie in bestehende Infrastrukturen.

Quantenkryptographie zur Erzeugung von Schlüssel

Die Quantenkryptographie ermöglicht die Erzeugung von identischen Schlüsseln zwischen zwei Partnern zur sicheren Nachrichtenübertragung. Sie nutzt besondere Eigenschaften der Quantenphysik aus: Die Schlüssel entstehen aus einzelnen Lichtteilchen die zwischen den Partnern ausgetauscht werden. Jede Messung an einem Lichtteilchen hinterlässt eindeutige Spuren. Daher können Lauscher sofort entdeckt werden, da sie die Fehlerrate der ausgetauschten Lichtteilchen deutlich erhöhen – eine Voraussetzung zur sicheren Verteilung der Schlüssel.

Die Schlüssel werden im Netzwerk weitergereicht

Das Besondere an diesem Quantenkryptographie-Netzwerk ist die Erzeugung und Weiterreichung von Schlüsseln. Ohne Netzwerk sind die Entfernungen zwischen den Partnern limitiert, da Lichtteilchen nicht beliebig weit übertragen werden können aufgrund von Absorption. Durch die Weiterreichung von Schlüsseln im Netzwerk wird dieses Problem gelöst. Außerdem ist es durch standardisierte Schnittstellen möglich, verschiedene Technologien in das Netzwerk zu integrieren.

Netzwerk in Wien: Fünf Knotenpunkte mit sieben Verbindungen

Das Quantennetzwerk des Projekts SECOQC, wie es in Wien demonstriert werden wird, besteht aus fünf Knotenpunkten, die über herkömmliche Glasfaserkabel miteinander verbunden sind. Insgesamt gibt es sieben solcher Links, deren Länge

zwischen 6km und 85km beträgt. In jedem Knotenpunkt befinden sich Module zur Schlüsselerzeugung (mittels Quantentechnologie) sowie weitere Module zur Verschlüsselung, Entschlüsselung und Weiterreichung von Schlüsseln.

Verbindungen durch Verschlüsselungen abgesichert

Zwischen zwei Partnern im Netzwerk werden Schlüssel mittels quantenphysikalischen Methoden erzeugt. Schlüssel, die im Netzwerk weitergereicht werden sollen, werden wie hochsensible Daten behandelt, die selbst wieder verschlüsselt werden müssen. Dadurch sind die Strecken zwischen den einzelnen Netzwerk-Knoten abgesichert. Damit an den Knotenpunkten keine Lauscher Informationen abfangen können, müssen die Knoten vertrauenswürdige Einrichtungen sein, wie etwa Zweigstellen einer Firma.

Projektdaten: Laufzeit, Partner, Budget

Das Projekt hat eine Laufzeit von vier Jahren und wird von der EU mit 11,4 Millionen Euro gefördert. Projektstart war im April 2004. Insgesamt beteiligen sich 41 Teilnehmer aus zwölf Ländern (Österreich, Belgien, Kanada, Tschechische Republik, Dänemark, Frankreich, Deutschland, Italien, Russland, Schweden, Schweiz und Großbritannien). Das Konsortium besteht aus drei KMUs, 25 Universitäten, fünf nationalen Forschungszentren und acht Privatunternehmen. Website des Projekts: www.secoqc.net

Kontakt ARC

Mag. Julia Petschinka
Austrian Research Centers GmbH – ARC
Bereich smart systems

Projektkoordination und Kommunikation der Gruppe Quantentechnologien
Tech Gate Tower Vienna
Donaucity Straße 1/3.OG
1220 Wien

Tel: 0664 8251064

Email: julia.petschinka@arcs.ac.at

Web: www.secoqc.net und www.smart-systems.at und www.quantenkryptographie.at

Kontakt Siemens

Sylvia Schwarz
Siemens AG Österreich
Corporate Communications

Siemensstraße 92
1210 Wien

Tel.: 051707 24045

E-Mail: sylvia.schwarz@siemens.com

Web: www.siemens.at