



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

Weltpremiere in Wien: Sichere Kommunikation in handelsüblichen Glasfasernetzen dank Quantenkryptographie

Zum ersten Mal werden Daten in einem handelsüblichen Telekommunikations-Netzwerk mittels Quantenkryptographie abgesichert. 41 Partner aus 12 Ländern arbeiteten seit April 2004 unter der Leitung der Austrian Research Centers im Projekt SECOQC („Development of a Global Network for Secure Communication Based on Quantum Cryptography“) an diesem prototypischen Netzwerk und der möglichen wirtschaftlichen Einsetzbarkeit von Quantenkryptographie.

Das Projekt wird heute im Rahmen einer Pressekonferenz vom Wiener Bürgermeister Dr. Michael Häupl gemeinsam mit Brigitte Ederer, CEO der Siemens AG Österreich, Prof. Anton Zeilinger von der Universität Wien sowie dem Projektleiter Dr. Christian Monyk von den Austrian Research Centers präsentiert. Im Anschluss daran findet die Live-Demonstration des Quantenkryptographie-Netzwerks im Siemens Forum in Wien statt. Die Veranstaltung wird als Live-Stream im Internet übertragen (Link: www.secoqc.net).

Wien, 8. Oktober 2008. Heute wird in Wien das erste handelsübliche Kommunikationsnetzwerk präsentiert, in dem vertrauliche Nachrichten mit Hilfe von Quantenkryptographie verschlüsselt werden. Die Gesetze der Quantenphysik ermöglichen dabei die sichere Erzeugung und Weiterleitung von Datenschlüsseln, die zur Verschlüsselung vertraulicher Kommunikation mit der höchstmöglichen Sicherheit verwendet werden können. Potenzielle Kunden für so ein Netzwerk sind alle, die vertrauliche Informationen vor dem Zugriff unautorisierter Dritter schützen wollen, wie etwa Regierungsstellen, Finanzinstitutionen oder Firmen mit mehreren Standorten.

Der Netzwerk-Prototyp besteht aus sechs Knotenpunkten, die mit acht Links verbunden sind (sieben Glasfaserkabel zwischen 6km und 85km Länge, ein so genannter „free-space Link“ mit direkter Sichtverbindung zwischen zwei Teleskopen). Insgesamt sind sechs unterschiedliche Quantenkryptographie-Technologien zur Erzeugung der Schlüssel über standardisierte Schnittstellen im Netzwerk integriert. Sie unterscheiden sich durch die Methode, wie aus Lichtteilchen Datenschlüssel erzeugt werden. Die unterschiedlichen Technologien sind auf der Internetseite des Projekts SECOQC beschrieben: <http://www.secoqc.net/html/technology/enablingtechnology.html>

Das Netzwerk ist für die Präsentation im von der Siemens AG Österreich bereitgestellten Glasfasernetz installiert, insgesamt sind fünf Siemens-Standorte miteinander verbunden. Der Einsatz des Netzwerks wird auf einer Großbildleinwand im Siemens Forum in Wien gezeigt und live über das Internet gestreamt (Link: www.secoqc.net). Die Erzeugung und Weiterreichung der Datenschlüssel im Netzwerk sowie deren Einsatz für sichere Kommunikation wird demonstriert, genauso wie die verschiedenen Funktionalitäten des Netzwerks selbst.

Telefonate und Videokonferenz mit Quantenschlüssel sicher gemacht

Zur Demonstration werden Voice-over-IP-Telefonate mittels „one-time-pad“-Verfahren verschlüsselt. Das ist die einzige Methode, die absolut abhörsichere Kommunikation garantiert – daher ist sie auch am aufwändigsten und benötigt Datenschlüssel, die genauso lange sind, wie die vertrauliche Nachricht, die man damit verschlüsseln will. Außerdem wird während der Demonstration eine Videokonferenz zwischen mehreren Knotenpunkten im Netzwerk mit der symmetrischen AES-Verschlüsselung abgesichert, für die laufend neue Datenschlüssel generiert werden. Wie potenzielle Anwender die Schlüssel aus dem Netzwerk beziehen können, zeigt ein sogenannter „Schlüsselverteiler“, der im Rahmen der Präsentation gezeigt wird.

Durch die intensive Weiterentwicklung bereits bestehender sowie komplett neuer Quantenkryptographie-Technologien im Rahmen des EU-Projekts SECOQC war es möglich, in das Glasfasernetzwerk Geräte zu integrieren, die stabil laufen, hohe Datenraten erzeugen und leicht transportiert werden können.

Schlüsselerzeugung mittels Quantenphysik: keine Chance für Lauscher

Um sicher zu gehen, dass vertrauliche Kommunikation nicht von unautorisierten Dritten angezapft wird, muss man verschlüsseln. Mittels Quantenkryptographie können Schlüssel erzeugt und verteilt werden – eine wesentliche Voraussetzung für die Verschlüsselung vertraulicher Informationen. Die Quantenkryptographie bietet eine langfristige Sicherheit und liefert die Voraussetzung für die Einhaltung einer Reihe an gesetzlichen Bestimmungen für geschützte Information.

Für die Erzeugung der Datenschlüssel werden einzelne Lichtteilchen speziell präpariert und zwischen Partnern im Netzwerk ausgetauscht. Nach der Messung der Lichtteilchen werden die Messergebnisse nachbearbeitet. Das Resultat: alle Partner, die an der vertraulichen Kommunikation beteiligt sind, haben identische Datenschlüssel bestehend aus einer zufälligen Abfolge von Nullen und Einsen.

Ein möglicher Lauscher kann prinzipiell keine Information über diesen Datenschlüssel bekommen – egal welche erdenklichen Möglichkeiten er zur Verfügung hat. Dafür sorgen die Gesetze der Quantenphysik, wo jede Messung dauerhafte Spuren hinterlässt. Während die Messung der Lichtteilchen durch die Partner im Netzwerk beabsichtigt ist, manifestiert sich eine Messung eines Lauschers in einer Fehlerrate im System, die von den Kommunikationspartnern bemerkt wird.

Es gibt einen quantitativen Zusammenhang zwischen der Fehlerrate des Lauschers und der Menge an Datenschlüssel, die übertragen werden kann. Ist die Fehlerrate unter einem Schwellenwert, bedeutet dies: der Angriff des Lauschers war zu schwach, um das System empfindlich zu stören – es kann aber trotzdem der für die Verschlüsselung notwendige Datenschlüssel erzeugt und verteilt werden, aber mit geringerer Geschwindigkeit. Der Lauscher hat durch seinen schwachen Angriff nichts an der Sicherheit im System geändert. Ist die Fehlerrate durch einen Angriff des Lauschers über einem gewissen Schwellenwert, kann kein Datenschlüssel mehr erzeugt und verteilt werden.

In einem Netzwerk mit nur einer Verbindungslinie würde das eine komplette Unterbrechung der Schlüsselerzeugung bedeuten. Gibt es in einem Netzwerk aber mehrere Verbindungen zwischen den Partnern wird auf andere ausgewichen und die Schlüsselverteilung ist nicht unterbrochen.

Vorteile eines Quantenkryptographie-Netzwerks

Bisherige Entwicklungen der Quantenkryptographie konzentrierten sich auf die Kommunikation zwischen zwei Partnern mit nur einer Verbindungslinie. Dazu gibt es bereits mehrere kommerzielle Produkte auf dem Markt (eines davon vom Schweizer SECOQC-Projektpartner id Quantique SA).

Für ausgewählte Szenarien, wie etwa die Verbindung zweier Datenzentren in einer Stadt, reichen diese Punkt-zu-Punkt-Lösungen aus. Sie können aber einige Anforderungen an sichere Kommunikation aufgrund prinzipieller Limitierungen nicht erfüllen: Die maximale Distanz zwischen den beiden Partnern in einer Punkt-zu-Punkt-Verbindung ist wegen der Absorption von Lichtteilchen in Glasfaserleitungen auf etwa 100 Kilometer beschränkt, die Rate der Schlüsselerzeugung ist relativ gering – vergleichbar mit einem Modem aus den 1980er Jahren – und ein Zerstören der Verbindungslinie bedeutet den kompletten Abbruch der Kommunikation.

In einem Netzwerk können automatisch alternative Verbindungswege zwischen Partnern gewählt werden, sollte aufgrund eines Lauschers in einer Verbindungslinie die Erzeugungsrate der Schlüssel zu gering oder die Linie komplett unterbrochen oder kaputt sein.

Ein weiterer Vorteil des Netzwerks: mehrere Partner können gleichzeitig Datenschlüssel für ihre vertrauliche Kommunikation erzeugen – eine Voraussetzung etwa für Videokonferenzen mit mehr als nur zwei Teilnehmern.

Die Entwicklung des Quantenkryptographie-Netzwerks eröffnet zum Beispiel Betreibern von Telekommunikations-Infrastrukturen die Möglichkeit, neue Services und Produkte basierend auf Quantenkryptographie anzubieten.

Weißbuch über die Wirtschaftliche Anwendbarkeit von Quantenkryptographie

Im Rahmen des EU-Projekts SECOQC wurde ein "Business-white-paper" vorbereitet, das die wirtschaftlichen Vorteile genauso wie die Grenzen dieser beweisbar sicheren Technologie aufzeigt. Das Weißbuch zur Quantenkryptographie bietet eine Entscheidungshilfe für den Einsatz von Quantenkryptographie in öffentlich-rechtlichen und privaten Organisationen.

Das Weißbuch wird im Rahmen einer internationalen Konferenz über Quantenkryptographie in Wien,

die im Anschluss an die Netzwerkpräsentation stattfindet, vorgestellt und kann auch von der Internetseite des EU-Projekts SECOQC heruntergeladen werden. Link: www.secoqc.net

Internationale Konferenz über Quantenkryptographie in Wien

Die Präsentation des Quantenkryptographie-Netzwerks ist der Start einer internationalen Konferenz über Quantenkryptographie in Wien. Renommierete Experten aus Europa, Japan, Singapur und den USA werden über die weltweiten Trends dieser Technologie diskutieren. Ein hoher Repräsentant der Europäischen Kommission wird über europäische Strategien in diesem Zusammenhang sprechen. Außerdem werden technische Details des Quantenkryptographie-Netzwerks erläutert und junge Wissenschaftler bekommen die Möglichkeit, im Rahmen einer Postersession ihre Arbeit zu präsentieren. Insgesamt nehmen an dieser Konferenz über 180 Besucher teil.

Standards für Quantentechnologien: Start der "ETSI – Industry Specification Group"

Am 9. Oktober findet während der Konferenz das Kick-off-Meeting der „Industry Specification Group on Quantum Key Distribution and Quantum Technologies“ statt. Unter der Leitung der Europäischen Standardisierungsbehörde ETSI (European Telecommunication Standards Institute) beginnen Vertreter von Industrie sowie mögliche zukünftige Anwender der Quantenkryptographie international gültige Standards zu entwickeln, die eine wirtschaftliche Einsetzbarkeit wesentlich erleichtern würden.

Bereits im Rahmen des EU-Projekts SECOQC wurde von den Austrian Research Centers und der Universität von Lausanne intensiv an der Standardisierung und Zertifizierung von Quantenkryptographie gearbeitet. Die neu gegründete Arbeitsgruppe der ETSI geht auf diese Initiative zurück.

Das EU-Projekt SECOQC unter der Leitung der Austrian Research Centers: Daten und Fakten

Im Integrierten EU-Projekt SECOQC (das steht für "Development of a Global Network for **Secure Communication Based on Quantum Cryptography**") wurden erstmals Ergebnisse der Quantenphysik mit Forschungen in den Bereichen Kryptographie, Netzwerk- und Computertechnologien sowie mit Anforderungen an wirtschaftliche Einsetzbarkeit kombiniert.

Das Projekt startete im April 2004, hatte eine Laufzeit von viereinhalb Jahren und wurde von der EU mit 11,4 Millionen Euro unterstützt.

Projektpartner

Insgesamt waren 41 Partner aus 12 Ländern beteiligt: Belgien, Dänemark, Deutschland, England, Frankreich, Italien, Kanada, Österreich, Russland, Schweden, Schweiz, Tschechische Republik.

Die Liste der Projektpartner gibt es unter: <http://www.secoqc.net/html/project/partners.html>

Fotos der Pressekonferenz und Demonstration können sie hier herunterladen

<http://www.secoqc.net/html/press/pressmedia.html>

Kontakt/Rückfragen: Mag.a Julia Petschinka, Austrian Research Centers | Quantentechnologien
Donau-City-Str. 1, 1220 Wien | Telefon: +43 (0)699 11902509 | email: julia.petschinka@arcs.ac.at
Web: www.arcs.ac.at | Projekt SECOQC im Internet: www.secoqc.net

Anhang:

Leiter der SECOQC-Subprojekte

Das EU-Projekt SECOQC war in acht Sub-Projekte geteilt, die von renommierten Wissenschaftlern geleitet wurden.

- Gesamtprojektleitung

Christian Monyk (Österreich) | *Austrian Research Centers*

- Netzwerkimplementierung – Zusammenführen der Systeme zu einem Netzwerk

Momtchil Peev (Österreich) | *Austrian Research Centers*

- Quanteninformationstheorie – Beweise für Quantenkryptographie

Norbert Lütkenhaus (Deutschland und Kanada) | *University of Waterloo, Institute for Quantum Computing (Kanada), Universität Erlangen-Nürnberg*

- Quantenkryptographie-Systeme (Quantenoptik, Erzeugung der Datenschlüssel mittels Quantenphysik)

Nicolas Gisin (Schweiz) | *University of Geneva*

Philippe Grangier (Frankreich) | *CNRS – Centre National de la Recherche Scientifique*

John Rarity (UK) | *University of Bristol*

Gregoire Ribordy (Schweiz) | *Id Quantique SA*

Andrew Shields (UK) | *Toshiba Research Europe Ltd*

Harald Weinfurter (Deutschland) | *Ludwig-Maximilian-Universität München*

Anton Zeilinger (Österreich) | *Institut für Quantenoptik und Quanteninformation IQOQI Wien und Universität Wien*

- Entwicklung von Komponenten, wie zB Detektoren für einzelne Lichtteilchen

Sergio Cova (Italien) | *Politecnico di Milano*

Vincenzo Piazza (Italien) | *Scuola Normale Superiore*

Andrew Shields (UK) | *Toshiba Research Europe Ltd*

- Netzwerkarchitektur – Funktionalität und Eigenschaft des Netzwerks

Romain Alleaume (France) | *Telecom ParisTech*

Oliver Maurhart (Österreich) | *Austrian Research Centers*

Michel Riguidel (Frankreich) | *Telecom ParisTech*

- Zertifizierung, Standardisierung, Business-White-Paper

Solange Ghernaoui-Helie (Schweiz) | *University of Lausanne*

Thomas Länger (Österreich) | *Austrian Research Centers*

- System Integration

Thomas Lorünser (Österreich) | *Austrian Research Centers*

Alexander Marhold (Österreich) | *Bearingpoint Infonova*

Die im Projekt beteiligten Industriepartner:

Biometrica (Russland), Hewlett Packard (Großbritannien), Id Quantique SA (Schweiz), Siemens AG Österreich (Österreich), Siemens IT Services and Solutions (Deutschland), Thales Communications SA (Frankreich), Toshiba Research Ltd (Großbritannien).

Die Webseite des Projekts www.secoqc.net enthält ausführliche Informationen über:

- Link zum live-streaming des Events
- Weißbuch Quantenkryptographie zum Herunterladen
- Beschreibung der sechs verschiedenen Technologien der Quantenkryptographie, die im Netzwerk implementiert sind
- Technische Beschreibung des Netzwerks
- Informationen über die internationale Konferenz und Zusammenfassungen der Vorträge
- Details über die Standardisierungs-Initiative und die Arbeitsgruppe der ETSI
- Liste der Projektpartner

SECOQC ist ein integriertes Projekt innerhalb des 6. EU-Forschungsrahmenprogrammes

http://ec.europa.eu/research/fp6/index_en.cfm?p=0 Priorität [2] der Europäischen Union. Das Projekt wurde von der EU mit 11,4 Millionen Euro finanziert.

