

Wien, 21. April 2004

## **Weltweit erste Banküberweisung quantenkryptographisch verschlüsselt**

**Gemeinsames Experiment der Gruppe um Prof. Anton Zeilinger der Universität Wien,  
ARC Seibersdorf research GmbH, Stadt Wien, Wien Kanal Abwassertechnologien  
GmbH und BA-CA**

Die Bank Austria Creditanstalt (BA-CA) hat heute im Auftrag der Stadt Wien die weltweit erste quantenkryptographisch verschlüsselte Überweisung durchgeführt.

Die neue Sicherheitstechnologie wurde demonstriert von der Gruppe um Prof. Anton Zeilinger in Zusammenarbeit mit der Arbeitsgruppe „Quantentechnologien“ des Bereichs Informationstechnologien von Seibersdorf research GmbH. Als Auftraggeber der Transaktion fungierte Wiens Bürgermeister Dr. Michael Häupl, der Empfänger war BA-CA Vorstandsvorsitzender Dr. Erich Hampel. Der Auftrag wurde über ein Glasfaser-Datenkabel der Firma Wien Kanal Abwassertechnologien GmbH vom Wiener Rathaus an die BA-CA Filiale Schottengasse geschickt.

### **Verschränkte Lichtteilchen ermöglichen abhörsichere Datenübertragung**

Unter Quantenkryptographie versteht man die Erzeugung eines Datenschlüssels zur Nachrichtenverschlüsselung mittels quantenphysikalischer Methoden. Sie bietet die Lösung für zwei Probleme der heute gängigen Verschlüsselungssysteme: Die Erzeugung absolut zufälliger Schlüssel und deren Übermittlung. Einerseits beruht in der Quantenkryptographie die Sicherheit der erzeugten Schlüssel auf Naturgesetzen und nicht mehr auf schwer lösbaren mathematischen Problemen, wie bei den heute eingesetzten Verfahren. Andererseits vereinfacht die Quantenkryptographie die Schlüsselverteilung, und vertrauenswürdige Boten, die den Schlüssel persönlich überbringen, wie es derzeit bei „Geheimstufe rot“ üblich, gehören endgültig der Vergangenheit an. Sie ermöglicht nämlich die abhörsichere Verteilung der Schlüssel indem diese beim Sender und beim Empfänger gleichzeitig erzeugt werden.

Die Schlüssel für die Nachrichtencodierung werden mit verschränkten Lichtteilchen erzeugt. Die Verschränkung wurde vom österreichischen Physiker Erwin Schrödinger als das wesentliche Charakteristikum der Quantenphysik beschrieben und Albert Einstein bezeichnete sie als „spukhafte Fernwirkung“. Die Grundlage dabei ist, dass die Messung an einem Teilchen die Eigenschaften eines zweiten Teilchens, unabhängig von seiner Entfernung beeinflusst.

In der Sendestation in der BA-CA Filiale Schottengasse erzeugt ein Laser die beiden verschränkten Lichtteilchen in einem Kristall. Eines der beiden Lichtteilchen wird in das Glasfaser-Datenkabel eingespeist und in Richtung Rathaus geschickt, das andere bleibt in der Bank. Beim Empfänger im Rathaus und beim Sender in der Bank werden die Teilchen dann gemessen. Ein wesentliches Merkmal der Quantenphysik ist, dass vor der Messung die Teilchen keine Eigenschaften haben. Erst bei der Messung nehmen die Teilchen ihre Eigenschaften an. Durch die Verschränkung sind die Eigenschaften beider Teilchen miteinander verbunden.

Die Messergebnisse werden anschließend in eine Folge von 0 und 1, den Schlüssel zur Nachrichtencodierung, umgewandelt. Die Reihenfolge der Zahlen 0 und 1 ist auf Grund der Quantenphysik vollkommen zufällig. Durch die oben beschriebene Verschränkung entstehen in der BA-CA Filiale und im Rathaus identische Folgen von Zufallszahlen, die als Schlüssel für die Nachrichtencodierung verwendet werden.

Die Verschlüsselung der Nachricht erfolgt über das so genannte „one time pad“-Verfahren. Hier ist der Schlüssel genauso lange wie die Nachricht selbst. Die Nachricht wird bit für bit mit dem Schlüssel verknüpft und anschließend durch das Glasfaser-Datenkabel übertragen. Die Entschlüsselung erfolgt wieder bit für bit. Ohne den genauen Schlüssel kann man die Nachricht nicht lesen.

Ein möglicher Lauscher kann schon während der Schlüsselerzeugung erkannt werden, also noch bevor mit der Übertragung der verschlüsselten Nachricht begonnen wird. Jeder Eingriff in die Übertragung der Lichtteilchen beeinflusst die Abfolge der Zahlenfolgen an den Messstationen. Wird abgehört, erhalten beide Partner eine unterschiedliche Folge von Zufallszahlen – also nicht den gleichen Schlüssel. Durch einen öffentlichen Vergleich eines Teils des Schlüssels kann herausgefunden werden, ob die Quantenleitung abgehört wurde. Wenn ja, erzeugt man einen neuen Schlüssel für die Übertragung der Nachricht.

Ein Lauscher kann also höchstens die Übertragung verhindern, nicht aber den Inhalt der Nachricht auslesen!

### **Österreichische Teams entwickeln Hard- und Software für diese Technologie**

Das Gerät zur Erzeugung des Schlüssels für die Nachrichtencodierung wurde am Wiener Institut für Experimentalphysik von der Gruppe um Prof. Anton Zeilinger in enger Zusammenarbeit mit der Arbeitsgruppe Quantentechnologien des Bereichs Informationstechnologien von ARC Seibersdorf research GmbH unter der Leitung von Dr. Christian Monyk entwickelt. Die beiden Partner arbeiten seit zwei Jahren zusammen mit dem Ziel, einen marktreifen Prototyp für Quantenkryptographie zu entwickeln.

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

Die Elektronik sowie die Implementierung der Protokolle für die Erzeugung des Schlüssels und die Nachrichtenverschlüsselung selbst wurde entwickelt von der Arbeitsgruppe „Quantentechnologien“ des Bereichs Informationstechnologien von ARC Seibersdorf research GmbH unter der Leitung von Dr. Christian Monyk.

### **Starke Partner aus der Wirtschaft**

Das Glasfaser-Datenkabel zwischen Wiener Rathaus und BA-CA Filiale Schottengasse wurde von der WKA – Wien Kanal Abwassertechnologien GmbH, einem Tochterunternehmen der Stadt Wien, für dieses Experiment verlegt. Die WKA unterstützt seit drei Jahren die Forschungstätigkeit der Gruppe um Prof. Zeilinger. Im Frühjahr 2003 fanden erste Experimente zur Übertragung von verschränkten Lichtteilchen über den freien Raum in Labors der WKA auf der Wiener Donauinsel statt.

Die Stadt Wien verbindet mit der Forschung im Bereich der Quantenphysik eine langjährige Partnerschaft. Die Bank Austria Creditanstalt, für die Datensicherheit höchste Priorität hat, hat sich ebenfalls gern für das neue Experiment zur Verfügung gestellt.

Rückfragen: Universität Wien, Institut für Experimentalphysik  
Andrea Aglibut, Tel. +43 (0)1 4277 DW 51166;  
E-Mail: [andrea.aglibut@univie.ac.at](mailto:andrea.aglibut@univie.ac.at)

ARC Seibersdorf research GmbH  
Julia Petschinka, Tel. +43 (0)664 825 10 64  
E-Mail: [julia.petschinka@arc.ac.at](mailto:julia.petschinka@arc.ac.at)

Bank Austria Creditanstalt Group Public Relations  
Tiemon Kiesenhofer, Tel. +43 (0)5 05 05 DW 52819;  
E-Mail: [tiemon.kiesenhofer@ba-ca.com](mailto:tiemon.kiesenhofer@ba-ca.com)

Stadt Wien  
Public Relations, Präsidialbüro des Bürgermeisters  
Dr. Ingrid Duschek, Tel. +43(0)1-4000-81857;  
E-Mail: [dus@mdp.magwien.gv.at](mailto:dus@mdp.magwien.gv.at)

WKA – Wien Kanal Abwassertechnologien GmbH & Co KG  
Monika Müllner, Tel. +43 1 795 14 - 93 015;  
E-Mail: [office@wienkanal.at](mailto:office@wienkanal.at)