idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Friedrich-Alexander-Universität Erlangen-Nürnberg
Gertraud Pickel

03/14/2002
http://idw-online.de/en/news45590

Research projects
Information technology, Mathematics, Physics / astronomy
transregional, national

Signale aus der Superposition

Quantencomputer gibt es nicht. Vielleicht können solche Rechner, die an Stelle von elektrischer Leitfähigkeit auf nicht-klassische Eigenschaften der Materie bauen, bald hergestellt werden, vielleicht bleibt das noch lang ein Wunschtraum. Dagegen ist die Quanteninformationstheorie weit fortgeschritten, und das Teilgebiet der Quantenkommunikation kommt auch ohne die neuartigen Computer aus. "Wir wollen herausfinden, was man heute schon machen kann und machen sollte", umreißt Dr. Norbert Lütkenhaus das Programm, dem er und seine zwei Mitarbeiter sich verschrieben haben. Das Arbeitsgebiet mag fantastisch wirken; der Ansatz der Gruppe am Physikalischen Institut der FAU ist pragmatisch.

Das Emmy-Noether-Programm der Deutschen Forschungsgemeinschaft (DFG), das die Einrichtung der Nachwuchsgruppe Quanteninformationstheorie im September 2001 ermöglichte, lässt sorgfältig ausgewählten jungen Wissenschaftlern große Freiräume. Am Lehrstuhl für Optik von Prof. Dr. Gerd Leuchs, der das Drei-Mann-Team unterstützt, findet sich in der Arbeitsgruppe zur Quanteninformationsverarbeitung unter Leitung von Dr. Natalia Korolkova die ideale thematische Ergänzung.

Wenn sie gebaut werden könnten, würden Quantencomputer bestimmte Aufgaben unvergleichlich schneller und effektiver lösen als die ausgeklügeltsten Hochleistungsrechner vom konventionellen Typus. Deren Arbeits- und Speicherkapazität kann erstaunlich rasch überfordert sein. Manche Probleme sind heute für eine bestimmte Eingabelänge innerhalb einer Sekunde lösbar. Für eine doppelt so lange Eingabe sind bereits Rechenzeiten erforderlich, die weit über der Lebensdauer unseres Universums liegen.

Ein Beispiel für ein solches Problem ist die Zerlegung großer Zahlen in die Primzahlen, durch die sie geteilt werden können. Die abhörsichere Übertragung von Daten ist darauf gegründet, dass kein Weg bekannt ist, diese Aufgabe mit konventionellen Rechnern zu bewältigen - allerdings nur, weil sie dafür viel zu lange brauchen.

Bewiesen ist außerdem, dass Quantencomputer an dieser Hürde nicht scheitern würden und gebräuchliche Codes knacken könnten. Die Theorie, die den wunden Punkt der gängigen Verschlüsselungssysteme offenlegt, liefert zugleich die Basis für eine neue, sichere Verteidigungslinie. Werden quantenmechanische Signale eingesetzt, ist die Abhörsicherheit der Datenübertragung durch die Naturgesetze garantiert. Allerdings sind die hier benötigten Quantenzustände recht empfindlich gegen Verluste und Rauschen in der Übertragung. Daher muss sichergestellt werden, dass jeder Abhörversuch misslingt.

Die Forschungsgruppe sucht nach Verschlüsselungsmethoden, die optimalen Schutz bieten und praktikabel sind. Wenn Signalzustände geschickt gewählt werden, so dass sie einfach zu verwirklichen sind und ein tolerierbares Maß an Empfindlichkeit aufweisen, sind außer der Geheimhaltung von Nachrichten weitere Anwendungen denkbar, die Probleme der heutigen Kommunikationstheorie überwinden können.

Die Nachwuchsgruppe in Erlangen orientiert sich am Anwendbaren und behält dabei das Gesamtbild im Auge, dessen Konturen sich allmählich abzeichnen. Ein weitgehend solides und erprobtes theoretisches Fundament wartet auf seinen

Einsatz. Dr. Lütkenhaus schildert die Situation so: "Bisher wurden noch nicht einmal Quanten-Taschenrechner gebaut, aber die Programme für den Quantencomputer stehen schon bereit!"

URL for press release: http://www.optik.uni-erlangen.de/leuchs/qit/

URL for press release:
http://www.uni-erlangen.de/docs/FAUWWW/Aktuelles/2002/Forschung_2002/623Quanteninfo.html