idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

## Press release

Technische Universität Berlin
Ramona Ehret

08/25/1998
http://idw-online.de/en/news6180

Miscellaneous scientific news/publications, Research projects, Scientific conferences
Economics / business administration, Information technology, Mathematics, Physics / astronomy
transregional, national

# ICM'98:Computer können Gemeincodes knacken

Nevanlinna-Preisträger Peter Shor bewies, daß die Faktorisierung großer Zahlen auf Quantencomputern ultraschnell geht

Als Peter Shor - auf den Tag genau vor vier Jahren - seinen Algorithmus zur Faktorisierung großer Zahlen auf Quantencomputern vortrug, ging sein Resultat wie ein Schock um die Welt. Der in den Forschungslabors von AT&T; arbeitende Mathematiker konnte beweisen, daß mit dieser neuen Generation von Rechnern die zur Zeit am häufigsten benutzten Geheimcodes ohne Probleme zu knacken sind. Zum ersten Mal gab es einen Dämpfer in der Euphorie, mit der die Sicherheit der sogenannten Public-Key-Codes wie beispielsweise das weitverbreitete RSA-Verfahren gelobt wurden. Gleichzeitig löste Shors Ergebnis einen Boom in Physik und Informatik aus. Arbeitsgruppen in aller Welt machten sich daran, den Quantencomputer, der damals nur als theoretisches Modell bekannt war, zu bauen. Allein in den USA werden von Forschungsinstitutionen rund 20 Millionen Mark für diese Forschung ausgegeben. Ein ganz neues Gebiet, die sogenannte Quanteninformatik, hat sich zwischen Quantenphysik und theoretischer Informatik herausgebildet.

Peter Shor wurde am Dienstag (18.8.1998) bei der Eröffnung des Internationalen Mathematiker-Kongresses in Berlin für seine bahnbrechenden Arbeiten mit dem Nevanlinna-Preis geehrt. Dieser Preis ist die höchste Auszeichnung, die innerhalb der Mathematik für die Theoretische Informatik bereitsteht. Am heutigen Mittwoch hält er auf dem Weltkongreß einen Plenarvortrag zum Thema Quantencomputing.

Bislang gibt es nur Prototypen der Quantencomputer. Sie rechnen nicht mehr mit Strom sondern mit Überlagerungszuständen einzelner Atome. Dadurch läßt sich ein Vielfaches an Informationen verarbeiten als es auf traditionellen Computern möglich wäre. Im April 1998 meldeten Forscher von IBM, MIT, der Universität von Kalifornien in Berkeley und der Universität Oxford, daß sie mit Hilfe einer Art von Chloroform einen kleinen Quantencomputer gebaut hätten. Eine Arbeitsgruppe in Innsbruck versucht es mit Ionenfallen. Experten schätzen aber, daß es noch mindestens zwei Jahrzehnte dauern wird, bis es funktionierende Quantenrechner gibt. Eine Gefahr für die Datensicherheit von Banken oder Internetbenutzer besteht noch nicht. "Zuvor muß die Wissenschaftlergemeinde wesentlich näherliegende Probleme lösen, etwa die Fehlerstabilisierng und -kontrolle der Quantenzustände dieser neuen Rechner. Auch hier hat Peter Shor grundlegende Vorschläge gemacht", sagt Prof. Thomas Beth von der Universität Karlsruhe. Beth ist neben Physikern aus Erlangen, Ulm und Magdeburg einer der Initiatoren des im Mai dieses Jahres von der Deutschen Forschungsgemeinschaft eingerichteten Schwerpunktprogrammes "Quanteninformationsverar-beitung".

Die Quanteninformatik verspricht mit der Kombination mathematischer Methoden mit den Gesetzen der Quantenphysik schnelle Lösung für Problemklassen zu finden, für die es auf klassischen Rechnern bislang keine effizienten Verfahren gibt und vielleicht auch nicht geben kann. Genau auf solchen Problemen bauen Verschlüsselungssysteme auf. So nutzt der 1977 entwickelte Geheimcode RSA (benannt nach seinen Erfindern Ronald Rivest, Adi Shamir und Leonhard Adleman) aus, daß es für herkömmliche Rechner schwer ist, große Zahlen in ihre Faktoren aufzuteilen. Shor zeigt nun, daß Quantenrechner so geschickt programmiert werden können, daß diese

Prozedur effizient abgearbeitet werden kann. Dazu entwickelte er ein neues algorithmisches Prinzip, den sogenannten Quantenparallelismus. Bei der Faktorisierung großer Zahlen wendet er die sogenannte Quanten-Fourier-Transformation an und teilte die Berechnungsschritte in physikalisch besonders günstige Teiltransformationen auf. Zentraler Baustein des Verfahrens ist das sogenannte Tensor-Parallelisierungsprinzip, das bereits in der 80er Jahren auf klassischen Parallelrechner angewandt wurden.

Auch wenn die Quantencomputer auf absehbare Zeit keine Gefahr für Verschlüsselungen zum Beispiel bei elektronischem Geld oder digitalen Unterschriften darstellt, suchen Kryptographen bereits nach neuen Kryptosystemen. Denn die heutigen, am häufigsten verwendeten Geheimcodes haben einen Schönheitsfehler. Ihre Sicherheit läßt sich mathematisch nicht beweisen. Nur indem die Datenschützer die Länge der Public-Key-Schlüsselzahlen nach und nach verlängern und damit die Rechenkomplexität beim Knacken nach und nach erhöhen, verschaffen sie sich Aufschub. Diese Schlüsselverlängerung ist durch die steigende Rechengeschwindigkeit klassischer Computer problemlos möglich, hebt aber den Schönheitsfehler der Geheimcodes nicht auf. Ein Verfahren, daß dagegen absolute Sicherheit verspricht, ist die sogenannte Quantenkryptographie. Auch sie nutzt die Erkenntnisse der Quantenphysik: Zentral ist ein Glasfaserkabel, durch das Lichtblitze geschickt werden. Ein Agent, der ein Lichtquant abfängt würde sofort auffliegen. Die Heisenbergsche Unschärferelation, ein zentrales Prinzip in der Physik, sagt nämlich aus, daß man ein Teilchen dieser Größenordnung nicht beobachten kann, ohne die Information, die es trägt, zu zerstören.

Vasco Alexander Schmidt

Weitere Informationen erteilt Ihnen gerne: Vasco Alexander Schmidt, Tel:030 851 84 93.

Diesen Beitrag können Sie im Rahmen Ihrer Berichterstattung ganz oder teilweise - auch ohne Namensnennung - verwenden. Wir möchten Sie aber bitten, uns ein Belegexemplar zuzusenden.

URL for press release: http://www.tu-berlin.de/presse/pi182.htm