Quanten.de Newsletter März/April 2002, ISSN 1618-3770

Drei mal fünf ist fünfzehn

Neue Bestleistung bei Quantencomputern

Günter Sturm, ScienceUp Sturm und Bomfleur GbR,
Camerloherstr. 19, D-85737 Ismaning
www.ScienceUp.de

Der Arbeitsgruppe von Isaac Chuang am Almaden-Forschungszentrum der IBM in Kalifornien haben vor kurzem eine neue Bestleistung bei Quantencomputern erzielt [1]: Die Zerlegung der Zahl 15 in ihre Primfaktoren 3 und 5. So einfach diese Rechnung auf den ersten Blick auch erscheint, sie eröffnet neue Möglichkeiten in der Krypthographie.

Sind verschlüsselte Daten noch sicher?

Ja, ganz bestimmt. Zumindest sind sie durch dieses Experiment nicht unsicherer geworden. Denn die praktische Anwendung liegt immer noch in weiter Ferne.

Was haben denn nun Quantencomputer mit Datensicherheit zu tun?

Drei mal fünf ist fünfzehn. Ganz einfach. Fast genau so einfach: Zerlegen Sie die Zahl 15 in ihre Primfaktoren, also in ein Produkt, das nur aus Primzahlen besteht. Die Lösung ist auch 3 * 5. Neue Aufgabe: Zerlegen Sie die Zahl 875747 in ihre Primfaktoren. Das ist schon schwieriger. Viel schwieriger. Durch Ausprobieren nicht mehr zu schaffen. Aber mit einem Computerprogramm werden Sie recht schnell zu dem Ergebnis 547 * 1601 kommen. Und das können Sie mit jedem Taschenrechner überprüfen.

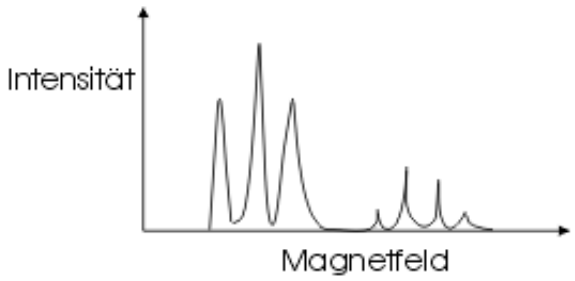
Das Produkt zweier Primzahlen ist einfach zu überprüfen, aber in der Praxis kaum zu zerlegen. Für die Zerlegung eines 500-stelligen Produktes würden auch die schnellsten heute verfügbaren Großrechner mehrere Milliarden Jahre benötigen. Auf dieser "Unmöglichkeit der Zerlegung" beruht das heutzutage sehr oft eingesetzte Public-Key Kryptographie-Verfahren.

Dieses Verschlüsselungsverfahren könnte aber von Quantencomputern "geknackt" werden. Denn die können solche Berechnungen viel schneller durchführen. Der amerikanische Mathematiker Peter Shor hat hierfür vor sieben Jahren eine Rechenvorschrift entwickelt, die nun von Isaac Chuang im Experiment demonstriert wurde. Die Umsetzung auf größere Zahlen ist prinzipiell möglich, aber experimentell schwierig. Quantencomputer beruhen auf einem quantenmechanischen "Überlagerungszustand", der empfindlich gegen Umwelteinflüsse ist. Diese quantenmechanische "Dekohärenz" macht das Rechnen mit Quantencomputern für größere Zahlen sehr aufwändig. Aber es gibt Ansätze ("Quantum error correction"), dieses Problem zu lösen. Wie gesagt ist dies nur ein experimentelles Problem. "Im Prinzip" sind mit

Quantencomputern alle auf Primfaktorzerlegung basierenden Verschlüsselungsalgorithmen in einer überschaubaren Zeit knackbar.

Aber wie funktioniert dies nun?

Die zur Zeit hierfür am häufigsten und erfolgreichsten eingesetzte Technik ist NMR (Nuclear Magnetic Resonance). Sie beruht darauf, dass viele Atomkerne einen intrinsischen Drehimpuls, den sogenannten Spin, aufweisen (siehe z. B. unseren Quanten.de Newsletter vom 1. November: Fermionen und Bosonen). Ein Kern mit zum Beispiel der Spin-Quantenzahl $I = 1/2$ kann, wenn durch ein äußeres Magnetfeld eine Vorzugsrichtung (nennen wir sie z-Richtung) vorgegeben ist, nur zwei Orientierungen relativ zu diesem Magnetfeld einnehmen, die durch die sogenannte magnetische Quantenzahl m_I beschrieben werden ($m_I = -1/2, +1/2$). Diese Orientierungen ("Spin rauf, Spin runter") unterscheiden sich in ihrer Energie. Es ist daher möglich, Übergänge zwischen diesen beiden Energieniveaus anzuregen. Genau das macht die NMR. Man erhält so ein Spektrum, das als "x-Achse" das Magnetfeld und als "y-Achse" die gemessene "Intensität" des Übergangs enthält:



Ganz ähnlich sehen die "Rechenergebnisse" von NMR-Quantencomputern (NMRQC) aus. Warum kann man mit NMRQC rechnen? Die oben angeführten Zustände "Spin rauf", Spin runter" erinnern stark an Schalter. Und man kann sie wie Schalter verwenden. Außerdem sind die einzelnen Kernspins eine Moleküls nicht unabhängig voneinander, sondern gekoppelt. Die Einstellung eines Kernspins beeinflusst die anderen. Voneinander abhängige Schalter also. Das ist alles, was man für einen Computer braucht. Ein einfaches Beispiel hierfür ist das soganannte INEPT-Experiment (*Insensitive Nuclei Enhanced by Polarization Transfer*),
in dem "Polarisation" (das entspricht in etwa der Intensität im nachher gemessenen Spektrum) von einem NMR-empfindlichen, also gut messbaren Kern, auf einen NMR-unempfindlichen, also schwer messbaren Kern übertragen wird. Man kann dies als einen logischen Schalter verstehen, der einen Spin umklappt (Polarisation überträgt), abhängig von der Orientierung des anderen Spins. Dies erfolgt durch Radiofrequenz-("rf")-Sender, die rf-Pulse in bestimmten Abständen senden.

Zusammengefasst: Spin 1/2 Kerne kann man sich wie Bits in einem Computer vorstellen. Durch rf-Pulse und bestimmte Puls-Abstände kann jeder beliebige logische Schaltkreis aufgebaut werden.

Was hat das mit Quantencomputern zu tun? Bisher nichts, denn soweit wie jetzt diskutiert handelt es sich um klassische Schalter und damit um einen herkömmlichen Computer. Aber: Kernspins sind echte Quanten-Objekte. Bezeichnen wir, in sogenannter Dirac-Notation, den "Spin-auf" Zustand entlang der z-Richtung mit |0> und den Spin-ab Zustand entlang -z mit |1>, so entspricht dies den klassischen Bit-Werten 0 und 1. Nun wird aber ein Spin "entlang der x-Achse" durch eine Superposition eines Spin-auf und Spin-ab Zustandes beschrieben, also als |0> + |1> (ohne Normierung).

Ein Spin 1/2 Teilchen ist daher mehr als ein einfaches Bit. Es dient als Quanten-Bit (qubit).

Vergleichen wir dies mit einem klassischen logischen Schalter, der eine Funktion f mit einem Input-Bit x und einem Output-Bit f(x) implementiert. Wenn x = 0, ist das Ergebnis f(0). Wenn x = 1, ist das Ergebnis f(1). Der analoge "Quanten-Schalter" wird durch eine unitäre Operation wie folgt beschrieben:

|0> => |f(0)> und |1> => |f(1)>

Aber durch die Möglichkeit, kohärente Superpositions-Zustände zu präparieren, kann derselbe Quanten-Schalter auch folgende Transformation ausführen:

|0> + |1> => |f(0)> + |f(1)>

Also kann man f(x) für **beide** Eingabewerte in **einem** Schritt berechnen!

Im Allgemeinen gilt, dass eine Funktion, die n qubits auf einem Quantencomputer implementiert, für alle 2^n Eingabewerte parallel ausgewertet werden kann. Die Zahl der parallelen Funktionsberechnungen steigt also exponentiell mit der Größe des Quantencomputers (der Zahl der qubits).

Nur mit qubits allein lassen sich aber noch keine Quantencomputer-Berechnungen durchführen. Die Postulate der Quantenmechanik bestimmen, dass eine Messung eines qubits in einer Superposition von |f(0)> + |f(1)> entweder "f(0)" oder "f(1)" ergibt, mit gleicher Wahrscheinlichkeit. Nötig sind daher zusätzlich Quantencomputer-Algorithmen:

Einer der wichtigsten ist der 1994 von **Peter Shor** vorgestellte Algorithmus [2], mit dem die Periode einer bestimmten Funktion exponentiell schneller gefunden werden kann als mit jeder klassischen Maschine. Mit einigen weiteren zahlungstheoretischen Erkenntnissen kann dies zur Zerlegung einer Zahl in ihre Primfaktoren verwendet werden. Die Anzahl der hierfür notwendigen Rechenschritte wächst nur mit der dritten Potenz der Länge der zu zerlegenden Zahl. Bei klassischen Rechnungen hingegen wächst die Anzahl der Rechenschritte exponentiell mit der Länge. Dies macht die Zerlegung einer 500-stelligen Zahl auf einem klassischen Computer unmöglich. Auf einem Quantencomputer - mit einer qubit-Zahl von einigen Dutzend

- ist dies aber sehr wohl möglich. Da zahlreiche Verschlüsselungsalgorithmen genau auf der Unmöglichkeit der Zerlegung einer langen ganzzahligen Zahl in ihre Primfaktoren beruhen, könnten also Quantencomputer auf diese Weise verschlüsselte Daten "knacken".

Von L. M. K. Vandersypen et al. [1] wurde nun am IBM Almaden Research Center in San Jose, Kalifornien, erstmals die **einfachste sinnvolle Anwendung von Shor's Algorithmus demonstriert**. Die Autoren führten NMR-Experimente an einem Molekül durch, in dem zwei ^{13}C-Kerne und fünf ^{19}F Kerne als insgesamt sieben qubits fungieren. Genauer gesagt verwendeten die Autoren - wie in NMR-Experimenten nicht anders möglich - nicht ein Molekül, sondern sehr viele identische (0,04 molare Lösung). Den Autoren gelang durch die Analyse der NMR-Spektren der Nachweis der Zerlegung der Zahl 15 in ihre Primfaktoren 3 und 5. Obwohl die erhaltenen Spektren einige Ungereimtheiten im Vergleich zu den simulierten Spektren enthalten, gelang es zum ersten Mal, NMR- Quantencomputerberechnungen durchzuführen, bei denen Dekohärenz die Haupt- Fehlerquelle ist.

Die Dekohärenz ist ein gravierendes Problem bei Quantencomputer-Berechnungen, da durch sie die kohärenten Superpositionszustände zerstört werden. Im Fall der NMR- Spektroskopie handelt es sich hierbei um sogenannte Spin-Spin und Spin-Gitter Relaxation. Es gibt jedoch Mechanismen, durch Dekohärenz verursachte Fehler zu korrigieren (Quantum error correction) und so im Prinzip beliebig lange Quantencomputer-Berechnungen durchzuführen.

Abschließend ist zu bemerken, dass Quantencomputer auf Grundlage der NMR in einem flüssigen Lösungsmittel (so wie in dem hier beschriebenen Experiment) wohl nie schneller als eine klassische Maschine rechnen werden. Der experimentelle Aufwand hierfür ist zu hoch. Und Ihre EC-Karte ist also immer noch sicher. Vielversprechender sind Techniken, die Festkörper-NMR, NMR an atomaren Verunreinigungen oder Flüssigkristalle einsetzen. Auch die SQUID-Technik ist vielversprechend.

Günter Sturm

Literatur:

[1] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, I. L. Chuang, Nature *414*, 883-887 (2001).

[2] P. Shor, in "Proc. 35th Annual Symposium on the Foundations of Computer Science", IEEE Comp. Soc. Press, Los Alamitos, CA, p. 124-134 (1994).

Weitere Infos zum Dekohärenz-Problem in der Quantenmechanik im Quanten.de-Newsletter September/Oktober 2001 unter www.Quanten.de/schroedingers_katze.html.

Eine - allerdings knapp gehaltene und nicht populärwissenschaftliche - Einführung in die magnetische Resonanzspektroskopie im Allgemeinen und Elektronenspinresonanz-

Spektroskopie im Besonderen finden Sie in der Dissertation von G. Sturm unter www.ScienceUp.de/diss.html.