Medieninformation der Universität Innsbruck
3. März 2016

SPERRFRIST: 3. März 2016, 20:00 Uhr

Tiroler Quantencomputer faktorisiert Zahlen effizienter

Der Shor-Algorithmus ist der wohl bekannteste Quantenalgorithmus. Er löst ein jahrtausendealtes Problem, nämlich die Primfaktorzerlegung von Zahlen. Innsbrucker Physiker um Rainer Blatt haben nun gemeinsam mit Wissenschaftlern am MIT um Isaac Chuang diesen Algorithmus in einem Ionenfallen-Quantencomputer so effizient umgesetzt, dass er auch für größere Zahlen anwendbar wird.

Rückfragehinweis:

Dr. Thomas Monz
Institut für Experimentalphysik
Universität Innsbruck
Telefon: +43 512 507 52452
E-Mail: thomas.monz@uibk.ac.at

Dr. Christian Flatz
Büro für Öffentlichkeitsarbeit
Universität Innsbruck
Telefon: +43 512 507 32022
E-Mail: christian.flatz@uibk.ac.at

Jede natürliche Zahl lässt sich als Produkt von Primzahlen darstellen. Für kleine Zahlen ist die Primfaktorzerlegung nur eine Denksportaufgabe, bei großen Zahlen erweist sie sich aber als extrem aufwändig. Darauf beruhen heute gängige Verschlüsselungsverfahren wie das RSA-Kryptosystem. Weil klassische Computer an der Primfaktorzerlegung großer Zahlen sehr lange rechnen, galt dieses Verfahren bisher auch als sehr sicher. 1994 hat der amerikanische Mathematiker und Informatiker Peter Shor aber einen Algorithmus entwickelt, der mithilfe eines Quantencomputers die Primfaktoren sehr viel rascher findet. In den vergangenen 15 Jahren wurde der Shor-Algorithmus im Labor bereits mehrmals mit unterschiedlichen Technologien demonstriert - allerdings nicht ohne das Ergebnis schon von vornherein vorauszusetzen und nur für kleine Zahlen. Physiker am Institut für Experimentalphysik der Universität Innsbruck und am Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften haben nun gemeinsam mit Physikern am Massachusetts Institute of Technology, USA, den Shor-Algorithmus erstmals ohne Vorwissen und so effizient umgesetzt, dass er auch für größere Zahlen anwendbar wird.

Zahl der notwendigen Quantenbits reduziert

Mit Hilfe des Shor-Algorithmus kann ein Quantencomputer große Zahlen sehr viel rascher in Primfaktoren zerlegen als klassische Computer. Um die Zahlen speichern und die Primfaktoren berechnen zu können, benötigt er allerdings entsprechend viele Quantenbits. Dies erweist sich heute noch als schwierig, denn die im Labor existierenden Quantenrechner verfügen nur über wenige Quantenbits. In Innsbruck haben Physiker nun einen Vorschlag von Alexei Kitaev aufgegriffen, der die Zahl der benötigten Quantenbits reduziert. „Um die Zahl 15 in ihre Primfaktoren zu zerlegen, benötigen wir statt zwölf nur noch fünf Quantenbits“, erklärt Experimentalphysiker Thomas Monz. „Möglich ist dies zum einen, weil wir ein Quantenbit im Rahmen der Rechnung recyceln können; zum anderen, weil wir das Ergebnis immer wieder in einem Cache-Bit zwischenspeichern und dann

weiterrechnen.“ Mit Hilfe dieses Ansatzes haben die Physiker in einem Ionenfallen-Quantencomputer mit fünf Quantenbits die Zahl 15 faktorisiert.

Parallelsuche führt schneller zum Ergebnis

Der Quantencomputer startet die Suche nach den Primfaktoren mit einer zufällig gewählten Zahl – hier unterscheidet sich die aktuelle Arbeit wesentlich von den bisherigen, weil sie keine Vorwegnahme des Ergebnisses enthält – und führt auf vier Quantenbits eine Reihe von Gatteroperationen durch. Um die Zahl der notwendigen Quantenbits zu begrenzen, wird das Ergebnis immer wieder in einem fünften Quantenbit zwischengespeichert und mit dem Ergebnis weitergerechnet. „Wir mussten dafür eine neue Kühlmethode implementieren, mit der die Ionen zwischen den Rechenschritten immer wieder abgekühlt werden können“, sagt Thomas Monz, der den Vorteil des Shor-Algorithmus noch einmal unterstreicht: „Klassische Computer tun sich mit der Primfaktorzerlegung sehr schwer, weil sie alle möglichen Zahlenkombinationen hintereinander durchprobieren müssen. Im Quantenrechner geschieht dies quasi parallel.“

Finanziell unterstützt wurde die Arbeit unter anderem vom österreichischen Wissenschaftsfonds FWF und der Europäischen Union.

Publikation: Realization of a scalable Shor algorithm. Thomas Monz, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl, Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang, Rainer Blatt. Science 2016 DOI: 10.1126/science.aad9480

Weitere Informationen: http://quantumoptics.at

Eine Medieninformation des Büros für Öffentlichkeitsarbeit der Universität Innsbruck (Anschrift: Christoph-Probst-Platz, Innrain 52, A-6020 Innsbruck, Tel.: +43 512 507 32000, E-Mail: presse@uibk.ac.at)