INTERVIEW

Quantentechnologie wird immer noch als Kuriosität wahrgenommen

Quanteninformationstechnologien gehören zu den boomenden Forschungsgebieten. Längst geht es nicht mehr allein um Grundlagenforschung, sondern um handfeste technische Anwendungen. Im Fokus ist die abhörsichere Kommunikation. Ein Interview mit Dieter Meschede, Leiter der Arbeitsgruppe Quantentechnologie an der Universität Bonn und künftiger Präsident der Deutschen Physikalischen Gesellschaft.

Physik in unserer Zeit: *Auf dem Gebiet der Quanteninformation tut sich enorm viel. Was finden Sie derzeit besonders spannend?*

Dieter Meschede: Mich beeindruckt, was sich auf der einen Seite an Förderpolitischem tut, zum Beispiel die mit einer Milliarde Euro dotierte Initiative „Quantum Technologies Flagship" der Europäischen Kommission [1]. Damit verknüpft ist ein Programm des Bundesministeriums für Bildung und Forschung, das im Moment den Namen Qutega für „Quantentechnologie – Grundlagen und Anwendungen" trägt [2]. Und ich habe kürzlich auf einem Seminar zur Quanteninformation im Physikzentrum Bad Honnef einen Vortrag von Cheng-Zhi Peng von der University of Science & Technology of China (USTC) in Hefei in China gehört, der über die chinesischen Aktivitäten berichtet hat. Das war außerordentlich eindrucksvoll.

Was hat Sie besonders beeindruckt?

Wir reden über Quantum Science, und das hat auch den Aspekt Quantum Technology, also die Übersetzung in Anwendungen. In vielen Dingen kennen wir ja die perfekte Lösung noch nicht, weder im Labor noch auf dem Papier. Und die Chinesen haben einfach mal angefangen. Sie haben eine Quantenkommunikationsstrecke von Peking nach Shanghai gebaut. Das ist eine etwa 2000 km lange Glasfaserverbindung mit 32 Netzknoten. Damit kann man schauen, wie das funktioniert. Die Technik ist überhaupt nicht perfekt, aber in China wird das Thema angepackt und umgesetzt.

Dieter Meschede lehrt am Institut für Angewandte Physik der Universität Bonn und ist dort Leiter der Arbeitsgruppe Quantentechnologie. Zudem ist er aktueller Herausgeber des „Gerthsen Physik", Autor des Buchs „Optik, Licht und Laser" und Hauptherausgeber von „Applied Physics B – Optics and Lasers". Ab dem nächsten Jahr wird er Präsident der Deutschen Physikalischen Gesellschaft sein.

Hinzu kommt der chinesische Quantenkommunikations-Satellit für das internationale QUESS-Netzwerk (Quantum Experiments at Space Scale) [4].

Genau, das Projekt läuft parallel. Damit will man auch auf dem Boden weit voneinander entfernte Stationen über Quantenkommunikation verbinden. Dafür haben sie mehrere Bodenstationen mit großen Teleskopen, die diese Signale senden oder empfangen und darüber untereinander kommunizieren. Das geht immer nur für etwa acht Minuten, während der Satellit drüberhuscht, aber auch dieses Projekt ist ziemlich eindrucksvoll. Hinter diesem Programm steht der Staat China.

Und wie ist die Lage in Europa?

In Europa müssen wir auch versuchen, Dinge auf der Basis unseres jetzigen Wissens auf dem Gebiet umzusetzen. Wir müssen erst einmal herausfinden, wo die wirklichen Hemmnisse liegen.

Hinter der Satellitentechnik steckt die Idee, dass man Quantenkommunikation weltweit betreiben kann?

Im Prinzip ja. Im Moment geschieht das in China zwischen nicht allzu weit voneinander entfernten Bodenstationen. Micius, so heißt der Satellit, fliegt in etwa 480 bis 580 km Höhe [3] (s. Physics News, S. 167). Sie können sich leicht ausrechnen, dass man da nicht allzu weit um die Erde herum kommt. Es gibt aber auch die Idee, geostationäre Satelliten zu benutzen, und dann hätte man genügend Raumwinkel, um weiter entfernte Punkte auf der Erde miteinander zu vernetzen.

Zur Quantenkommunikation via Satellit gibt es auch in Europa Bemühungen.

Ja, am Max-Planck-Institut für die Physik des Lichts in Erlangen zum Beispiel versucht eine Gruppe von Gerhard Leuchs, Satelliten der Stuttgarter Firma Tesat Spacecom zu verwenden, die sowieso Kommunikation über die sogenannten Freistrahlstrecken betreiben. Sie versuchen, diese Satelliten zu trimmen, um damit auch Quantenkommunikation zu realisieren.

Und das Motiv ist abhörsichere Kommunikation mit Hilfe der Quantenkryptografie?

Genau. Kryptografie ist ein wichtiges Thema. Wegen der Cyberkriminalität hat das Thema IT-Sicherheit eine sehr schnell wachsende Bedeutung. Da geht es nicht nur um die abhörsichere Übermittlung einer Nachricht, sondern um die ganze Infrastruktur. In Deutschland sind

zum Beispiel Stahlwerke angegriffen und vorübergehend lahmgelegt worden. Da müssen wir offensichtlich etwas tun. Im Vergleich mit allen anderen Systemen für eine sichere Datenübertragung, die wir kennen, beruht einzig die Quantenkommunikation auf physikalisch beweisbar sicheren Verfahren.

Die heute am weitesten verbreitete Kryptografiemethode ist die sogenannte asymmetrische Verschlüsselung, wo der Empfänger dem Sender einen öffentlichen Schlüssel mit einer mathematischen Einweg-Funktion schickt [5]. Diese Verschlüsselung basiert auf der Faktorisierung von Zahlen, und wir gehen davon aus, dass es keinen Computer gibt, der sie knacken kann. Aber ein Quantencomputer könnte dazu in der Lage sein.

Quantencomputer würden also die Karten neu mischen?

Ja! Denken Sie an die Geschichte der Enigma. Im Zweiten Weltkrieg haben es die britischen Geheimdienste unter Mitwirkung von Alan Turing geschafft, das deutsche Kryptografiesystem auf Basis der Enigma zu entschlüsseln. Wie ihnen das gelungen ist,wurde aber erst in den 1970er Jahren öffentlich gemacht. Die Geschichte lehrt uns: Es ist durchaus denkbar, dass jemand schon im Geheimen über Maschinen verfügt, die die sichersten modernen Verschlüsselungen knacken können. Wir können es jedenfalls nicht ausschließen. Wenn es heute schon funktionierende Quantencomputer gäbe, dann wären die beliebten asymmetrischen Public-Key-Verfahren sehr verletzlich.

Als Gegenmaßnahme gibt es allerdings auf der algorithmischen Seite Bemühungen, die sich Post-Quantenkryptografie-Verfahren nennen. Diese Verfahren setzen auf symmetrische Verschlüsselung, Sender und Empfänger haben also ähnliche Schlüssel. Symmetrische Schlüssel sind durch Quantenalgorithmen weniger gefährdet, weil sie nicht auf Primzahlfaktorisierung beruhen. Die Post-Quantenkrytografie-Verfahren sollen symmetrische Schlüssel trotz Nutzung von rein klassischer Physik so absichern, dass sie durch die heute bekannten Quantencomputer-Algorithmen nicht gefährdet wären. Aber da höre ich von Kollegen, dass diese Algorithmen sicher auch ein Jahrzehnt brauchen werden, bis man sie umfangreicher einsetzen kann.

Die Gefährdung von Verschlüsselungen durch Quantencomputer ist ein bedenkenswerter Punkt. Doch es sieht ja so aus, als sei die Technologie noch sehr am Anfang. Um das erste kommerzielle Gerät der kanadischen Firma D-Wave Systems, das supraleitende Quantenbits (Abbildung 1)nutzt, gab es intensiven Streit, ob es überhaupt ein Quantencomputer sei.

Wir würden das eher einen Quanten-Annealer nennen. Das ist eine Maschine, die einfach gesagt versucht, Zustände von gewissen komplexen Systemen zu finden und auf diese Art und Weise einen bestimmten Typ von Rechnungen auszuführen. Sie ist kein universeller Quantencomputer in dem Sinne, dass sie aus Quantengattern aufgebaut und darüber programmierbar ist. Es ist auch nicht klar, was sie wirklich kann.

Das führt uns zur Physik. Es gibt noch die Hoffnung, mit sogenannten Quantensimulatoren komplexe Moleküle oder Materialien, Festkörper, berechnen zu können. Wie sehen Sie den gegenwärtigen Entwicklungsstand?

Das ist eine sehr große und außerordentlich aktive Community. Ich würde das als analogen Quantencomputer bezeichnen, im Gegensatz zum digitalen Quantencomputer, der auf Gatteroperationen beruht. Das ist ein bisschen wie die alten Analogrechner, die wir früher zum Beispiel aus Operationsverstärkern gebaut haben, und die elementare Operationen wie Addieren, Multiplizieren usw. konnten. Vielleicht kann man Quantensimulatoren ein bisschen damit vergleichen.

Warum sind Quantensimulatoren so interessant?

In der Praxis hat man häufig Quanten-Vielteilchensysteme, die einen hohen Grad von Komplexität besitzen. Wenn wir jetzt versuchen, die auf einem gewöhnlichen Computer zu simulieren, dann wächst der Raum der Zustände exponentiell stark an. Das geht mit 2^N, und N ist die Zahl der Teilchen, die berücksichtigt werden müssen. Bis $N = 40$ oder 50 kann man das mit einem konventionellen Computer bewältigen, aber dann ist das Ende der Fahnenstange erreicht. Auch wenn man berücksichtigt, dass die Computertechnik sich weiter entwickelt, ist es nicht vorstellbar, dass man es bei N auf sehr viel größere Werte bringt. Das wächst ja exponentiell, während die Leistungsfähigkeit herkömmlicher Computer eher linear wächst.

Der Simulator erlaubt dagegen, bestimmte Klassen von Phänomenen, die gerade in der Vielteilchenphysik sehr wichtig sind, einfach über das Einstellen äußerer Parameter zu untersuchen. Dazu gehören zum Beispiel Leitfähigkeitssysteme in Kristallgittern oder Supraleitungsphänomene. Ich bin allerdings skeptisch, inwieweit ein Quantensimulator wirklich geeignet sein wird, um ernsthafte technologische Fragestellungen zu untersuchen. Aber das muss man abwarten.

Manche Wissenschaftler auf dem Gebiet neigen dazu, ihre Forschung im Hinblick auf Anwendungen zu optimistisch zu verkaufen.

Es wird von manchen behauptet, dass wir mit dieser Methode in absehbarer Zeit sogar schon Wirkstoffdesign für die Medikamentenentwicklung vornehmen könnten. Ich kann mir einfach nicht vorstellen, dass wir da bald in sinnvoller Form hinkommen. Das halte ich für übertrieben. Ich finde, die Community sollte solche Versprechungen besser nicht machen, sondern lieber auf dem Teppich bleiben.

Solche voreiligen Versprechungen schlagen irgendwann auch zurück. Das hat schon dazu geführt, dass man zum Quantencomputer seit Jahren die Frage hört: Wann kommt er denn endlich? Und

das kommt daher, dass sich einige Forscher schon vor zehn, fünfzehn Jahren zu weit aus dem Fenster gelehnt haben.

Ja, das ist immer sehr bedauerlich! Man braucht für alle diese Forschungsarbeiten einen sehr langen Atem. In *Physics Today* haben Frank Wilczek und andere 2016 Artikel zum Thema „Physik im Jahr 2116" geschrieben. Wilczek sagte darin auch: Es wird den Quantencomputer geben, wir werden damit Probleme der Chemie und anderer Gebiete lösen.

Mal abgesehen davon, dass Wilczek eine große Autorität ist, finde ich, dass das in dieser zeitlichen Perspektive eine sinnvolle Aussage ist. Technisch sind wir im Labor ganz ordentlich vorangekommen. Es geht im Moment eher stetig voran als mit großen Revolutionen – wobei man sagen muss, dass diese supraleitenden Qubits schon eine gewisse Revolution waren. Die haben in sehr kurzer Zeit sehr viel Boden gut gemacht und sind jetzt eines der wichtigsten Systeme geworden.

Die Quantenkryptografie ist die auf dem Gebiet der Quanteninformation am weitesten entwickelte Technologie, es gibt schon länger kommerzielle Produkte zu kaufen. Noch sind es jedoch Nischenlösungen, warum?

Es ist auch ein Problem der Wahrnehmung. In dem Quantenwissenschafts-Programm hier in Deutschland bin ich sehr dahinter her, dass wir dazu ein Bildungsprogramm starten. Dabei denke ich auch an die Entscheider in Unternehmen. Ein Problem der Quantentechnologie ist ja, dass sie noch immer als Kuriosität wahrgenommen wird. Das müssen wir unbedingt ändern.

Vor ein paar Jahren erzählte mir Gregoire Ribordy, CEO der Genfer Pionierfirma für kommerzielle Quantenkryptographie-Lösungen ID Quantique, wie schwierig es zum Beispiel sei, diese abhörsichere Technologie bei Banken zu etablieren.

Ja, das kann ich mir aus eigener Erfahrung gut vorstellen.

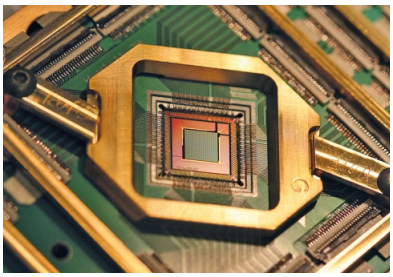

Abb. 1 ***Integrierter Schaltkreis für die ersten kommerziellen „Quantencomputer" von D-Wave Systems. Diese ICs nutzen vernetzte supraleitende Qubits, zum Beispiel 128 Stück, für „adiabatisches Quantenrechnen". Das zählt zu den Methoden des „Quantum Annealings", das mit speziellen Näherungsverfahren (Metaheuristiken) Optimierungsprobleme lösen sollen. Sie sollen Quantenfluktuationen nutzen, um globale Minima einer Kostenfunktion, die das System beschreibt, aufzuspüren. Was die Maschinen von D-Wave Systems tatsächlich können, ist bislang aber unklar*** *(Foto: D-Wave Systems).*

Wie erleben Sie das von Seiten des Staates, ist man sich da dieser Problematik bewusster?

Wenn ich an eine IT-Sicherheitskonferenz in Berlin denke, an der ich kürzlich teilgenommen habe, dann haben wir außerhalb der engeren Community bis vor ein paar Jahren fast Glaubenskämpfe ausfechten müssen. Seit der Konferenz in Berlin glaube ich, diese Zeit liegt hinter uns. Ich hoffe, dass wir jetzt in eine Phase kommen, wo klar wird, dass es einfach sinnvoll ist, sich mit diesem Thema zu beschäftigen. Wo es hinführen wird, ist nicht klar! Wir sollten nicht versprechen, dass wir alle Probleme lösen. Aber die Quanteninformationstechnologie ist ein Weg, um bestimmte Probleme zu lösen. Sie ist anspruchsvoll, sie zieht gute Leute an, und sie bietet Lösungen an, die keine andere Form von Technologie bieten kann.

Und diese Sensibilität gibt es inzwischen zum Beispiel beim Bundesministerium für Bildung und Forschung?

Die Ministerin, Frau Wanka, hat im Eingangsreferat zur IT-Konferenz gesagt: Wir investieren in die Technologie der Quantenkommunikation. Dieses Forschungsprogramm kommt jetzt. Inzwischen sind auch ganz andere Communities bereit, sich etwas zu diesem Thema anzuhören. Auf der Konferenz ist dann sehr sachlich diskutiert worden, das fand ich sehr gut.

Das heißt, dass Projekte wie das Q.Com-Projekt zur Entwicklung von Quantenrepeatern, das Sie in „Physik in unserer Zeit" vorgestellt haben [5], mit weiterer Förderung rechnen darf?

Ohne Förderung geht das nicht. Ich glaube aber, dass inzwischen auch Industrieunternehmen, vor allem kleinere Firmen, bereit sind, sich mit dem Thema auseinanderzusetzen. Schauen wir mal, was daraus entsteht. Die größeren Unternehmen sind dagegen sehr zurückhaltend. Das ist hier in Deutschland bedauerlicherweise anders als in anderen Ländern. Wir haben auch das Problem, dass es auf diesem Technologiefeld noch zu wenige Start-ups gibt. Das ist in anderen Ländern ebenfalls sehr viel besser.

Das Interview führte
Roland Wengenmayr

Literatur

[1] https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-quantum-technologies-flagship
[2] www.qutega.de/en/home/
[3] www.nature.com/news/chinese-satellite-is-one-giant-step-for-the-quantum-internet-1.20329
[4] Physics News, Physik in unserer Zeit **2016**, *47*(2), 271
[5] C. Becher, Physik in unserer Zeit **2016**, *47*(1), 20.