ETH zürich

NR. 2/2016

GLOBE

NEUES DENKEN

Schlüsseltechnologien und was wir daraus machen

SEITE 14

Materialforschung: besser und billiger

SEITE 10

Warum Tiermodelle für die Forschung wichtig sind

SEITE 42

Ulrich Graf – ein pragmatischer Flugnarr

SEITE 50

Die späten Früchte einer neuen Idee

Der Physiker Renato Renner will zeigen, unter welchen Bedingungen die Quantenkryptographie sicher ist. Die Grundlagen, die er dazu erarbeiten muss, öffnen ihm die Tür zu einer völlig neuen Welt.

Text Felix Würsten

Wenn Renato Renner über seine Arbeit spricht, dann fühlt man sich als Laie schnell einmal in eine sehr abstrakte Welt versetzt. Der Professor für Quanteninformationstheorie befasst sich unter anderem mit den Grundlagen der Quantenkryptographie, von der man sich sicherere Verfahren für die Datenübermittlung erhofft. Im Gegensatz zu den heutigen Verschlüsselungsverfahren, die auf den Gesetzen der klassischen Physik beruhen, stützt sich die Quantenkryptographie auf die Regeln der Quantenmechanik. Das Grundkonzept besteht darin, dass Sender und Empfänger einzelne verschränkte Photonen austauschen, also speziell präparierte Lichtteilchen. Sicher ist dieser Austausch, weil Sender und Empfänger dank der quantenmechanischen Verschränkung sofort bemerken, wenn ein unbefugter Dritter die Daten mitliest.

Auch wenn dieser Austausch von Photonen noch sehr futuristisch tönt: Auf dem Markt sind bereits kommerzielle Geräte erhältlich, mit denen sich Informationen quantenkryptographisch verschlüsseln lassen. Allerdings hat das Verfahren noch einen grossen Nachteil. Da nur einzelne Photonen ausgetauscht werden, lassen sich nur beschränkte Distanzen von maximal 100 Kilometern überwinden. Will man ein grosses Datennetz aufbauen, braucht es also noch Relaisstationen, mit denen man das Signal unterwegs verstärken kann.

ETH in einer speziellen Situation

An diesen sogenannten Quantenrepeaters wird heute intensiv geforscht. «Die Herausforderung besteht darin, Quanteninformationen nicht nur zu übermitteln, sondern auch für kurze Zeit zu speichern», erklärt Renner. Wie das genau gehen soll, dazu gibt es verschiedene konkurrierende Ansätze. Sie werden deshalb so intensiv erforscht, weil man diese Ansätze dereinst auch für den Bau von sogenannten Quantencomputern brauchen wird. Die ETH Zürich befindet sich dabei in einer einmaligen Situation, erklärt Renner: «Die Forschung in unserem Departement deckt alle wichtigen Ansätze ab.»

Renner selbst forscht nicht an einer einzelnen Technologie, sondern ihm geht es um die theoretischen Grundlagen. Die entscheidende Frage für ihn ist: Wie lässt sich mathematisch-physikalisch beweisen, dass die Quantenkryptographie sicher ist? Um diese Frage zu beantworten, braucht es ein Umdenken. Man muss nicht nur zeigen, dass die Quantenmechanik den Austausch der Photonen korrekt erklären kann, sondern man muss auch zeigen, dass diese Theorie vollständig ist, dass sie also alle denkbaren Ereignisse hinreichend beschreiben kann. ›

INFORMATION UND QUANTENPHYSIK

Die Gruppe für Quanteninformationstheorie an der ETH Zürich befasst sich mit der Frage, wie die Verarbeitung und Übermittlung von Informationen mit den physikalischen Gesetzen zusammenhängt. Die Mitglieder der Forschungsgruppe untersuchen zum einen, welche Chancen die Quantenphysik für die Informationsverarbeitung eröffnet und wie man diese Chancen konkret nutzen könnte. Zum anderen erhoffen sich die Forscher auch ein tieferes Verständnis der physikalischen Zusammenhänge, wenn sie quantenmechanische Phänomene unter dem Aspekt der Informationsverarbeitung betrachten.

Bild: Marc Tittgemeyer, Max Planck Institute for Metabolism Research; Nico Gorbach, ETH Zürich

Renato Renner ist Professor für Theoretische Physik und Leiter der Gruppe für Quanteninformationstheorie. Nach seiner Promotion an der ETH Zürich arbeitete er als Research Fellow an der University of Cambridge. 2007 kehrte er als Assistenzprofessor an die ETH zurück.

In einer idealen Welt werden die Photonen so verschränkt, dass ein Angreifer von aussen keine Chance hat, die Informationen unbemerkt mitzulesen. In der realen Welt funktionieren die Geräte allerdings nicht perfekt. Es könnte beispielsweise sein, dass der Sender nicht einzelne Photonen losschickt, sondern jeweils mehrere aufs Mal. Dann wäre es für den Angreifer im Prinzip möglich, einzelne Photonen unbemerkt abzufangen und so die Informationen mitzulesen. Mit Hilfe von komplexen statistischen Berechnungen möchte Renner zeigen, welche Voraussetzungen erfüllt sein müssen, damit Daten auch mit nicht perfekten Geräten sicher übermittelt werden.

Eintritt in eine neue Welt

Die Quantenkryptographie ist für ihn allerdings «nur» Mittel zum Zweck. «Mir geht es um das grundlegende Verständnis der Physik. Wir sind daran, die Türe zu einer völlig neuen Welt zu öffnen, die wir erst ansatzweise kennen. Durch das Öffnen dieser Türe erweitert sich unser Bild, wie die Welt funktioniert.»

Die Quantenphysik ist für Renner ein Musterbeispiel, dass sich Investitionen in die Grundlagenforschung lohnen. Die Grundlagen zur Quantenmechanik wurden vor etwa hundert Jahren entwickelt. Lange schien diese Theorie ein eher abstraktes Konstrukt zu sein, um Phänomene im Mikrokosmos zu beschrieben. Erst als es durch den technologischen Fortschritt in vielen Bereichen möglich wurde, Materialien bis hin auf die atomare Ebene zu erforschen und zu bearbeiten, wurden plötzlich konkrete Anwendungen denkbar.

«Wenn wir die Grundlagen verstehen, dann ergeben sich die Anwendungen von selbst», ist Renner überzeugt. «Die Quantenkryptographie stand nicht am Anfang der Entwicklung, sondern aus dem Verständnis der Quantenphysik kam man auf die Idee, die Quantenmechanik zur Verschlüsselung von Daten zu nutzen.» Und ein Ende ist noch lange nicht absehbar: leistungsfähige Quantencomputer, die bestimmte Aufgaben viel effizienter lösen als heutige Rechenmaschinen, oder hochpräzise Messgeräte sind nur zwei Beispiele, wie die Quantenmechanik unseren Alltag verändern könnte. «Als die ersten Elektronenröhren entwickelt wurden, konnte sich noch niemand vorstellen, wie wir heute mit Handys kommunizieren», meint Renner. «In einer vergleichbaren Situation befinden wir uns zurzeit in den Quantenwissenschaften.»

Klar ist für ihn aber auch: Welche dieser Anwendungen tatsächlich realisiert werden, ist letztlich keine Frage der Technik. «Wenn man ein quantenkryptographisches Datennetz aufbauen will, braucht es dazu grosse Investitionen. Ob diese Investitionen getätigt werden sollen, um eine sichere Datenübermittlung zu ermöglichen, das entscheiden nicht die Physiker, sondern die Gesellschaft.» ○

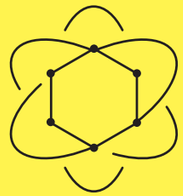
Gruppe für Quanteninformationstheorie:
→ www.qit.ethz.ch

Bild: Daniel Winkler

Wie die Quantenmechanik unsere Welt verändert

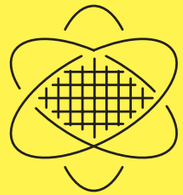
Zusammengestellt von Felix Würsten

Die Grundlagen der Quantenmechanik wurden zwischen 1925 und 1936 erarbeitet, da die klassische Physik das Verhalten von Atomen und Molekülen nicht korrekt beschreiben konnte. Die Quantenmechanik verwendet Begriffe und Konzepte, die der klassischen Physik fundamental widersprechen und daher für Laien nicht mehr anschaulich sind. Dennoch hat die Quantenmechanik inzwischen in vielen Bereichen konkrete Auswirkungen auf unseren Alltag.



Chemie

Basierend auf der Quantenmechanik lässt sich genau voraussagen, wie sich Atome und Moleküle verhalten. Deshalb ist sie eine wichtige Grundlage für Computermodelle, die chemische Reaktionen simulieren.



Materialforschung

Materialien können heute bis auf die atomare Ebene untersucht und verändert werden, unter anderem dank dem Rastertunnelmikroskop, das Anfang der 1980er-Jahre am IBM-Forschungszentrum Rüschlikon entwickelt wurde. Dieses basiert auf einem wichtigen Phänomen der Quantenmechanik, dem Tunneleffekt.

Elektronik

Elektronische Bauteile werden immer kleiner. Doch die Miniaturisierung stösst bald an ihre Grenzen. Wenn Transistoren nur noch wenige Atomlagen dick sind, funktionieren sie nicht mehr nach den Gesetzen der klassischen Physik, sondern verhalten sich nach den Regeln der Quantenmechanik.

Informatik

Es ist der grosse Traum vieler Physiker: ein Computer, der nach den Gesetzen der Quantenmechanik funktioniert. Mit einem solchen Rechner könnten bestimmte Probleme der Informatik effizienter gelöst werden als heute, zum Beispiel die Suche in extrem grossen Datenbanken und die Produktzerlegung extrem langer Zahlen.

Kryptographie

Eine konkrete technische Anwendung der Quantenmechanik zeichnet sich bei der Verschlüsselung von Daten ab (s. Hauptartikel). Die Quantenkryptographie ermöglicht es, Daten so zu übermitteln, dass auch ein Gegner mit beliebig starken Rechenressourcen die Informationen unmöglich mitlesen kann.

Messtechnik

Atomuhren sind äusserst präzise Zeitmesser. Doch die Physiker denken bereits weiter: Sie wollen Atomkernuhren entwickeln, die noch viel genauer sind. Auch sie basieren auf quantenmechanischen Phänomenen. Mit ihnen wäre das GPS, das wir im Alltag für die Positionsbestimmung nutzen, viel präziser.