QUANTENINFORMATIK
QUANTENPHYSIK IN DER INFORMATIONSÜBERTRAGUNG UND INFORMATIONSVERARBEITUNG*

Harald Weinfurter
Sektion Physik, LMU München, Schellingstr 4/III, D-80799 München

Quantenteleportation und Quantencomputer erweitern und verbessern herkömmliche Methoden der Informationsverarbeitung und –übertragung. Diese und weitere Ideen aus dem noch jungen Gebiet der Quanteninformatik basieren auf grundlegenden, aber einfachen Gesetzen der Quantenmechanik. Erste Experimente demonstrieren die faszinierenden Möglichkeiten und bilden heute den Grundstein für eine Informationstechnologie des nächsten Jahrhunderts.

Auf dem Weg zur Quanteninformatik

Informationsübertragung und Informationsverarbeitung sind Schlüsseltechnologien unserer Gesellschaft. Die Verteilung aktueller Nachrichten und der schnelle Zugriff auf gigantische Datenmengen bilden einen wichtigen Baustein des wirtschaftlichen aber auch des politischen Gefüges. Noch vor kurzem undenkbare Szenarien gehören heute zum Alltag:

- Fernsehnachrichten bringen Direktberichterstattungen von allen möglichen und unmöglichen Ereignissen, Zeitungen können daher nur mit detaillierter recherchierten (oder oft auch mit reißerischeren) Nachrichten mit diesen schnellebigen konkurrieren.
- Die Möglichkeit, mit kleinen, tragbaren Telefonen von (fast) allen Orten Gespräche in alle Welt zu führen, möchten viele Leute nicht mehr missen. Dabei ist die Größe der Handy's schon lange nicht mehr durch die erforderliche Elektronik bedingt, sondern lediglich durch die Tatsache, daß wir Menschen sie handhaben müssen. Immerhin werden auf dem freien Platz neue Zusatzfunktionen integriert.
- Seit circa 15 Jahren stehen die immer gleichen, grauen Kisten auf oder unter unseren Schreibtischen. Doch das Innenleben und damit die Leistung der PCs veränderte sich drastisch - für den gleichen Preis bekommt man heute die tausendfache Rechenleistung, eine Rechenleistung, die früher nur von Kubikmeter großen Rechenanlagen erzielt wurde. Und über Internet haben wir heute Zugriff auf Informationsmengen, die keine Bibliothek der Welt alleine zur Verfügung stellen könnte - direkt vom Schreibtisch aus, mit immer höheren Übertragungsraten.

Wesentlich für die Entwicklung der Kommunikationstechnologien waren und sind die enormen Fortschritte auf dem Gebiet der Halbleitertechnik. Mit der Erfindung des Transistors und des Mikrochips begann eine rasante Miniaturisierung elektronischer Bauteile. Am Besten wird das durch das Mooresche Gesetz verdeutlicht. Bereits 1965 legte J. Moore, einer der Gründer der Firma Intel, als Zielvorgabe fest, daß sich die Zahl der Transistoren auf einem Chip jeweils alle 18 Monate verdoppeln sollte. Auch wenn die Verdopplungszeit inzwischen bei 2 Jahren liegt, gibt es keinen anderen Industriezweig, in dem ähnlich Fortschritte über einen solch langen Zeitraum erreicht wurden. Eine derart lawinenartige (exponentielle) Steigerung, wie die der Transistordichte, kommt auch in der Natur nur in wenigen Fällen vor. Die Zahl von Seucheninfizierten oder das Wachstum eines Heuschreckenschwarms wären Beispiele. Allerdings kommt es in diesen Fällen bald zu einer Verlangsamung und schließlich zu einem Stop des Wachstums, etwa wenn es nicht mehr genug Nahrung für alle Heuschrecken gibt.

Nur die Miniaturisierung der Halbleiterbauteile scheint ungehemmt und ohne Grenzen fortzuschreiten. Oder doch nicht? Im Moment kann der Strom zwischen den Transistoren, das heißt das Fließen der Elektronen, mit dem Fließen von Wasser in Schläuchen verglichen werden, entsprechend den Gesetzen der klassischen Physik. Werden jedoch bei fortschreitender Miniaturisierung immer weniger

* aus: Verhandlungen der 120. Tagung der Gesellschaft deutscher Naturforscher und Ärzte, Berlin, September 1998.

Elektronen durch immer engere Leiterbahnen geführt, so kann deren Ausbreitung nur mehr im Rahmen der Quantenmechanik beschrieben werden. Wird die prognostizierte Miniaturisierung eingehalten, wird man spätestens in 15 Jahren die auftretenden Quanteneffekte berücksichtigen müssen. Vielleicht wird man eine Weile diese Effekte umgehen können. Schlußendlich ist aber eine "natürliche" Grenze durch die Größe der Atome gegeben: eine Leiterbahn muß zumindest immer durch eine Kette von Atomen gebildet werden. Auf aktuellen Chips verbinden Bahnen mit einer Breite von 600 nm (Nanometer, millionstel Millimeter) die Transistoren, und sind daher immerhin noch ca. 6000 Atome breit. Doch sehr bald wird man in wesentlich kleinere Dimensionen vorstoßen.

Aber ist es sinnvoll und überhaupt notwendig die auftretenden Quanteneffekte zu vermeiden oder zu umgehen? In herkömmlichen Technologien wird Information durch elektrische Ströme oder starke Lichtpulse dargestellt. Dies ermöglicht die digitale Kodierung von Information und eine große Unempfindlichkeit gegen Rauschen und andere Störungen. Treten aber bei der Weiterleitung von Information Quanteneffekte auf, so erwarten sich viele auf den ersten Blick einen Verlust an Genauigkeit. Denn einerseits besagt die Heisenbergsche Unschärfebeziehung, daß gewisse physikalische Größen, wie Ort und Impuls, nicht zugleich mit beliebiger Genauigkeit gemessen werden können. Und andererseits sind Messungen in der Quantenwelt grundsätzlich statistischer Natur. All das läßt vermuten, daß jedwede Quanteneffekte starkes Rauschen und hohe Fehlerraten verursachen würden. Sicher Gründe genug diese Effekte zu meiden.

Das neue Gebiet der Quanteninformatik zeigt jedoch auf, wie diese und weitere grundlegende Quanteneffekte für die Formulierung neuartiger Kommunikationsmethoden genutzt werden können [1]. So ermöglicht die Quantenkryptographie, gerade unter Ausnutzung der Unschärfebeziehung, erstmals eine vollkommen abhörsichere Übermittlung von Nachrichten. Quantenteleportation erlaubt die Übertragung von Quanteneigenschaften von einem Teilchen auf ein anderes und stellt damit wiederum einen wichtigen Baustein für eine Reihe weiterer Kommunikationsmethoden dar. Die Quanteninformatik beschreibt nicht nur neue Möglichkeiten zur Übertragung sondern auch zur Verarbeitung von Information. Für Quantencomputer wurden leistungsfähigere und schnellere Rechenprogramme vorgeschlagen, als sie für herkömmliche Computer möglich sind. Sollte es gelingen, einen Quantencomputer zu bauen, kann er im Moment schier unlösbare Aufgaben, wie die Primzahlzerlegung großer Zahlen, durchführen.

Es ist eine gewisse Ironie: Auf der einen Seite sind durch den Einsatz der Quantenphysik gebräuchliche Verschlüsselungsverfahren, deren Sicherheit auf der Unmöglichkeit einer effektiven Primzahlzerlegung beruht, mit einem Schlag völlig überholt und nutzlos. Auf der anderen Seite stellt die Quantenkryptographie neue Möglichkeiten zur Nachrichtenübermittlung bereit, deren Sicherheit aber nun nicht mehr durch mathematische Tricks, sondern durch physikalische Gesetze gewährleistet wird.

Im folgenden werden die wichtigsten Elemente der Quantenmechanik besprochen und gezeigt wie sie für neue Kommunikationsmethoden eingesetzt werden können. Im weiteren wird ein Überblick über den momentanen Stand der ersten Experimente zur Quantenteleportation und zum Quantencomputer und der Entwicklungen zu kommerziell nutzbarer Quantenkryptographie gegeben.

Physikalische Grundlagen der Quanteninformatik

Die Leistungsfähigkeit der neuen Quanteninformationsverfahren beruht auf einer Erweiterung der herkömmlichen digitalen Kodierung von Information. Üblicherweise wird die Grundeinheit der Information, das Bit, durch die Werte "0" und "1" dargestellt. Der physikalische Träger der Information ist der jeweiligen technischen Realisierung angepaßt, meist kommt Strom, Spannung oder Licht zum Einsatz. Zum Beispiel wird bei der TTL-Logik in Mikrochips ein Spannungspegel von 0 Volt für logisch "0" und ein Pegel von 5 Volt für "1" verwendet, oder bei der Informationsübertragung mittels Glasfaserleitungen wird kein Licht für "0" und ein kurzer Lichtpuls für "1" gesendet.

Was aber passiert, wenn wir die Lichtpulse immer schwächer machen, bis schließlich nur mehr ein einzelnes Lichtteilchen, ein Photon, übertragen wird? Oder was können wir erwarten, wenn der Schaltvorgang eines Transistors bereits durch ein einzelnes Elektron verursacht wird?

Die Quanteninformatik verwendet als Träger der Information Quantenobjekte. Gibt es für eine bestimmte Eigenschaft zwei mögliche Einstellungen, können diese zur Darstellung von "0" und "1" verwendet werden. Um diese Einstellungen von den klassischen Werten des Bits zu unterscheiden verwenden wir die Quantenschreibweise $|0\rangle$ und $|1\rangle$.

Abbildung 1 zeigt eine Reihe von möglichen Realisierungen: zum Beispiel lineare Polarisation eines Lichtquants mit den Einstellungen $|H\rangle$ (horizontal) und $|V\rangle$ (vertikal) für $|0\rangle$ und $|1\rangle$, oder Grund- und angeregter Zustand eines Atoms.

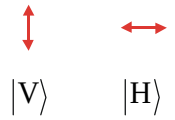
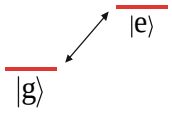
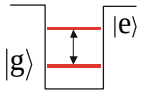
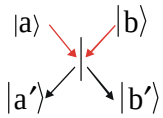
"0"	"1"	Qubit
		Photon: *Lineare* Polarisation
$\|V\rangle$	$\|H\rangle$	
		Photon: *Zirkulare* Polarisation
$\|L\rangle$	$\|R\rangle$	
		Elektron, Neutron, Atomkern: *Spin*
$\|+\frac{1}{2}\hbar\rangle$	$\|-\frac{1}{2}\hbar\rangle$	
		Atom, Ion: *interne Zustände*
$\|e\rangle$		
$\|g\rangle$		
		Quantenpunkte: *Energieniveaus*
$\|e\rangle$		
$\|g\rangle$		
		Teilchen: *Moden am Strahlteiler*
$\|a\rangle$ $\|b\rangle$		
$\|a'\rangle$ $\|b'\rangle$		

Abb. 1: Verschiedene, mögliche experimentelle Realisierungen für ein Qubit. Bei einem Photon zum Beispiel kann man entweder linear polarisiertes oder zikular polarisiertes Licht verwenden, bei einem Elektron oder Neutron den Spin, bei einem Atom Energiezustände und bei jeder Art von Strahlung die beiden Moden vor und hinter einem Strahlteiler.

Während aber für ein klassisches Bit lediglich die zwei Möglichkeiten "0" und "1" erlaubt sind, kann das Quantensystem jeden Zustand, der sich aus einer Überlagerung (Superposition) der beiden Basiseinstellungen ergibt, annehmen. Der allgemeine Zustand lautet daher

$$a_0|0\rangle + a_1|1\rangle \ .$$

Physikalisch bedeutet dies, daß sich das Quantensystem mit der Wahrscheinlichkeit $|a_0|^2$ im Zustand $|0\rangle$ befindet, d.h. den Wert "0" besitzt, und daß es sich mit Wahrscheinlichkeit $|a_1|^2$ im Zustand $|1\rangle$ befindet, also den Wert "1" hat. Der Wert des Bits selbst ist damit quantenmechanisch ungewiß, eine Beobachtung wird einen der beiden Werte mit der angegebenen Wahrscheinlichkeit liefern. Ist aber mit dieser Ungewißheit nicht ein Verlust an Information verbunden?

In der Quantenmechanik ist hier strikt zwischen Superposition und dem klassischen Gemisch zweier Möglichkeiten zu unterscheiden. Wenn wir zum Beispiel an einem Ensemble von Photonen mit gleicher Wahrscheinlichkeit horizontale und vertikale Polarisation detektieren, so kann es sich dabei um ein inkohärentes Gemisch ohne jedweden Informationsgehalt gehandelt haben. Es könnte aber auch eine kohärente Superposition gewesen sein, z.B.

$$\left(|H\rangle + |V\rangle\right)/\sqrt{2} = |45°\rangle \ ,$$

das heißt ein unter 45° linear polarisiertes Ensemble mit eindeutig definierter Information. Wie wir später sehen, bildet diese Gleichzeitigkeit von Ungewißheit und definierter Information den Grundstein für die Sicherheit der Quantenkryptographie.

Die Möglichkeit der Superposition führt, zusammen mit den daraus folgenden Interferenzphänomenen, zu all den Paradoxa und Interpretationsproblemen der Quantenmechanik. Aber sie ist auch einer der Gründe für das wesentlich Neue gegenüber der klassischen Informatik. Wegen diesen zusätzlichen Fähigkeiten hat es sich eingebürgert, für ein Bit, dessen Darstellung und Dynamik quantenmechanisch repräsentiert werden kann, die Bezeichnung Qubit zu verwenden.

Noch interessanter wird es, wenn wir die Überlagerung von Zuständen *mehrerer* Qubits betrachten. Für ein Paar klassischer Bits gibt es die Wertekombinationen "00", "01", "10" und "11". Und in Analogie zu vorher kann man für ein Paar von Qubits die Basiseinstellungen $|00\rangle, |01\rangle, |10\rangle$ und $|11\rangle$ definieren. Die beiden Qubits können nun aber natürlich wieder in jeder Überlagerung dieser Basiszustände präpariert werden. Nehmen wir etwa an, wir hätten ein System von 2 Qubits in folgendem Zustand

$$\left(|01\rangle - |10\rangle\right)/\sqrt{2} \ .$$

Dieser Zustand bedeutet, daß die beiden Qubits in entgegengesetzten Einstellungen gefunden werden. Beobachten wir Qubit 1 mit dem Wert "0", so beobachten wir Qubit 2 mit dem Wert "1", und umgekehrt. Beobachtet man nur ein einziges Qubit, so wird man es mit gleicher Wahrscheinlichkeit in einem der beiden Werte "0" oder "1" beobachten, unter diesen Bedingungen hat das einzelne Qubit also keinen eindeutigen Wert, ihm kann daher kein eindeutiger ("reiner") Quantenzustand zugeordnet werden.

Ein ähnliches Verhalten kennen wir von hochgeworfenen Münzen. Völlig zufällig sehen wir entweder den Wert "Kopf" oder "Zahl" oben liegen. Aber wir wissen, daß der entgegengesetzte Wert auf der unteren Seite ist.

Im Gegensatz zu diesem einfachen klassischen Beispiel kann das Qubit-Paar unter unterschiedlichen

Richtungen, d.h. auch in Überlagerungen der Basiszustände der einzelnen Qubits, beobachtet werden. Nehmen wir ein Paar von Lichtquanten, Photonen. Dieses Paar könnte sich im Zustand $\left(|HV\rangle - |VH\rangle\right)/\sqrt{2}$ befinden. Mißt man das erste Photon mit horizontaler Polarisation, so wird das andere vertikale Polarisation haben, und umgekehrt. Orientiert man aber den Polarisator unter 45° $(=\left(|H\rangle + |V\rangle\right)/\sqrt{2})$ und detektiert das erste Photon, so wird man das andere Photon unter -45° $(=\left(|H\rangle - |V\rangle\right)/\sqrt{2})$ finden! Unabhängig in welche Richtung man den Analysator für das erste Photon einstellt, sobald es in dieser Richtung gefunden wurde (und es wird mit 50% Wahrscheinlichkeit entlang dieser Richtung detektiert), weiß man, daß das zweite Photon genau entgegengesetzt orientiert gemessen werden kann.

E. Schrödinger verwendete den Begriff Verschränkung (engl. entanglement) um dieses charakteristische, quantenmechanische Verhalten zu bezeichnen. Für ihn waren diese nichtklassischen Korrelationen "die Essenz der Quantenmechanik" und auch noch 60 Jahre nach dieser Aussage werden immer neue Eigenschaften dieses *merkwürdigen* Zustands gefunden. Das bekannteste Phänomen wurde von Einstein, Podolski und Rosen in einem Gedankenexperiment aufgezeigt, mit dem sie die Unvollständigkeit der Quantenmechanik demonstrieren wollten. Unter der Annahme, daß sich Messungen an verschränkten Teilchen ähnlich wie klassische Korrelationen beschreiben lassen, leiteten sie Widersprüche innerhalb der Quantenmechanik her. Später konnte aber J. Bell zeigen, daß es eine obere Schranke für klassische Korrelationen in Messungen an Systemen von zwei Teilchen gibt, die von quantenmechanischen Vorhersagen für Messungen an verschränkten Systemen verletzt wird. Da aber viele Experimente darauf hindeuten, daß diese Schranke auch tatsächlich gebrochen wird, müssen wir von hergebrachten Anschauungen abgehen. Nach einer schlußendlichen Bestätigung der Experimente müssen wir akzeptieren, daß das Resultat vor der Messung eines einzelnen Teilchens prinzipiell unbestimmt ist, oder daß dieses Meßergebnis, wie es Einstein schaudernd formulierte, durch "spukhafte Einflüsse" selbst über große Entfernungen hinweg bestimmt wird. Oder es sind überhaupt beide Erklärungen richtig, auch wenn sie für unser klassisches Verständnis nicht sehr plausibel klingen [2].

Wie auch immer diese für das physikalische Verstehen wichtige Diskussion endet, in der Quanteninformatik ist die Verschränkung zwischen Qubits und die dadurch verursachten nichtklassischen Korrelationen der Grundstein für die Quantenteleportation und für den Quantencomputer.

Quantenkryptographie

Seit langer Zeit versuchen Menschen Nachrichten so zu übermitteln, daß außer Sender und Empfänger kein unbefugter Dritter Kenntnis über diese Nachricht erhält. Die klassische Kryptographie stellt viele trickreiche Methoden zur Verfügung, die seit jüngstem nicht nur für militärische, sondern mehr und mehr auch für wirtschaftliche Zwecke genützt werden. Eine dieser Methoden, die "one-time-pad" Verschlüsselung wäre im Prinzip sicher gegen Abhörer. Erreicht wird die hohe Sicherheit dadurch, daß jedes Zeichen des Textes durch ein zufälliges Schlüsselzeichen kodiert wird. Wie von C. Shannon gezeigt wurde, kann man einen derart chiffrierten Text nur bei Kenntnis der richtigen Schlüsselzeichen entschlüsseln. Ein Abhörer kann die Nachricht nicht verstehen, wenn er den Schlüssel nicht kennt.

Sender und Empfänger, nennen wir sie Alice und Bob, können eine Nachricht sicher übermitteln, allerdings nur, wenn der Schlüssel auch wirklich geheim ist. Sie stehen aber damit vor einer sehr schwierigen Aufgabe – vor der eigentlichen Nachrichtenübertragung muß der Schlüssel absolut sicher zwischen Alice und Bob übermittelt werden. In der klassischen Welt kann aber eine Messung übertragener Signale immer so durchgeführt werden, daß Alice und Bob das Abhören nicht bemerken. Und selbst ein durch Kuriere überbrachtes Magnetband könnte, ohne Spuren zu hinterlassen, gelesen worden sein. Wie können Alice und Bob dann gewährleisten, daß der Schlüssel geheim ist?

Hier kann nun die Quantenkryptographie eingesetzt werden, wie sie 1984 von Ch. Bennett und G. Brassard vorgeschlagen wurde [3]. Wie schon erwähnt, sind Quantenobjekte und besonders Superpositionszustände so empfindlich, daß eine einzelne Beobachtung sie vollständig verändern kann. Werden zur Schlüsselübertragung und -erzeugung Quantenobjekte übermittelt, stört ein Abhörer diesen Vorgang dermaßen, daß er leicht zu erkennen ist.

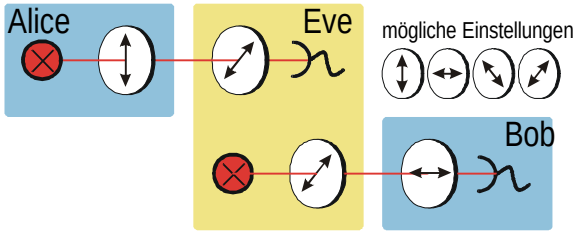


Abb. 2: Versucht Eve (*eavesdropper*, engl., für Abhörer) die Übermittlung von Qubits zwischen Alice und Bob abzuhören, verursacht sie Fehler in den Schlüsselbits. Unterbricht ein Abhörer die Leitung, so kann es sein, daß Bob (wie in diesem Beispiel) ein horizontal polarisiertes Photon detektiert, obwohl Alice ein vertikal polarisiertes Photon abschickte.

Zur sicheren Schlüsselerzeugung und -übertragung sendet Alice Qubits, zum Beispiel polarisierte Photonen zu Bob. Zufällig wählte sie eine von vier Möglichkeiten, entweder H, V, +45° oder -45° für die Polarisationsrichtung. Bob schaltet seinen Polarisationsanalysator ebenfalls zufällig zwischen der H/V Basis und der +45°/-45° Basis, und teilt Alice mit, wann und unter welcher Basiseinstellung er ein Photon detektierte (nicht aber, welches Resultat er erhielt). Alice überprüft in ihrer Liste die Detektionszeitpunkte (es können durch Absorption entlang der Strecke viele Photonen verloren gegangen sein) und teilt ihrerseits Bob mit, wann sie beide die gleiche Basis verwendeten. Da ein von Alice z.B. als horizontal polarisiert gesendetes Photon in der H/V Basis *nur* im H Ausgang detektiert werden kann, besteht für den Fall das beide die gleiche Basis verwendeten eine eindeutige Beziehung zwischen dem von Alice eingestellten Wert und dem von Bob detektierten. Sie können daher diese Bitfolge als Schlüssel verwenden.

Wie können Alice und Bob nun auch sicher sein, daß dieser Vorgang nicht abgehört wurde? Ein Abhörvorgang bei der Quantenübertragung entspricht einer Messung, bei der der Abhörer versucht, die Polarisation des von Alice gesendeten Photons zu detektieren, und ein entsprechend polarisiertes an Bob weiter zu schicken. Ist der Meßaparat des Abhörers gleich orientiert wie der von Alice, so wird er das richtige Bit beobachten und es entsprechend an Bob weiter schicken. Ist dieser Apparat aber in der anderen Basis orientiert, so wird mit 50% Wahrscheinlichkeit ein falscher Bitwert beobachtet, und an Bob gesendet, der seinerseits dann ein falsches Bit detektieren kann (Abb. 2). Im völligen Gegensatz zur Übertragung klassischer Signale verursacht ein Abhören unweigerlich Fehler im Schlüssel. Durch Vergleich einiger weniger Bits des Schlüssels können Alice und Bob daher sofort feststellen, ob die Schlüsselübertragung sicher und ungestört durchgeführt wurde. Der so erhaltene Schlüssel kann ideal zur one-time-pad Chiffrierung verwendet werden und garantiert damit erstmals wirklich sichere Kommunikation.

Quantenteleportation

Nehmen wir an, Alice will einen Gegenstand zu Bob schicken. Wenn sie das Objekt nicht direkt an Bob senden kann, so kann sie doch, innerhalb der klassischen Physik, alle Eigenschaften des Gegenstands genau bestimmen und diese Information an Bob weitergeben. Geeignete Technologie vorausgesetzt, kann er dann eine perfekte Kopie des ursprünglichen Gegenstands herstellen. Unglücklicherweise funktioniert solch eine Strategie nicht wirklich. Versucht man immer kleinere Teile des Objekts zu messen, wie etwa seine Atome und Moleküle, so besagt die Quantenmechanik, daß wir nicht mehr alle seine Eigenschaften beliebig genau bestimmen können. Damit wird eine Übertragung aber

Es gibt aber noch einen anderen Weg. Genauer betrachtet besteht die Aufgabe nur darin, daß Bobs Gegenstand am Ende der Übertragung genau die gleichen Eigenschaften hat wie jener, den Alice am Beginn hatte. Aber es ist nicht notwendig, daß die beiden oder irgendein Dritter Kenntnis über diese Eigenschaften hat. 1993 zeigten Ch. Bennet, G. Brassard, C. Crepeau, R. Josza, A. Peres und W. Wootters, daß mit Hilfe von Verschränkung zwischen Quantenobjekten eine Lösung für diese Problem möglich ist [4].

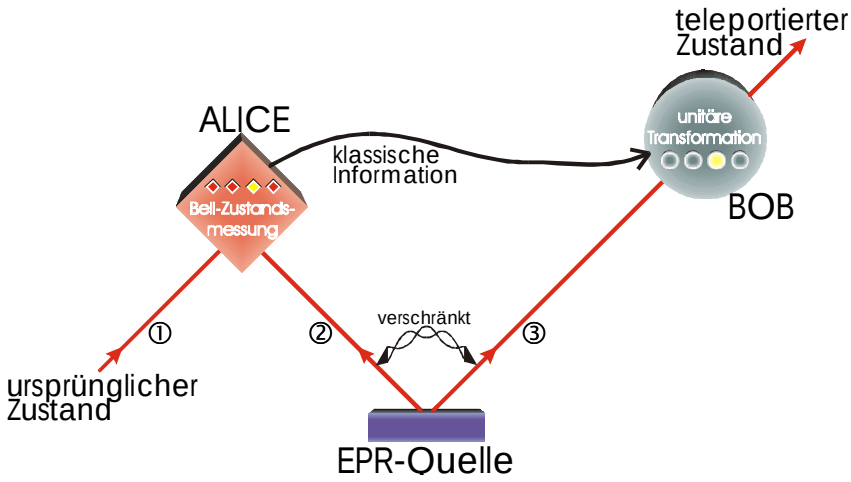


Abb. 3: Schema für Quantenteleportation :

Erhalten Alice und Bob von einer EPR-Quelle (für Einstein-Podolsky-Rosen) jeweils ein Teilchen eines verschränkten Paares, so kann der Quantenzustand von Teilchen 1 auf Teilchen 3 übertragen (teleportiert) werden.

Wie vorher besprochen haben zwei verschränkte Teilchen, oder Qubits, für sich keinen wohlbestimmten Zustand, allerdings wissen wir, daß für die oben angegebene, sogenannte asymmetrische Verschränkung die beiden Teilchen immer in entgegengesetzten Richtungen polarisiert sein werden. Vor Beginn der Teleportation teilen Alice und Bob ein verschränktes Paar von Qubits unter sich auf (Abb. 3). Alice kann dann eine Messung an ihrem und dem zu teleportierenden Qubit durchführen, die keinerlei Information über den Quantenzustand dieser beiden Qubits gibt. Die sogenannte Bell-Zustandsmessung bildet das Qubit-Paar bei Alice auf verschränkte Zustände ab, gibt also nicht über die einzelnen Zustände, sondern über die Korrelationen zwischen den beiden Qubits Auskunft. Nehmen wir an, daß als eines von vier möglichen Resultaten wieder der oben angegebene Zustand gefunden wurde. Dann wissen wir, daß das zu teleportierende Qubit entgegengesetzt zum Zustand des zweiten Qubits von Alice orientiert ist. Da aber dieser Zustand auch entgegengesetzt auf den Zustand von Bobs Teilchen steht, ist der ursprüngliche Zustand gleich dem von Bobs Teilchen. Findet Alice ihre zwei Qubits in einem der anderen vier orthogonalen, verschränkten Zuständen, muß Bob eine von drei festgelegten Manipulationen an seinem Qubits durchführen um dieses in den richtigen Ausgangszustand zu transformieren.

Durch die Messung erfährt Alice also nichts über den zu teleportierenden Zustand. Allerdings wird eine Korrelationskette zwischen Einstellungen der drei Teilchen gebildet, die es Bob erlaubt sein Qubit, nach Erhalt des Meßresultats, in den richten Zustand zu bringen. Im Gegensatz zum klassischen Fall wird keine Kopie erzeugt, da das erste Teilchen bei der Bell-Zustandsmessung seine Eigenschaften verliert, es quasi als leere, gestaltlose Hülle zurückbleibt. Auch wird während des Teleportierens *keine* Materie übertragen. Es genügt die Information über die relativen Eigenschaften zu übermitteln, um den Zustand erfolgreich von einem Teilchen auf ein anderes zu übertragen.

Quantencomputer

Ein klassischer Computer ist eine Maschine, die aufgrund einer bestimmten Eingabe eine Ausgabe, das Resultat der Rechneroperationen, erzeugt. Bei einem klassischen Computer bestehen Eingaben und Ausgaben aus Bits, die stets einen wohldefinierten Wert besitzen. Die Operationen des Computers werden durch die Boolesche Algebra dargestellt. Vom physikalischen Standpunkt ist ein solcher Computer als eine klassische Maschine zu verstehen, bei der die Werte der Bits zum Beispiel durch elektrische Potentiale der Speicherelemente gegeben sind.

In einem Quantencomputer haben wir als Input und Output eine Anzahl von Qubits, und der Computer erzeugt mit Hilfe quantenmechanischer Operationen aus der Eingabe die Ausgabe (Abb. 4). Formal beschrieben läßt sich die Operation eines solchen Computer darstellen als

$$|Ausgabe\rangle = U|Eingabe\rangle \ ,$$

wobei im einfachsten Fall der Eingabezustand, z.B. $|Eingabe\rangle = |0110...010\rangle$, einfach die direkte Übersetzung der klassischen Eingabe sein kann, und U die Rechenoperation, eine sogenannte unitäre Transformation, ist. Aus diesem Eingangszustand wird durch die Operation ein Ausgangszustand entstehen, der natürlich gerade der Bitfolge des klassischen Resultats entsprechen muß. Wir haben also diese spezielle Berechnung mittels unseres Quantensystems durchgeführt - aber offensichtlich noch nichts gewonnen.

Allerdings haben wir noch nicht auf die charakteristischen Eigenschaften der Quantenmechanik zurückgegriffen, wie etwa Superposition, Interferenz und die Verschränkung zwischen Qubits.

Die Superposition ermöglicht uns, den Eingabezustand als Überlagerung vieler einzelner klassischer Möglichkeiten zu konstruieren:

$$|Eingabe\rangle = \{|Eingabe\rangle_1 + |Eingabe\rangle_2 + ... + |Eingabe\rangle_N\} / \sqrt{N}$$

Mit diesem Eingabezustand erhalten wir als Ausgabe eine Überlagerung der Resultate aller Einzelrechnungen, die durch den Quantencomputer parallel durchgeführt wurden:

$$|Ausgabe\rangle = \{|Ausgabe\rangle_1 + |Ausgabe\rangle_2 + ... + |Ausgabe\rangle_N\} / \sqrt{N}$$

Beim Auslesen des Ausgaberegisters wird jedoch jeweils nur eines dieser Resultate mit der entsprechenden, hier gleich großen Wahrscheinlichkeit beobachtet werden. Wir müßten den Rechenvorgang daher wieder sehr oft wiederholen und haben also soweit noch immer nichts gewonnen.

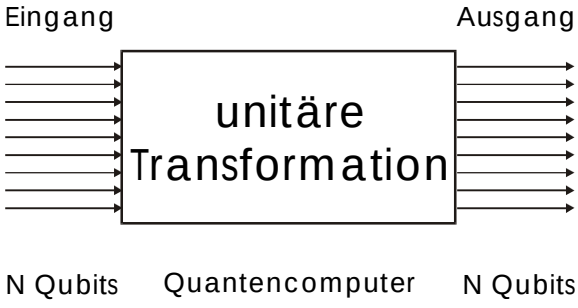


Abb. 4: Prinzip eines Quantencomputers : Der Rechenalgorithmus wird durch eine unitäre Operation repräsentiert, die N Eingangs-Qubits mit den N Ausgangs-Qubits verknüpft.

Der wesentliche Punkt liegt jedoch darin, daß es mit Hilfe des massiven Quantenparallelismus möglich ist, Eigenschaften herauszufinden, die allen Resultaten gemeinsam ist, ohne daß man die Rechnung für jeden einzelnen Eingangszustand separat durchführen muß. Eine Möglichkeit ist zum Beispiel die Bestimmung der Periode einer Funktion durch die Quanten-Fourier-Transformation. Beträgt die Periode der Funktion M, so haben die Ausgabewerte im Abstand M jeweils den gleichen Wert, das heißt wir erhalten den gleichen Quantenzustand für viele der Einzelrechnungen. Nehmen wir an, daß der Quantencomputer die Rechnung gleichzeitig für so viele Eingangszustände durchführte, daß bereits mehrere Perioden der Funktion abgedeckt werden. Dann haben viele Komponenten der Ausgabesuperposition den gleichen Wert und können, nach der abschließenden Fourier-Transformation, interferieren. Durch weitreichende destruktive Interferenz wird der Ausgabezustand auf sehr wenige Komponenten reduziert, aus deren Messung sich die Periode M ableiten läßt. An Stelle von vielen Einzelrechnungen und der klassischen Fourier-Transformation genügen wenige Quantenparallelrechnungen zur Lösung des Problems.

Diese Tatsachen erlaubten P. Shor die Formulierung des bisher effektivsten Quantenalgorithmus. Die Zerlegung einer großen Zahl wird exponentiell schwieriger, je größer die Zahl ist. Verdoppelt man bei einer Multiplikation die Anzahl der Stellen der zu multiplizierenden Zahl, so verdoppelt sich auch die benötigte Rechenzeit und der Speicherbedarf. Hingegen wird die Rechendauer bei der Primzahlzerlegung sehr schnell so groß, daß es ohne weiteres möglich ist, eine Zahl zu finden, die so groß ist, daß sie von keinem Computer in vernünftiger Zeit in ihre Primfaktoren zerlegt werden kann (man kann z.B. sehr schnell das Ergebnis von 107x53 berechnen, aber es dauert schon sehr viel länger die Primfaktoren von 5671 zu finden). Für seinen Quantenalgorithmus verwendete Shor ein bekanntes Theorem der Zahlentheorie, demzufolge die Faktorisierung einer Zahl zurückgeführt werden kann auf das Auffinden einer Periode einer Funktion [5].

Experimentelle Realisierungen und Entwicklungen

Während der letzten Jahrzehnte wurden große Fortschritte im Experimentieren mit einzelnen Quanten erzielt. Mittels besserer Laser und leistungsfähigerer Vakuumapparaturen gelangen wichtige Ergebnisse beim Fangen und Kühlen von Atomen und einzelnen Ionen, bei der resonanten Überhöhung von Atom-Lichtwechselwirkung und bei Experimenten mit einzelnen Photonen. Gerade letztere bilden, wegen der Möglichkeit die Lichtquanten über große Entfernungen zu senden, einen soliden Grundstock für die Entwicklung der experimentellen Quantenkommunikation. Wesentlich schwieriger ist der Bau des Quantencomputers. Die große Empfindlichkeit eines Quantenzustands gegen äußere Einflüsse wirkt sich natürlich besonders beim Arbeiten mit vielen Qubits aus. Im folgenden geben wir einen kurzen Überblick über den Stand der Experimente zur Realisierung der faszinierenden Vorschläge aus dem Gebiet der Quanteninformationsübertragung und -verarbeitung.

Die Übertragung einzelner Qubits genügt bereits für die Quantenkryptographie. Daher gibt es seit den ersten Experimenten 1991 schon weit fortgeschrittene Systeme zur geheimen Schlüsselerzeugung. Die Entwicklung geht zu einfach handhabbaren Geräten, die mit möglichst wenig Eingriffen durch die Benutzer selbständig über längere Zeiten hinweg arbeiten. Waren noch vor kurzem große optische Tische in klimatisierten Labors für ein gutes Rauschverhalten der Quantenkryptographie notwendig, gibt es heute bereits Systeme, die in Behältern, etwa von der Größe eines Fernsehers, überallhin getragen werden können. So gelang es der Gruppe von N. Gisin an der Universität Genf Quantenkryptographie über 25 km Entfernung durchzuführen. Die Geräte von Alice und Bob befanden sich in zwei Postämtern und die Photonen wurden durch eine kommerzielle Glasfaserleitung der Swisscom gesendet [6].

Wichtig für das Funktionieren der Quantenkryptographie ist, daß die "Quantenleitung" nicht durch Verstärker oder Umschalter unterbrochen ist. Nur die vollkommen ungestörte Weiterleitung der Photonen gewährleistet eine korrekte Schlüsselerzeugung. Aufgrund der Absorption in den Glasfasern sinken aber die Raten mit denen Schlüsselbits entstehen, bis schließlich das Detektorrauschen zu große Fehlerraten verursacht. Eine Weiterentwicklung der Detektoren und anderer Komponenten läßt eine maximale Übertragungsstrecke in Glasfasern von ca. 100 km realistisch erscheinen. Um noch größere Distanzen zu überbrücken, arbeitet das Team von R. Hughes am National Laboratory in Los Alamos, USA, an der sogenannten "free-space" Quantenkryptographie [7]. Hier sollen die Photonen zwischen Alice und Bob mittels erdnaher Satelliten übertragen werden. Unter der Annahme, daß der Abhörer nicht auf den Satellit zugreifen kann, besteht sogar die Möglichkeit, daß Alice und Bob jeweils mit dem Satelliten Schlüsselaustausch durchführen. Aus den beiden Einzelschlüsseln kann ein neuer, genauso geheimer Schlüssel zwischen Alice und Bob erzeugt werden, der ihnen damit sichere Kommunikation über, im Prinzip, beliebig große Distanzen erlaubt.

In unseren Labors versuchen wir, Sender- und Empfängermodule möglichst kompakt und stabil zu

bauen. Damit der Benutzer wirklich alle Vorteile der Quantenkryptographie genießen kann, sollen die Module zumindest auf die Größe eines Modems reduziert werden, und sich direkt an den Tischcomputer anschließen lassen. Ohne Eingriff von außen werden nur selten notwendige Nachjustierungen automatisch vorgenommen, die sichere Schlüsselerzeugung lauft im Hintergrund mit einem Netzwerk von Anwendern. In ersten Prototypen werden als Photonenquelle Laserdioden verwendet, deren nanosekundenlange Pulse entsprechend polarisiert und abgeschwächt in eine Glasfaserleitung eingekoppelt werden. Hochempfindliche Detektoren registrieren einzelne Lichtquanten in Bobs Modul.

Die Pulse enthalten nur mit geringer Wahrscheinlichkeit ein Photon und noch wesentlich unwahrscheinlicher enthalten sie mehr als eines. Die Sicherheit des Systems kann erhöht werden, wenn richtige Einzelphotonenquellen verwendet werden. Zur Zeit werden dazu mehrere Möglichkeiten untersucht. Eine bereits realisierte, aber für einfache Quantenkryptographie noch zu aufwendige Methode ist durch den Prozeß der parametrischen Fluoreszenz gegeben. Dabei wird bei Durchgang eines ultravioletten (UV) Laserstrahls durch einen optisch nichtlinearen Kristall ein Bruchteil der UV-Photonen in Paare von roten Photonen umgewandelt. Die beiden roten Photonen die in solch einem Prozeß entstehen fliegen auf Grund von Impuls- und Energieerhaltung in ganz bestimmte Richtungen (Abb. 5). Detektiert man daher in einem Ausgangsstrahl ein Photon, so weiß man, daß in den anderen Strahl ebenso ein Photon emittiert wurde - die fast ideale Einzelphotonquelle. Allerdings ist zu ihrem Betrieb wegen des geringen Wirkungsgrades ein sehr starker, aufwendiger Laser notwendig. Für Wellenlängen, die zur Übertragung in Glasfasern ($\lambda \approx 1.5$ mikrometer) geeigneter sind, kann man bereits kompakte und trotzdem leistungsstarke Laserdioden verwenden. Für die Quantenkryptographie erhält man so, verbesserte Detektoren vorausgesetzt, eine geeignete Einzelphotonquelle.

Die parametrische Fluoreszenz ist aber unerläßlich für die Erzeugung von verschränkten Photonenpaaren [8], wie sie für die Quantenteleportation benötigt werden. Es ist nach wie vor eine große Herausforderung in der experimentellen Quantenoptik verschränkte Teilchenpaare zu erzeugen. Spontane Umwandlungsprozesse, wie die parametrische Fluoreszenz oder die Dissoziation von Molekülen, sind seit längerem in Verwendung. Allerdings erschwert die geringe Effizienz und die prinzipielle Unkontrollierbarkeit des Emissionszeitpunktes manche Anwendung. Kürzlich gelang es Forschern an der ENS Paris und am NIST in Boulder, USA, erstmals die Zustände von Atomen beziehungsweise von Ionen zu verschränken [9]. Zwar ist die Qualität der Verschränkung zwischen den Atomen und Ionen noch nicht so gut wie die von Photonenpaaren, aber wie wir weiter unten sehen werden, bilden diese Experimente den Grundstein für die ersten Quantenlogikoperationen zukünftiger Quantencomputer.

In unserem Experiment zur Quantenteleportation [10] verwendeten wir zur Erzeugung der Photonen durch die parametrische Fluoreszenz einen gepulsten UV-Laserstrahl (Abb. 6). In einigen wenigen Pulsen wurden zwei Photonenpaare erzeugt, von denen das eine, verschränkte Paar zwischen Alice und Bob aufgeteilt wurde. Das Photon, das das zu teleportierende Qubit tragen sollte, wurde wie oben erwähnt durch die Detektion eines vierten Photons als Einzelphoton präpariert. Durch einen Polarisator kann ein bestimmtes Qubit für dieses Photon eingestellt werden. Aufgabe für Alice und Bob ist es nun, den Zustand dieses Photons zu übertragen, abschließend wird durch Polarisationsanalyse überprüft, ob und wie gut die Teleportation funktioniert hat.

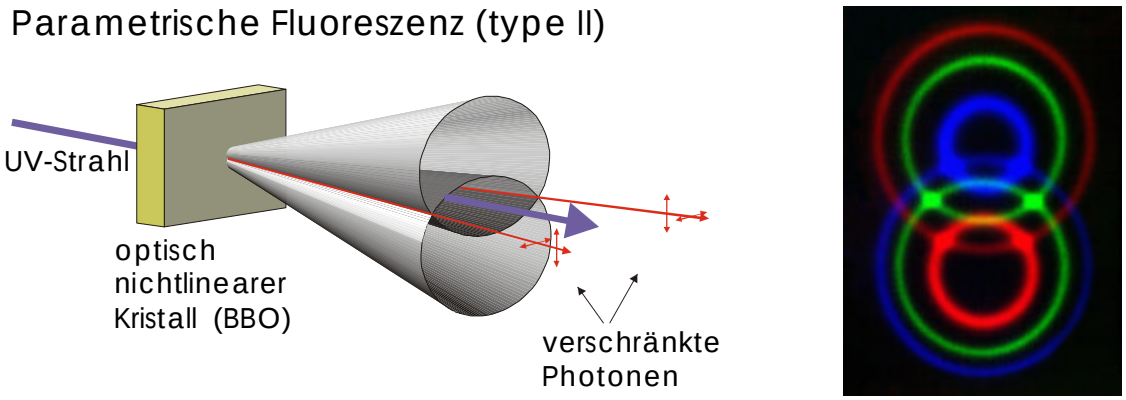


Abb. 5: Typ II parametrische Fluoreszenz : Ein optisch nichtlinearer Kristall wird von einem ultra-violetten (UV) Laserstrahl beleuchtet. Es werden mit geringer Wahrscheinlichkeit dann 2 Photonen emittiert, die verschieden polarisiert sind. Unter ganz bestimmten Emissionsrichtungen (Schnittlinien der beiden Kegeln) sind diese Photonen miteinander verschränkt. Das Photo rechts zeigt die emitierten Photonen für drei verschiedene Wellenlängen, Photonen in den Kreuzungspunkten der mittleren Kreise sind verschränkt.

Die größte Herausforderung bei diesem Experiment war die Bell-Zustandsanalyse. Dabei werden die beiden Photonen von Alice derart zusammen gemessen, daß sie auf einen verschränkten Zustand abgebildet werden. Es genügt nicht, die Photonen gleichzeitig zu messen. Im Prinzip ist eine Wechselwirkung zwischen zu analysierenden Qubits notwendig, wie sie auch für die Erzeugung von Verschränkung und später für die Quantenlogikoperationen des Quantencomputers benötigt wird.

Im Experiment verwendeten wir Interferenzeffekte zwischen den beiden Photonen. Hierbei reduziert sich zwar die Effizienz auf die Hälfte, aber die gute Qualität der interferometrischen Analyse wird im Moment mit keiner anderen Methode erreicht. Zu diesem Zweck werden die beiden Photonen an einem Strahlteiler, ein halbversilberter Spiegel, überlagert. Sind die einfallenden Strahlen gut justiert, kann man hinter dem Strahlteiler nicht mehr entscheiden, welches Photon aus welcher Richtung auf den Strahlteiler fiel und Interferenz tritt auf. Befinden sich zwei Photonen im antisymmetrischen, verschränkten Zustand, so verhalten sie sich auch am Strahlteiler gerade "entgegengesetzt", das heißt, sie verlassen den Strahlteiler immer in entgegengesetzten Ausgängen. In den anderen drei möglichen Fällen gehen beide Photonen immer gemeinsam in einen Ausgang.

Wir beschränkten uns für die erste Demonstration der Quantenteleportation auf die Analyse eines einzigen verschränkten Zustands. Beobachtet Alice hinter dem Strahlteiler in jedem der beiden Detektoren ein Photon, so registriert sie damit den antisymmetrischen, verschränkten Zustand. Wir wissen, daß dann Bobs Photon bereits den Zustand des zu teleportierenden Qubits hat, und Bob kann daher dieses Photon zur Polarisationsanalyse freigeben um die Qualität der Teleportation zu demonstrieren.

Ähnlich wie bei der Quantenkryptographie gibt auch hier wieder die Absorption der Photonen entlang der Glasfaserstrecke eine obere Grenze für die Entfernung zwischen Alice und Bob. Verschränkung zwischen 2 Photonen konnte an der Universität Genf bereits für Entfernungen von 10km nachgewiesen werden.

Während unser erstes Experiment ein Qubit von einem Photon auf ein anderes teleportierte, gelang es vor kurzem auch einen vielwertigen, kontinuierlichen Quantenzustand zu übertragen. In einem Experiment am Caltech, USA, konnten die Eigenschaften eines Lichtfeldes auf ein anderes übertragen werden [11]. Nach der erstmaligen Erzeugung von Verschränkung zwischen Atomen wird als nächster Schritt bald die Übertragung von Quanteneigenschaften von einem Atom auf ein anderes möglich sein. Zwar reicht das sicher noch nicht um Science-fiction Träume wahr werden zu lassen, aber solch ein Experiment bildet die Grundlage für Quantenspeicher und den Quantencomputer.

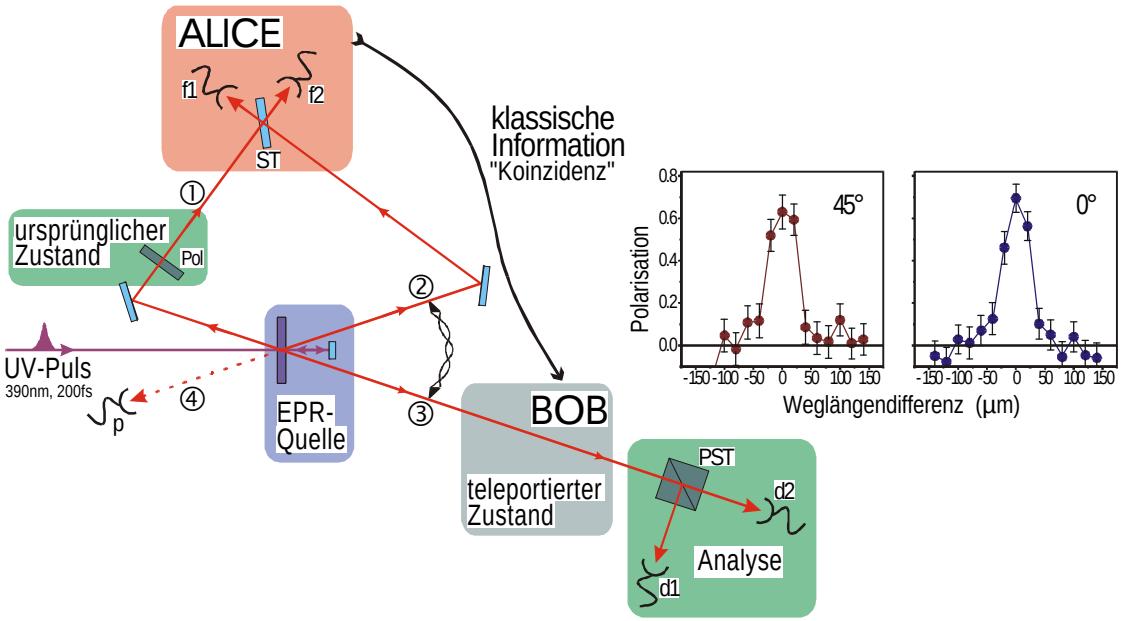


Abb. 6: Experimenteller Aufbau des Quantenteleportationsexperiments : Ein kurzer UV-Puls beleuchtet einen nichtlinearen Kristall und erzeugt 4 Photonen in unterschiedlichen Richtungen. Überlappen Photon 1 und 2 am Strahlteiler (ST), d.h. die Weglängendifferenz ist gleich 0, so kann der Quantenzustand (hier Polarisation) von Photon 1 auf Photon 3 teleportiert werden.
Mittels Polarisationsanalyse am polarisierenden Strahlteiler (PST) wird die Qualität der Übertragung überprüft. Die Meßreihen zeigen, daß die Polarisation mit ca. 65% Genauigkeit übertragen werden konnte.

Bei der Implementierung des Quantencomputers gehen wir davon aus, daß wir die Qubits in einer geeigneten Form als Reihe von Atomen, Ionen oder etwa Kernspins vorliegen haben. Es ist nun möglich, die gesamte unitäre Transformation U in Einzelschritte zu zerlegen. Diese einzelnen Operationen werden durch sogenannte Quantengatter durchgeführt, die jeweils 2 Qubits miteinander koppeln. Die Kopplung muß konditionelle Logikoperationen durchführen, bei denen die Änderung eines Qubits bedingt ist durch den Zustand des anderen Qubits, ähnlich einer logischen XOR-Verknüpfung beim herkömmlichen Computer. Mithilfe dieser Operation und Manipulationen an einzelnen Qubits können zwei Qubits miteinander verschränkt werden, und sie können, in der Umkehrung der Operation, auf einen verschränkten Zustand abgebildet werden. Es können aber dann auch durch Aneinanderreihen vieler 2 und 1-Qubit-Operationen alle beliebigen unitären Transformationen und Rechenoperationen durchgeführt werden.

Wie kann solch ein Quantengatter realisiert werden? Es gibt in der Literatur verschiedene Vorschläge die starke Kopplungen beschreiben: zum Beispiel zwischen Quantenpunkten, zwischen den Kernspins der Atome eines Moleküls, oder zwischen den Ionen in einer Falle.

Erste mini-Quantenalgorithmen wurden bereits mittels Kernspinresonanz von Molekülen mit 2 und 3 Qubits durchgeführt [12]. Wichtig dabei war vor allem der hohe Entwicklungsstand kommerzieller Kernspinresonanzanlagen, als Nachteil kommt aber die schlechte Skalierbarkeit dieser Systeme zum Tragen. Da alle beteiligten Qubits auf einem Molekül sitzen, und es zwischen Qubits unterschiedlicher Moleküle zu keiner Kopplung kommen kann, ist der Schritt zu mehr und mehr Qubits sehr schwierig. Leichter erweiterbar scheint eine Reihe von Kernspins in einem Festkörper zu sein, welche über elektronische Zustände gekoppelt sind [13].

Eine vielversprechende Idee zur Implementierung eines Quantengatters verwendet Ketten von Ionen, die in einer Falle gespeichert wurden [14] (Abb. 7). Die Änderung eines Qubits kann eine Änderung des Schwingungsverhaltens verursachen. Zum Beispiel werden alle Ionen der Kette gemeinsam zu schwingen beginnen, wenn durch einen bestimmten Laserpuls auf eines der Ionen dessen Zustand invertiert wird. Umgekehrt, wenn ein anderes Ion durch einen zweiten Laserpuls beleuchtet wird, so ist die Änderung dessen Zustands abhängig davon, ob die Kette schwingt oder in Ruhe ist. Mehrere Labors weltweit versuchen nun, solch eine Kette so weit zu kühlen, bis wirklich alle Ionen in Ruhe sind. Auch wenn dies am NIST in Boulder, USA, und am MPQ in Garching bereits für zwei Ionen gelang, so ist es auch hier noch ein langer Weg zu einer hinreichend großen Zahl von Ionen.

Aber es ist nicht nur die Handhabung und Kontrolle vieler Qubits die Schwierigkeiten bereitet. Die Qubits eines Quantencomputers koppeln im Idealfall nur untereinander, aber nicht an andere externe Systeme oder Teilchen. Kommt es doch zu einer Wechselwirkung und Kopplung mit der Außenwelt, so wird der Zustand eines Qubits gestört, im schlimmsten Fall völlig gelöscht. Dieser Verlust von Quanteninformation an nicht kontrollierbare Teilchen wird als Dekohärenz bezeichnet. Die mittlere Dauer, bis durch Streuung, Stöße oder andere Prozesse die Quanteninformation zerstört ist, ist die Dekohärenzzeit bezeichnet. Sie ist um so kürzer, je stärker andere Systeme mit dem Qubit wechselwirken. Koppeln sehr viele andere Teilchen an ein Qubit, zum Beispiel in einem Festkörper, so ist diese Zeit (weniger als eine Nanosekunde) viel kürzer als für ein einzelnes Ion im Hochvakuum einer Ionenfallenkammer (länger als eine Sekunde). Handelt es sich aber um einen verschränkten Quantenzustand aus vielen Qubits, reicht bereits die Störung nur eines einzelnen dieser Qubits um die Information des Gesamtzustands zu löschen. Die Dekohärenzzeit sinkt dann exponentiell – längere Rechnungen mit vielen Qubits werden dadurch unmöglich [15]. Glücklicherweise entdeckten Shor und Steane Methoden zur Quantenfehlerkorrektur [16]. Dabei wird die Quanteninformation eines Qubits auf mehrere aufgeteilt, so daß die Störung eines einzelnen wieder rückgängig gemacht werden kann. So gibt es doch wieder gute Chancen, daß auch komplexe Berechnungen eines Tages am Quantencomputer gelöst werden können.

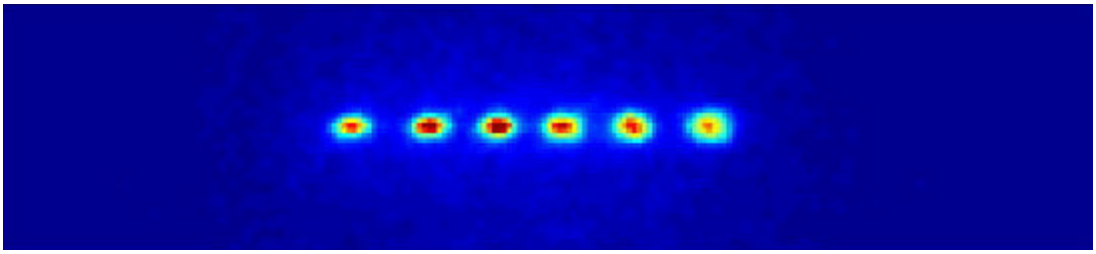


Abb. 7: Fluoreszenz einer Ionenkette : In einer linearen Ionenfalle werden die Ionen gespeichert und mit Laserlicht zur Fluoreszenz angeregt. Werden diese Ionen bis zum absoluten Stillstand abgebremst, können sie als die Qubits eines Quantencomputers verwendet werden. (Foto H.-C. Nägerl)

Zusammenfassung

Die grundlegenden Gesetze der Quantenmechanik bilden die Basis für faszinierende Erweiterungen und Verbesserungen herkömmlicher Methoden zur Informationsübertragung und –verarbeitung. Die Quantenkryptographie ermöglicht erstmals absolut sichere Kommunikation. Erste Prototypen beweisen bereits ihre Leistungsfähigkeit abseits von geschützten Laborbedingungen. In weitläufigen Glasfaserleitungen wurde geheimes Schlüsselmaterial über 25 km erzeugt. Die nächste Generation dieser Geräte sollte bereits auf Ihrem Schreibtisch Platz finden und sichere Datenübertragung in Computernetzwerken garantieren.

Quantenteleportation ermöglicht die Übertragung von Quanteneigenschaften und damit im Prinzip – auch innerhalb der Quantenphysik – die Rekonstruktion eines Objekts an einem entfernten Ort. Auch wenn sie sicher nicht für Reisen zu fremden Planeten verwendet werden kann, so bildet diese Idee die Grundlage für wichtige Elemente der Quanteninformatik. Die Speicherung von Quanteneigenschaften, effiziente Kommunikation über verrauschte Leitungen und Datentransfer zwischen Quantencomputer basieren auf der Quantenteleportation.

Der Quantencomputer ist die wohl faszinierendste Neuerung. Obwohl die Grundidee durchaus ähnlich zu klassischen Computerstrukturen ist, ermöglicht das Superpositionsprinzip und Quanteninterferenzeffekte radikale Erweiterungen von herkömmlichen Rechenalgorithmen. Es ist noch nicht absehbar, welche Aufgaben besser mit Quantenalgorithmen gelöst werden können. Erste Beispiele, wie die Primfaktorzerlegung zeigen, daß Berechnungen, für die herkömmliche Computer Jahrhunderte benötigen, auf einem Quantencomputer in einigen Minuten gelöst werden können.

Allerdings gibt es diesen Quantencomputer heute erst auf dem Papier. Unterschiedliche Methoden wie Kernspinresonanz oder Spektroskopie an Ionenketten und Quantenpunkten werden zur Zeit untersucht und für eine mögliche Anwendung entscheidend weiterentwickelt. Welches der Systeme sich am Besten eignet und es eines Tages erlaubt die Leistungsfähigkeit der Quanteninformatik nutzbar zu machen, ist noch nicht absehbar. Die Lösung wartet nicht an der nächsten Ecke, aber der Weg dahin bringt auch für andere Zweige von Wissenschaft und Industrie wertvolle technologische Entwicklungen und vielleicht auch ein besseres Verständnis für die oft so paradoxen und kontraintuitiven Quantenphänomene.

Ich danke meinen ehemaligen Kollegen aus der Gruppe von Anton Zeilinger am Institut für Experimentalphysik der Universität Innsbruck für lebhafte Diskussionen und die intensive, aber immer freudige Arbeit an unseren Experimenten. Diese Arbeit wurde unterstützt von der *Österreichischen Akademie der Wissenschaften* und dem österreischischen *Fonds zur Förderung der wissenschaftlichen Forschung* (Proj. S6502, Y48-PHY).

Literatur

[1] *Bennett, C.H.*: Quantuminformation. Physics Today, Oktober 1995, pp. 24; *Lo, H.-K., Popescu, S., Spiller, T.P.* (eds.): Introduction to Quantum Computation. Clarendon Press, Oxford, 1998; *Bouwmeester, D., Ekert, A., Zeilinger, A.* (eds.): The Physics of Quantum Information. Springer-Verlag, Berlin, 1999.

[2] Eine umfassende Sammlung der Originalarbeiten zum Thema Verschränkung, Bellsches Theorem und den Interpretationen der Quantenmechanik findet sich in *Wheeler, J. A., Zurek, W. H.* (eds.): Quantum Theory and Measurement. Princeton University Press, Princeton, 1983.

[3] *Benett, C.H., Brassard, G.*: Quantum Cryptography: Public Key Distribution and Coin Tossing, Proc. IEEE Int. Conf. Computer Systems and Signal Processing, Bangalore, India. IEEE, New York, pp.175, (1984).

[4] *Bennet, C.H., Brassard, G., Crépeau, C., Josza, R., Peres, A., Wootters, W.K.*: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett., 70, 1895-1899 (1993).

[5] *Shor, P.W.*: Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26, 1484 (19974). Ein weiterer wichtiger Quantenalgorithmus stammt von *Gover, L.*: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. 79, 325-328 (1997).

[6] *Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., Gisin, N.*: 'Plug and Play' systems for quantum cryptography. Appl. Phys. Lett. 70, 793 (1997).

[7] *Buttler, W.T., Hughes, R.J., Kwiat, P.G., Lamoreaux, S.K., Luther, G.G., Morgan, G.L., Nordholt, J.E., Peterson C.G., Simmons, C.M.*: Practical Free-Space Quantum Key Distribution over 1 km. Phys. Rev. Lett. 81, 3283-3286 (1998).

[8] *Kwiat, P.G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A.V., Shih, Y.H.*: New high-intensity source of polarization-entangled photon pairs. Phys. Rev. Lett. 75, 4337-4341 (1995).

[9] *Hagley, E., Maître, X., Nogues, G., Wunderlich, C., Brune, M., Raimond, J.M., Haroche, S.*: Generation of EPR-pairs of atoms. Phys. Rev. Lett., 79, 1-5 (1997); *Turchette, Q.A., Wood, C.S., King, B.E., Myatt, C.J., Leibfried, D., Itano, W.M., Monroe, C., Wineland, D.J.*: Deterministic entanglement of two trapped ions. Phys. Rev. Lett., 81, 3631-3634 (1998).

[10] *Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.*: Experimental Quantum Teleportation. Nature, 390, 575-579 (1997).

[11] *Furusawa, A., Sørenson, J.L., Braunstein, S.L., Fuchs, C.A., Kimble, H.J., Polzik, E.S.*: Unconditional quantum teleportation. Science, 282, 706 (1998).

[12] *Jones,J. A., Mosca, M., Hansen, R. H..:* Implementation of a quantum search algorithm on a quantum computer, Nature, 393, 344-346 (1998); *Chuang, I.L., Gershenfeld, N., Kubinec, M.G.:* Experimental Implementation of Fast Quantum Searching Phys. Rev. Lett., 80, 3408-3411 (1998).

[13] Kane, B.E.: A Si-based nuclear-spin quantum computer, Nature, 393, 133-138 (1998).

[14] *Cirac, J.I., Zoller, P.*: Quantum computation with cold trapped ions. Phys. Rev. Lett., 74, 4091-4094 (1995).

[15] *Landauer, R.*: Is information physical?. Physics Today, May 1991, pp23-29.

[16] *Shor,P.W.*: Scheme for reducing decoherence in quantum computer memory Phys. Rev. A 52, R2493-R2496 (1995); *Steane, A.*: Multiple particle interference and quantum error correction Proc. Roy. Soc. Lond. A. 452, 2551 (1996).