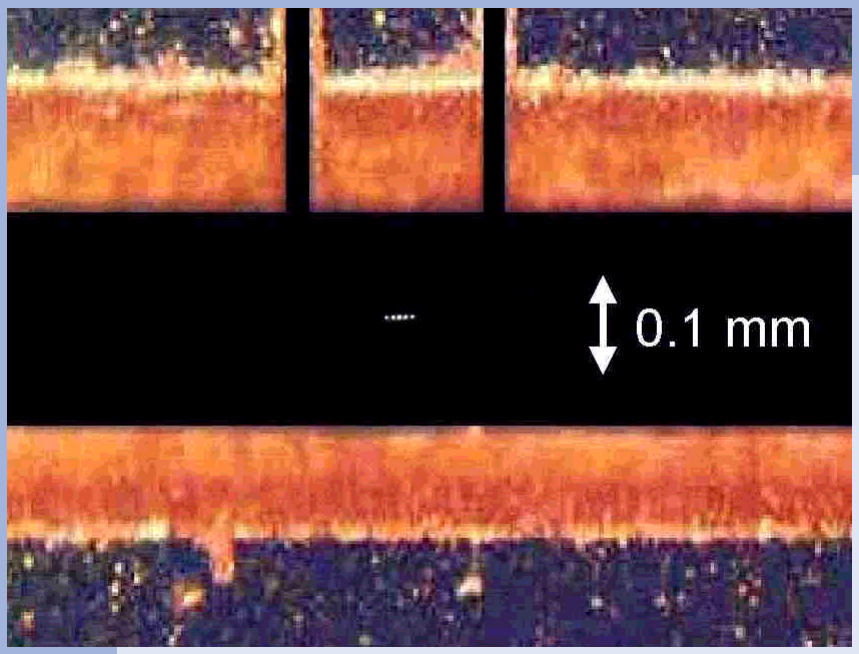
Physikalische Blätter

Web-Spezial

Nr. 1



Quanteninformation

Kryptographie

Computer

Korrelationen

Auszüge aus den
Physikalischen Blättern

DPG WILEY-VCH

Quantenoptik

Quantenkryptographie

Die eigentümliche Natur der Quantenmechanik läßt sich für die Übertragung geheimer Nachrichten ausnutzen

Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden

Obwohl die Quantenmechanik sämtliche Gebiete der modernen Physik durchzieht, stoßen wir immer wieder auf Probleme, wenn wir ihre Vorhersagen mit unserer klassischen Anschauung zu verstehen versuchen. Seit einigen Jahren geht der Trend dahin, die seltsam anmutenden Eigenheiten der Quantenwelt – Nichtlokalität, Superpositionsprinzip, Unschärferelation – auszunutzen, um Dinge zu realisieren, die innerhalb der klassischen Physik unmöglich sind. Die Quanten-Informationsverarbeitung, auch Quantenkommunikation genannt, ist aus diesem Ansatz hervorgegangen; erste Demonstrationsexperimente zum Quantencomputer sowie Quantenkryptographie-Prototypen haben gezeigt, welches Potential diese Entwicklung birgt [1, 2]. In diesem Artikel verdeutlichen wir, wie die Grundprinzipien der Quantentheorie in der Quantenkryptographie zur Anwendung kommen.

Die Quantenkryptographie ist seit einigen Jahren den Kinderschuhen entwachsen. Hier gezeigt ist das „Labor", in dem wir Verletzungen der Bell-Ungleichungen über 10 Kilometer nachweisen und so den Grundstein für Quantenkryptographie basierend auf nichtlokalen Korrelationen verschränkter Photonen legen konnten. Die Photonenpaarquelle befand sich in der Nähe des Genfer Bahnhofs Cornavin, die Analysatoren in Bellevue bzw. Bernex.

Kryptographie ist ganz allgemein die Kunst, eine Nachricht so zu verschlüsseln, daß sie für unbefugte Personen unlesbar und ohne jeglichen Informationsgehalt ist [3] (siehe Abb. 1). Erste Ansätze lassen sich bis zurück ins alte Ägypten verfolgen. Klassische Benutzer waren vor allem Militärs. Mit der Zunahme des elektronischen Datenverkehrs, bedingt durch die steigende Vernetzung durch das Internet, werden zuverlässige und schnelle Verschlüsselungsverfahren immer wichtiger für jeden von uns. Im folgenden werden wir zunächst die zwei Klassen der Kryptographie – mit öffentlichen oder geheimen Schlüsseln zur Chiffrierung einer Nachricht – kurz vorstellen und dann beschreiben, wie die Quantenmechanik das Problem der Übertragung eines geheimen Schlüssels lösen und die zuletzt genannte Klasse zu einem physikalisch sicheren Verfahren vervollständigen kann.

Kryptographie mit Hilfe „öffentlicher Schlüssel" wurde 1976 von Whitfield Diffie und Martin Hellman vorgeschlagen. Dabei gibt Bob als potentieller Empfänger einer Nachricht einen Schlüssel öffentlich bekannt. Jeder der möchte, kann diesen Schlüssel nun zum Chiffrieren seines Textes verwenden und diesen dann gefahrlos an Bob senden. Die Sicherheit dieses Verfahrens beruht darauf, daß der Schlüssel zum Dechiffrieren nicht aus der Kenntnis des öffentlichen Schlüssels abgeleitet werden kann. Die Grundlage dazu liefern „one way"-Funktionen, die in einer Richtung – der Verschlüsselung – leicht, in der umgekehrten Richtung – der Entschlüsselung – jedoch sehr schwer zu berechnen sind. Das bekannteste Beispiel dafür ist das von Ronald Rivest, Adi Shamir und Leonard Adleman 1977 entwickelte „RSA-Kryptographieverfahren", welches auf der Faktorisierung großer Zahlen beruht: Jeder von uns kann innerhalb kürzester Zeit ausrechnen, daß 107 mal 53 den Wert 5671 ergibt. Die Aufgabe jedoch, die Primfaktoren von 5671 zu finden, läßt sich nur durch viel Probieren lösen, ein effizienter Algorithmus ist bisher nicht bekannt. Nur Bob, der die beiden Primfaktoren im voraus kennt und aus diesen – seinem privaten Schlüssel – den öffentlichen Schlüssel berechnet, kann auf die Originalnachricht schließen. Die Rechenzeit für die Primfaktorenzerlegung wächst exponentiell mit der Anzahl der Eingabebits. Ein solches Rechenproblem wird in der Informationstheorie als schwierig bezeichnet. Im Falle der Kryptographie garantiert die Tatsache, daß das „Knacken" des öffentlichen Schlüssels lange dauert, die Sicherheit der Übertragung. Diese

Dipl.-Phys. Wolfgang Tittel, Dr. Jürgen Brendel, Prof. Dr. Nicolas Gisin, Dipl.-Phys. Grégoire Ribordy, Dr. Hugo Zbinden, GAP-Optique, Université de Genève, 20 rue de l'Ecole de Médecine, CH-1211 Genf, Schweiz

Physikalische Blätter 55 (1999) Nr. 6
0031-9279/99/0606-25
$17.50+50/0

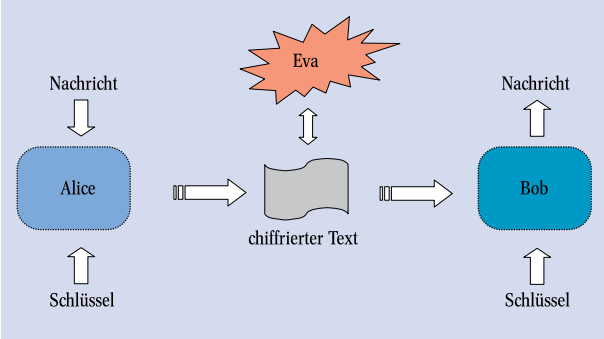


Abb. 1:
Allgemeines Schema für die Übertragung geheimer Nachrichten. Der Sender Alice kombiniert Nachricht und Schlüssel zu einem chiffrierten Text, den sie dann Bob sendet. Bob entschlüsselt den erhaltenen Text mit Hilfe seines Schlüssels und erhält so die ursprüngliche Nachricht. Eva ist die unerwünschte Lauscherin, die versucht, möglichst viel von der Nachricht mitzuhören.

Tabelle 1: Beim „one time pad" addiert Alice zu der aus Nullen und Einsen bestehenden Nachricht einen geheimen Schlüssel der gleichen Länge modulo 2 (d. h. 0 + 0 = 0; 0 + 1 = 1 + 0 = 1; 1 + 1 = 0). Den so chiffrierten Text schickt sie Bob. Dieser addiert den gleichen Schlüssel erneut modulo 2 und erhält die ursprüngliche Nachricht zurück.

Alice								
Nachricht	0	1	1	0	1	0	0	1
Schlüssel	1	0	0	1	1	0	1	0
Summe (modulo 2) = chiffrierter Text	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**1**
Übertragung								
Bob								
chiffrierter Text	1	1	1	1	0	0	1	1
Schlüssel	1	0	0	1	1	0	1	0
Summe (modulo 2) = Nachricht	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**

wäre aber in dem Moment hinfällig, in dem ein entsprechender Algorithmus entdeckt würde. Eine weitere Gefahr droht durch die Entwicklung des sogenannten Quantencomputers, einer „Maschine", die die Faktorisierung von großen Zahlen in Zeiten bewerkstelligen könnte, die lediglich in Form einer Polynomfunktion von der Zahl der Eingabebits abhängen.

Die zweite Klasse von Verschlüsselungsverfahren beruht auf geheimen Schlüsseln zur Chiffrierung der Nachricht. In Verbindung mit dem elektronischen Datenverkehr wird zumeist der „Data Encryption Standard" (DES, 1977) eingesetzt. Diese Methode benutzt den gleichen, bekannten Algorithmus zum Chiffrieren und zum Dechiffrieren sowie einen geheimen Schlüssel von 56 Bit Länge. Genau wie bei Methoden mit öffentlichen Schlüsseln basiert die Sicherheit auf mathematischer Komplexität, d.h. der Tatsache, daß der Spion viel Zeit zum Entschlüsseln der Nachricht benötigt. Eine andere, ebenfalls der Klasse geheimer Schlüssel zugehörende Möglichkeit wurde 1935 von Gilbert Vernam vorgeschlagen. Bei diesem, als „one time pad" bekannt gewordenen Verfahren addiert der Sender Alice zu dem aus Nullen und Einsen bestehenden Text Bit für Bit einen Schlüssel modulo 2 (siehe Tabelle 1). Besteht der Schlüssel aus einer zufälligen Abfolge von Nullen und Einsen, ist er genauso lang wie die zu übermittelnde Nachricht und wird er nur einmal benutzt, so ist der Informationsgehalt in der resultierenden Zahlenkette Null. Die so chiffrierte Nachricht kann nun über öffentliche Kanäle verschickt werden. Nur diejenigen Personen, die den Schlüssel kennen, können durch abermalige Addition (modulo 2) die ursprüngliche Nachricht finden. Im Gegensatz zu zuvor beschriebenen, auf mathematischer Komplexität beruhenden Methoden ist die Sicherheit dieses Verfahrens mathematisch bewiesen. Das Problem der Übermittlung einer geheimen Nachricht ist somit auf die sichere Verteilung eines Schlüssels reduziert. An diesem Punkt kommen nun die besonderen Eigenschaften der Quantenmechanik zum Tragen. Grob gesagt läßt sich ausnutzen, daß die Messung eines unbekannten Zustandes diesen im allgemeinen verändert. Sind Bits des Schlüssels während der Übertragung verändert worden, so kann man auf die Anwesenheit einer dritten Person schließen. Ist dies nicht der Fall, so ist der Schlüssel sicher und eignet sich zur Kodierung einer Nachricht.

Quantenkryptographie in der Theorie

Wir unterscheiden hier zwischen zwei Klassen der quantenmechanischen Schlüsselübertragung, basierend auf der Verwendung von Ein- oder Zweiteilchensystemen. Abbildung 2 skizziert Kryptographie mit Einteilchensystemen am Beispiel von Polarisationskodierung mit einzelnen Photonen. Dieses Protokoll wurde 1984 von Charles Bennett (IBM) und Gilles Brassard (Universität Montreal) vorgeschlagen und ist nun als BB84 Protokoll bekannt [4]. Alice, die die Übertragung initiiert, schickt Bob linear polarisierte Photonen. Wir identifizieren horizontal sowie unter – 45° polarisierte Photonen mit dem Bitwert „0" und vertikal sowie unter + 45° polarisierte mit dem Bitwert „1". Alice sendet einzelne Photonen in einem dieser vier Polarisationszustände und verzeichnet den gewählten Zustand jedes Photons in einer Liste. Bob, der legitime Empfänger, hat zwei Analysatoren zur Verfügung. Der erste ermöglicht die Unterscheidung zwischen horizontal und vertikal polarisierten Photonen, der zweite die zwischen diagonal polarisierten Photonen. Vor jeder Messung wählt Bob einen dieser beiden Analysatoren und dokumentiert die getroffene Wahl, sowie ob und wo er ein Photon registriert hat in seiner Liste. Nach Übertragung einer genügend großen Anzahl von Photonen vergleichen Alice und Bob öffentlich ihre Listen. Sie verständigen sich über diejenigen Ereignisse, bei denen Bobs Analysator an den Zustand des von Alice präparierten Photons angepaßt war. In diesen Fällen haben beide identische Bit-Werte: Die von Bob detektierten Photonen befinden sich in exakt dem Zustand, in dem sie von Alice präpariert worden sind. Alle Ereignisse, bei denen kein Photon detektiert wurde oder aber der Zustand des gesendeten Photons und der gewählte Analysator nicht im Einklang standen, werden nicht weiter berücksichtigt. Hierbei ist es wichtig, sich zu verdeutlichen, daß die öffentliche Kommunikation zwischen Alice und Bob zwar bekannt gibt, ob ein Photon horizontal-vertikal oder diagonal polarisiert war, jedoch keine detailliertere Information über den Zustand des gesendeten Teilchens verraten wird. Auf diese Art und Weise gelingt es Alice und Bob, Zahlenketten mit gleicher Abfolge von Nullen und Einsen aufzustellen.

Wie aber gewährleistet diese Art der Schlüsselverteilung die Sicherheit, daß keine dritte Person Information über den Kode erhält? Wir betrachten dazu beispielhaft die folgende Strategie der Spionage. Da die

Übertragung auf einzelnen Photonen basiert, ist es dem Spion unmöglich, einen kleinen, von Bob nicht bemerkbaren Anteil des optischen Signal abzuzweigen um seine Messung daran vorzunehmen. Er kann ein Photon entweder unbeobachtet zu Bob passieren lassen, in welchem Fall er keinerlei Information über dessen Zustand erhält, oder dieses als Ganzes messen und ein entsprechend dem Resultat der Messung präpariertes Ersatzphoton weiterschicken. Bedingt durch die Verwendung nichtorthogonaler Zustände ist es ihm jedoch unmöglich, den Zustand jedes Photons korrekt zu ermitteln: Wählt er z. B. ähnlich Bob für jede Messung einen von zwei Analysatoren, so wird er bei der Hälfte aller Messungen in einer falschen Basis messen und ein zufälliges Ergebnis erhalten. Demnach kommen in 50 % der Fälle, in denen der Zustand des von Alice gesendeten Photons und der von Bob gewählte Analysator übereinstimmen, veränderte Photonen bei Bob an. Bei wiederum 50 % dieser Photonen erhält Bob ein Ergebnis, das dem ursprünglich von Alice gewählten Zustand widerspricht. In Alice und Bobs Listen schleichen sich folglich 25 % Fehler ein. Um dies zu überprüfen, vergleichen beide nach der Übertragung eine zufällige Auswahl von Bits öffentlich. Stimmen diese exakt überein, können sie darauf schließen, daß auch die nicht veröffentlichten Bits identisch sind, daß also kein Spion die Datenleitung abhörte. Diese Bits formen dann den geheimen Schlüssel. Es gibt andere, subtilere Strategien der Spionage als die hier vorgestellte [5], allen gemein ist aber die Eigenschaft, daß sie in Alice und Bobs Protokoll Fehler hinterlassen, die von diesen entdeckt werden können.

1991 wies Artur Ekert darauf hin, daß auch nichtlokale Korrelationen verschränkter Zweiteilchensysteme zur Aufstellung korrelierter Bitsequenzen dienen können [6] (siehe auch Kasten „Das Superpositionsprinzip, Schrödinger-Katzen und die Nichtlokalität“). Wir beschreiben im folgenden kurz die ursprüngliche Idee der Schlüsselübertragung, die sich stark an Tests der Bell-Ungleichungen anlehnt. Genau wie im vorangehenden Abschnitt betrachten wir Polarisationszustände. Jede andere Art der Verschränkung (Ort-Impuls, Energie-Zeit, Spin....) ist aber ebenfalls einsetzbar. Eine spezielle Quelle produziert Paare verschränkter Photonen, die dann voneinander getrennt und zu Alice bzw. Bob geschickt werden (Abb. 3). Alice und Bob wählen vor jeder Messung zufällig eine von drei Stellungen ihrer polarisierenden Strahlteiler (bzw. wählen einen von drei unterschiedlich orientierten Strahlteilern). Analog dem zuvor beschriebenen Protokoll mit einzelnen Photonen notieren sie Orientierung und Resultat jeder Messung und vergleichen nach einer hinreichend großen Zahl von detektierten Photonenpaaren öffentlich die Wahl der Stellungen. Sämtliche Messungen werden einer von drei Kategorien zugeordnet: Entweder es ergeben sich perfekte korrelierte, aber nur Alice und Bob bekannte Ergebnisse. Oder die gewählten Orientierungen ermöglichen einen Test der Bell-Ungleichungen. Die dritte Klasse beinhaltet nichtkompatible Orientierungen sowie all die Fälle, bei denen nur ein oder kein Photon detektiert werden konnte; sie wird nicht weiter betrachtet. Die Möglichkeit, einen Lauschangriff zu entdecken, ist bei dieser Methode besonders elegant: Falls eine dritte Person Photonen abfängt, diese mißt und entsprechend dem Ergebnis der Messung präparierte Ersatzphotonen weiterschickt, so bricht sie notgedrungen die Verschränkung der beiden Photonen auf und die Bell-Ungleichung wird nicht mehr verletzt – daran erkennen Alice und Bob den Spion.

Quantenkryptographie in der Praxis

Alle bisherigen Experimente verwendeten Photonen als Informationsträger. Sie sind experimentell relativ einfach zu erzeugen und lassen sich mit Hilfe von Glasfasern transportieren, eine Technik, die innerhalb der letzten Jahrzehnte, bedingt durch die enorme Expansion der Telekommunikation, große Fortschritte zu verzeichnen hat. So sind etwa die Transmissionsverluste von mehreren dB pro Kilometer um etwa eine

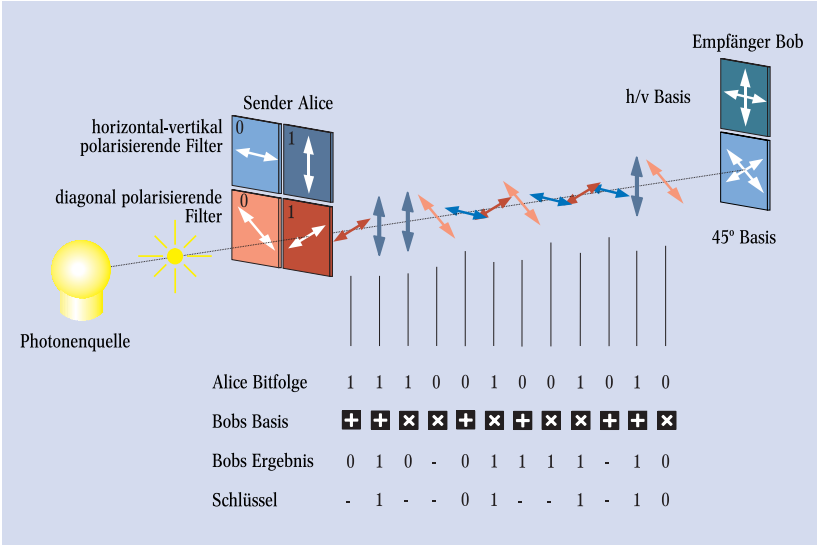
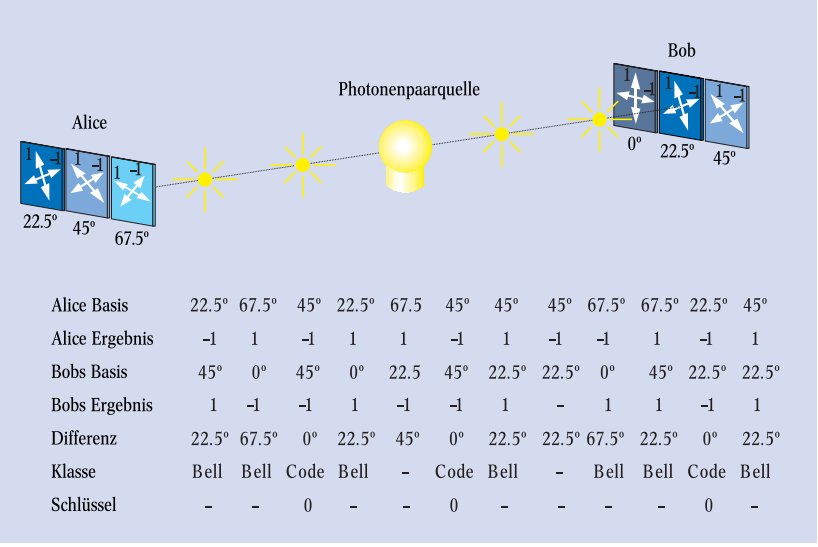


Abb. 2:
Quantenkryptographie (auch quantenmechanische Schlüsselübertragung, *quantum key distribution* genannt) löst das Problem der sicheren Schlüsselübertragung und vervollständigt den „one time pad“ so zu einem abhörsicheren System. Hier dargestellt ist das BB84-Protokoll. Die Bits sind als Polarisationszustände der einzelnen Photonen kodiert.



Alice Basis	22.5°	67.5°	45°	22.5°	67.5	45°	45°	45°	67.5°	67.5°	22.5°	45°
Alice Ergebnis	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
Bobs Basis	45°	0°	45°	0°	22.5	45°	22.5°	22.5°	0°	45°	22.5°	22.5°
Bobs Ergebnis	1	-1	-1	1	-1	-1	1	–	1	1	-1	1
Differenz	22.5°	67.5°	0°	22.5°	45°	0°	22.5°	22.5°	67.5°	22.5°	0°	22.5°
Klasse	Bell	Bell	Code	Bell	–	Code	Bell	–	Bell	Bell	Code	Bell
Schlüssel	–	–	0	–	–	0	–	–	–	–	0	–

Abb. 3:
Schlüsselübertragung mit verschränkten Photonen. Beim öffentlichen Vergleich der Analysatorstellungen teilen Bob und Alice alle Messungen entsprechend der relativen Orientierung der polarisierenden Strahlteiler in drei Klassen ein: Messungen mit Differenzen von 45° und solche, bei denen nur ein oder kein Photon detektiert wurde, werden nicht weiter berücksichtigt (Klasse „-“). Bei paralleler Orientierung ergeben sich korrelierte Ergebnisse, die im Weiteren als Schlüssel benutzt werden können (Klasse „Code“). Messungen mit Differenzen von 22,5° bzw. 67,5° ermöglichen Tests der Bell-Ungleichung. Wird sie verletzt, folgt, daß die von Bob und Alice registrierten Photonen quantenmechanisch verschränkt sind. Die Übertragung wurde nicht abgehört, denn ein Lauschangriff hätte die Korrelationen zerstört.

Größenordnung reduziert worden und betragen heute bei einer Wellenlänge von 1310 nm – im sogenannten zweiten Telekomfenster – nur noch 0,35 dB/km. Nach Transmission von zehn Kilometern Faser ist also erst die Hälfte der Photonen absorbiert worden, ein Wert, der Quantenkryptographie in lokalen Netzwerken ermöglicht.[1)] Es sei an dieser Stelle darauf hingewiesen, daß, obwohl fast alle Experimente auf Glasfasern zurückgreifen, ebenfalls Bestrebungen bestehen, Systeme zur Schlüsselübertragung zu Satelliten bzw. zwischen Satelliten zu entwickeln.

Wie immer in der Physik unterscheiden sich Theorie und Praxis in nicht vernachlässigbarer Art und Weise. Haben wir weiter oben behauptet, daß die Bitabfolgen von Alice und Bob bei Abwesenheit eines Spions perfekt korreliert sind, so entspricht dies mehr einem Wunschtraum als der Realität. Tatsächlich gibt es immer einige Fehler, sie liegen normalerweise im Bereich weniger Prozente. Das Verhältnis der Zahl der fehlerhaften zur Gesamtzahl der übertragenen Bits, die sogenannte Quantenbit-Fehlerrate, ist somit neben Distanz und Frequenz der Übertragung eine der charakteristischen Größen eines Quantenkryptographie-Systems.

Unkorrelierte Bits können durch verschiedene experimentelle Ungenauigkeiten hervorgerufen werden. Sendet Alice z. B. anstelle eines vertikal polarisierten Photons ein unter einem Winkel von 84° polarisiertes, so wird Bob in einem Prozent der Fälle das Photon im Kanal „horizontal“ entdecken. Entsprechendes gilt für Bobs Analysatoren. Eine weitere Fehlerquelle entspringt der Möglichkeit, daß die von Alice gewählten Quantenzustände während der Transmission zu Bob verändert werden können. Ein vertikal polarisiertes Photon muß auch vertikal polarisiert bei Bob ankommen. Bedingt durch die Doppelbrechung optischer Fasern ist dies im allgemeinen jedoch nicht der Fall. Da die Eigenschaften von Fasern zeitlich nicht konstant sind – mechanisch oder thermisch bedingte Spannungen etwa ändern sich auf einer Zeitskala von Minuten – ist also eine ständige Überwachung und Regelung vonnöten. Dies ist zwar möglich, aber nicht sehr praktisch. Eine dritte Ursache für nichtkorrelierte Bits ist das Rauschen der Detektoren. Es führt immer dann zum falschen Ergebnis, wenn ein Photon auf dem Weg zu Bob absorbiert worden ist und der Detektor des „falschen“ Kanals in dem Moment anspricht, in dem das Photon hätte ankommen sollen. Da für Wellenlängen mit geringen Faserverlusten nur Germanium- und InGaAs-Avalanche-Photodioden eingesetzt werden können, die sich durch relativ geringe Quantenausbeuten und viel Rauschen auszeichnen, sind die meisten Fehler einer Schlüsselübertragung in aller Regel nicht der Detektion von Photonen in einem falschen Kanal, sondern dem Detektorrauschen zuzuschreiben.

Nach einer Schlüsselübertragung muß der sogenannte Rohschlüssel folglich zunächst von Fehlern bereinigt werden. Dazu dienen klassische Fehlerkorrektur-Algorithmen. Da Alice und Bob jedoch nie sicher sein können, daß die gefundenen Fehler tatsächlich experimentellen Ungenauigkeiten und nicht der Präsenz einer dritten Person zuzuschreiben sind, wird in einem als „privacy amplification“ bekannten weiteren Schritt das hypothetische Wissen eines Lauschers bis auf beliebig kleine Werte reduziert. Dazu werden z. B. mehrere Bits zu einem einzigen zusammengefaßt, eine Prozedur, die bei zwei Schlüsseln nur dann zum gleichen Ergebnis führt, wenn alle ursprünglichen Bits gleich sind. Dies ist der Fall bei Alice und Bob. Kennt der Lauscher jedoch nur einen kleinen Teil des Rohschlüssels, so endet er mit einer völlig anderen Bitfolge. Leider verkürzt dieses Verfahrens vor allem bei großen Fehlerraten den Rohschlüssel sehr stark und ist nur bis hin zu einer Quantenbit-Fehlerrate von 15 % anwendbar. Alice und Bob haben daher ein großes Interesse daran, die Fehler bei der Übertragung so gering wie möglich zu halten.

Experimente

Zum ersten Mal wurde die Quantenkryptographie 1989 von Forschern bei IBM experimentell demonstriert. Der von ihnen gebaute Prototyp basierte auf Polarisationskodierung mit einzelnen Photonen[2)] und übertrug einen Schlüssel über 30 cm Luftweg. Seitdem sind enorme Fortschritte erzielt worden, und mehrere Gruppen konnten über Systeme berichten, die außerhalb des Labors funktionieren [7]. Wir geben im folgenden einen Überblick über die letzten Entwicklungen, werden diesen aber auf Systeme beschränken, die bei Wellenlängen arbeiten, welche für große Übertragungsstrecken geeignet sind.

1995 konnten wir zeigen, daß Quantenkryptographie, beruhend auf schwachen Pulsen, auch über große

[1)] Im Gegensatz zur „standard“ Telekommunikation lassen sich bei der Quanten-Kryptographie keine Verstärker einsetzen, da der Zustand einzelner Photonen nicht kopiert werden kann.

Das Superpositionsprinzip, Schrödingerkatzen und die Nichtlokalität

Hat die Schrödinger-Gleichung mehrere Lösungen – etwa $|\Psi_1\rangle$ und $|\Psi_2\rangle$ –, so entspricht die allgemeine Lösung der Linearkombination der beiden Wellenfunktionen: $|\Psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_2\rangle$. Diese als Superpositionsprinzip bekannte Tatsache folgt aus der Linearität der Wellengleichung. Sie ist eine der grundlegenden Regeln der Quantenmechanik und wird normalerweise ohne weiteres akzeptiert. Und doch führt genaueres Hinterfragen zu seltsam anmutenden Eigenschaften. Beschreiben die beiden Wellenfunktionen $|\Psi_1\rangle$ und $|\Psi_2\rangle$ etwa zwei verschiedene Orte, an denen sich ein Teilchen aufhalten kann, so entspricht die Linearkombination der beiden einem Teilchen, welches sich an beiden Orten gleichzeitig befindet. Oder aber wir gelangen zu einem Atom, welches zur gleichen Zeit existiert und bereits radioaktiv zerfallen ist. Diese Aussage wirkt besonders bizarr beim Übergang in die makroskopische Welt. Schrödinger brachte dies mit einem makabren Gedankenexperiment auf den Punkt: Koppelt man das quantenmechanische Einteilchensystem an einen Mechanismus, der eine Katze tötet, so ist die Katze gleichzeitig lebendig und tot.

Wenden wir das Superpositionsprinzip auf Zweiteilchensysteme an, so gelangen wir zu sogenannten verschränkten Zuständen. Ein solcher Zustand kann z. B. – um bei polarisierten Photonen zu bleiben – durch $|\Psi\rangle = 1/\sqrt{2}(|\mathrm{h}\rangle_1|\mathrm{v}\rangle_2 - |\mathrm{v}\rangle_1|\mathrm{h}\rangle_2)$ beschrieben werden: Photon 1 befindet sich im Polarisationszustand horizontal und Photon 2 im Zustand vertikal, überlagert mit der Möglichkeit, daß sich Photon 1 im Zustand vertikal und Photon 2 im Zustand horizontal befindet. Die Eigenschaft eines einzelnen Photons eines solchen Paares ist gemäß der Quantenmechanik also völlig undefiniert. Eine Messung in der Basis horizontal/vertikal kann sowohl horizontal als auch vertikal ergeben, die Natur entscheidet sich rein zufällig für eines der beiden Ergebnisse. Das Problem, woher das andere Photon, welches sich zur Zeit der Messung beliebig weit entfernt aufhalten kann, instantan „weiß“, welche Eigenschaft es annehmen muß – gemäß der Wellenfunktion immer orthogonal zum Ergebnis der Messung des anderen Photons –, hat schon immer für philosophische Debatten gesorgt. So führte es Albert Einstein, Boris Podolsky und Nathan Rosen im Jahre 1935 zur Formulierung eines als EPR-Paradoxon bekanntgewordenen Gedankenexperimentes und zu der Frage, ob die quantenmechanische Beschreibung durch eine Unterstruktur zu ergänzen sei [10]. Diese könnte das Verhalten der Teilchen im vornherein festlegen und somit den Aspekt „Zufall“ aus der Quantentheorie entfernen und die Nichtlokalität vermeiden. John Bell konnte 1964 mit den sogenannten Bell-Ungleichungen zeigen, daß die quantenmechanischen Voraussagen für Korrelationsmessungen von den Voraussagen lokaler Theorien, die auf den Vorschlag von Einstein, Podolsky und Rosen zurückgehen, abweichen [11, 12].

Der erste Test der Bell-Ungleichungen wurde 1972 von Freedman und Clauser durchgeführt, die bekanntesten Untersuchungen sind der Gruppe um Alain Aspect zu Beginn der achtziger Jahre zuzuschreiben [13]. Alle Experimente bestätigen die Voraussagen der Quantenmechanik, können damit aber das Unbehagen hinsichtlich der Nichtlokalität nicht ausräumen.

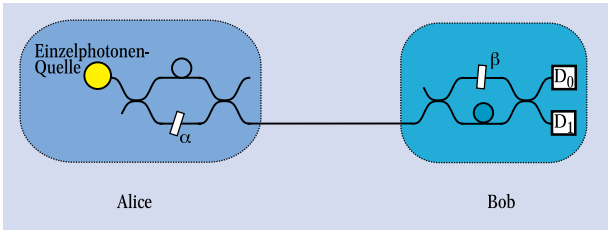


Abb. 4:
Quantenkryptographie, basierend auf Phasenkodierung mit einzelnen Photonen. Haben beide Interferometer – hier als Faserinterferometer angedeutet – gleiche Armlängenunterschiede, so sind die beiden Wege „langer Arm bei Alice, kurzer Arm bei Bob“ und „kurzer Arm bei Alice, langer Arm bei Bob“ ununterscheidbar und man beobachtet Interferenz, d. h. die Wahrscheinlichkeit für die Detektion eines Photons in Detektor D_0 bzw. D_1 hängt von den Phasen α und β ab. Zur Realisierung des BB84-Protokolls wählt Alice für jedes Photon zufällig eine der Phasen 0, $\pi/2$, π oder $3\pi/2$. Wählt Bob die Phase 0, so kann er zwischen Alices Wahl von 0 (Detektion in D_0) und π (Detektion in D_1) unterscheiden, wählt er eine Phase von $\pi/2$, kann er entsprechend $\pi/2$ von π trennen. Alles Weitere entspricht der Polarisationskodierung (Abb. 2).

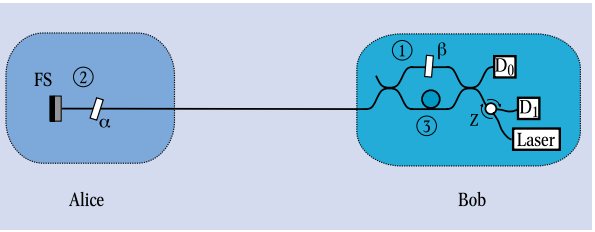


Abb. 5:
Das von uns entwickelte „Plug&Play“ System. Im Gegensatz zu dem in Abb. 4 gezeigten Aufbau sind die interferierenden Wege räumlich identisch, werden aber in unterschiedlicher Reihenfolge durchlaufen (1-2-3 interferiert mit 3-2-1). Dies führt zu einem automatischen Ausgleich aller Längenänderungen. Der Faraday-Spiegel (FS) – ein 45° Faraday-Rotator gefolgt von einem gewöhnlichen Spiegel – gewährleistet darüber hinaus die Kompensation sämtlicher Polarisationsänderungen während der Transmission von Bob zu Alice und wieder zurück zu Bob. Nach Reflexion an einem solchen Spiegel ist das Licht an jedem beliebigen Punkt immer orthogonal zum Zustand beim Hinweg polarisiert. α und β sind von Alice und Bob gewählte Phasen, D_0 und D_1 sind Detektoren und Z ist ein sogenannter Zirkulator, der dafür sorgt, daß alles vom Laser ausgesendete Licht in den optischen Aufbau und alles zurückkommende Licht in den Detektor D1 gelangt.

Entfernungen möglich ist. Wir verschickten dazu polarisierte Photonen über eine Strecke von 23 km unterhalb des Genfer Sees, wozu wir uns des Telekommunikations-Fasernetzes der Swisscom bedienten. Eine andere Art, die verschiedenen Quantenzustände für eine Schlüsselübertragung zu realisieren, beruht auf Phasenkodierung. Sie wurde 1993 von der Gruppe um Paul Townsend bei der British Telecom entwickelt und wird mittlerweile auch von Richard Hughes Gruppe am Los Alamos National Laboratory in New Mexiko benutzt. Abbildung 4 zeigt das Prinzip dieser Methode. Alice und Bob besitzen jeweils ein Mach-Zehnder-Interferometer mit gleichen Armlängendifferenzen. Die Interferometer dienen zur Präparation bzw. Detektion von Pulssequenzen mit bestimmten Phasenbeziehungen. Genau wie bei der Polarisationskodierung bedarf dieses System aktiver Kontrolle. Zum einen müssen die Armlängendifferenzen auf Bruchteile einer Wellenlänge gleich groß gehalten werden. Darüber hinaus ist nur dann ein gutes Ergebnis zu erwarten, wenn die Entwicklung des Polarisationszustands in den verschiedenen Armen jedes Interferometers identisch ist. Auch hier ist also eine Polarisationskontrolle notwendig. Innerhalb der letzten zwei Jahre konnten wir ein neues interferometrisches System entwickeln, welches im Gegensatz zu dem zuvor beschriebenen „wartungsfrei“ ist und weder Armlängen- noch Polarisationskontrolle bedarf (Abb. 5). Auch dieses System wurde erfolgreich für die Übertragung geheimer Schlüssel unterhalb des Genfer Sees verwendet.

Wie im theoretischen Teil gesagt, lassen sich auch Zweiteilchensysteme für die Quantenkryptographie einsetzen. Sämtliche Bell-Experimente zeigen die prinzipielle Machbarkeit auf. Es gibt allerdings bisher nur zwei Experimente, die im Zusammenhang mit Quantenkryptographie über große Distanzen zu nennen sind[3]. 1994 konnte die Gruppe um John Rarity vom DRA Malvern in Großbritannien Verletzungen der Bell-Ungleichungen mit in Energie und Zeit verschränkten Photonen im Labor demonstrieren, wobei einer der Analysatoren durch eine 4,3 km lange, auf einer Spule aufgerollte optische Faser von der Quelle getrennt war [8]. Basierend auf der gleichen Art der Verschränkung gelangen uns in den Jahren 1997 und 1998 eine Serie von Experimenten, mit denen wir nichtlokale Korrelationen auch außerhalb des Labors über eine Distanz von mehr als 10 Kilometern nachweisen konnten [9] (siehe Abb. auf der ersten Seite dieses Artikels). Die Photonenpaarquelle befand sich in einer Telekommunikationszentrale in der Nähe des Genfer Bahnhofs Cornavin, die Analysatoren in den 5 Kilometer südlich bzw. nördlich von Genf gelegenen Vororten Bellevue bzw. Bernex. Die das Zweiteilchensystem beschreibende Wellenfunktion erstreckte sich somit über einen Bereich von der Größe einer Kleinstadt. Dieses Experiment veranschaulicht die von Einstein angezweifelte „geisterhafte Fernwirkung“ zwischen den beiden Photonen besonders drastisch: Die Messung des einen Teilchens – der Kollaps der Wellenfunktion – führt instantan zu korreliertem Verhalten des anderen, 10 Kilometer entfernten Teilchens.

Wie bereits erwähnt, gibt es neben den hier präsentierten Experimenten weitere Prototypen, die bei Wellenlängen um 800 nm – im sogenannten ersten Telekom-Fenster – arbeiten. Aufgrund höherer Faserverluste ist die maximale Reichweite jedoch auf wenige Kilometer begrenzt. Mit einem solchen System hat die British Telecom 1997 ein auf Polarisationskodierung mit einzelnen Photonen beruhendes System entwickelt, das die bisher mit Abstand höchste Quantenbitrate von 1,2 MHz erzielen konnte. Forscher der Universität Innsbruck unter Leitung von Anton Zeilinger konnten im letzten Jahr ebenfalls über eine auf der Eigenschaft „Polarisation“ basierende Übertragung eines Schlüssels in Verbindung mit einem Test der Bell-Ungleichungen über 500 Meter berichten.

Die Zukunft

Quantenkryptographie, die am weitesten entwickelte Anwendung des neuen Gebietes der Quantenkommunikation, hat seit vier Jahren das Labor verlassen. Experimente unter realen Bedingungen sind, zumindest was Systeme angeht, die auf Kodierung mit „schwachen Pulsen“ beruhen, heutzutage schon fast eine Rou-

[2] Tatsächlich wurden in diesem wie in allen bisher durchgeführten Experimenten einzelne Photonen durch sogenannte „schwache Pulse“ simuliert, kohärente Zustände mit einer mittleren Photonenzahl von 0,1 Photonen pro Puls.

[3] Das liegt vor allem daran, daß fast alle Experimente mit Photonen einer Wellenlänge arbeiten, bei der es zwar gute Detektoren gibt, bei denen jedoch starke Absorptionsverluste in optischen Fasern bestehen.

tineübung. Reichweiten liegen in der Gegend von 20 – 30 Kilometern, und Quantenbit-Fehlerraten von wenigen Prozent sind niedrig genug, um einen Lauschangriff detektieren und die sichere Übertragung eines Schlüssels gewährleisten zu können. Somit können existierende System schon heute eine sichere Übertragung von Nachrichten garantieren, falls Verfahren, die auf mathematischer Komplexität beruhen, „geknackt" werden sollten. Verbesserungsbedarf besteht vor allem in der Distanz sowie der Übertragungsrate, die z. Zt. bei einigen hundert Hertz liegt. Zum Beispiel würde die Erstellung eines Schlüssels zur Kodierung dieses Textes – etwa 44 KByte ohne Bilder – mit Hilfe des „one time pads" unter Anwendung des in Abb. 5 gezeigten „Plug & Play" Systems etwa 20 Minuten dauern. Erste Systeme, die auf nichtlokalen Korrelationen verschränkter Photonen beruhen, wurden ebenfalls außerhalb des Labors demonstriert. Die tatsächliche Übertragung eines Schlüssels steht aber noch aus, zumindest über große Entfernungen. Ein dreijähriges ESPRIT-Projekt mit dem Namen „European Quantum Cryptography and Single Photon Optical Technologies" untersucht momentan, welche Methode der quantenmechanischen Schlüsselübertragung die beste ist.

Literatur

[1] Physics World, März 1998, Schwerpunktheft Quantenkommunikation.

[2] *H. K. Lo, S. Popescu* und *T. P. Spiller*, Introduction to Quantum Computation and Information, World Scientific, Singapore 1998

[3] *A. J. Menezes, P. C. Oorschot* und *S. A. Vanstone*, Handbook of Applied Cryptography, CRC, New York 1997

[4] *C. H. Bennett* und *G. Brassard*, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, S. 175 (1984)

[5] *C. A. Fuchs, N. Gisin, R. B. Griffiths*, *C.-S. Niu* und *A. Peres*, Phys. Rev. A **56**, 1163 (1997)

[6] *A. K. Ekert*, Phys. Rev. Lett. **67**, 667 (1991)

[7] *H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin* und *G. Ribordy*, Appl. Phys. B **67**, 743 (1998)

[8] *P. R. Tapster*, *J. G. Rarity* und *P. C. M. Owens*, Phys. Rev. Lett. **73**, 1923 (1994)

[9] *W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden* und *N. Gisin*, Phys. Rev. A **57**, 3229 (1998); *W. Tittel, J. Brendel, H. Zbinden* und *N. Gisin*, Phys. Rev. Lett. **81**, 3563 (1998)

[10] *A. Einstein, B. Podolsky* und *N. Rosen*, Phys. Rev. **47**, 777 (1935)

[11] *J. S. Bell*, Physics **1**, 195 (1964)

[12] *N. D. Mermin*, Am. J. Phys. **49**, 940 (1981)

[13] *J. Freedman* und *J. F. Clauser*, Phys. Rev. Lett. **28**, 938 (1972); *A. Aspect, P. Grangier* und *G. Roger*, Phys. Rev. Lett. **47**, 460 (1981); *A. Aspect, P. Grangier* und *G. Roger*, Phys. Rev. Lett. **49**, 91 (1982) *A. Aspect, J. Dalibard* und *G. Roger*, Phys. Rev. Lett. **49**, 1804 (1982)

Quanteninformation

Quantencomputer

Wie sich Verschränkung für die Informationsverarbeitung nutzen läßt

Hans-Jürgen Briegel, Ignacio Cirac und Peter Zoller

Die Quantenmechanik eröffnet faszinierende Perspektiven für die Kommunikation und die Informationsverarbeitung. Auf einen universell programmierbaren Quantenrechner wird man zwar noch längere Zeit warten müssen. Doch die beachtlichen Fortschritte in einigen Labors lassen elementare Quantenprozessoren realistisch erscheinen, die in einigen Jahren mit einer Anzahl von etwa zehn Quantenbits und einer Fehlerrate im Prozentbereich arbeiten könnten. Auch wenn man damit noch keine beeindruckenden Rechnungen durchführen kann, lassen sich solche Prozessoren für wichtige Aufgaben in der Quantenkommunikation einsetzen. Für ihre Vernetzung spielen die Teleportation und der „Quantenrepeater“ eine zentrale Rolle.

Wir sind gegenwärtig Zeugen der Entwicklung eines neuen interdisziplinären Fachgebietes, der „Quanteninformatik“, das auf Ideen und Konzepten aus der Informationstheorie, Mathematik und Physik aufbaut. Die Quanteninformatik beschäftigt sich mit der Informationsverarbeitung und Kommunikation auf der Grundlage der Quantenphysik sowie mit einer physikalischen Fundierung des Informationsbegriffes überhaupt [1, 2].

Das beachtliche Interesse an den Themenkreisen Quantencomputer und Quantenkommunikation hat mehrere Gründe. Es beinhaltet einerseits grundsätzliche Fragen über die Beziehung zwischen Quantenphysik und Informationstheorie [2] und verspricht andererseits Anwendungen wie geheime Kommunikation und effiziente Quantenalgorithmen [1]. Beispiele sind der Shor-Algorithmus zur Faktorisierung großer Zahlen in Primfaktoren [3] und der Grover-Algorithmus zur Datenbanksuche [4]. Die gegenwärtige Entwicklung erinnert in mancher Hinsicht an die Pionierzeit der klassischen Informationstheorie und des Computers, als die Grundlagen für die moderne Informationstechnologie geschaffen wurden. Während die Fragestellungen von Forschern wie Shannon und Turing zur Zeit ihrer Entstehung hauptsächlich abstrakter Natur waren, haben sie, zusammen mit der Entwicklung von konkreten physikalischen Implementierungen, die Grundlage unseres Kommunikationszeitalters geschaffen.

Bei einigen Problemen und Fragestellungen in der Quanteninformationstheorie kann man auf ein reichhaltiges Repertoire von Methoden der klassischen Informationstheorie zurückgreifen, wie zum Beispiel aus der Codierungstheorie und der Fehlerkorrektur [2]. Andererseits gibt es auch fundamental neue Konzepte, die kein klassisches Analogon besitzen. Das bekannteste Beispiel ist die Verschränkung von Quantenzuständen [5], die als Grundlage für Teleportation, superdichte Kodierung [6 – 8] und Quantenalgorithmen dient.

Während auf Seite der Theorie durch die Entwicklung von Quantenalgorithmen, Quantenfehlerkorrektur und fehlertoleranten Schemata große Fortschritte erzielt worden sind [2, 9], steckt die experimentelle Realisierung und die praktische Implementierung dieser Konzepte erst in den Kinderschuhen. Zwar sind in einer Reihe von bemerkenswerten Experimenten der letzten Jahre die Grundelemente der Quanteninformationsverarbeitung und -kommunikation, wie Quantengatter [10] und Teleportation [6], im Labor demonstriert worden [7]. Es ist derzeit jedoch nicht absehbar, wann und in welcher Form diese Entwicklungen zu technologischen Anwendungen führen werden. Die Anforderungen an die technische Präzision bei den Experimenten sind zum Teil überwältigend. Andererseits sollte auch nicht vergessen werden, welch enorme Fortschritte in der klassischen Informationsverarbeitung innerhalb eines halben Jahrhunderts erzielt worden sind.

Grundbegriffe der Quanteninformation

Quanteninformation wird gespeichert in Quantenzuständen eines physikalischen Systems. Die Informationseinheit ist hierbei das *Qubit*. Es mißt den Informationsgehalt, der in einem Zwei-Zustands-System (zum Beispiel einem Spin-1/2-Teilchen) gespeichert werden kann. Die Basiszustände eines solchen Systems werden – in Anlehnung an die klassische Konvention – häufig mit $|0\rangle$ und $|1\rangle$ bezeichnet. Der Unterschied zur klassischen binären Information besteht darin, daß die Information auch im Sinne einer quantenmechanischen Überlagerung vorliegen kann. Anstelle von „Schalterstellungen“ $|0\rangle$ und $|1\rangle$ sind ebenso beliebige Linearkombinationen $\alpha|0\rangle + \beta|1\rangle$ mit komplexen Koeffizienten α, β erlaubt ($|\alpha|^2 + |\beta|^2 = 1$). „Registerzustände“ entsprechen hierbei Tensorprodukten von Qubits, zum Beispiel $|0\rangle|1\rangle|0\rangle$ oder $|1\rangle|0\rangle|1\rangle$, und Superpositionen wie $\alpha|0\rangle|1\rangle|0\rangle + \beta|1\rangle|0\rangle|1\rangle$ sind verschränkte Zustände.

Quanteninformationsverarbeitung besteht (im idealen Fall) aus einer Sequenz von unitären Operationen mit Registerzuständen, die möglicherweise durch Meß-

Dr. Hans-Jürgen Briegel, Sektion Physik, Ludwig-Maximilians-Universität, Theresienstr. 37, D-80333 München; Prof. Dr. Ignacio Cirac, Prof. Dr. Peter Zoller, Institut für Theoretische Physik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck

Physikalische Blätter 55 (1999) Nr. 9
0031-9279/99/0909-37
$17.50+50/0

und Ableseprozesse unterbrochen und gesteuert werden können [1, 2]. Die einfachsten Fälle sind sogenannte 1-bit- und 2-bit-*Quantengatter*, die unitäre Operationen mit einzelnen Qubits beziehungsweise Paaren von Qubits bezeichnen. Ein Beispiel für ein 2-bit-Quantengatter ist das kontrollierte NOT-Gatter (CNOT), das durch folgende Tabelle beschrieben wird:

$$
\begin{aligned}
|0\rangle|0\rangle &\rightarrow |0\rangle|0\rangle \\
|0\rangle|1\rangle &\rightarrow |0\rangle|1\rangle \\
|1\rangle|0\rangle &\rightarrow |1\rangle|1\rangle \\
|1\rangle|1\rangle &\rightarrow |1\rangle|0\rangle,
\end{aligned}
$$

wobei sich die linke (rechte) Spalte auf den Zustand der Qubits vor (nach) der Gatteroperation bezieht. In der Sprechweise der Boolschen Algbra wird also eine Negation des zweiten Qubits durchgeführt, *sofern* das erste Qubit sich im Zustand $|1\rangle$ befindet. Man kann zeigen, daß sich jede Rechenoperation in eine Folge (d.h. ein logisches Netzwerk) von Operationen eines CNOT-Gatters zusammen mit allgemeinen unitären Rotationen eines einzelnen Qubits zerlegen läßt [2].

Als *Quantencomputer* [3, 11] bezeichnen wir jedes System, das eine kontrollierte Verarbeitung von Quanteninformation erlaubt. Die *Quantenkommunikation* [1, 8] befaßt sich hingegen mit der spezielleren Aufgabe, Quanteninformation über verrauschte Kanäle intakt zu übertragen und Quanteneigenschaften für bestimmte Kommunikationszwecke zu verwenden, wie zum Beispiel die geheime Nachrichtenübermittlung. Die Definition des Informationsbegriffes und der Informationsverarbeitung basiert hier explizit auf einer physikalischen Theorie, nämlich der Quantentheorie, die die möglichen Zustände und die Dynamik der Informationsträger bestimmt. Insofern, als die Informationsträger den Gesetzen der Quantentheorie unterliegen, ist das Problem der Quanteninformationsverarbeitung eng mit dem Problem der Dekohärenz verbunden. Unitäre Operationen lassen sich zum Beispiel nur in einem vollständig isolierten System durchführen. Jedes reale System ist jedoch, wenn auch nur schwach, an Freiheitsgrade einer Umgebung gekoppelt, und die unkontrollierte Wechselwirkung der Informationsträger mit der Umgebung entspricht einer *Dekohärenz* im Zustandsraum der Qubits. Quantenmechanische Verschränkung und Superpositionszustände werden dadurch empfindlich gestört. Die *Quantenfehlerkorrektur* wird daher zu einem wesentlichen Bestandteil eines Quantencomputers.

Die Erweiterung des Informationsbegriffes erlaubt es, neue, sogenannte Quantenalgorithmen zu entwickeln. Die Möglichkeit, durch quantenmechanische Überlagerung verschiedene Registerzustände quasi gleichzeitig zu verarbeiten, wurde von manchen Autoren als „Quantenparallelismus“ bezeichnet und verspricht, gewisse mathematische Probleme auf einem Quantencomputer effizienter zu lösen, als dies mit einem klassischen Computer möglich ist. Die Anforderungen an die Präzision, mit der die Gatteroperationen realisiert werden müssen, um beliebige Quantenalgorithmen implementieren zu können, sind allerdings sehr hoch. Die Theorie des fehlertoleranten Quantenrechnens liefert einen Wert in der Größenordnung von 10^{-5} als relative Ungenauigkeit pro Rechenschritt bzw. Gatteroperation [2]. Mit anderen Worten, von 100 000 Operationen darf höchstens eine Operation fehlerhaft sein, damit der Quantencomputer noch funktioniert.

Die Quantenkommunikation bietet bedingungslos sichere Protokolle für die Quantenkryptographie und damit die Möglichkeit einer geheimen Kommunikation, bei der prinzipiell jeder Lauschangriff feststellbar ist [12]. Dies setzt die Möglichkeit voraus, intakte Quantenzustände über verrauschte Kanäle zu schicken. Im Prinzip läßt sich dies ebenfalls durch Methoden der Quantenfehlerkorrektur erreichen, da die Transmission von Information durch einen verrauschten Kanal eng mit dem Problem der Informationsspeicherung zusammenhängt. Andererseits gibt es für die Quantenkommunikation die wesentlich effizientere Methode der Verschränkungsreinigung. Die tolerierbare Ungenauigkeit der Operationen liegt hier bei etwa 10^{-2} [13].

Implementierung von Quantencomputern

Für die Implementierung eines Quantencomputers ist es notwendig, ein physikalisches System zu identifizieren, das es erlaubt, Quantenzustände verläßlich zu speichern und gezielt und präzise mit Quantenoperationen zu manipulieren. In der Praxis gibt es bisher nur wenige Kandidaten, die diese Voraussetzung erfüllen.

Zur Realisierung eines Quantencomputers müssen eine Reihe von Bedingungen erfüllt sein: (i) Identifikation einzelner Qubits; (ii) Adressierbarkeit und Auslesen der Bits; (iii) Implementierung von Quantengattern; (iv) schwache Dekohärenz; (v) effiziente Implementierung von Fehlerkorrektur; (vi) Skalierbarkeit von wenigen auf viele Qubits.

Eine Vorreiterrolle spielt dabei die Quantenoptik. Als Träger der Quanteninformation kommen in der Quantenoptik einzelne Atome und Photonen in Frage. Mit Methoden der Quantenoptik lassen sich beispielsweise einzelne Atome in Fallen speichern und mit Laserkühlen im Grundzustand der Falle präparieren [10, 14 – 17]. Laserpulse erlauben es, die internen Zustände dieser kalten Atome gezielt zu manipulieren. Außerdem kann man mit Methoden der Hohlraumelektrodynamik die Wechselwirkung einzelner Photonen mit Atomen kohärent steuern [14, 18, 19]. Somit lassen sich 1-bit-Gatter durch Wechselwirkung von Laserlicht mit Atomen realisieren. 2-bit-Gatter lassen sich durch Ankopplung an Hilfsfreiheitsgrade wie zum Beispiel kollektive Schwingungsmoden von gespeicherten Atomen oder Ionen in einem Resonator realisieren. Diese Phononmoden spielen dabei die Rolle eines „Quantendatenbusses“. Bislang wurde eine kontrollierte Verschränkung von zwei Ionen bzw. Atomen im Labor demonstriert [10, 19]. Wir werden auf einige dieser Systeme im folgenden Abschnitt im Detail eingehen.

Ein Vorschlag, der in letzter Zeit besonderes Interesse gefunden hat, ist ein Kernspin-Quantenrechner (NMR-Quantum Computing [20]). Dabei werden Quantenbits in Kernspins von Molekülen gespeichert und Quantengatter durch Einstrahlen von Radiofrequenzpulsen realisiert. Der wesentliche Unterschied zu den oben genannten Vorschlägen aus der Quantenoptik besteht darin, daß anstelle von Einzelsystemen ein *Ensemble* von Molekülen verwendet und das System außerdem bei *endlicher Temperatur* betrachtet wird. Dieser Vorschlag greift direkt auf Methoden zurück, die man heute in der Kernspinresonanz-Spektroskopie im Labor verwendet. In letzter Zeit hat es eine Reihe von interessanten Experimenten mit NMR-Quantencomputern gegeben, die einfache Quantenalgorithmen erstmals im Labor demonstrierten. Allerdings wurde vor kurzem gezeigt, daß die mit NMR-Methoden bis-

lang erzeugten Quantenzustände bei endlicher Temperatur separabel sind, d.h. keine Verschränkung aufweisen [21]. Dies gibt Anlaß für eine interessante aktuelle Diskussion, inwieweit die NMR-Verfahren tatsächlich als Quanteninformationsverarbeitung aufgefaßt werden sollen, oder ob die von uns oben gegebene „klassische" Definition eines Quantencomputers zu eng ist.

Für künftige praktische Anwendungen mit technologischem Potential kommt der Festkörperphysik eine besondere Bedeutung zu. Denn hier gibt es ein wissenschaftliches Umfeld mit Erfahrung in der Erzeugung von immer kleineren geordneten Strukturen (Mikrochips, Nanotechnologie), auf die man aufbauen kann. Für Quantenspeicher und -operationen in Festkörpern ist allerdings die Dekohärenz in vielen Fällen ein vorrangiges Problem. Als Beispiele zur Realisierung eines Quantengatters verweisen wir auf Vorschläge mit Cooper-Paaren in Josephson-Kontakten [22] und mit Spinzuständen von Elektronen in Quantenpunkten [23] als Trägern von Qubits. Außerdem gibt es einen Vorschlag, einen NMR-Quantencomputer mit Methoden der Festkörperphysik zu realisieren [24].

Wir erwarten, daß innerhalb der nächsten zehn Jahre kleine Quantencomputer mit etwa zehn Qubits im Labor zur Verfügung stehen werden. Dies wird sicher die experimentelle Grundlage für eine Reihe von fundamentalen Experimenten zu Teilchenverschränkung, Meßprozeß und Dekohärenzstudien in der Quantenmechanik, sowie „Proof of Principle"-Experimenten in der Quanteninformationsverarbeitung sein. Für eine tatsächliche Anwendung als Quantencomputer im Sinne von Shor und Grover sind diese Systeme allerdings viel zu klein. Somit stellen sich für die Zukunft zwei wesentliche Aufgaben. Erstens ist es erforderlich, Konzepte zur Implementierung von Quantencomputern zu entwickeln, die sich auf eine große Anzahl von Quantenbits skalieren lassen. Zweitens gilt es, relevante Anwendungen zu finden, die mit einer kleinen Zahl von Quantenbits auskommen. Wir werden unten einige Ideen im Rahmen der Quantenoptik diskutieren, mit dem Ziel, Netzwerke von Quantencomputern [27] zu implementieren. Dies ist interessant sowohl vom Standpunkt der Quantenkommunikation als auch im Hinblick auf eine Skalierung kleiner Quantencomputer zu größeren Systemen.

Ionenfallen

Ein Quantenrechner, der auf der Wechselwirkung von Lasern mit gekühlten Ionenketten basiert, wurde in Ref. [25] vorgeschlagen, und in mehreren Labors wird derzeit an einer experimentellen Realisierung gearbeitet (u. a. NIST Boulder, Universität Innsbruck, MPQ Garching, Oxford, Los Alamos). Bei diesem System speichert man ein Quantenbit in einer Überlagerung von zwei ausgewählten metastabilen Energiezuständen eines Ions, wobei die Zustände $\{|0\rangle,|1\rangle\}$ des Qubits zum Beispiel zwei Zeeman-Grundzuständen eines Ions entsprechen. Die Ionen sind in einer elektromagnetischen (Paul-) Falle gespeichert und dadurch eindeutig identifizierbar (Abb. 1).

Die internen Ionenzustände lassen sich mit Laserlicht manipulieren, indem Übergänge $|0\rangle \leftrightarrow |1\rangle$ induziert werden. Für den Fall, daß die Qubits in Zeeman-Grundzuständen gespeichert werden, entspricht dies Übergängen durch nichtresonante Raman-Prozesse. Indem man einzelne Ionen mit Lasern anspricht, kann man somit 1-bit-Quantengatter realisieren. Um 2-bit-Quantengatter zu implementieren, müssen die Ionen in kontrollierter Weise miteinander wechselwirken. Diese Wechselwirkung wird durch die Coulomb-Abstoßung zwischen den Ionen vermittelt. Den Schwingungen der Ionenkette entsprechen kleine Auslenkungen der Ionen um ihre Gleichgewichtslage. Die Eigenmoden dieser Oszillationen, zum Beispiel die Schwerpunktsbewegung der Kette, sind quantisiert. Durch Laserkühlen kann man den Bewegungszustand der Ionenkette im Schwingungsgrundzustand der Falle präparieren. Die quantisierte Schwerpunktsbewegung dient nun als Datenbus zur Verschränkung der internen Ionenzustände. Insbesondere kann ein einzelnes Ion derart mit einem rotverstimmten Laserpuls bestrahlt werden, daß es vom Zustand $|1\rangle$ in den Zustand $|0\rangle$ übergeht und dabei die Ionenkette durch die Abgabe eines Phonons in Schwingung versetzt. Falls das Ion im Zustand $|0\rangle$ ist, wird der Zustand nicht verändert.

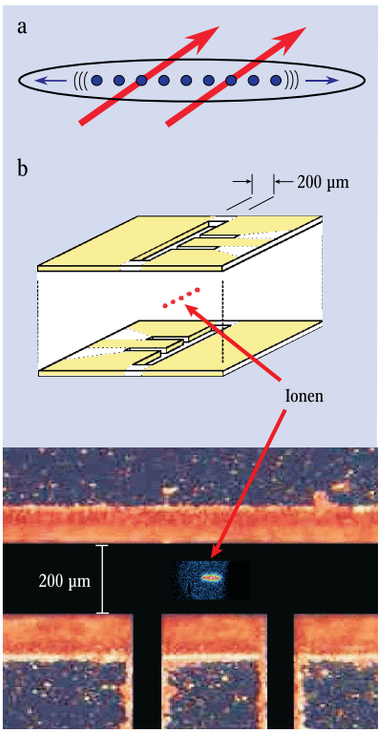


Abb. 1:
▶ a) Schema eines Quantencomputers mit gespeicherten Ionen nach [24]. Jedes einzelne Ion fungiert als „Quantenbit" mit zwei inneren Zuständen $|0\rangle$ und $|1\rangle$, die sich mit Laserstrahlen manipulieren lassen. Über Schwingungsmoden der Ionenkette werden die Quantenbits miteinander gekoppelt.
▶ b) und c) Lithographisch hergestellte Ionenfalle vom NIST in Boulder/Colorado mit fünf Ionen als potentiellem Quantenrechner. (Die Abbildungen wurden uns dankenswerterweise von C. Myatt, C. Monroe und D. J. Wineland überlassen.)

Bei einer Ionenkette kann man nun in einem beliebigen zweiten Ion den internen Zustand gemäß $|0\rangle \leftrightarrow |1\rangle$ „umschalten". Insgesamt erhält man so einen Prozeß, bei dem der interne Zustand des zweiten Ions wechselt, *sofern* das erste Ion sich im Zustand $|1\rangle$ befindet. Wird abschließend der Anfangszustand des ersten Ions wiederhergestellt, so läßt sich damit ein CNOT-Quantengatter realisieren. Jede Rechenoperation läßt sich als eine Folge von solchen Gatteroperationen zusammen mit einfachen Zustandsänderungen der einzelnen Ionen darstellen. Am Beginn einer Rechnung setzt man dabei durch optisches Pumpen den Zustand aller Ionen auf einen gewünschten Anfangswert, zum Beispiel $|0\rangle|0\rangle...|0\rangle$. Um die Bitzustände der Ionen am Ende einer Rechnung auszulesen (Meßprozeß), verwendet man die Methode der Quantensprünge. Dabei wird die Ionenkette mit Laserlicht einer geeigneten Frequenz bestrahlt, so daß ein Ion im Zustand $|1\rangle$ Fluoreszenzlicht ausstrahlt, während es im Zustand $|0\rangle$ dunkel bleibt. Experimentell wurden bisher quantenlogische (Verschränkungs-) Operationen mit einem und mit zwei Ionen demonstriert [10] (siehe auch [15]).

Neutrale Atome in Lichtresonatoren

Andere Vorschläge zur Implementierung von Quantengattern beruhen auf Atomen in optischen Resonatoren hoher Güte [26]. Der physikalische Mechanismus ist dabei sehr ähnlich zu den Ionenfallen, wobei hier Photonen die Rolle eines „Datenbusses" zur Kommunikation zwischen den Atomen spielen, im Gegensatz zu Phononen bei den Ionenfallen. Da es sehr schwierig ist, neutrale Atome auf ähnlich kontrollierte Weise zu speichern wie Ionen in einer Paul-Falle, gibt es derzeit noch keine experimentelle Realisierung dieser Vorschläge.

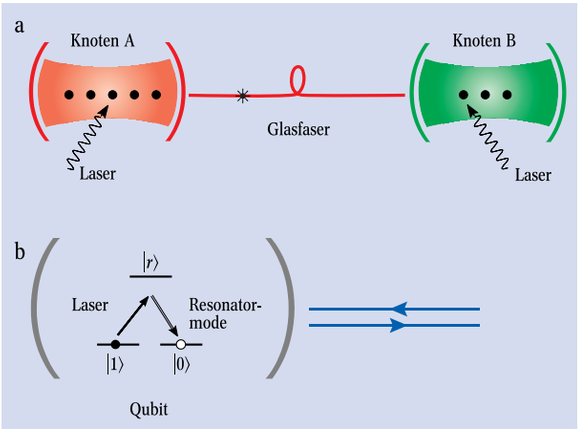


Abb. 2:
▶ a) Quantennetzwerk mit Atomen in optischen Resonatoren und einer Glasfaser als Kommunikationskanal. ▶ b) Atomschema: Das Quantenbit wird in dem Grundzustand eines Dreiniveauatoms gespeichert. Ein Raman-Prozeß überträgt das Qubit auf die Resonatormode. Falls sich das Atom A im Zustand $|0\rangle_A$ befindet, „sieht" es den Laserpuls am Übergang $|1\rangle_A \rightarrow |r\rangle_A$ nicht und verbleibt im Zustand $|0\rangle_A$. Falls es sich im Zustand $|1\rangle_A$ befindet, transferiert ein Laserpuls das Elektron in den Zustand $|0\rangle_A$, wobei ein Photon in die Resonatormode kohärent emittiert wird. Das Photon entweicht aus dem Resonator und propagiert durch die Glasfaser bis zum zweiten Resonator. Durch einen geeigneten Laserpuls kann ein solcher Photonüberlagerungszustand in einen Qubit-Zustand des Atoms B verwandelt werden [26].

Photonen lassen sich nicht nur zur Kommunikation zwischen den Atomen im Resonator verwenden, sondern auch zur Übertragung von Qubits zwischen zwei verschiedenen Resonatoren [27]. Mit solchen Systemen lassen sich somit *Quantennetzwerke* zur Quantenkommunikation aufbauen. Die intakte Übertragung eines Quantenzustandes von einem Knoten A des Netzwerkes zu einem anderen Knoten B entspricht im einfachsten Fall der Transmission eines Qubits gemäß:
$(\alpha|0\rangle_A + \beta|1\rangle_A) \otimes |0\rangle_B \rightarrow |0\rangle_A \otimes (\alpha|0\rangle_B + \beta|1\rangle_B)$.

Die Quantenkommunikation mit Hohlraumresonatoren hoher Güte wurde in mehreren Arbeiten der Innsbrucker Gruppe diskutiert, die sich unter dem Begriff *Photonic Channels* zusammenfassen lassen [27].

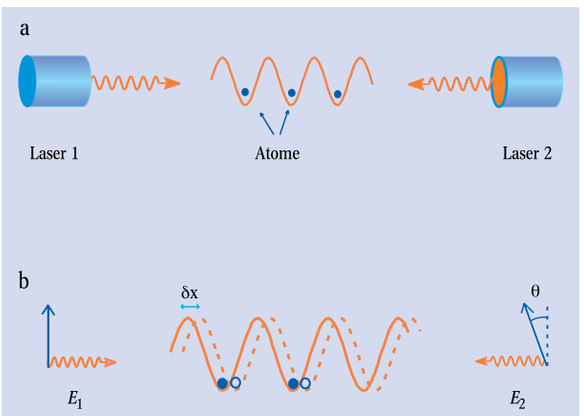


Abb. 3:
a) Fangen und b) Verschieben von neutralen Atomen in stehenden Lichtfeldern. Wird der relative Polarisationswinkel θ zwischen den Werten $\pi/2$ und 0 variiert, dann bewegen sich die Potentiale in entgegengesetzte Richtungen bis sie vollständig überlappen, um anschließend wieder in ihre Ausgangsposition zurückgebracht zu werden. Die durch den Stoß aufgenommene Phasenverschiebung kann groß genug sein, um die Quantenzustände zu verschränken und damit Quantengatter zu implementieren.

Dabei werden interne elektronische Zustände von Atomen (analog zum Ionenfallencomputer) zum Speichern von Qubits verwendet. Photonen dienen zur Übertragung der Qubits von einem Atom auf ein anderes. Um eine kontrollierte Übertragung zu ermöglichen, werden die Atome in optische Resonatoren hoher Güte „eingebettet", die durch eine Glasfaser miteinander verbunden sind (Abb. 2).

Ziel ist es, in einem Resonator nicht nur ein Atom, sondern eine ganze Kette zu speichern, wie zum Beispiel einen Ionenfallencomputer. Das von uns beschriebene Schema entspricht dann einer Vernetzung von Quantencomputern.

Optische Gitter

Ein neuer Vorschlag [28, 31] für einen Quantencomputer basiert auf Stößen zwischen ultrakalten Atomen als Mechanismus zur kontrollierten Erzeugung von Verschränkung (siehe auch [29]). Mit diesem Mechanismus sollten sich wichtige Konzepte der Quanteninformationstheorie in Systemen wie optischen Gittern und magnetischen Mikrofallen experimentell studieren lassen [31]. Als „optische Gitter" bezeichnet man eine Anordnung aus interferierenden Laserstrahlen, in deren Kreuzungspunkt neutrale Atome durch die Dipolkraft an Orten niedriger oder hoher Intensität gehalten werden. So entsteht ein Gitter aus periodisch angeordneten Mikrofallen für neutrale Atome, das Speicherzeiten von bis zu 20 Minuten erlaubt [33]. Die Atome im Gitter dienen dabei als *Datenträger*. Ein *Qubit* entspricht zwei metastabilen internen Zuständen eines Atoms, zum Beispiel zwei Zeeman-Grundzuständen. Übergänge zwischen diesen Zuständen lassen sich wie bei Ionenfallen durch Raman-Laserpulse induzieren. Ein Quantengatter läßt sich realisieren, indem die internen Atomzustände an zwei verschiedene Fallenpotentiale koppeln, die räumlich gegeneinander verschoben werden [28]. Dies kann man durch eine Variation der Polarisation der Laser erreichen, wie in Abb. 3 angedeutet. Dabei bringt man zwei ursprünglich benachbarte Atome für ein bestimmtes Zeitintervall an einen Ort, wo sie miteinander wechselwirken (stoßen). Durch den globalen Effekt der Gitterverschiebung können ganze *Gruppen* von benachbarten Atomen durch eine einzige Gitterverschiebung verschränkt werden. Eine Voraussetzung ist dabei, daß möglichst viele benachbarte Gitterplätze besetzt und die Atome in den Grundzustand gekühlt worden sind [30, 32]. Durch solche kontrollierte Stoßprozesse wäre der Weg zu einer Vielzahl neuer Anwendungen eröffnet. Eine dieser Anwendungen ist die Erzeugung von hochparallelen Quantengattern für Quantencomputing. Außerdem lassen sich an einem solchen System der Verschränkungsgrad und die Dekohärenz von Bell- und Greenberger-Horne-Zeilinger-Zuständen [8] studieren [31].

Quantennetzwerke

Aufgrund der extremen Empfindlichkeit verschränkter Zustände gegenüber der Dekohärenz und der hohen Anforderungen an die Präzision von Gatteroperationen wird man sich auf längere Zeit mit dem Studium von Prototypen von Quantencomputern begnügen müssen. Es geht mittelfristig nicht darum, einen universell programmierbaren Quantenrechner zu bauen. Realistisch sind elementare Quantenprozessoren mit einer kleinen Anzahl von beispielsweise zehn Qubits, die mit einer Genauigkeit bzw. Fehlerrate im Prozentbereich arbeiten. Auch wenn sich damit noch keine großen Zahlen faktorisieren lassen, so können solche „kleinen Prozessoren" für wichtige Aufgaben in der Quanten*kommunikation* eingesetzt werden. Als Beispiel soll im

folgenden ein aktuelles Problem der Quantenkommunikation in Quantennetzwerken (siehe Abb. 4) besprochen werden, das die Übertragung von Quantenzuständen über weite Distanzen betrifft.

Mit den oben diskutierten Methoden lassen sich verschränkte Zustände zwischen räumlich entfernten Atomen erzeugen. Dabei werden einzelne Photonen zum Beispiel durch eine optische Glasfaser geschickt, die die Atome miteinander verbindet. Diese Methode ist anwendbar, solange die Absorptionswahrscheinlichkeit für die Photonen nicht zu groß ist. Für *lange* Kanäle tritt jedoch ein Problem auf, das auch in der klassischen Kommunikation bekannt ist: Wird ein klassisches Signal durch eine Glasfaser oder auch eine elektrische Leitung geschickt, dann wird das Signal gedämpft, d.h. die Amplitude nimmt ab; außerdem wird es verzerrt. Um diese Probleme zu lösen, werden sogenannte „Repeater“ (Verstärker) in bestimmten Abständen in den Kanal eingebaut.

Bei der *Quantenkommunikation* bestehen die „Signale“ jedoch aus einzelnen Photonen, die zudem miteinander verschränkt sein können. Diese Photonen dürfen nicht verstärkt werden, da jeder Verstärkungsprozeß Rauschen in das System einführt, wodurch die subtilen Quanteneigenschaften verlorengehen und mögliche Quantenkorrelationen zerstört werden. Man befindet sich dabei in einem scheinbaren Dilemma: Solange das Photon noch nicht absorbiert ist, darf es nicht verstärkt werden; sobald es absorbiert wird, ist die Information, die es trug, verloren. Im Rahmen der Quantenkommunikation gibt es in der Tat Schemata, die dieses Problem lösen. Im folgenden werden wir zunächst auf die Teleportation und die Verschränkungsreinigung eingehen. Diese liefern die Grundlage für die nachfolgende Diskussion des Quantenrepeaters.

Protokolle der Quantenkommunikation

Ziel der Quantenkommunikation ist es, einen Quantenzustand $|\phi\rangle$, z. B. ein Qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, zwischen zwei räumlich getrennten Parteien A und B, üblicherweise „Alice“ und „Bob“ genannt, störungsfrei zu übertragen. Im allgemeinen findet die Kommunikation jedoch durch ein Medium statt, das mit den Informationsträgern wechselwirkt. Ein Beispiel dafür ist in Abb. 2 gegeben: Bei der Übertragung der Photonen in der Glasfaser kommt es zur Streuung und Absorption. Das gesamte, aus den Atomen, den Resonatoren und der Glasfaser bestehende System läßt sich abstrakt als *verrauschter und dissipativer Quantenkanal* auffassen. Solch eine Situation ist noch einmal in Abb. 5 skizziert. Werden die Qubits direkt durch den Kanal transmittiert, so erhält Bob anstelle des reinen Zustandes $|\phi\rangle$ einen gemischten Zustand, der durch eine Dichtematrix $\varrho \neq |\phi\rangle\langle\phi|$ beschrieben wird und der im allgemeinen nicht mehr genau mit dem ursprünglichen Zustand des Qubits übereinstimmt. Der quantenmechanische Überlapp $\langle\phi|\varrho|\phi\rangle$, das heißt der Anteil des reinen am gemischten Zustand wird dabei als Maß für die Güte der Transmission verwendet (engl. *fidelity F*). Im Beispiel der Absorption in einer Glasfaser erwarten wir $F \sim \exp(-l/l_0)$ mit l_0 der Absorptionslänge (allgemeiner: Kohärenzlänge) und l der Länge der Glasfaser, wobei in typischen Experimenten $l_0 \sim 10 - 20$ km. Für die Sicherheit beziehungsweise Effizienz von Protokollen der Quantenkommunikation sind im allgemeinen Werte $F \simeq 1$ erforderlich. Das Problem ist also: Wie kann man eine Übertragung hoher Güte erreichen, wenn der zur Verfügung stehende Kanal verrauscht ist?

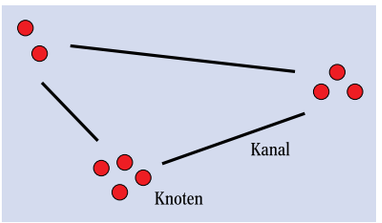


Abb. 4:
Schema eines Quantennetzwerkes. Knoten repräsentieren Quantenspeicher und Quantenprozessoren, die über verrauschte Quantenkanäle verbunden sind.

Dieses Problem ist gelöst, falls Alice und Bob vorab im Besitz eines verschränkten Zustandes zweier Teilchen sind, wie etwa dem „Singulett-Zustand“ $|\psi\rangle_{AB}$ in Abb. 5. Will Alice nun einen unbekannten Quantenzustand eines Teilchens C zu Bob senden, so braucht sie diesen nicht durch den Kanal zu schicken, sondern kann die Methode der *Teleportation* [6 – 8] verwenden (siehe Kasten 1).

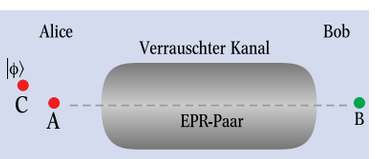


Abb. 5:
Teleportation eines Qubits $|\phi\rangle$, welches in C gespeichert ist, mittels eines EPR-Paares (Atome A und B). Alice führt zunächst eine Messung durch, die die Atome A und C miteinander verschränkt. Dadurch ändert sich der Zustand von B, den Bob durch eine unitäre Transformation – nach Rücksprache mit Alice – in den Zustand $|\phi\rangle$ umwandeln kann.

Die Frage ist allerdings, wie man einen verschränkten Zustand zweier Teilchen A und B wie in Abb. 5 überhaupt erzeugt. Da Verschränktheit nicht allein durch lokale Operationen erzeugt werden kann, müssen Alice und Bob letztlich doch Qubits durch den Quantenkanal schicken. Da der Kanal verrauscht ist, erhält man kein reines Singulett wie in Abb. 5, sondern zunächst ein imperfektes EPR-Paar. Verwendet man ein solches Paar direkt für die Teleportation, so ist dadurch nichts gewonnen, und der teleportierte Zustand wird wiederum zu einem Gemisch, wie bei der direkten Transmission durch den Kanal. Die Idee ist nun, das imperfekte EPR-Paar vorab zu reinigen, bevor man es für die Teleportation verwendet. Der Prozeß der *Verschränkungsreinigung* [35] entspricht dabei einer Art Destillation eines reinen Singuletts aus einem Ensemble von vielen imperfekten Paaren (siehe Kasten 2). Die Methode der Verschränkungsreinigung ist anwendbar, falls man Ausgangspaare der Güte $F > 1/2$ zur Verfügung hat, wobei $F = {}_{AB}\langle\psi|\varrho_{AB}|\psi\rangle_{AB}$. Daraus folgt wiederum: Falls Alice und Bob im Besitz eines hinreichend großen Ensembles von EPR-Paaren mit $F > 1/2$ sind, dann ist – zumindest im

Kasten 1 – Teleportation

Beim Prozeß der Teleportation wird eine bestehende Verschränkung zwischen zwei entfernten Teilchen A und B dazu verwendet, den unbekannten Quantenzustand eines dritten Teilchens C zu übertragen. Dazu gehen der Sender (Alice) und der Empfänger (Bob) wie folgt vor. (Siehe auch Abb. 5).

- Alice führt eine sogenannte Bell-Messung an den beiden Teilchen A und C durch, die deren Zustand auf einen von vier Bell-Zuständen projeziert:

$$|\psi^{\pm}\rangle = 1/(\sqrt{2})(|0\rangle_A|1\rangle_C \pm |1\rangle_A|0\rangle_C),$$

$$|\phi^{\pm}\rangle = 1/(\sqrt{2})(|0\rangle_A|0\rangle_C \pm |1\rangle_A|1\rangle_C).$$

Eine Möglichkeit, diese Bell-Messung durchzuführen, besteht in der Anwendung eines CNOT-Gatters auf die Teilchen A and C, gefolgt von einer Zustandsmessung dieser Teilchen.

- Alice teilt das Ergebnis ihrer Messung Bob über einen klassischen Kanal mit (zum Beispiel über Telephon oder E-mail).
- Bob wendet je nach Meßergebnis eine von vier unitären Operationen an, die den ursprünglichen Zustand von Teilchen C auf Teilchen B wiederherstellen.

Man beachte, daß bei dieser Prozedur der Quantenkanal zwischen A und B keine Rolle spielt. Im extremsten Fall könnte der Kanal (wie zum Beispiel die Glasfaser in Abb. 2) auch zerstört sein.

Prinzip – das Problem der Quantenkommunikation über den verrauschten Kanal gelöst.

Für die Absorption in der Glasfaser bedeutet $F \sim \exp(-l/l_0) > 1/2$ allerdings, daß eine Verschränkungsreinigung nur anwendbar ist für Distanzen der Größenordnung l_0. Somit bleibt die Quantenkommunikation über große Entfernungen $l \gg l_0$ weiterhin ein Problem. Die Lösung dieses Problems ist der Quantenrepeater.

Quantenrepeater

Ein naheliegender Ansatz für einen Quantenrepeater besteht darin – analog zum klassischen Repeaterkonzept – einen Kanal der Länge l zunächst in N kürzere Segmente der Länge $l_s = l/N$ zu unterteilen. Die Länge l_s ist dabei so gewählt, daß es möglich wird, über diese Segmente EPR-Paare der Güte $F > 1/2$ zu erzeugen, die anschließend auf einen hohen Wert $F_{max} \sim 1$ gereinigt werden. In einem zweiten Schritt werden die so erzeugten Paare mittels Teleportation zu einem einzigen EPR-Paar über die Distanz l verbunden. Die Teleportation bewirkt dabei einen *Verschränkungstransfer* (engl. *entanglement swapping* [34, 6]), bei dem die Verschränkung zwischen zwei Teilchen auf weiter entfernte Teilchen übertragen wird (siehe Kasten 2).

Für perfekt gereinigte Paare ($F_{max} = 1$) und für eine ideale Implementierung der Teleportation wäre damit das Problem bereits gelöst. Für jedes reale System ist dies aber nicht der Fall, denn ein reines EPR-Singulett kann auch durch die Methode der Verschränkungsreinigung [35] nicht erzeugt werden, da die Operationen, aus denen das Reinigungsprotokoll besteht, selbst bis zu einen gewissen Grad verrauscht sind [13]. Für die meisten Anwendungen der Quantenkommunikation ist dies kein wesentliches Hindernis, solange die maximal erreichbare Güte F_{max} hinreichend nahe bei 1 liegt (d. h. die Bellschen Ungleichungen durch ein solches Paar deutlich verletzt werden). Beim Quantenrepeater führt dies jedoch dazu, daß mit jedem Verschränkungstransfer (siehe Kasten 2) die Güte der Verschränkung abnimmt. Die Güte F_N des am Ende erhaltenen Paares skaliert dadurch wieder exponentiell mit N, das heißt $F_N \sim \exp(-N)$. Man hat durch diese Methode also scheinbar nichts gewonnen.

Die Lösung des Problems besteht nun darin, daß man nach einer gewissen Anzahl von Verschränkungstransfer-Schritten die erhaltenen Paare wieder auf den maximalen Wert F_{max} *nachreinigt*. Die Übertragung von Verschränkung auf sehr weit entfernte Teilchen wird dann durch eine alternierende Sequenz von Transfer- und Reinigungsschritten erreicht, wie in Kasten 3 näher erläutert.

Eine quantitative Größe, die die Effizienz des Verfahrens mißt, ist die Anzahl der erforderlichen *Resourcen*. Bei der oben diskutierten quantenoptischen Implementierung entspricht dies der gesamten Anzahl der über den Kanal ausgetauschten Photonen. Eine genauere Analyse zeigt, daß diese Anzahl nur *polynomial* mit der Länge des Kanals wächst. Abstrakt gesprochen ist damit ein Problem mit exponentieller Skalierung auf ein Problem mit polynomialer Skalierung transformiert worden. Stellt man sich unter den Teilchen Atome vor, die in einem Quantennetzwerk wie in Abb. 6 an verschiedenen Knoten gespeichert werden, dann erfordert

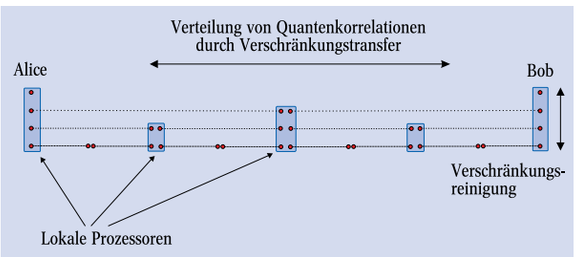


Abb. 6:
Realisierung eines Quantenrepeaters [13]: Die Verteilung von Quantenkorrelationen gelingt über weite räumliche Entfernungen mit Hilfe der Verschränkungsreinigung und des Verschränkungstransfers. Der Quantenrepeater ist, anders als die klassische Signalverstärkung, ein *nichtlokales* Konzept, das sowohl lokale Verknüpfungspunkte als auch ein globales Reinigungsprotokoll (siehe Kasten 3) erfordert. Das Schema vermeidet eine Signalverstärkung wie in der klassischen Kommunikation.

der Aufbau eines verschänkten Zustands zwischen Alice und Bob an jedem Knoten eine gewisse Anzahl von Atomen, zwischen denen wiederholt Photonen ausgetauscht werden.

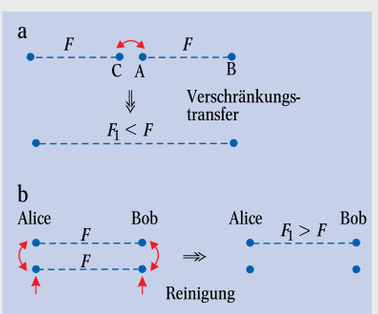
Wie in Ref. [13] gezeigt wird, ist die Zahl von Atomen pro Knoten allerdings nicht sehr groß und wächst nur *logarithmisch* mit der Entfernung zwischen Alice und Bob. Dies ist ein wichtiger Punkt für eine praktische Implementierung, bei der eine Hauptschwierigkeit darin besteht, eine große Anzahl von Teilchen zu speichern und mit hinreichender Präzision kohärent zu manipulieren. Die Rolle der klassischen Verstärker wird hier sozusagen von kleinen „Quantenprozessoren“ übernommen, die in bestimmten Abständen in den Transmissionskanal eingebaut werden. Ein Zahlenbeispiel: Nimmt man für den Abstand l_s zwischen benachbarten Knoten eine typische Entfernung von 10 km an, so genügt eine Anzahl von größenordnungsmäßig zehn Atomen pro Knoten für Quantenkommunikation über Entfernungen von etwa 1000 km. Die erforderliche Präzision, mit der die Gatteroperationen an den Knoten ausgeführt werden müssen, liegt dabei im Bereich eines Prozents [13].

Ausblick

Die Gesetze der Quantenmechanik eröffnen faszinierende Perspektiven für die Kommunikation und die Informationsverarbeitung. Die Entwicklung der letzten

Kasten 2 – Verschränkungsreinigung und -transfer

▸ a) Verschränkungstransfer (entanglement swapping): Durch die Teleportation des Zustandes eines Teilchens C, das bereits mit einem weiteren Teilchen verschränkt ist, wird diese Verschränkung auf das Teilchen B übertragen.
▸ b) Verschränkungsreinigung (entanglement purification): Alice und Bob besitzen ein Ensemble von imperfekten EPR-Paaren mit Güte $F > 1/2$. Ein typischer Reinigungsschritt besteht darin, daß Alice und Bob an jeweils zwei Paaren eine Sequenz von *lokalen* unitären Operationen (z. B. CNOT-Gatter) durchführen und anschließend den Zustand der Teilchen eines Paares messen. Am Ende vergleichen Alice und Bob ihre Meßergebnisse: stimmen diese überein, so hat das verbleibende Paar eine höhere Güte $F_1 > F$, andernfalls verwerfen sie auch die anderen Teilchen. Die genaue Sequenz von Operationen und Messungen hängt dabei

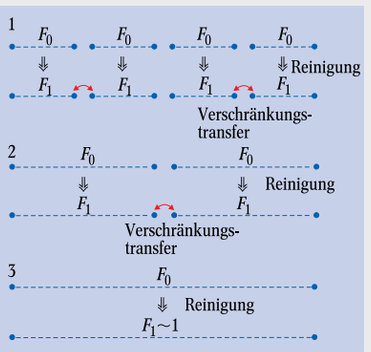


vom sogenannten Reinigungsprotokoll ab. Durch iterierte Anwendung des Protokolls wird so aus dem anfänglichen Ensemble von Paaren niedriger Güte ein Subensemble von Paaren sehr hoher Güte „destilliert“. In der Literatur sind eine Reihe von Reinigungsprotokollen bekannt, die sich vor allem durch ihre Effizienz unterscheiden.

Jahre in diesem Forschungsfeld zeigt auch, wie eng theoretische Grundlagendiskussionen mit praktischen Anwendungen verknüpft sein können, wie etwa die Diskussion über die Rolle der quantenmechanischen Verschränkung als Kommunikationsresource [1, 6, 36]. Für die nähere Zukunft wird es nun darum gehen, physikalische Systeme zu identifizieren, die kontrollierte Verschränkungsoperationen mit einer kleineren Anzahl von Teilchen erlauben. Dadurch können Grundkonzepte der Quanteninformationstheorie, wie zum Beispiel die Kontrolle der Dekohärenz durch Quantenfehlerkorrektur und Verschränkungsreinigung, experimentell getestet werden. Es läßt sich derzeit zwar nicht absehen, wann und in welcher Form diese Entwicklungen zu technischen Anwendungen führen werden, oder gar welche grundlegenden konzeptionellen Fragen noch auf uns warten. Aus unserem gegenwärtigen Verständnis der Physik gibt es aber keinen fundamentalen Grund, der die Realisierung eines Quantencomputers verbieten würde. Die Frage ist daher nicht *ob*, sondern vielmehr *wann* dies stattfinden wird. Am spannendsten (wenn auch unwahrscheinlich) aus der Sicht des Physikers wäre es zumal, wenn wir, im Rahmen der Untersuchung von Quantencomputern und deren experimenteller Realisierbarkeit, an die Grenzen der Quantentheorie und möglicherweise auf neue physikalische Prinzipien stoßen würden. Bislang gibt es zu dieser Annahme keinen Grund.

Kasten 3 – Rekursiver Verschränkungstransfer

Zum Aufbau verschränkter Zustände zwischen weit entfernten Teilchen werden die Protokolle der Verschränkungsreinigung und des Verschränkungstransfer zu einen einzigen Protokoll (engl. *nested entanglement purification*) synthetisiert. Für einen aus vier Segmenten bestehenden Kanal sieht der Prozeß zum Beispiel folgendermaßen aus. Schritt (1): Über jedes der vier Segmente wird gleichzeitig ein Ensemble von EPR-Paaren der Güte $F_0 > 1/2$ erzeugt. Durch Verschränkungs*reinigung* (siehe Kasten 2) wird aus jedem Ensemble ein Subensemble von Paaren der Güte $F_1 \leq F_{\max}$ destilliert. Abschließend werden diese gereinigten Paare mit Hilfe von Verschränkungs*transfer* paarweise verbunden. Am Ende dieser Prozedur erhält man zwei Subensembles von Paaren der Güte F_0 mit der *doppelten Länge*. Dieselbe Prozedur wird nun in Schritt (2) mit den längeren Paaren wiederholt, wodurch man ein noch kleineres Subensemble von Paaren der Güte F_0 mit der vierfachen ursprünglichen Länge erhält. Im letzten Schritt (3) können daraus Paare der Güte $F_1 \leq F_{\max}$ destilliert werden.



In einer etwas informelleren Sprechweise werden durch den beschriebenen Prozeß Quantenkorrelationen, die über kurze Distanzen bestehen, sukzessive „verknüpft“ zu Quantenkorrelationen, die sich schließlich über den gesamten Kanal erstrecken.

Literatur

[1] *C. H. Bennett*, Phys. Today **48** (10), 24 (1995); *D. P. DiVincenzo*, Science, **270**, 255 (1995)
[2] *A. M. Steane*, Rept. Prog. Phys. **61**, 117 (1998)
[3] *A. Ekert, R. Josza*, Rev. Mod. Phys. **68**, 733 (1995)
[4] *L. K. Grover*, Phys. Rev. Lett. **79**, 325 (1997)
[5] *A. Einstein, B. Podolsky, N. Rosen*, Phys. Rev. **47**, 777 (1935)
[6] *C. H. Bennett* et al., Phys. Rev. Lett. **70**, 1895, (1993)
[7] *D. Bouwmeester* et al., Nature **390**, 575 (1997); *D. Boschi* et al., ibid. **80**, 1121 (1998); *A. Furusawa* et al., Science **282**, 706 (1998)
[8] *H. Weinfurter, A. Zeilinger*, Phys. Bl., März 1996, S. 219
[9] *T. Beth, G. Brassard* (Hrsg.), Quantum Algorithms, Dagstuhl-Seminar-Report 210, (1998)
[10] *C. Monroe* et al., Phys. Rev. Lett. **75**, 4714 (1995); *Q. A. Turchette* et al., ibid. **81** 3631 (1998)
[11] *R. P. Feynman*, Int. J. theor. Phys. **21**, 467 (1982)
[12] *W. Tittel* et al., Phys. Bl., Juni 1999, S. 25
[13] *H.-J. Briegel* et al., Phys. Rev. Lett. **81**, 5932 (1998)
[14] *H. Walther*, Adv. At. Mol. Opt. Phys. **32**, 379 (1994)
[15] *H. C. Nägerl* et al., Phys. Rev. A **60**, 145 (1999)
[16] *E. Peik* et al., Phys. Rev. A **60**, 439 (1999)
[17] *S. Chu*, Rev. Mod. Phys. **70**, 686 (1998); *C. Cohen-Tannoudji*, ibid., 707; *W. D. Phillips*, ibid., 721
[18] *Q. A. Turchette*, Phys. Rev. Lett. **75**, 4710 (1995)
[19] *E. Hagley* et al., Phys. Rev. Lett. **79**, 1 (1997)
[20] *D. G. Cory* et al., Proc. Natl. Acad. Sci. USA **94**, 1634 (1997); *N. A. Gershenfeld, I. L. Chuang*, Science **275,** 350 (1997)
[21] *S. L. Braunstein* et al., e-print quant-ph/9811018
[22] *A. Shnirman, G. Schön, Z. Hermon*, Phys. Rev. Lett. **79**, 2371 (1997)
[23] *D. Loss, D. P. DiVincenzo*, Phys. Rev. A **57**, 120 (1998)
[24] *B. E. Kane*, Nature **393**, 133 (1998)
[25] *J. I. Cirac, P. Zoller*, Phys. Rev. Lett. **74**, 4091 (1995)
[26] *T. Pellizzari* et al., Phys. Rev. Lett. **75**, 3788 (1995)
[27] *J. I. Cirac* et al., Phys. Rev. Lett. **78**, 3221 (1997); *S. J. van Enk* et al., Science **279**, 205 (1998)
[28] *D. Jaksch* et al., Phys. Rev. Lett. **82,** 1975 (1999)
[29] *G. K. Brennen* et al., Phys. Rev. Lett. **82**, 1060 (1998)
[30] *D. Jaksch* et al., Phys. Rev. Lett. **81**, 3108 (1998)
[31] *H.-J. Briegel* et al., e-print quant-ph/9904010
[32] *M. T. DePue* et al., Phys. Rev. Lett. **82,** 2262 (1999)
[33] *S. Friebel* et al., Phys. Rev. A **57**, R20 (1998)
[34] *M. Zukowski* et al., Phys. Rev Lett. **71**, 4287 (1993); *J. W. Pan* et al., Phys. Rev. Lett. **80**, 3891 (1998)
[35] *C. H. Bennett* et al., Phys. Rev. Lett. **76**, 722 (1996)
[36] *R. F. Werner*, Phys. Rev. A **40**, 4277 (1989); *M. Lewenstein, A. Sanpera*, Phys. Rev. Lett. **80**, 2261 (1998); *M. Horodecki, P. Horodecki, R. Horodecki*, ibid., 5239

Quantenphysik

Quantenkorrelationen und die Bellschen Ungleichungen

Von der Grundlagenforschung zur technologischen Anwendung

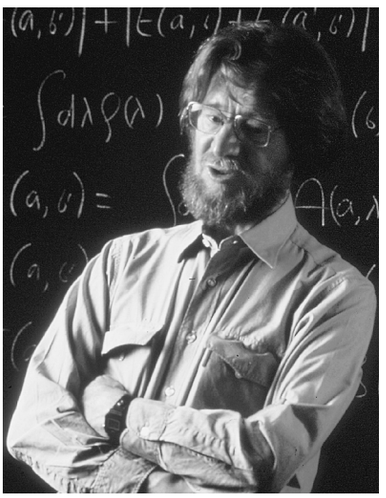
Gernot Alber und Matthias Freyberger

Seit der Geburt der modernen Quantenmechanik macht jede Generation von Physikern aufs Neue eine befremdende und faszinierende Erfahrung: Ihre an der klassischen, makroskopischen Erfahrungswelt geschulte Intuition prallt auf erstaunliche Voraussagen quantenphysikalischer Gesetzmäßigkeiten. Im Zentrum dieses Staunens stehen die nichtlokalen Korrelationen quantenmechanischer Teilchen. Keine klassische Theorie scheint in der Lage zu sein, diese Korrelationen korrekt zu modellieren. Woran liegt das und wo stehen wir heute am Ende des Jahrhunderts der Quantenmechanik?

Die Zustandsbeschreibungen der klassischen Mechanik auf der einen Seite und der Quantenmechanik auf der anderen Seite sind vollkommen verschieden. Klassisch ist der Zustand eines Systems vollständig festgelegt, sobald Orts- und Impulskoordinaten aller beteiligten Teilchen bekannt sind. Durch den Zustand des Gesamtsystems ist das Ergebnis einer Orts- und Impulsmessung an einem einzelnen Teilchen eindeutig festgelegt und unabhängig von den Messungen, die an den übrigen Teilchen durchgeführt werden. Das ist der typische lokale Charakter der klassischen Physik.

Die Quantentheorie stellt dieses Bild radikal in Frage. Der Zustandsbegriff ist ein völlig anderer. Die Gesamtinformation über ein Quantensystem wird durch einen Zustandsvektor $|\psi\rangle$ beschrieben, dessen Eigenschaften durch die mathematische Struktur des Hilbert-Raumes bestimmt werden. Insbesondere können charakteristische Eigenschaften des Quantenzustandes eines Gesamtsystems zwischen zwei oder mehreren Subsystemen *verschränkt* sein (siehe dazu Kasten 1), wobei keines der einzelnen Subsysteme jeweils für sich alleine diese Charakteristika aufweist. Folglich reichen lokale Messungen an den Subsystemen nicht aus, um den quantenmechanischen Gesamtzustand zu rekonstruieren. Das Ergebnis einer Messung an einem Subsystem hängt entscheidend davon ab, welche Größe an den anderen Subsystemen beobachtet wird. Erst mit diesen nichtlokalen Korrelationen ergibt sich eine quantenmechanisch vollständige Beschreibung des Gesamtsystems: „Das Ganze ist mehr als die Summe seiner Teile."

Sind diese auf rätselhafte Weise verwobenen Quantenzustände nur ein seltsamer Zug einer Theorie, der auf mikroskopische Distanzen beschränkt ist? Neue Experimente in Genf [1] und Innsbruck [2] untermauern nicht nur die ungewöhnlichen Korrelationen verschränkter Quantenzustände, sondern belegen auch in eindrucksvoller Weise, daß die damit verbundenen Quantenphänomene über makroskopische Distanzen (> 10 km) auftreten können. Neben der großen Bedeutung dieser Ergebnisse für die Grundlagenforschung eröffnen sich damit zugleich interessante Perspektiven für ungewöhnliche neue Anwendungen im Rahmen der Quanteninformationsverarbeitung. Die rätselhaften Züge der Quantenmechanik lassen sich vorteilhaft für technologische Anwendungen nutzen. Das Potential möglicher Anwendungen reicht von der Quantenkryptographie über Quantenteleportation bis hin zum Quantencomputer.



John Bell versuchte die Quantenmechanik durch verborgene Parameter zu ergänzen, um wieder zu einer lokalen und deterministischen Naturbeschreibung zurückzukehren. Dabei entdeckte er die später nach ihm benannten Ungleichungen. Sie erlauben es, die von der Quantenmechanik implizierte Nichtlokalität experimentell zu überprüfen. Mit raffinierten Experimenten könnten schon bald die letzten Schlupflöcher für lokale Theorien geschlossen werden. (Foto: CERN)

Die Geschichte der mit verschränkten Quantenzuständen zusammenhängenden Fragen, die die Physiker immer wieder bewegt haben, läßt sich bis ins Jahr 1935 zurückverfolgen, als Schrödinger den Begriff der Verschränkung prägte [3] und Einstein, Podolsky und Rosen (EPR) das später nach ihnen benannte Gedankenexperiment formulierten. Das EPR-Gedankenexperiment brachte die bizarr anmutenden Vorhersagen der Quantenmechanik auf den Punkt: Entweder, so die Schlußfolgerung, die Quantenmechanik ist nichtlokal, oder sie ist unvollständig. Nichtlokal heißt hier, daß die Messung an einem Teilchen die Messung an einem anderen Teilchen unmittelbar beeinflussen kann, auch wenn beide weit voneinander entfernt sind. Mit der Nichtlokalität verschränkter Systeme konnten sich Einstein, Podolsky und Rosen nicht anfreunden, daher schlossen sie auf die Unvollständigkeit der Quantenmechanik [4]. Die kreative Unruhe, die von dieser Schlußfolgerung ausging, führte schließlich 1964 John Bell zu einer bahnbrechenden Entdeckung. Er versuchte die vermeintliche Unvollständigkeit der Quantenmechanik durch noch unbekannte, „verborgene" Para-

Priv.-Doz. Dr. Gernot Alber und Priv.-Doz. Dr. Matthias Freyberger, Abteilung für Quantenphysik, Universität Ulm, D-89069 Ulm

Physikalische Blätter 55 (1999) Nr. 10
0031-9279/99/1010-23
$17.50+50/0

meter im Rahmen einer lokalen und kausalen Theorie zu ergänzen (siehe dazu Kasten 2). Dabei entdeckte er, daß verschränkte Quantenzustände zu statistischen Vorhersagen führen, die niemals mit Vorhersagen von solchen lokalen und kausalen Theorien in Einklang zu bringen sind. Die quantitative Fassung dieses entscheidenden Ergebnisses sind die Bellschen Ungleichungen [5]. Damit war der Weg offen, die grundlegenden Unterschiede zwischen der Quantenmechanik und einer lokalen, kausalen Theorie experimentell zu überprüfen. Als Bell seine Ungleichungen aufstellte, waren die Möglichkeiten experimenteller Tests freilich noch relativ bescheiden. Erst ab den achtziger Jahren verfügte man über ausreichende Präzision. Bevor wir im Abschnitt „Experimentelle Tests“ auf die Ergebnisse dieser Experimente eingehen, skizzieren wir im folgenden Exkurs die Herleitung der Bellschen Ungleichungen.

Kasten 1 – Verschränkte Quantenzustände

Der Begriff der Verschränkung zwischen Quantensystemen läßt sich in einfachster Weise an einem Quantensystem erläutern, das nur aus zwei Subsystemen (Teilchen) besteht. Ein verschränkter Quantenzustand zweier Quantensysteme besitzt die charakteristische Eigenschaft, daß er sich nicht faktorisieren läßt. Betrachten wir als Beispiel zwei Photonen mit den orthogonalen Einteilchenzuständen $|+1\rangle$ und $|-1\rangle$, die sich in dem verschränkten Bell-Zustand

$$|\psi\rangle = (1/\sqrt{2})(|+1\rangle|-1\rangle - |-1\rangle|+1\rangle) \quad \text{(I)}$$

befinden. Dieser Zustand ist verschränkt, da er sich *nicht* als Produkt

$$|\psi\rangle = |\mu\rangle|\nu\rangle.$$

schreiben läßt. Dies wird klar, wenn wir die Zustände $|\mu\rangle$ und $|\nu\rangle$ in der Basis der orthogonalen Photonenzustände entwickeln und die Bedingungen für Faktorisierbarkeit explizit untersuchen. Mit dem Ansatz

$$|\mu\rangle = C_{+1}|+1\rangle + C_{-1}|-1\rangle,$$
$$|\nu\rangle = D_{+1}|+1\rangle + D_{-1}|-1\rangle$$

gilt für einen faktorisierbaren Zustand

$$|\mu\rangle|\nu\rangle = C_{+1}D_{+1}|+1\rangle|+1\rangle + C_{-1}D_{-1}|-1\rangle|-1\rangle + C_{+1}D_{-1}|+1\rangle|-1\rangle + C_{-1}D_{+1}|-1\rangle|+1\rangle.$$

Wenn der Zustand (I) faktorisierbar wäre, müßte er folgende Beziehungen erfüllen:

$$C_{+1}D_{+1} = 0 \quad , C_{-1}D_{-1} = 0,$$
$$C_{+1}D_{-1} = 1/\sqrt{2} \quad , C_{-1}D_{+1} = -1/\sqrt{2}.$$

Man erkennt leicht, daß sich diese Beziehungen nicht gleichzeitig erfüllen lassen. Der Quantenzustand (I) ist somit nicht faktorisierbar, also verschränkt. Eine Messung des ersten Teilchens legt den Polarisationszustand des zweiten Teilchens fest. Falls eine Messung der Polarisation des ersten Teilchens das Resultat (+1) ergibt, befindet sich das zweite Teilchen im Zustand $|-1\rangle$ und umgekehrt.

Die Bellschen Ungleichungen

Um die wesentliche Aussage der Bellschen Ungleichungen genauer zu verstehen, betrachten wir ein Photonenpaar, das in einem atomaren Zwei-Photonen-Zerfallsprozeß oder in einem nichtlinearen optischen Prozeß entsteht (siehe dazu Abb. 1). Jedes einzelne dieser Photonen werde von räumlich getrennten Beobachtern A und B mit Polarisatoren auf Polarisationseigenschaften hin untersucht. Außerdem wollen wir annehmen, daß die Beobachter A und B ihre Polarisatoren zufällig zwischen zwei Richtungen mit Einheitsvektoren $\vec{\alpha}_1$ und $\vec{\alpha}_2$ bzw. $\vec{\beta}_1$ und $\vec{\beta}_2$ hin und her schalten. Für jede Orientierung der Polarisatoren sind nur zwei Ergebnisse möglich: horizontal zum jeweils gewählten Einheitsvektor polarisiert (kodiert durch +1) oder vertikal polarisiert (kodiert durch –1). Die Meßergebnisse werden folglich durch eine zweiwertige (dichotome) Variable beschrieben.

Wir wollen nun untersuchen, welche Einschränkungen sich für die Korrelationen der Meßergebnisse von A und B ergeben, wenn wir annehmen, daß diese Meßergebnisse durch eine lokale realistische Theorie (LRT) mit verborgenen Parametern unbekannter Natur bestimmt werden (siehe dazu Kasten 2). Ein wichtiger Punkt ist hierbei, daß man zu konkreten Aussagen gelangen kann, obwohl über die Theorie selbst wenige Annahmen gemacht werden. Die wesentliche Annahme besteht darin, daß man mit Hilfe der LRT jederzeit voraussagen kann, wie der Polarisationsvektor der beiden Photonen orientiert ist. Demzufolge hängen die Meßergebnisse der Beobachter A und B nur von den verborgenen Parametern (λ) des Photonenpaares und ihrer jeweils eigenen Meßapparatur ab (Lokalität). Insbesondere sind die Meßergebnisse des einen Beobachters unabhängig von der Wahl der Polarisatorrichtung des anderen Beobachters, im Gegensatz zu den Vorhersagen der Quantenmechanik für verschränkte Zustände. Im Formalismus der Quantenmechanik ist die Polarisation der beiden Photonen unbestimmt, bis sie durch den Meßprozeß auf eine bestimmte Richtung im Raum projeziert wird.

Zusammenfassend können sich so für einen beliebigen Zustand des Photonenpaares folgende Meßergebnisse einstellen: Beobachter A findet die Resultate $a(\vec{\alpha}_1, \lambda) \equiv a_1 = \pm 1$ oder $a(\vec{\alpha}_2, \lambda) \equiv a_2 = \pm 1$; Beobachter B entsprechend $b(\vec{\beta}_1, \lambda) \equiv b_1 = \pm 1$ oder $b(\vec{\beta}_2, \lambda) \equiv b_2 = \pm 1$. Wichtig ist, daß die LRT-Observablen $a(\vec{\alpha}_i, \lambda)$ und $b(\vec{\beta}_i, \lambda)$ diese Meßergebnisse schon vor der eigentlichen Messung voraussagen. Um eine experimentell zugängliche Meßgröße zu erhalten, betrachtet man den Ausdruck $(a_1 + a_2)b_1 + (a_2 - a_1)b_2$. Für alle möglichen Meßergebnisse gilt $(a_1 + a_2)b_1 + (a_2 - a_1)b_2 = \pm 2$.

Bei oftmaliger Wiederholung des Experiments können die verborgenen Parameter λ verschiedene Werte annehmen, die innerhalb einer LRT durch eine normierte Wahrscheinlichkeitsverteilung $P(\lambda)$ gewichtet werden. Mitteln wir über ein statistisches Ensemble von Experimenten, so fordert jede LRT

$$\int_\Lambda d\lambda\, P(\lambda)|(a_1 + a_2)b_1 + (a_2 - a_1)b_2| = 2\,. \qquad (1)$$

Daraus folgt aber sofort

$$\left|\int_\Lambda d\lambda\, P(\lambda)[(a_1 + a_2)b_1 + (a_2 - a_1)b_2]\right| \le 2 \qquad (2)$$

und damit

$$|\langle a_1 b_1\rangle_{\mathrm{LRT}} + \langle a_2 b_1\rangle_{\mathrm{LRT}} + \langle a_2 b_2\rangle_{\mathrm{LRT}} - \langle a_1 b_2\rangle_{\mathrm{LRT}}| \le 2. \qquad (3)$$

Diese Variante der Bellschen Ungleichung wurde erstmals von Clauser, Horne, Shimony und Holt (CHSH) hergeleitet [6]. Sie definiert im Rahmen einer lokalen Theorie mit verborgenen Parametern eine obere Schranke für mögliche Korrelationen der Meßergebnisse der beiden räumlich separierten Beobachter A und B. In der Ungleichung (3) stehen nun experimentell zugängliche Meßgrößen. So läßt sich zum Beispiel der erste Term dadurch ermitteln, daß Beobachter A und Beobachter B den Mittelwert über das Produkt ihrer Messungen mit den Polarisatoren in Stellung $\vec{\alpha}_1$ und $\vec{\beta}_1$ bilden.

Welche Vorhersagen macht im Gegensatz dazu die Quantentheorie für die statistischen Mittelwerte, die die CHSH-Ungleichung bestimmen? Quantenmechanisch wird die Messung der dichotomen Polarisationsvariablen $\hat{a}_i$ und $\hat{b}_i$ durch Spinoperatoren von der Form $\hat{a}_i \equiv \vec{\alpha}_i \cdot \vec{\sigma}^{\mathrm{A}}$ und $\hat{b}_i \equiv \vec{\beta}_i \cdot \vec{\sigma}^{\mathrm{B}}$ charakterisiert. Dabei sind die kartesischen Komponenten von $\vec{\sigma}^{\mathrm{A}}$ und $\vec{\sigma}^{\mathrm{B}}$ Paulische Spinmatrizen für Beobachter A und B. Betrachten wir als Beispiel einen verschränkten quantenmechanischen Zustand (siehe dazu Infokasten 1) von der Form

$$|\psi\rangle = (1/\sqrt{2})(|+1\rangle_{\mathrm{A}}|-1\rangle_{\mathrm{B}} - |-1\rangle_{\mathrm{A}}|+1\rangle_{\mathrm{B}}), \qquad (4)$$

wobei $|\pm 1\rangle_{\mathrm{A}}$ ($|\pm 1\rangle_{\mathrm{B}}$) Eigenzustände des Spinoperators

σ_z^A (σ_z^B) mit Eigenwerten ± 1 bezeichnen und somit wieder die horizontale bzw. vertikale Polarisationsrichtung kodieren. Welche charakteristischen Eigenschaften hat dieser verschränkte Quantenzustand? Zunächst erkennen wir leicht die Eigenschaft

$$\varrho^A = \mathrm{Tr}_B[|\psi\rangle\langle\psi|] = 1/2(|+1\rangle_A\langle+1| + |-1\rangle_A\langle-1|) \qquad (5)$$

und analog für ϱ^B (Tr_B bedeutet dabei Mittelung über die Freiheitsgrade von Teilchen B). Was die Polarisationseigenschaften betrifft, die die Beobachter A und B jeweils für sich alleine feststellen können, ist daher dieser quantenmechanische Zustand völlig unpolarisiert. Die Meßwerte der Operatoren $\hat{a}_i$ und $\hat{b}_i$ sind somit bei vielen Wiederholungen des Experiments völlig zufällig verteilt, d. h. $\langle\hat{a}_i\rangle = \langle\hat{b}_i\rangle = 0$. Wird aber der Polarisationszustand des Photonenpaares von beiden Beobachtern gleichzeitig entlang derselben Polarisationsrichtung gemessen, so ergeben sich perfekte Korrelationen zwischen den Meßergebnissen: Wenn Beobachter A den Wert +1 mißt, stellt Beobachter B den Wert –1 fest und umgekehrt (siehe dazu Kasten 1). Die charakteristischen Polarisationseigenschaften sind also vollständig auf beide Teilchen verteilt, ohne in einem der beiden Teilchen jeweils für sich alleine vorhanden zu sein. Für den quantenmechanischen Mittelwert $\langle\hat{a}_i\hat{b}_j\rangle_{QM}$ ergibt sich in diesem Zustand

$$\langle\hat{a}_i\hat{b}_j\rangle_{QM} = \langle\psi|(\vec{\alpha}_i\cdot\vec{\sigma}^A)(\vec{\beta}_j\cdot\vec{\sigma}^B)|\psi\rangle = -\vec{\alpha}_i\cdot\vec{\beta}_j. \qquad (6)$$

Wählen wir die Polarisationsrichtungen speziell so, daß $(\vec{\alpha}_1, \vec{\beta}_1)$, $(\vec{\beta}_1, \vec{\alpha}_2)$, $(\vec{\alpha}_2, \vec{\beta}_2)$ jeweils den Winkel $\pi/4$ einschließen, erhalten wir

$$|\langle\hat{a}_1\hat{b}_1\rangle_{QM} + \langle\hat{a}_2\hat{b}_1\rangle_{QM} + \langle\hat{a}_2\hat{b}_2\rangle_{QM} - \langle\hat{a}_1\hat{b}_2\rangle_{QM}| = 2\sqrt{2} > 2. \qquad (7)$$

Die durch die Quantenmechanik für den verschränkten Zustand (4) und diese Wahl der Polarisationsrichtungen vorausgesagten Korrelationen der Meßergebnisse von A und B verletzen somit die CHSH-Ungleichung (3) und sind stärker als jede mögliche Korrelation, die im Rahmen einer lokalen Theorie mit verborgenen Parametern möglich ist. Dieses wichtige Ergebnis eröffnet folglich einen Weg, um experimentell zu entscheiden, ob es überhaupt möglich ist, die Quantenmechanik durch eine lokale Theorie zu ersetzen. Das wäre nur dann möglich, wenn die gemessenen Korrelationen Ungleichung (3) erfüllen.

Experimentelle Tests

Erste experimentelle Tests der Bellschen Ungleichungen wurden bereits vor über 20 Jahren durchgeführt [7]. Seitdem gab es zahlreiche Nachfolgeexperimente. Alle diese Experimente bestätigten Gleichung (7) und damit die Vorhersage der Quantenmechanik, daß Korrelationen verschränkter Zustände nicht durch lokale Theorien mit verborgenen Parametern beschreibbar sind. Warum ist es trotzdem von Interesse, experimentelle Tests dazu auch heute noch durchzuführen? Einer der Gründe dafür ist sicherlich die fundamentale Bedeutung dieser Ergebnisse für die Grundlagen der Quantenmechanik und die noch immer nicht vollständig widerlegten Zweifel daran, ob bisher durchgeführte Experimente auch wirklich eine Verletzung der Bellschen Ungleichungen logisch zwingend bestätigen. Derzeit beziehen sich diese Zweifel vor allem auf zwei Schwachpunkte (*loopholes*) in der Argumentationskette. Der eine Schwachpunkt betrifft die Lokalitätsannahme, die der Bellschen Ungleichung zugrunde liegt (*locality* oder *communication loophole*). Der andere Schwachpunkt betrifft die nicht perfekte Effizienz, mit der die korrelierten Ereignisse durch Detektoren registriert werden (*detection loophole*).

Nach der Lokalitätsannahme dürfen die Meßergebnisse der Beobachter A und B nur von den verborgenen Parametern des Photonenpaares und der Wahl der jeweils eigenen Polarisatorrichtung abhängen. Es muß also ausgeschlossen sein, daß Information über die jeweils eingestellten Polarisatorrichtungen über irgendeinen Kanal zwischen den Detektoren ausgetauscht wird. Um diese Lokalitätsannahme zu realisieren, haben bereits Aspect et al. in ihrem berühmten Experiment die Richtungen der Polarisatoren nach der Erzeugung des Photonenpaares durch quasi-periodische Polarisationsmodulatoren geändert [8]. An diesem Experiment wurde allerdings kritisiert, daß diese Polarisationsänderungen nicht zufällig, sondern deterministisch erfolgten [9]. Vor kurzem wurde daher in Innsbruck ein Experiment mit zufällig gewählten Polarisationsrichtungen durchgeführt [2], um die Argumentationslücke bezüglich der Lokalitätsannahme zu schließen. In diesem Experiment wurden die beiden Beobachter 400 m separiert und die Polarisationsrichtungen von Zufallszahlengeneratoren gesteuert. Jedes einzelne Experiment dauerte weniger als 1,3 μs. Eine Signalübertragung zwischen den Beobachtern A und B, selbst mit Lichtgeschwindigkeit, konnte somit ausgeschlossen werden. Die CHSH-Ungleichung (3) wurde in diesem Experiment mit 30 Standardabweichungen verletzt. Unter der Voraussetzung einer idealen Arbeitsweise der Zufallszahlengeneratoren und ideal arbeitender Detektoren wäre mit diesem Experiment in der Tat die Argumentationsschwäche bisheriger Experimente in bezug auf die Lokalitätsannahme beseitigt. Leider lag in diesem Experiment die Detektoreffizienz nur bei etwa 5 %.

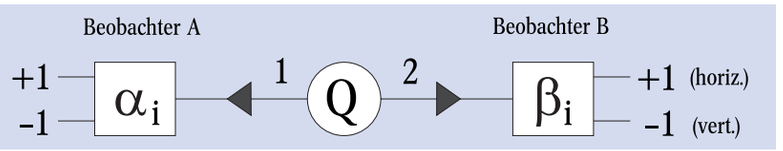


Abb. 1:
Grundexperiment zur Bell–Ungleichung. Die Quelle *Q* emittiert die korrelierten Photonen 1 und 2. Beobachter A und B messen die Polarisation ihres jeweiligen Photons mit einem Polarisator entlang der Richtungen $\vec{\alpha}_i$ und $\vec{\beta}_i$, wobei sie den Polarisator zufällig zwischen zwei Richtungen $\vec{\alpha}_1$ und $\vec{\alpha}_2$ bzw. $\vec{\beta}_1$ und $\vec{\beta}_2$ hin und her schalten. Als Ergebnis finden sie entweder horizontal (–1) oder vertikal (+1) polarisierte Photonen. In der klassischen Physik hat die Messung an Photon 1 keinen Einfluß auf das Ergebnis der Polarisationsmessung an Photon 2. In der Quantenmechanik ist das anders: Vor der Messung ist die Polarisation der einzelnen Photonen unbestimmt. Erst durch den Meßprozeß an einem Photon, z. B. 1, wird dessen Polarisation auf das Koordinatensystem des Polarisators projeziert. Damit steht sofort auch die Polarisation von Photon 2 fest. Diese nichtlokale, „geisterhafte Fernwirkung" wollte Einstein Zeit seines Lebens nicht akzeptieren.

Auch bei allen anderen bisher durchgeführten Experimenten war die Effizienz der verwendeten Detektoren zur Messung der Polarisationseigenschaften des Photonenpaares nicht sehr hoch. Dadurch war die Anzahl der registrierten Ereignisse immer wesentlich kleiner als die Anzahl der tatsächlich präparierten Photonenpaare. Es mußte für die Auswertung der experimentellen Daten angenommen werden, daß die registrierten Daten ein repräsentatives statistisches Ensemble darstellen (*fair sampling assumption*). Vom Standpunkt einer lokalen Theorie mit verborgenen Parametern aus betrachtet, wäre es allerdings möglich, daß diese unbekannten, verborgenen Parameter auch die Wahrscheinlichkeit be-

einflussen, mit der ein Photonenpaar registriert werden kann. Unter dieser Annahme läßt sich sogar ein Modell einer LRT konstruieren, das zu denselben Korrelationen führt wie der verschränkte Zustand (4) und damit die CHSH-Ungleichung ebenfalls maximal verletzt [10]. Unter der Annahme eines solchen Mechanismus könnten also alle bisherigen Experimente zur Verletzung der Bellschen Ungleichungen durch eine lokale Theorie mit verborgenen Parametern erklärt werden. Eine der Schlußfolgerungen dieses theoretischen Modells ist es, daß es aussichtslos ist, mit Detektoreffizienzen von weniger als 75 % die Argumentationslücke des *detection loophole* zu beseitigen [10]. Schon früher wurde gezeigt, daß diese Argumentationslücke mit Detektoreffizienzen besser als $2/(1+\sqrt{2}) \approx 82{,}8\,\%$ geschlossen werden kann [11]. Ob dies auch für kleinere Detektoreffizienzen im Bereich zwischen 75 % und 82,8 % möglich ist, ist noch eine offene Frage. In allen bisher durchgeführten Experimenten waren die Detektoreffizienzen jedenfalls wesentlich kleiner als die untere Schranke von 75 %. Zur Zeit versuchen verschiedene Gruppen, das Nachweisverfahren entsprechend zu verbessern, um diese Argumentationslücke endgültig zu schließen [12, 13]. Eine Idee dabei ist, die bisher verwendeten verschränkten Photonenpaare durch verschränkte Zustände von Atomen zu ersetzen, denn übliche Detektoren für Atome weisen wesentlich bessere Effizienzen auf. Einen ersten Schritt in diese Richtung stellt das Experiment der Gruppe von J. M. Raimond und S. Haroche dar, in dem erstmals zwei Atome nichtlokal miteinander korreliert wurden [13]. Auch die Gruppe von H. Walther am Max-Planck-Institut für Quantenoptik konnte vor kurzem verschränkte Atome nachweisen [14].

Kasten 2 – Grundzüge einer lokalen realistischen Theorie (LRT) verborgener Parameter

Unsere an einer klassischen Welt geschulte Vorstellungskraft tut sich schwer mit dem nichtlokalen Charakter der Quantenmechanik. Deshalb entstanden immer wieder alternative Theorien, die auf Lokalität und Realität physikalischer Größen aufbauen. Albert Einstein glaubte zeitlebens, daß die Quantenmechanik eines Tages durch eine solche LRT abgelöst werden wird. Wir beschreiben im folgenden ihre Struktur. Es ist erstaunlich, wie wenig Annahmen dazu notwendig sind. Wir beziehen uns bei der Beschreibung dieser Annahmen auf das in Abb. 1 dargestellte Experiment. Innerhalb einer LRT wird der physikalische Zustand der beiden von der Quelle Q gelieferten Teilchen (Photonen) vollständig durch den „versteckten" Parametersatz λ beschrieben. Dieses λ kann eine Menge komplexer Zahlen, Funktionen, etc. bezeichnen. Wenn die Quelle Q nicht perfekt arbeitet, wird sie Teilchen mit unterschiedlichem λ liefern. Dies wird in einer LRT durch eine Wahrscheinlichkeitsverteilung $P(\lambda)$ berücksichtigt. Die Summe über den Raum Λ aller möglichen λ-Kombinationen wird normiert:

$$\int_\Lambda d\lambda P(\lambda) = 1.$$

Das sind die wesentlichen Elemente für die Zustandsbeschreibung im Rahmen einer LRT. Bei der Charakterisierung der Observablen kommt der lokale und realistische Charakter einer solchen Theorie zum Vorschein. Zum einen sollen die Werte, die von den einzelnen Beobachtern gemessen werden, nur von ihren jeweils eigenen Meßeinstellungen abhängen (Lokalität). Für unser Beispiel in Abb. 1 bedeutet das, daß die Observable von Beobachter A (B) *nur* von der Polarisatorrichtung $\vec{\alpha}_i$ ($\vec{\beta}_i$) abhängt. Zum anderen sind die Meßwerte, die ein Beobachter abliest, a priori festgelegt, sobald das zugehörige λ bekannt ist (Realität). Für das Polarisationsexperiment von Abb. 1 heißt das folglich: je nach λ und der gewählten Polarisatorrichtung $\vec{\alpha}_i$ nimmt die Observable a von Beobachter A nur zwei Werte an:

$$a(\vec{\alpha}_i, \lambda) = +1 \text{ } oder \text{ } -1.$$

Entsprechendes gilt für die Observable b von Beobachter B. Über viele Experimente gemittelt findet Beobachter A also die Erwartungswerte

$$\langle a_i \rangle_{\mathrm{LRT}} = \int_\Lambda d\lambda P(\lambda) a(\vec{\alpha}_i, \lambda),$$

falls eine LRT die korrekte Beschreibung darstellt. Für die Konstruktion einer Bellschen Ungleichung (siehe Text) sind insbesondere die Korrelationen

$$\langle a_i b_j \rangle_{\mathrm{LRT}} = \int_\Lambda d\lambda P(\lambda) a(\vec{\alpha}_i, \lambda) b(\vec{\beta}_j, \lambda)$$

wichtig. Diese allgemeinen Elemente genügen, um die quantitativen Vorhersagen einer LRT mit denen der Quantenmechanik zu vergleichen.

Drei verschränkte Teilchen: GHZ-Zustände

Die Lokalitätsannahme, die den Bellschen Ungleichungen zugrunde liegt, kann auch zu andersartigen Widersprüchen mit der Quantenmechanik führen. Im Gegensatz zu den Bellschen Ungleichungen beziehen sich diese Widersprüche auf die logische Konsistenz von möglichen Einzelmessungen und nicht auf statistische Ensembleeigenschaften. Besonders deutlich wird dies anhand verschränkter Quantenzustände, die aus mehr als zwei Teilchen oder Untersystemen bestehen. Um dies zu erläutern, betrachten wir als einfaches Beispiel einen verschränkten Dreiphotonenzustand der Form

$$|\psi\rangle_{\mathrm{GHZ}} = (1/\sqrt{2})(|+1\rangle_A|+1\rangle_B|+1\rangle_C - |-1\rangle_A|-1\rangle_B|-1\rangle_C), \quad (8)$$

einen sogenannten GHZ-Zustand. Dieser Zustand ist benannt nach Greenberger, Horne und Zeilinger [15], die erstmals auf die im folgenden beschriebenen Konsequenzen der Lokalitätsannahme hingewiesen haben. Dieser verschränkte Zustand dreier räumlich weit separierter Photonen werde von drei ebenfalls räumlich weit voneinander entfernten Beobachtern auf seine Polarisationseigenschaften hin untersucht.

Betrachten wir zunächst die Konsequenzen einer LRT. Da die drei Beobachter räumlich weit voneinander entfernt sind, können sie unter Voraussetzung der Lokalitätsannahme an jedem der Photonen die Polarisationen messen, ohne sich dabei gegenseitig zu beeinflussen. Die möglichen Polarisationswerte, die jeder der Beobachter dabei messen kann, sind $a_i = \pm 1$, $b_i = \pm 1$, $c_i = \pm 1$ für Beobachter A, B und C entlang der Richtungen $\vec{\alpha}_i$, $\vec{\beta}_i$ und $\vec{\gamma}_i$. Betrachten wir nun vier mögliche Ergebnisse solcher Dreifachkoinzidenzmessungen entlang speziell ausgewählter Polarisationsrichtungen mit den Resultaten (a_x, b_x, c_x), (a_x, b_y, c_y), (a_y, b_x, c_y), (a_y, b_y, c_x). Für das Produkt dieser vier Koinzidenzmessungen ergibt sich im Rahmen einer LRT

$$E_{\mathrm{LRT}} \equiv (a_x b_x c_x)(a_x b_y c_y)(a_y b_x c_y)(a_y b_y c_x) = a_x^2 b_x^2 c_x^2 a_y^2 b_y^2 c_y^2 = 1. \quad (9)$$

Welches Ergebnis liefert die Quantenmechanik für den Zustand aus Gleichung (8)? In der Quantenmechanik werden die Polarisationsvariablen a_i, b_i, c_i durch Spinoperatoren $\hat{a}_i = \vec{\alpha}_i \cdot \vec{\sigma}^{\mathrm{A}}$, $\hat{b}_i = \vec{\beta}_i \cdot \vec{\sigma}^{\mathrm{B}}$, $\hat{c}_i = \vec{\gamma}_i \cdot \vec{\sigma}^{\mathrm{C}}$ charakterisiert. Für den GHZ-Zustand (8) gelten für die Spinoperatoren, die diese vier Koinzidenzmessungen beschreiben, die Relationen

$$\hat{a}_x \hat{b}_x \hat{c}_x |\psi\rangle_{\mathrm{GHZ}} = -|\psi\rangle_{\mathrm{GHZ}}, \quad (10)$$
$$\hat{a}_x \hat{b}_y \hat{c}_y |\psi\rangle_{\mathrm{GHZ}} = \hat{a}_y \hat{b}_x \hat{c}_y |\psi\rangle_{\mathrm{GHZ}} = \hat{a}_y \hat{b}_y \hat{c}_x |\psi\rangle_{\mathrm{GHZ}} = |\psi\rangle_{\mathrm{GHZ}}.$$

Für das Produkt der vier Koinzidenzmessungen ergibt die Vorhersage der Quantenmechanik in diesem Zustand daher

$$E_{\mathrm{QM}} = (-1) \times (+1) \times (+1) \times (+1) \equiv -1$$

im Widerspruch zum entsprechenden klassischen Resultat. Das ist natürlich eine äußerst elegante Argumentation, um Voraussagen einer LRT mit denen der Quantenmechanik zu konfrontieren. Denn während man bei zwei verschränkten Teilchen eine ganze Meßreihe durchführen muß, um die Bellsche Ungleichung (3) zu überprüfen, genügt hier im Prinzip eine

einzige Messung, um die lokalen Theorien verborgener Parameter zu widerlegen.

Im Labor bedarf die Präparation eines reinen GHZ–Zustands großer Kunstfertigkeit. Vor kurzem wurden in ersten Experimenten in Los Alamos und Innsbruck solche verschränkten Dreiteilchenzustände vom GHZ-Typ hergestellt. Während beim Experiment in Los Alamos [16] der verschränkte Zustand aus drei Kernspins in einem Molekül gebildet wurde, demonstrierte das Innsbrucker Experiment [17] die Erzeugung eines räumlich separierten, verschränkten Dreiphotonenzustands aus ursprünglich zwei verschränkten Photonenpaaren. Von der Innsbrucker Gruppe wird darauf aufbauend derzeit auch ein Test der Verletzung lokaler, realistischer Theorien mit GHZ-Zuständen vorbereitet. Diese Experimente sind erste, vielversprechende Schritte zur Erzeugung verschränkter Zustände, mit denen sich auch Aspekte der Nichtlokalität testen lassen, die über die Bellschen Ungleichungen hinausgehen.

Verschränkte Zustände für die Anwendung

Neben der fundamentalen Bedeutung für Tests der Grundlagen der Quantenmechanik ist in letzter Zeit die technologische Bedeutung verschränkter Quantenzustände für die Quanteninformationsverarbeitung immer mehr in den Vordergrund getreten [18]. Verschränkte Quantenzustände lassen sich etwa dazu benutzen, geheime Schlüssel zwischen verschiedenen Parteien annähernd abhörsicher zu übertragen (Quantenkryptographie) [19]; sie können für die Übertragung eines beliebigen Quantenzustands von einem Teilchen auf ein anderes genutzt werden (Quantenteleportation [20]) oder sie können algorithmisch beispielweise zum schnellen Faktorisieren von Zahlen verwendet werden (Quantencomputer) [21]. Für alle diese technologisch interessanten Anwendungen ist es erforderlich, die Frage zu beantworten, über welche makroskopischen Distanzen eine Verschränkung zwischen Quantenzuständen aufrechterhalten werden kann. Sowohl das Innsbrucker Experiment [2] als auch das vor kurzem in Genf durchgeführte Experiment [1] sind hierzu eindrucksvolle Demonstrationen. Im Genfer Experiment werden quantenmechanische Korrelationen, die die Bellschen Ungleichungen verletzen, sogar über makroskopische Distanzen von rund 11 km nachgewiesen. Das dabei verwendete Photonenpaar wurde in Genf erzeugt, über Glasfaserkabel in die Orte Bellevue und Bernex gesendet und in diesen Orten detektiert. Die Verletzung der Ungleichung (3) betrug 16 Standardabweichungen.

Bei allen diesen Entwicklungen der letzten Jahre ist es besonders interessant festzustellen, wie sich die Blickrichtung auf das quantenmechanische Phänomen der Verschränkung geändert hat. Das anfängliche Staunen ist mehr und mehr dem Bestreben gewichen, dieses grundlegende Phänomen technologisch zu nutzen. Die sich daraus entwickelnde Quanteninformationsverarbeitung[1)], die sich in ihren Grundzügen bereits abzuzeichnen beginnt und die bereits erste Erfolge zeigt, könnte eine der Zukunftstechnologien des neuen Jahrhunderts werden.

Literatur

[1] *W. Tittel, J. Brendel, H. Zbinden* und *N. Gisin*, Phys. Rev. Lett. **81**, 3563 (1998)
[2] *G. Weihs, T. Jennewein, Ch. Simon, H. Weinfurter* und *A. Zeilinger*, Phys. Rev. Lett. **81**, 5039 (1998)
[3] *E. Schrödinger*, Die Naturwissenschaften **48**, 807 (1935).
[4] *A. Einstein, B. Podolsky* und *N. Rosen*, Phys. Rev. **47**, 777 (1935).
[5] *J. S. Bell*, Physics **1**, 195 (1964)
[6] *J. F. Clauser, M. A. Horne, A. Shimony* und *R. A. Holt*, Phys. Rev. Lett. **23**, 880 (1969)
[7] *F. Selleri*, Quantum Paradoxes and Physical Reality (Kluwer, Dordrecht, 1989)
[8] *A. Aspect, J. Dalibard* und *G. Roger*, Phys. Rev. Lett. **49**, 1804 (1982)
[9] *A. Zeilinger*, Phys. Lett. A **118**, 1 (1986)
[10] *N. Gisin* und *B. Gisin*, quant-ph/9905018 (1999)
[11] *J. F. Clauser* und *M. A. Horne*, Phys. Rev. D **10**, 526 (1974); *A. Garg* und *N. D. Mermin*, Phys. Rev. D **35**, 3831 (1987)
[12] *E. S. Fry, Th. Walther* und *S. Li*, Phys. Rev. A **52**, 4381 (1995); *Th. Walther* und *E. S. Fry*, Phys. Bl., März 1997, S. 229; *M. Freyberger, P. K. Aravind, M. A. Horne* und *A. Shimony*, Phys. Rev. A **53**, 1232 (1996).
[13] *E. Hagley, X. Maitre, G. Nogues, C. Wunderlich, M. Brune, J. Raimond* und *S. Haroche*, Phys. Rev. Lett. **79**, 1 (1997).
[14] *B.-G. Englert, M. Löffler, O. Benson, B. Varcoe, M. Weidinger* und *H. Walther*, Fortschr. Phys. **46**, 987 (1998)
[15] *D. M. Greenberger, M. A. Horne* und *A. Zeilinger*, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, S. 73, hrsg. von *M. Kafatos* (Kluwer Academics, Dordrecht, 1989); *N. D. Mermin*, Am. J. Phys. **58**, 731 (1990).
[16] *R. Laflamme, E. Knill, W. H. Zurek, P. Catasti* und *S. V. S. Mariappan*, Philos. Trans. R. Soc. London A **356**, 1941 (1998)
[17] *D. Bouwmeester, J. W. Pan, M. Daniell, H. Weinfurter* und *A. Zeilinger*, Phys. Rev. Lett. **82**, 1345 (1999)
[18] Siehe das Sonderheft von Physics World, März 1999, S. 33 ff.
[19] *W. Tittel* et al., Phys. Bl., Juni 1999, S. 25
[20] *C. H. Bennett, G. Brassard, C. Crepeau, R. Josza, A. Peres* und *W. K. Wootters*, Phys. Rev. Lett. **70**, 1895 (1993)
[21] *H.-J. Briegel, J. Cirac* und *P. Zoller*, Phys. Bl., September 1999, S. 37

1) vgl. Schwerpunktprogramm „Quanten-Informationsverarbeitung" der DFG, Koordinator: Prof. G. Leuchs, Erlangen, http://kerr.physik.uni.erlangen.de/giv/