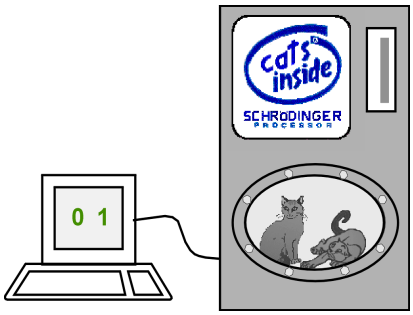
VDI TECHNOLOGIEZENTRUM

Technologiefrüherkennung

Technologieanalyse

Quanten-informations-techniken



VEREIN DEUTSCHER INGENIEURE

GEFÖRDERT DURCH DAS

bmb+f

Bundesministerium für Bildung und Forschung

Quanteninformationstechniken

Technologieanalyse

Herausgeber

VDI-Technologiezentrum Physikalische Technologien

im Auftrag und mit Unterstützung des

Bundesministeriums für Bildung und Forschung (BMBF)

Diese Technologieanalyse entstand im Rahmen des Vorhabens „Identifikation und Bewertung von Ansätzen Zukünftiger Technologien“ (Förderkennzeichen NT 2051C), gefördert durch das Bundesministerium für Bildung und Forschung; Referat 511.

Dank gilt einer Vielzahl von Experten, die wertvolle Beiträge und Anregungen geliefert haben.

Durchführung: VDI-Technologiezentrum
Abteilung: Zukünftige Technologien
Dr. Martin Böltau

Zukünftige Technologien Nr. 30
Düsseldorf, im Juli 1999
ISSN 1436-5928

VDI-Technologiezentrum
Abteilung Zukünftige Technologien
Graf-Recke-Straße 84
40239 Düsseldorf

Das VDI-Technologiezentrum ist als Einrichtung des **Vereins Deutscher Ingenieure (VDI)** im Auftrag und mit Unterstützung des **Bundesministeriums für Bildung und Forschung** tätig.

Vorwort

Im Rahmen der Analyse und Bewertung zukünftiger Technologien des VDI-Technologiezentrums werden Informationen über zukunftsrelevante Technologiefelder zusammengetragen, ergänzt und erarbeitet. Dabei spielen technologisch-wissenschaftliche Gesichtspunkte, wie Realisierungshemmnisse oder -zeiträume eine ebensolche Rolle, wie damit in Zusammenhang stehende Fragen von langfristiger Marktentwicklung oder sozioökonomischen Faktoren. Die einzelnen während dieses Technologiefrüherkennungsprozesses identifizierten und bewerteten Technologiefelder befinden sich in sehr unterschiedlichen Forschungs- und Entwicklungsstadien.

Die vorliegende Technologieanalyse zur Quanteninformationstechnik greift in vielen Aspekten in die weiter entfernte Zukunft. Das besondere Interesse an diesem Technologiefeld ergibt sich aus der Tatsache, daß sich Informations- und Kommunikationstechniken zu den wichtigsten Schlüsseltechnologien unserer Zeit entwickelt haben. Von besonderer Bedeutung für die Gesellschaft der Zukunft, wie auch für die Wettbewerbsfähigkeit einzelner Weltwirtschaftsregionen, sind daher neue, leistungsfähige Werkzeuge mit völlig neuen Ansätzen für die Informationsverarbeitung.

Ein entsprechendes Teilgebiet der Physik, das sich mit diesen Fragestellungen auseinandersetzt, wird im allgemeinen als „Physik verschränkter quantenmechanischer Zustände“ bezeichnet. Sie konnte in ersten Demonstrationsexperimenten bereits zeigen, daß es prinzipiell möglich ist, fundamentale quantenmechanische Effekte für eine deutlich effizientere Art der Informationsverarbeitung nutzbar zu machen.

Da es sich bei diesem neuen Gebiet um einen der schwierigsten Sachverhalte handelt, mit denen sich die moderne Physik derzeit befaßt, bedarf es einer frühzeitigen ersten Thematisierung bezüglich der Inhalte und Perspektiven dieses Gebietes als Basis für weitere Entscheidungen in Forschung und Entwicklung.

Angesprochen sind hierbei Entscheidungsträger der öffentlichen und industriellen Forschungslandschaft, die über keine oder nur oberflächliche Sachkenntnisse auf dem Gebiet der Quanteninformationsverarbeitung verfügen und sich einen ersten Überblick über die verschiedenen Aspekte dieses Zukunftsfeldes verschaffen möchten.

Dr. Dr. Axel Zweck

1 EINFÜHRUNG

Die Informationsverarbeitung kann als die zentrale Technologie des zwanzigsten Jahrhunderts betrachtet werden.

Im 19. Jahrhundert ermöglichte es die industrielle Revolution auf Basis der Dampfmaschine und später des Elektromotors, dem Menschen erstmals, beinahe jede Art der körperlichen Arbeit zu automatisieren und damit eine Produktivität zu erreichen, die diejenige des apparativ unbewehrten Menschen um viele Größenordnungen übersteigen kann. Insbesondere die zweite Hälfte des 20. Jahrhunderts muß als die Ära angesehen werden, in der es möglich wurde, auch geistige Arbeiten an Maschinen zu delegieren.

Gelang es der Rechenmaschine dabei zunächst nur umfangreiche Datenmengen relativ simplen mathematischen Operationen zu unterziehen, so gehört heute auch die Bewältigung kompliziertester Simulationen, die dem Menschen ohne Hilfsmittel niemals zugänglich wären, zu den Aufgaben des Computers.

Das "Human Genom"-Projekt wäre ohne Computer ebensowenig denkbar, wie ein Flug zum Mars oder moderne bildgebende Verfahren in der Medizin.

Obwohl der Mensch insbesondere in denjenigen Bereichen, die im allgemeinen mit Kreativität und Phantasie in Zusammenhang gebracht werden, dem Computer nach wie vor überlegen ist, liegt nach dem derzeitigen Kenntnisstand der Kognitionsforschung kein zwingender Grund dafür vor, daß derartige Fähigkeiten nicht auch von einer Maschine übernommen werden könnten. Schon werden neue Methoden, wie neuronale Netze und Fuzzy-Logic in Computer implementiert und auf diese Weise Grundprinzipien des menschlichen Denkens auf spezielle Problemstellungen der Informationsverarbeitung übertragen.

Die Tatsache, daß mit IBMs "Deep Blue" vor kurzem erstmals ein Computer über einen amtierenden Schachweltmeister triumphierte, unterstreicht die Vielseitigkeit der oftmals als stupide bezeichneten Maschinen.

Um so dringlicher stellt sich die Frage nach den Grenzen der Rechenmaschine. Welche Art von Problemen ist der Computer zu lösen imstande und welche nicht? Was wird überhaupt von zukünftigen Maschinen erwartet bzw. sind die heutigen Geräte nicht vielleicht schon ausreichend für die wichtigsten Aufgaben, die ihnen vom Menschen übertragen werden?

Hierzu ist festzustellen, daß es gerade auch in der Informationstechnologie nicht nur gilt, dem Menschen lästige Routinearbeiten abzunehmen, sondern insbesondere auch eine Datenver-

arbeitung zu ermöglichen, die durch ihren Umfang und vor allem ihre Geschwindigkeit die Realisierung völlig neuer Techniken ermöglicht. Gerade hierin liegt die eigentliche Bedeutung der Informationsverarbeitung. Moderne Kommunikationstechniken wären ohne die Bewältigung des enormen Rechenaufwands, der mit diesen einher geht, nicht realisierbar. Die Vision der "Virtual Reality", d.h. die möglichst perfekte Simulation eines begrenzten Ausschnitts der realen Welt, was derzeit nur in ersten Ansätzen demonstriert wird, erfordert die Beherrschung einer so ungeheuren Datenmenge, daß es schwer fällt an die Möglichkeit einer zufriedenstellenden Verwirklichung dieser Idee zu glauben, geschweige denn, daß dies in naher Zukunft unter Nutzung der konventionellen Computersysteme möglich wäre.
Es läßt sich letztlich konstatieren, daß die derzeitigen Grenzen für die potentiellen Aufgaben eines Computers nur aufgrund der Endlichkeit der menschlichen Phantasie überhaupt festgelegt werden können.
Generell nimmt die Informationsverarbeitung eine Schlüsselstellung bei der Frage nach der Relevanz und der Realisierbarkeit zukünftiger Technologien ein. Medizin, Pharmazie, Verkehrs-, Umwelt- und Sicherheitstechnik, in keinem dieser Bereiche ist heute ein Fortschritt denkbar, an dem die Informationsverarbeitung nicht mehr oder minder Anteil hätte.
Wenn also der Weg zu mehr sozialer Gerechtigkeit und erhöhter Lebensqualität über die Verfügbarmachung neuer Technologien führt, so ist er auf das Engste mit der Informationsverarbeitung verknüpft.

Welche Aufgabe kommt nun der Physik auf dem Gebiet der Informationsverarbeitung zu ?
Bekanntermaßen setzt sich der Computer aus Hard- und Software zusammen. Für die Hardware gilt hierbei, daß sie in der Regel an den Grenzen des gerade technisch machbaren angesiedelt ist. Dies bedeutet, daß diejenige Hardware, die kommerziell erhältlich ist, der bestmöglichen, die mit dem zu diesem Zeitpunkt vorhandenen technischen Wissen realisiert werden kann, sehr nahe liegt. Technisches Wissen fußt jedoch auf naturwissenschaftlichen Erkenntnissen und so ist es wenig verwunderlich, daß Innovationen in Richtung einer qualitativ neuen Technologie meist auf wissenschaftliche Entdeckungen zurückgeführt werden können. Der Transistoreffekt ist hierfür ein geradezu dramatisches Beispiel.
Aktuelle Vorschläge der Naturwissenschaften für Innovationen in der Computertechnik kommen aus der Physik und der Biologie:
Bereits seit längerer Zeit wird die Idee des **optischen Computers** verfolgt. Bedingt durch die hohe Ausbreitungsgeschwindigkeit von Licht, verglichen mit der elektronischen Datenüber-

tragung in Halbleitern, ließe sich bei Verwendung optischer Komponenten die Rechengeschwindigkeit eines Computers entscheidend steigern.
Derzeit ist jedoch die Tendenz zu beobachten, daß nicht in erster Linie die zentrale Recheneinheit durch einen optischen Prozessor ersetzt werden soll, diese Möglichkeit liegt tatsächlich noch in weiter Ferne, sondern daß zunächst die Peripherie, wie z.B. rechnerinterne Kommunikation und Datenspeicherung, sukzessive auf optische Komponenten umgestellt werden wird.
Auf biologischen Prinzipien basiert der **DNA-Computer**. Die Funktionsweise dieses Entwurfs konnte bereits an einfachen Systemen mit einem vergleichsweise geringen experimentellen Aufwand eindrucksvoll demonstriert werden. Darüber hinaus sind auch Datenspeicher auf biologischer Basis derzeit Gegenstand der Forschung.
Ein völlig neues Paradigma bei der Verarbeitung von Information wird mit der Idee des **Quantencomputers** eingeführt. Dieses Prinzip zielt vor allem auf den Ersatz der CPU (Central Processing Unit) für bestimmte, klassisch nicht durchführbare Berechnungen ab. Die technische Realisierung eines Quantenlogik - Prozessors erschließt Problembereiche, die allen denkbaren, auf klassischer Physik beruhenden Funktionsprinzipien (also insbesondere auch biologischen Rechnern) aus fundamentalen Gründen verschlossen bleiben müssen.

In der vorliegenden Technologieanalyse wird der Entwicklungsstand des Quantencomputers und der auf den selben Prinzipien beruhenden Quantenkommunikation dargelegt. Es stehen dabei nicht wissenschaftliche Detailfragen im Vordergrund, sondern es soll ein erster Einblick in das Themengebiet der ***„Physik verschränkter quantenmechanischer Zustände“*** und ihre potentiellen Anwendungsmöglichkeiten gegeben werden. Dies soll als Ausgangsbasis für vertiefte Studien in den jeweils spezifischeren Teilgebieten dienen.
Für detailliertere Ausführungen sei auf die Fachliteraturzitate in den jeweiligen Kapiteln verwiesen.
Obschon die Quanteninformationsverarbeitung ein inderdisziplinäres Arbeitsfeld im Grenzgebiet zwischen Physik und Informatik definiert, soll hier nur ein Überblick über die grundlegenden physikalischen Problemstellungen gegeben werden. Bezüglich der Beiträge, die von Seiten der Informatik beigesteuert werden, wie z.B. Quantenalgorithmen, fehlerkorrigierende Codes oder Quantensimulation sei auf eine für 1999 geplante Machbarkeitsstudie im Zuständigkeitsbereich des BMBF-Referats 524 Informatiksysteme verwiesen.

2 ZIELSETZUNG

Das Gebiet der Quanteninformationstechniken ist in den letzten Jahren zunehmend in das Blickfeld der physikalischen Forschung gerückt. Während zu Beginn vor allem die Entschlüsselung fundamentaler Mechanismen der Natur im Vordergrund stand, rückte in jüngerer Zeit die mögliche Anwendung der gefundenen Erkenntnisse immer weiter in den Mittelpunkt des Interesses.

Bedauerlicherweise gehören die physikalischen Grundprinzipien der Quanteninformationsverarbeitung zu den unkonventionellsten und anspruchsvollsten Sachverhalten, mit denen sich die Physik derzeit beschäftigt. Es verwundert daher nicht, daß die potentielle Zielgruppe außerhalb des unmittelbar involvierten Expertenkreises wenn überhaupt allenfalls lückenhaft über dieses interessante und zukunftsweisende Gebiet informiert ist.

Die vorliegende Technologieanalyse richtet sich daher im wesentlichen an drei Zielgruppen:

- Entscheidungsträger im Bundesministerium für Bildung und Forschung (BMBF) und in anderen Förderungsinstitutionen, um diesen einen ersten Einblick in nationale und internationale Aktivitäten zu geben, sowie Informationen zu Anwendungspotential, Entwicklungshemmnissen und Stand der Forschung zur Verfügung zu stellen.
- Wissenschaftler aus angrenzenden Themengebieten, die einen Überblick über das Gebiet und vor allem eine Zusammenstellung der wichtigsten Literatur erhalten, aus der die Detailinformationen zu jeweils relevanten Teilgebieten zu beziehen sind.
- Potentielle industrielle Anwender sollen an das Themengebiet herangeführt, sowie über internationale (auch industrielle) Aktivitäten in diesem Arbeitsfeld aufgeklärt werden. Ebenso finden sich die wichtigsten Ansprechpartner im Anhang der Analyse, um eine gezielte Kontaktaufnahme zu ermöglichen.

Diese Technologieanalyse kann nicht als Lieferant wissenschaftlicher Detailinformationen genutzt werden. Hierzu sei ausdrücklich auf die zitierte Fachliteratur verwiesen.

Die Absicht ist es, den aufgeführten Zielgruppen eine Grundlage zum ersten qualitativen Verständnis der Grundprinzipien dieses Fachgebiets zu geben, die dann als Basis für eine vorläufige Entscheidungsfindung im Hinblick auf ein mögliches Engagement, und sei es nur eine intensivierte Beobachtung des Themenfeldes, dienen kann.

3 DEFINITION DER QUANTENINFORMATIONSTECHNIKEN

Unter diesem Oberbegriff sollen diejenigen physikalischen Techniken zusammengefaßt werden, die auf der Verwendung verschränkter quantenmechanischer Zustände beruhen. Unter Verschränkung ist dabei die Korrelation zwischen mehreren Teilchen derart zu verstehen, daß eine Wechselwirkung mit einem der Teilchen immer auch zu einer Änderung des Zustands der anderen führt. Verschränkte Teilchen können also nicht isoliert voneinander, sondern müssen als ein einziges quantenmechanisches System betrachtet werden.
Es ist hierbei völlig sinnlos sich einen solchen verschränkten Zustand mit den Mitteln des menschlichen Vorstellungsvermögens plausibel machen zu wollen, da in unserem makroskopischen Erfahrungsraum keinerlei Phänomen existiert, das hierzu als Referenz dienen könnte. Nichtsdestotrotz sind diese Gesetzmäßigkeiten existent und mit den Mitteln der Quantentheorie beschreibbar und seit einiger Zeit auch experimentell präparierbar. Genaueres hierzu findet sich in den nachfolgenden Kapiteln.

Der ***Quantencomputer*** nutzt die Verschränktheit seiner elementaren Einzelkomponenten aus um in hochgradig paralleler Art und Weise (siehe Kapitel **5.3**) Information zu verarbeiten.
Die ***Quantenkryptographie*** beruht auf dem Prinzip, daß eine Messung an einem quantenmechanischen System bei Unkenntnis des Präparationszustandes zu dessen Zerstörung führt, allerdings muß hierbei nicht notwendig ein verschränkter Zustand vorliegen.
Bei der ***Quantenteleportation*** wird die Verschränktheit zur Übertragung eines quantenmechanischen Zustandes auf ein möglicherweise weit entferntes Teilchen herangezogen.
Die ***Quantendatenkompression*** erlaubt die physikalische Komprimierung von Information über die klassische theoretische Obergrenze hinaus.
Im weiteren Sinne soll hier auch die ***nicht quantenzerstörende Messung (quantum non demolition, QND)*** zu diesem Themenbereich gezählt werden. Ziel dieser Technik ist es, eine Messung bei minimaler, von der Quantenmechanik bestimmter Wechselwirkung durchzuführen. Insbesondere ermöglicht dies, photonische Zustände vermessen zu können, ohne dabei die betreffenden Photonen in einem Detektor absorbieren zu müssen.
Der ***Quantenzufallsgenerator*** ist in der Lage durch Nutzung physikalischer Zufallsereignisse ideale Zufallszahlen zu produzieren, was mit klassischen Methoden nur näherungsweise möglich ist. Der Quantenzufallsgenerator ist als Spin-Off der Forschungsaktivitäten zur Quantenkommunikation anzusehen.

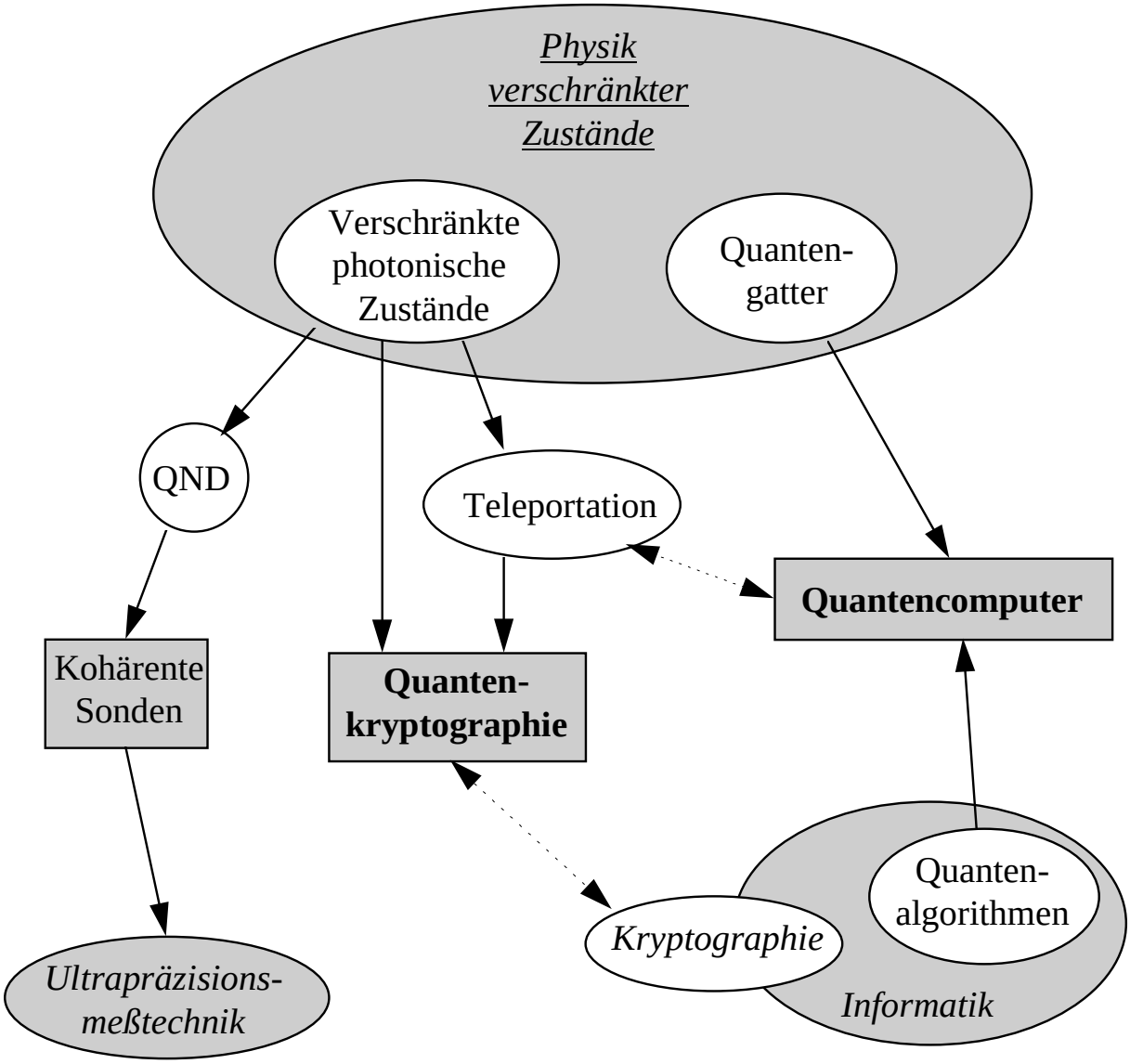


Abb. 1: Querverbindungen zwischen unterschiedlichen Teilbereichen des neu entstandenen Gebiets der Quanteninformationsverarbeitung. Insbesondere der Quantencomputer stellt eine Herausforderung für die interdisziplinäre Zusammenarbeit zwischen Physik und Informatik dar.
Genaueres zu den jeweiligen Zusammenhängen findet sich in den folgenden Kapiteln.

4 ZEITLICHE ENTWICKLUNG DES GEBIETS

Die Ursprünge der Physik der Quanteninformation gehen zurück bis zu den Anfängen der Quantenmechanik selbst.

Früh wurde erkannt, daß die Quantenmechanik Aspekte beinhaltet, die mit den gewohnten Vorstellungen über die Beschaffenheit der Natur nicht in Einklang zu bringen waren und sind. Der Welle-Teilchen-Dualismus, ein Phänomen, das an nahezu jeder experimentellen Anordnung, die auf quantenmechanischen Prinzipien beruht, illustrierbar ist, stellt ein zentrales Charakteristikum der Quantenmechanik dar.

Obschon der Welle-Teilchen-Dualismus bereits seit langem als ein wesentliches Merkmal der Quantenmechanik akzeptiert ist, steht eine zufriedenstellende Interpretation, die es uns auf einfache Weise gestattet diese Gesetzmäßigkeiten in gewohnter Weise anschaulich zu verstehen, noch aus und ist möglicherweise sogar grundsätzlich nicht formulierbar.

Die korpuskulare Natur quantenmechanischer Objekte teilt sich einem Beobachter im Zuge des Meßprozesses mit, während die Welleneigenschaft vor allem die Dynamik eines ungestörten Systems sehr gut wiedergibt. Die Messung ist dabei immer mit einem Verlust der Welleneigenschaft in Bezug auf die untersuchte Eigenschaft des Objekts verbunden.

Dieser Sachverhalt wurde unter dem Begriff "Kollaps der Wellenfunktion" zu einem zentralen Punkt in der bis heute andauernden Diskussion um die Art und Weise, wie die Quantenmechanik zu interpretieren sei.

Den vielleicht berühmtesten Beitrag zu dieser Kontroverse veröffentlichten 1935 Albert Einstein, Boris Podolski und Nathan Rosen [Ein35]. In ihrer Publikation formulierten sie ein subtiles Gedankenexperiment (EPR-Paradoxon, Kap. **5.3.4**), welches, bei Berücksichtigung zentraler Inhalte der speziellen Relativitätstheorie, beweisen sollte, daß die Quantenmechanik eine unvollständige Theorie und nur als Teilaspekt einer noch ausstehenden, umfassenderen Theorie anzusehen sei. Diese neue Theorie könnte dann wieder in Einklang mit den klassischen Vorstellungen bezüglich der Beschaffenheit der physikalischen Realität gebracht werden.

Lange war nicht klar, ob sich zwischen der bestehenden und einer Quantenmechanik als Folge einer deterministischen, mikroskopischen Theorie überhaupt Unterschiede finden lassen, bis John Bell zeigen konnte, daß bei einer bestimmten Art von Korrelationsexperimenten, die

noch durchzuführen wären, Abweichungen auftreten müßten, je nachdem, welche der beiden Theorien mit der Realität im Einklang steht [Bel64].
Im Anschluß an diese Erkenntnis begann die experimentelle Überprüfung der Problematik [Fre72, Cla76]. Zu Anfang waren die Resultate keineswegs eindeutig und ein besonders wichtiger Kritikpunkt, die Separation quantenmechanisch korrelierter Teilchen derart, daß eine Kommunikation über gewöhnliche, lichtschnelle Wechselwirkungen im Experiment ausgeschlossen werden kann, konnte in den ersten Experimenten nicht berücksichtigt werden.
Erst zu Beginn der 80er Jahre gelang Alain Aspect eine Reihe von Experimenten, bei denen eine mit der speziellen Relativitätstheorie vereinbare klassische Kommunikation zwischen den korrelierten Photonen erstmals gezielt unterbunden wurde [Asp81, Asp82]. Da auch gegen diese Versuche noch Einwände geltend gemacht wurden, werden bis heute immer noch Experimente durchgeführt, die eine möglichst umfassende Absicherung der Quantenmechanik liefern sollen [Wei98].

Unabhängig davon beschrieb Wisner bereits 1970 ein Kryptographieverfahren, das anders als alle bisherigen nicht auf mathematischen Transformationen sondern auf fundamentalen physikalischen Prinzipien beruht [Wie70]. Eine erste experimentelle Umsetzung dieser Idee wurde 1989 von Bennett und Brassard veröffentlicht, [Ben89] und seitdem konnten zahlreiche bemerkenswerte Fortschritte auf diesem Gebiet realisiert werden.

Die quantenmechanische Beschreibung eines gewöhnlichen Computers (Turing-Maschine, nach dem Mathematiker Alan Turing) wurde 1980 von Paul Benihoff gegeben [Ben80], der dabei auf frühere Überlegungen von Bennett zurückgriff. Benihoffs Maschine war noch kein wirklicher Quantencomputer, da in seinem Modell nach jedem Rechenschritt der quantenmechanische Überlagerungsszustand in einen klassischen Zustand überführt wurde und der eigentliche Vorteil daher nicht zum Tragen kommen konnte.
Die grundsätzliche Überlegenheit des quantenmechanischen Systems erkannte als erster Richard Feynman, der 1982 zeigen konnte, daß eine klassische Turing-Maschine bei der Simulation bestimmter quantenmechanischer Abläufe eine exponentielle Verlangsamung erfahren müsse, während dies bei einem "universellen Quantensimulator", der selbst auf quantenmechanischen Prozessen fußt, nicht der Fall wäre [Fey82].
Die erste Quanten-Turing-Maschine wurde im Anschluß daran von Deutsch [Deu85] beschrieben. Sein Konzept erfaßte nun auch die Möglichkeit sogenannte quantenmechanische

Superpositionen zur Berechnung heranzuziehen und damit unterschiedliche Zustände simultan zu bearbeiten. Der Begriff des "Quantenparallelismus" wurde für diese erstaunliche Eigenschaft der Quanten-Turing-Maschine eingeführt.

Mit der Erkenntnis der qualitativen Andersartigkeit des Quantencomputers stellte sich nun auch die Frage, inwieweit eine solche Maschine auch Vorteile bei der Lösung alltäglicher Problemstellungen bietet, die auf einem klassischen Computer als nicht bearbeitbar gelten.

Ein solcher Quantenalgorithmus wurde 1994 von Peter Shor vorgestellt [Sho94]. Es konnte gezeigt werden, daß die Faktorisierung in Primzahlen, auf der eine Vielzahl heutiger Kryptographieverfahren beruht, auf einem Quantencomputer in sehr viel kürzerer Zeit möglich ist, als auf einem klassischen Rechner.

Dieser Erfolg hat dem gesamten Gebiet des "Quantum Computing" beträchtlichen Auftrieb verliehen, da seither insbesondere auch die Hoffnung besteht, daß für andere, derzeit nicht bearbeitbare, aber für die Anwendung sehr wichtige Probleme (z. B.: Travelling Salesman Problem) ein effizienter Quantenalgorithmus gefunden werden kann.

Die technische Realisierung des Quantencomputers steckt allerdings noch in den Anfängen. Bislang konnten nur einfachste Modellsysteme präpariert werden, und ein Verfahren, das mit einfachen Mitteln den Bau eines Quantencomputers erlaubt, der heutigen klassischen Rechnern überlegen sein könnte, ist zur Zeit nicht abzusehen.

Die Nutzung der Kernspinresonanz zur Demonstration einfacher quantenlogischer Operationen hat hier keinen Durchbruch erzielt, jedoch gezeigt, daß innerhalb kürzester Zeit in nicht vorhersehbarer Weise völlig neue Konzepte zu einem bemerkenswerten Fortschritt auf diesem Gebiet führen können.

Eine beträchtliche Anzahl neuer Ideen wurde bereits erdacht, und man darf gespannt sein, ob sich hinter einem dieser Vorschläge der Weg zum Bau eines kommerziell erhältlichen Quantenprozessors verbirgt.

5 DER QUANTENCOMPUTER

5.1 Limits klassischer Computer

Unter den zahlreichen Aufgaben, die man mit Hilfe von klassischen Computern lösen möchte, lassen sich unterschiedliche Problemklassen definieren (Abb. 2). Diese Klassen geben einen qualitativen Schwierigkeitsgrad wieder, der die Zeitdauer, die zur Bearbeitung eines Problems notwendig ist, in Relation zum Umfang des Problems setzt.

Möchte man beispielsweise eine N-stellige Zahl in ihre größten Primfaktoren zerlegen, so steigt die Rechenzeit nach einem Exponentialgesetz mit N an.

Von bearbeitbaren Problemen spricht man, wenn die Rechenzeit in Abhängigkeit von der Problemgröße nach einem Polynomialgesetz ansteigt. Dies bezeichnet die einfachste Klasse der sogenannten polynomialen Probleme. Die nächste Komplexitätsstufe sind dann die nicht-deterministisch polynomialen Probleme (NP), d.h. solche, für die zwar kein polynomialer Algorithmus gefunden werden kann, bei denen aber die Überprüfung einer potentiellen Lösung in einer Zeit möglich ist, die nur nach einem Polynomialgesetz mit der Komplexität ansteigt. Diese Art von Problemen besitzt eine beachtliche praktische und damit auch ökonomische Bedeutung. Ein bekanntes Beispiel ist das sogenannte "Travelling Salesman"-Problem. Hierbei gilt es, den kürzesten Weg durch eine gegebene Anzahl von Städten, die sich in unterschiedlichen Entfernungen voneinander befinden, zu ermitteln. Hierfür gibt es keinen deterministisch polynomialen Algorithmus, und mit Näherungsverfahren kann man sich bei praxisrelevanten Problemen dieser Art derzeit nur auf ca. 95 % der exakten Lösung annähern.

Gerade die Bewältigung dieser Aufgabenstellungen stellt eine wesentliche Motivation für die Suche nach effizienteren Algorithmen einerseits, aber auch nach neuen Prinzipien der Informationsverarbeitung andererseits dar. Insbesondere die massive Parallelisierung der Berechnungen erscheint für diese Problemklasse als ein sehr vielversprechender Weg hin zu besseren Lösungsverfahren.

Die Klasse der NP-Probleme läßt sich nochmals unterteilen in diejenigen, auf die sich alle anderen NP-Probleme zurückführen lassen, diese werden als NP-vollständig bezeichnet, und solche, bei denen dies nicht möglich ist. Das bedeutet, daß das Finden eines Algorithmus, der

ein vollständiges NP-Problem effizient löst, die gesamte Klasse dieser Probleme bearbeitbar machen würde. Das Travelling-Salesman-Problem ist in solcher Weise NP-vollständig.
Noch schwerer zu lösen sind die exponentiell wachsenden Aufgaben, wie die angesprochene Faktorisierung in Primzahlen.
Schließlich bleiben noch die Probleme, bei denen ein klassischer Algorithmus niemals zu einem Ende kommt, die Lösung also auch bei beliebig langem Rechnen nicht erhalten wird.

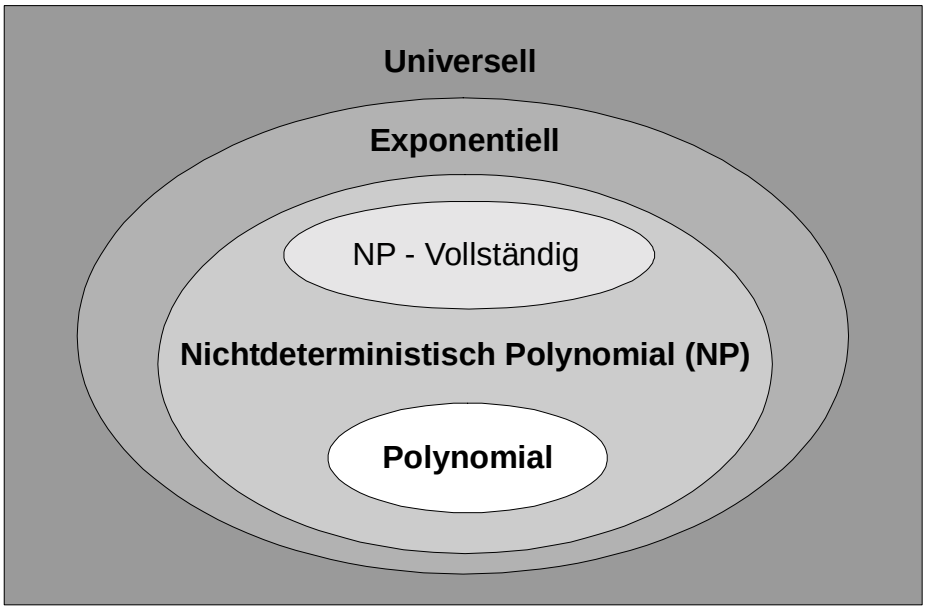


Abb. 2: Einteilung von Algorithmen in unterschiedliche Problemklassen. Klassische Computer können polynomiale Probleme exakt und NP-Probleme näherungsweise lösen. Ein Quantencomputer würde die deterministische Bearbeitung bestimmter exponentieller und NP-Probleme erlauben.

Zu dieser Art der Einteilung der Probleme ist zu sagen, daß sie in vielerlei Hinsicht vorläufigen Charakter hat. So liegt es beispielsweise für etliche NP- wie auch exponentielle Probleme durchaus im Bereich des möglichen, daß in Zukunft doch ein polynomialer Algorithmus gefunden werden wird. Dies gilt zum Beispiel auch für das Kryptographie-problem der Faktorisierung in Primzahlen. Bei weitem nicht für alle Problemstellungen liegt zu den gefundenen Algorithmen auch ein Beweis dafür vor, daß es sich um die jeweils schnellstmöglichen handelt.
Kann ein solcher Beweis allerdings erbracht werden, so ist damit in eindeutiger Weise eine Grenze bezüglich der prinzipiellen Lösbarkeit des entsprechenden Problems festgelegt. Für

eine konventionelle Turing-Maschine besteht dann nur noch die Möglichkeit durch erhebliche technische Anstrengungen eine Verkürzung der "Hardware"-Rechenzeit zu erreichen. Es fällt leicht, einzusehen, daß eine solche "brute force"-Vorgehensweise bei exponentiellen Problemen sehr schnell an ihre Grenzen stößt. Berechnet man beispielsweise ein "Travelling Salesman"-Problem mit 50 Städten und erhält nach 5 sec die Lösung, so dauert die Berechnung bei 100 Städten 100.000 Jahre, da die Rechenzeit mit N! (= $1 \cdot 2 \cdot 3 \cdot \ldots \cdot N$) ansteigt. Bei Hinzufügen nur einer weiteren Stadt würde sich der Rechenaufwand mehr als verhundertfachen. Der entsprechende Aufwand wäre gemessen am Ergebnis für ein solches Problem unbezahlbar.

Gerade das "Travelling Salesman"-Problem und verwandte Aufgabenstellungen haben eine beträchtliche wirtschaftliche Bedeutung. Beispielsweise handelt es sich bei der Forderung nach einer optimalen Belegung von Leiterplatten, integrierten Schaltungen und auch Mikroprozessoren um genau so ein Problem, das sich aus den angeführten Gründen ab einer bestimmten Komplexität heutzutage nicht exakt lösen läßt.

Ob und inwieweit der Quantencomputer für die Klasse der NP-Probleme eine wesentliche Verbesserung bringt, ist derzeit noch nicht entscheidbar. Aufgrund seiner massiven Parallelität ist er jedoch auf der Hardwareseite der aussichtsreichste Kandidat, was die mögliche zukünftige Bearbeitbarkeit heute unlösbarer Probleme betrifft.

Fazit: Die exakte Bearbeitung mathematischer Probleme auf realen Rechenmaschinen, die wohldefinierten (physikalischen) Funktionsprinzipien unterliegen, ist bezüglich der Geschwindigkeit, mit der der zugehörige Algorithmus maximal durchlaufen werden kann, limitiert.
Der Grad der Beschränkung wird dabei letztlich auch von den physikalischen Gesetzmäßigkeiten vorgegeben, auf denen die Funktionsweise des Rechners basiert.

5.2 Alternative Computerkonzepte

Neben dem Quantencomputer werden noch andere Konzepte für zukünftige informationsverarbeitende Systeme diskutiert, die den klassischen von Neumann - Computer ersetzen sollen. Die Initiativen kommen hierbei aus unterschiedlichsten Disziplinen, von der Infomatik über die Physik bis hin zur Biologie. Der DNA-Computer soll als Vertreter eines besonders unkonventionellen Alternativkonzeptes im folgenden kurz dargestellt werden.

5.2.1 DNA-Computer

1994 veröffentlichte Leonard Adleman ein Experiment bei dem er mit Hilfe von DNA-Molekülen ein dem "Travelling Salesman" (TSP) ähnliches Problem in effizienter Weise zu lösen versuchte [Adl94].
Es handelt sich dabei um das Problem des hamiltonschen Pfads. Hierbei hat man eine bestimmte Anzahl von Städten, die über eine begrenzte, fest vorgegebene Anzahl von Verbindungen miteinander verknüpft sind. Eine einzelne Verbindung repräsentiert dabei jeweils nur eine Richtung.
Die Aufgabe besteht nun darin festzustellen, ob für eine bestimmte Anzahl von Städten und Verbindungen zwischen diesen ein Pfad existiert, der bei fest vorgegebener Start- und Zielstadt alle Städte miteinander verbindet, ohne eine Stadt zweimal zu durchlaufen.
Bei diesem Problembeispiel handelt es sich wie beim TSP um eine NP-Problemstellung, d.h auf klassischen Computern wächst der Rechenaufwand mit der Anzahl der gegebenen Städte und Verbindungen exponentiell an.

Der Grundgedanke beim DNA-Computer besteht darin, Rechenoperationen auf einer sehr kleinen (Nano-)Skala durchzuführen, so daß man durch gleichzeitige parallele Benutzung mehrerer Rechenelemente eine ungeheure Anzahl von Berechnungen in kurzer Zeit durchführen kann. Als Rechenelement fungiert dabei eine bestimmte Anzahl von DNA-Einzelmolekülsträngen. Diese Stränge bestehen aus einer zufälligen Abfolge von insgesamt vier verschiedenen chemischen Verbindungen (den Basen: Thymin, Adenin, Guanin und Cytosin). Die Einzelstränge können sich zu Doppelsträngen verbinden, vorausgesetzt die Basenabfolgen

in den Einzelsträngen korrespondieren in der Art und Weise, daß immer ein Guanin- einem Cytosin-Basenabschnitt gegenüberliegt bzw. Tymin und Adenin ein Basenpaar bilden. Es läßt sich also durch die Abfolge der Basen festlegen, welche Einzelstränge sich zu einem Doppelstrang verbinden können und welche nicht. Derartige Vorgänge laufen auch in biologischen Systemen, beispielsweise bei der Zellteilung ab.

Für eine Rechnung würde man nun gezielt solche Einzelstränge synthetisieren, die sich nur auf eine dem Algorithmus des Problems entsprechende Weise zu einem Doppelstrang verbinden können. Die dabei entstehenden Doppelstränge werden dann anhand weiterer physikalischer Eigenschaften, die mit konkreten abstrakten Inhalten des zu bearbeitenden Problems in Zusammenhang stehen, mittels naßchemischer Verfahren selektiert. Die zuletzt übrigbleibenden DNA-Doppelstränge enthalten die gesuchte Lösung der gestellten Aufgabe. Diese Lösung bestimmt sich aus der Art und Reihenfolge der Einzelstränge, aus denen sich die „End“-Doppelstränge zusammensetzen.

Für das Problem des hamiltonschen Pfads bedeutet dies, daß gleichzeitig sehr viele mögliche Lösungen daraufhin überprüft wurden, ob alle Bedingungen für die potentielle Lösung erfüllt werden.

Im zu Beginn angesprochenen Experiment von Adleman wurde für jede von insgesamt sieben Städten ein zwanzig Basen langer DNA-Einzelstrang präpariert (Abb. 3). Ebenso wurde jede vorgegebene Verbindung zwischen zwei Städten in Form eines eigenen Stranges implementiert und zwar derart, daß die ersten 10 Basen mit denen des Ausgangspunktes (Startstadt) und die Basen 11 bis 20 mit der zweiten Hälfte des zur Zielstadt gehörenden Stranges übereinstimmen.

Alle möglichen Stränge, die Verbindungen zwischen zwei Städten entsprechen, werden dann vermischt. Zu diesem Gemenge werden die "Watson-Crick"-komplementären Ribonukleinsäurestränge die den Städten zugeordnet sind, hinzugegeben.

Unter Watson-Crick komplementär versteht man dabei einen Strang, der so aufgebaut ist, daß beim direkten Vergleich des Original- und des Komplementärstrangs jeweils eine Guanin- einer Cytosin- und eine Thymin- einer Adenin-Base gegenübersteht. Nur dann können sich die beiden Stränge zu einem einzigen Doppelstrang verbinden.

Hat man nun für die Städte die komplementären und für die Stadtverbindungen die Originalstränge vorliegen, so können jeweils ein Verbindungsstrang der eine bestimmte Stadt zum Ausgangspunkt hat und ein solcher der dieselbe Stadt als Ziel hat, vom zugehörigen komplementären "Stadtstrang" zu einer Kette verbunden werden. In einer Mischung aus den

Funktionsprinzip des DNA-Computers

1. Präparation der "Stadt - Stränge" und der Verbindungen:

Bsp.:	Stadt 2:	TATCGGATCG-GTATATCCGA
	Watson-Crick-Trf.:	ATAGCCTAGC-CATATAGGCT
	Stadt 3:	GCTATTCGAG-CTTAAAGCTA
	Watson-Crick-Trf.:	CGATAAGCTC-GAATTTCGAT
	Verbindung 2 nach 3:	GTATATCCGA-GCTATTCGAG
	Verbindung 3 nach 2:	CTTAAAGCTA-TATCGGATCG

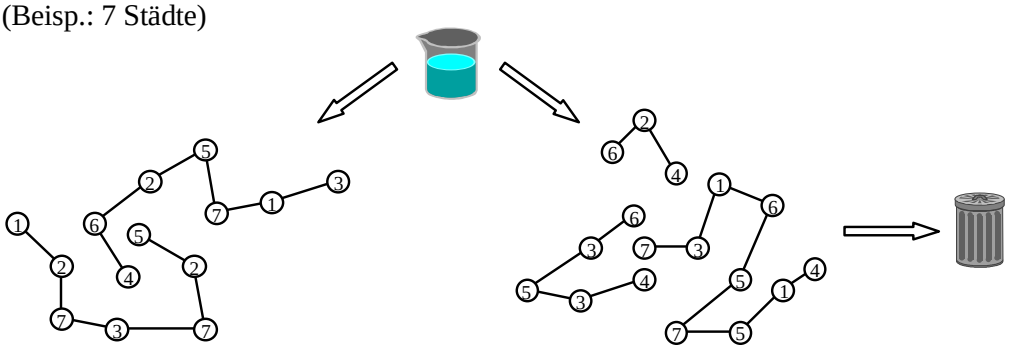
---

2. Mischung der Ribonukleinsäuren => Entstehung von Ketten
Bsp.: Stadt 2 nach Stadt 3

GTATATCCGA-GCTATTCGAG
ATAGCCTAGC-CATATAGGCT CGATAAGCTC-GAATTTCGAT

---

3. Abtrennung der Ketten, die nicht durch sieben Städte gehen:
(Beisp.: 7 Städte)



---

4. Abtrennung der Ketten, die nicht alle Städte mindestens einmal enthalten:

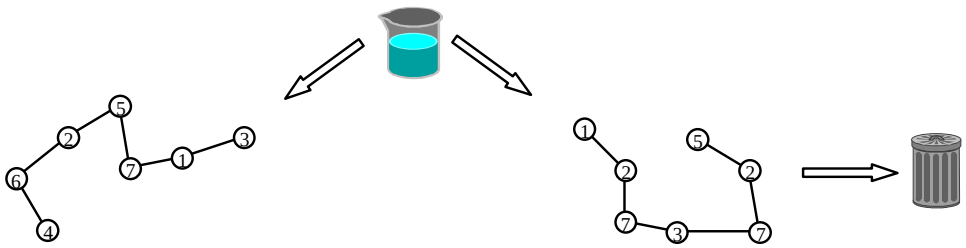


Abb. 3: Funktionsprinzip eines DNA-Rechners entsprechend dem Adlemanschen Experiment.

verschiedenen Ribonukleinsäuren bilden sich also auf zufällige Weise Ketten aus, die die Städte in beliebiger Weise miteinander verbinden.
Durch eine Kettenreaktion (PCR: polymerase chain reaction) kann nun erreicht werden, daß nur solche Ketten vervielfacht werden, die mit dem zum Ausgangspunkt gehörenden Stadtstrang beginnen und mit einer Ribonukleinsäure enden, die den gewünschten Zielort darstellt.
In einem weiteren Arbeitsgang können nun alle diejenigen Ketten aussortiert werden, die mehr Stadtstränge enthalten, als tatsächlich Städte vorhanden sind, die also mindestens eine Stadt zweimal enthalten.
Danach gilt es noch sicherzustellen, daß jede Stadt auch mindestens einmal vorkommt. Die verbliebenen Ketten repräsentieren dann die verschiedenen Möglichkeiten mit denen man die Städte in geforderter Weise miteinander verbinden kann.
Die Berechnung erfolgt also dadurch, daß in massiv paralleler Weise eine große Zahl von verschiedenen Lösungen erzeugt wird und diese Lösungen dann in weitergehenden Schritten daraufhin überprüft werden, ob sie gültig sind oder nicht.
Der Nachteil dieser Methode besteht darin, daß die Menge an Material, die für die Bearbeitung eines Problems benötigt wird, mit der Komplexität stark anwächst.
Gibt es sehr viele Möglichkeiten, die verschiedenen Städte miteinander zu verknüpfen, so benötigt man auch eine sehr große Anzahl von zufällig gebildeten Kette, da die Wahrscheinlichkeit, daß die gesuchten Ketten in zufälliger Weise entstehen, mit der Anzahl der möglichen Konfigurationen stark absinkt.
Dadurch ist die Komplexitätsgrenze auch von vornherein relativ eng begrenzt. Sobald zur Erreichung einer Wahrscheinlichkeit von 50 % für das Entstehen der richtigen Lösungen ein Volumen in der Größe eines ganzen Raumes benötigt wird, liegt auf der Hand, daß das Verfahren seine praktische Grenze erreicht hat. Aus diesem Grunde wird daher auch ein 70 Bit Problem als Obergrenze für ein in solcher Weise paralleles Verfahren angesehen.
Beim NMR-Quantencomputer (vgl. Kapitel **5.5.3**) ergibt sich aus analogen Gründen ebenfalls eine Begrenzung auf ca. 70 Bit, obwohl das zugrundeliegende Rechenprinzip ein völlig anderes ist.

Es kann also resümiert werden, daß der DNA-Computer auf der Basis, wie sie bislang formuliert wurde nur einen graduellen Fortschritt darstellt, da der Parallelisierung dadurch, daß sie durch massiven Materialeinsatz realisiert wird, letztlich relativ klar definierte Grenzen gesetzt sind.

Fazit: Der DNA-Computer basiert auf einer konsequenten Miniaturisierung seiner elementaren Rechenkomponenten. Man kann also in diesem Zusammenhang von einer Art Nanocomputer reden. Die zur Anwendung kommenden Prinzipien sind allerdings klassisch, so daß für den DNA-Computer letztlich dieselben Begrenzungen gelten wie für konventionelle Rechner.

5.2.2 Weitere Ansätze für neuartige Computersysteme

- **Optische Computer:**

  Entsprechende Entwürfe zielen auf den sukzessiven Ersatz der heute gebräuchlichen Halbleiterkomponenten durch optische Bauteile ab. Aufgrund der hohen Geschwindigkeit optischer Datenverarbeitung würde dies einen beträchtlichen Geschwindigkeitszuwachs bedeuten. Weiterhin erhofft man sich von optischen Datenspeichern höhere Informationsdichten. Die prinzipiellen Leistungsgrenzen der klassischen Turing-Maschine gelten allerdings auch für einen optischen Computer.

- **Neuroinformatik:**

  Mehrere Ideen beruhen auf der Nachahmung der biologischen Datenverarbeitung. Dies kann auf unterschiedliche Art und Weise erfolgen. Auf der Softwareebene werden schon seit geraumer Zeit Anwendungen auf der Basis neuronaler Netze programmiert. Die entsprechenden Programme laufen dabei auf konventionellen Rechnern. Wesentlicher Punkt hierbei ist nicht ein signifikanter Zeitgewinn, sondern die Lernfähigkeit und Fehlertoleranz des Systems.

  Man kann sagen, daß die heutige Software die beträchtliche Leistungsfähigkeit der zur Verfügung stehenden Hardware bei vielen Anwendungen noch längst nicht optimal ausnutzt. Dies bedeutet, daß signifikante Verbesserungen der Rechnerleistung auch durch intelligentere Software erzielt werden können, die sich in Anlehnung an die Natur neuronalen Prinzipien bedient. Allerdings ist es mit diesen Verfahren nicht möglich, die grundsätzliche Klassifizierung von Problemen als P, NP, etc. zu umgehen, sofern ein Beweis für die jeweilige Klassenzugehörigkeit bereits vorliegt.

- **Bioelektronische Ansätze:**

  Weitergehende Bemühungen zielen auf die Konstruktion von neuronaler Hardware, sowohl unter Benutzung klassischer Siliziumtechnologien als auch durch Verwendung biologischer Nervensysteme bzw. von Hybridsystemen, d.h. Anordnungen, bei denen Nervenzellen mit Siliziumchips verbunden werden.

5.3 Physikalische Grundlagen des Quantencomputers

5.3.1 Einleitung

Um die Prinzipien, nach denen die Quanteninformationsverarbeitung funktioniert, verstehen zu können, muß man sich mit den dazugehörigen physikalischen Phänomenen und Gesetzmäßigkeiten vertraut machen. Man begibt sich dabei in einen Bereich der Natur, der vom menschlichen Vorstellungsvermögen nicht mehr erfaßt werden kann, da es auf makroskopischer Skala keinerlei analoge Phänomene gibt, auf die der Verstand zurückgreifen könnte, um sich damit die Ereignisse, wie sie in der Quantenwelt stattfinden, zu illustrieren.
Es erweist sich daher als sinnvoll, bestimmte Sachverhalte, die das Resultat vielfältiger Messungen sind, als gegebenen Teil der Realität hinzunehmen und die daraus abgeleiteten Gesetzmäßigkeiten in vollständig abstrakter Weise zu behandeln. Es wird dringend davon abgeraten, der Versuchung zu erliegen, sich von Quantenprozessen eine bildhafte Vorstellung zu machen, da dies unweigerlich auf Widersprüche führt und demzufolge einem umfassenden Verständnis abträglich ist, obwohl sich einzelne Experimente dadurch scheinbar zufriedenstellend erklären lassen.
Zunächst soll hier der bekannte Welle-Teilchen Dualismus am Beispiel des Doppelspaltexperiments kurz erläutert werden. Von besonderer Bedeutung ist dabei die Interferenz als Ursache für die grundsätzliche Andersartigkeit des Quantencomputers verglichen mit klassischen digitalen Rechnern.
Der Übergang zwischen der klassischen und der Quantenwelt wird insbesondere vor dem Hintergrund des Problems der praktischen Realisierung von, auf der Nutzung verschränkter Quantenzustände basierenden, Anwendungen am Beispiel des bekannten Einstein-Podolski-Rosen-Paradoxons dargestellt. Das Problem der Messung in der Quantenmechanik wird kurz angerissen.
Auf eine formale mathematische Darstellung wird verzichtet. Bezüglich einer ausführlichen, auch quantitativen wissenschaftlichen Ausarbeitung der vorgestellten Sachverhalte sei auf die entsprechenden Publikationen verwiesen. Die folgenden Ausführungen zielen vor allem auf das qualitative Verständnis der zugrundeliegenden Phänomene ab.

5.3.2 Quantisierung

Begibt man sich vom Gültigkeitsbereich der klassischen Physik in den Anwendungsbereich der Quantenmechanik, so wird man zunächst mit dem ungewohnten Sachverhalt der Quantisierung konfrontiert.
Physikalische Zustände, wie beispielsweise der Eigendrehimpuls eines Teilchens oder die Energieniveaus eines Atoms oder Moleküls kommen nur in diskreten Werten vor und können nicht, wie in der klassischen Mechanik gewohnt, beliebige Werte oder, im Falle von Vektoren, Richtungen annehmen.
Die klassische, uns bekannte physikalische Welt geht aus der quantisierten in der Weise hervor, daß die diskreten Niveaus um so dichter zusammenrücken, je weiter man sich vom Grundzustand des Systems entfernt. Die jeweiligen Grundzustände sind dabei in aller Regel mit sehr geringen Energien bzw. Längenskalen verbunden und befinden sich, von wenigen Ausnahmen abgesehen, außerhalb der Reichweite unserer Wahrnehmung und sind in der Regel überhaupt nur mit sehr aufwendigen Apparaturen nachzuweisen. Auf makroskopischer Ebene liegen die Zustände dann derart dicht, daß sie als quasi kontinuierlich wahrgenommen werden.
Zu den wenigen Ausnahmen gehören die Supraleitung und die Suprafluidität, die als makroskopische Quantenphänomene bezeichnet werden und auch auf großen Längenskalen ihre kontraintuitiven Eigenschaften behalten.
Die Experimente zur Quanteninformationsverarbeitung werden gegenwärtig an Zuständen durchgeführt, die sehr nahe am Grundzustand des entsprechenden Systems liegen. Man ist also sehr weit vom quasiklassischen Kontinuum entfernt.
Auch in der Quantenkommunikation hat man es in aller Regel mit Zwei- oder Vierniveau-systemen, also fundamental quantenmechanischen Zuständen zu tun.

Die Quantisierung ist letztlich Ursache dafür, daß der Informationsübertragung physikalische Grenzen gesetzt sind. Es ist eben nicht möglich durch immer bessere Präparationsmethoden bestimmte Eigenschaften, wie etwa eine Polarisationsrichtung, sehr genau festzulegen und von einer geringfügig um einen kleinen Winkel geneigten, abzugrenzen. Vielmehr kann aufgrund der Quantisierung an einem Photon nur eine von zwei möglichen linearen Polarisationen präpariert und auch gemessen werden, so daß der Informationsgehalt auf ein Bit beschränkt ist. Eine solche Einschränkung gilt für alle physikalische Eigenschaften.

Beispielsweise kann man auch die Frequenz eines Photons nicht beliebig genau festlegen, da man dafür theoretisch eine unendliche lange Präparationszeit benötigen würde.

5.3.3 Interferenz, Welle-Teilchen-Dualismus

Die Quantisierung bedeutet in keiner Weise den Endpunkt bzw. den Kern der Quantenmechanik. Vielmehr stellt sie eine Art beobachtbare Schnittstelle zur klassischen Physik dar. Die Quantisierung bezieht sich daher auch immer auf Beobachtungen. Resultate von Messungen an Quantensystemen sind quantisiert. Man spricht in diesem Zusammenhang auch von Eigenzuständen des gemessenen Systems. Die zugrundeliegende Realität als Folge deren Messung bzw. Manipulation die diskreten Werte auftreten, ist jedoch nicht in diesem Sinne quantisiert. Auf dieser tieferliegenden Ebene betrachtet man quantenmechanische Zustände als bestmögliche Beschreibung der physikalischen Objekte, die sich nun nicht mehr als massive, lokalisierte Körper, wie wir es im Alltag gewohnt sind, behandeln lassen. Quantenmechanische Objekte (i.allg. als Wahrscheinlichkeitsamplituden bezeichnet) sind insbesondere auch nichtlokal, d.h. nicht eindeutig einem bestimmten Ort zuzuordnen. Sie sind mit Wahrscheinlichkeiten des Nachweises einer bestimmten Eigenschaft eines Teilchens an einem bestimmten Ort korreliert.
Wichtig ist an dieser Stelle, daß quantenmechanische Zustände nicht die Wahrscheinlichkeit selbst sind, sondern erst das Quadrat der Wahrscheinlichkeitsamplituden, die diese Objekte beschreiben, eine konkrete Nachweiswahrscheinlichkeit im Sinne der Vorhersage eines individuellen lokalen Meßresultats, wie man es klassisch gewohnt ist, ergibt.
Würde nun die Dynamik quantenmechanischer Objekte auf der Ebene der Wahrscheinlichkeiten ablaufen, so hätte man eine der klassischen Physik analoge Situation. Auf der Quantenebene findet die Interaktion zwischen den Objekten jedoch über die Wahrscheinlichkeitsamplituden statt, d.h. noch bevor man überhaupt unter Nutzung des klassischen Begriffs der Aufenthaltswahrscheinlichkeit eine statistische Interpretation versuchen könnte. Wie bereits angeführt, schlägt der Versuch sich die entsprechenden Abläufe bildlich vorzustellen fehl. Die Tatsache, daß Interaktion und Dynamik bereits auf dem Niveau der Wahrscheinlichkeitsamplituden abläuft, ist jedoch ursächlich für das Auftreten von Interferenzeffekten als physikalische Grundlage des Quantenparallelismus.

Besonders deutlich wird das Problem des Welle-Teilchen-Dualismus am Beispiel des Doppelspaltexperiments.
Wie sich die mit quantenmechanischen Effekten verbundenen tiefere Ebene der Realität im Experiment mitteilt, wird insbesondere auch am Aharonov-Bohm-Effekt sehr deutlich, der ebenfalls kurz skizziert werden soll.

Das Doppelspaltexperiment:

Beleuchtet man einen Doppelspalt mit ausreichend kohärentem Licht (z.B. aus einer Laserlichtquelle) so erhält man ein charakteristisches Interferenzmuster (Abb. 4), wie es nicht durch bloße additive Überlagerung der Muster zweier Einzelspaltinterferenzen erzeugt werden kann.
Betrachtet man das Licht zunächst als einen Teilchenschauer, so wäre noch eine Interpretation denkbar, wonach das Interferenzmuster über eine Wechselwirkung der Photonen zustande kommt, die durch unterschiedliche Spalte zum Detektor gelangen.
Schwächt man die Intensität des Lichtstrahls soweit ab, daß sich immer nur maximal ein Photon in der gesamten Apparatur befindet, so würde man in der klassischen Sichtweise erwarten, daß das Photon immer nur einen der beiden möglichen Wege nehmen kann und man demzufolge zwei überlagerte Einzelspaltinterferenzmuster registrieren sollte. Dies ist jedoch nicht der Fall.
Ein Einzelspaltmuster erhält man erst, wenn man experimentell nachprüft, durch welchen der beiden Spalte das Photon getreten ist.
Solange beide Spalte ungehindert durchquert werden können, kann dem Photon also nicht eine wohldefinierte Trajektorie zugewiesen werden, da es sich eben nicht nur formal, sondern tatsächlich gleichzeitig physisch auf den beiden möglichen Wegen befindet. Eine Messung an einem der beiden Spalte bewirkt dann den Kollaps der Wellenfunktion in den korrespondierenden Einzelspaltzustand. Man bezeichnet diese Situation, bei der gleichzeitig beide Möglichkeiten realisiert sind allgemein als Superposition von Zuständen.

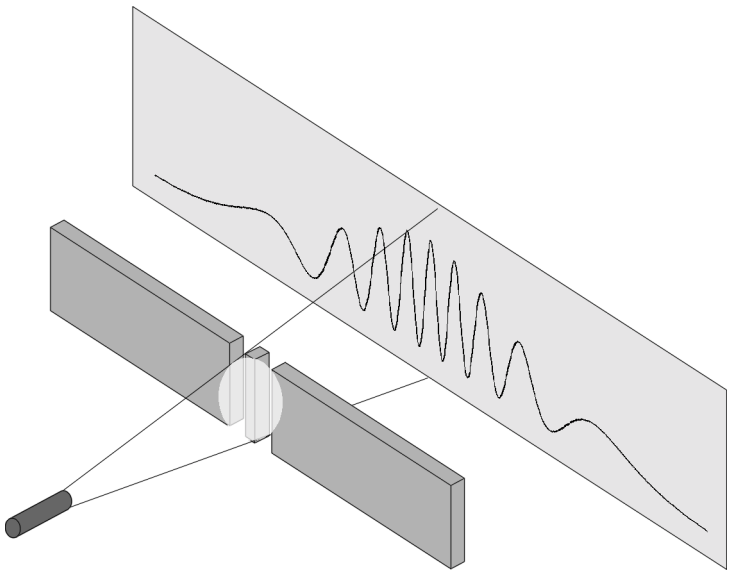


Abb. 4: Doppelspaltversuch: Das Interferenzmuster des Doppelspalts läßt sich nicht durch additive Überlagerung zweier Einzelspaltmuster erhalten. Des weiteren ändert sich das Muster selbst dann nicht, wenn man eine so geringe Belichtung wählt, daß sich immer nur ein Photon in der Apparatur befindet. Dies ist nach der Kopenhagener Interpretation so zu deuten, daß ein einzelnes Photon hier als nichtlokales Wellenobjekt angesehen werden muß, das in der Lage ist, beide Spalte gleichzeitig zu durchlaufen.

Nicht nur Teilchen, sondern auch Felder müssen auf die tieferliegende quantenmechanische Realität zurückgeführt werden. Die Notwendigkeit hierfür liefert in besonders eindrucksvoller Weise der Aharonov-Bohm-Effekt. Schon seit langem ist bekannt, daß das Magnetfeld, wie es in den maxwellschen Gleichungen enthalten ist, mathematisch formal auf eine fundamentalere Größe, das Vektorpotential, zurückgeführt werden kann. Im Rahmen der klassischen Physik kommt dieser mathematischen Reduzierung keine Bedeutung zu. Im Zusammenhang mit der Quantenmechanik wurde jedoch deutlich, daß dies nicht zwei beliebige Beschreibungen desselben Phänomens sind, sondern bei Betrachtung von Wellenfunktion und Vektorpotential Effekte erhalten werden, die durch die bloße Berücksichtigung des Magnetfeldes nicht erfaßt werden. Zu beachten ist hierbei, daß dem Absolutwert des Vektorpotentials, als nicht eichinvarianter Größe, keine Bedeutung zukommt, sondern nur die Potentialdifferenz ein physikalisch reales Phänomen beschreibt.

Aharonov-Bohm Effekt:

Beim Aharonov-Bohm-Experiment werden elektrische Ladungen (Elektronen) auf zwei zueinander symmetrischen Bahnen um eine Spule, die in ihrem Innern ein Magnetfeld erzeugt, herumgeführt (Abb. 5). Klassisch betrachtet weiß man, daß elektrische Ladungen im Magnetfeld aufgrund der Lorentzkraft abgelenkt werden. Da die Bahnen der Elektronen im vorliegenden Fall jedoch nicht durch das Feld führen, erwartet man klassisch keinerlei Störung der Elektronenbewegung.

Bei quantenmechanischer Betrachtungsweise muß man jedoch sowohl die Elektronen, als auch das Magnetfeld auf der Basis der zugrundeliegenden Quantenrealität beschreiben. D.h. man betrachtet die Wahrscheinlichkeitsamplitude der Elektronen und beschreibt den Magnetismus nicht durch sein Feld sondern in analoger Weise durch das fundamentalere Vektorpotential. Anders als das klassische Magnetfeld ist dieses Vektorpotential außerhalb der Spule nicht Null sondern beeinflußt die Wahrscheinlichkeitsamplituden der Elektronen auf den beiden Bahnen in unterschiedlicher Weise.

Nachweisbar ist dies, indem man die auf den beiden unterschiedlichen Pfaden propagierenden Elektronenstrahlen miteinander interferieren läßt.

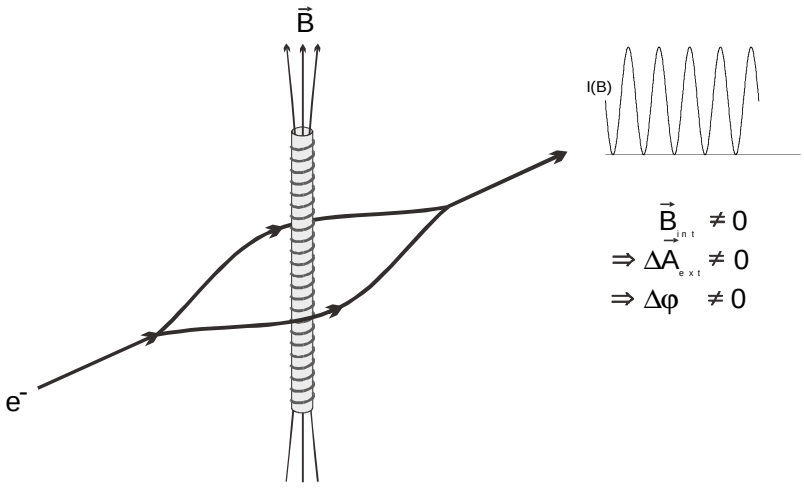


Abb. 5: Führt man einen kohärenten Elektronenstrahl in symmetrischer Weise um ein abgeschirmtes Magnetfeld $\vec{B}$ herum, so ist die Intensität des Strahls am Vereinigungspunkt abhängig von der Stärke dieses Magnetfeldes, obwohl die Elektronen zu keinem Zeitpunkt eine Magnetkraft erfahren. Dieser Effekt beruht auf der quanten-mechanischen Wechselwirkung mit dem Vektorpotential $\vec{A}$, das im Gegensatz zum Magnetfeld außerhalb der Spule nicht verschwindet.

Bei jedem Interferenzexperiment ist die Phasendifferenz eine empfindliche Größe, die die Form des Interferenzmusters bestimmt. So führt das An- und Ausschalten des Magnetfeldes in der abgeschirmten Spule zu einer Veränderung des Interferenzmusters der beiden Teilstrahlen, obwohl die Elektronen weder in dem einen noch dem anderen Fall eine Magnetkraft erfahren.
Es ist zu beachten, daß eine mögliche direkte Wechselwirkung der Elektronen mit dem Magnetfeld im Spuleninnern, beispielsweise aufgrund der quantenmechanischen Nichtlokalität, alleine nicht ausreicht, um den Effekt zufriedenstellend zu erklären.
Weiterhin muß man realisieren, daß über die tatsächliche physikalische Substanz sowohl des Feldes, wie auch des Potentials keinerlei Kenntnisse vorliegen. Beide werden ausschließlich über ihre Wirkung auf physikalische Testobjekte erfaßt. Da jedoch die Feldbeschreibung alleine nicht ausreicht, um beobachtbare quantenmechanische Phänomene wie den Aharonov-Bohm-Effekt zu erklären, stellt das Vektorpotential wohl die tiefgreifendere Beschreibung der magnetischen Wechselwirkung dar.
Der Aharonov-Bohm-Effekt illustriert in beeindruckender Weise die Tatsache, daß das klassische mechanistische Weltbild die Natur nur unvollständig wiedergibt und bestimmte Phänomene, die in Messungen heutzutage problemlos beobachtet werden können, nicht erfaßt. Die umfassendere quantenmechanische Darstellung verlangt allerdings die Aufgabe der gewohnten intuitiven Vorstellungen hinsichtlich physikalischer Prozesse und die Akzeptanz von Welle-Teilchen-Dualismus und Nichtlokalität als derzeit unverzichtbare Elemente bei der Interpretation quantenmechanischer Phänomene.

5.3.4 Das EPR-Paradoxon

Noch deutlicher wird die Eigenschaft der Nichtlokalität bei den sogenannten EPR-Experimenten, die auf einem von Albert Einstein, Boris Podolsky und Nathan Rosen formulierten scheinbaren Paradoxon basieren.
In diesem Gedankenexperiment versuchten die Autoren unter Zuhilfenahme der speziellen Relativitätstheorie die Quantenmechanik als eine unvollständige Theorie darzustellen. Die Quantenmechanik wäre demnach nur eine Art Extrapolation einer noch unbekannten mikroskopischen Theorie, die in ähnlicher Weise wie die Statistik für die Thermodynamik einen soliden mechanistischen Hintergrund liefern und frei von Interpretationsproblemen sein sollte.

In Anlehnung an das EPR-Gedankenexperiment wurden dann auch mehrfach solche Theorien "verborgener Parameter" entwickelt.

Es konnte jedoch von Bell gezeigt werden, daß derartige klassische Erklärungsversuche in bestimmten Fällen Abweichungen zur Quantentheorie aufweisen, die experimentell überprüfbar sein sollten [Bel62]. Solche experimentellen Realisierungen des EPR-Paradoxons wurden wiederholt durchgeführt und müssen nach heutigem Ermessen klar zugunsten der bestehenden Quantentheorie gedeutet werden [Wei98].

Hiernach ist es also nicht möglich eine auf klassisch mechanistischen Paradigmen beruhende Mikrotheorie als Ersatz für die Quantentheorie zu formulieren.

Im folgenden soll das EPR-Argument genauer erläutert und die experimentelle Realisierung an einem Beispiel beschrieben werden.

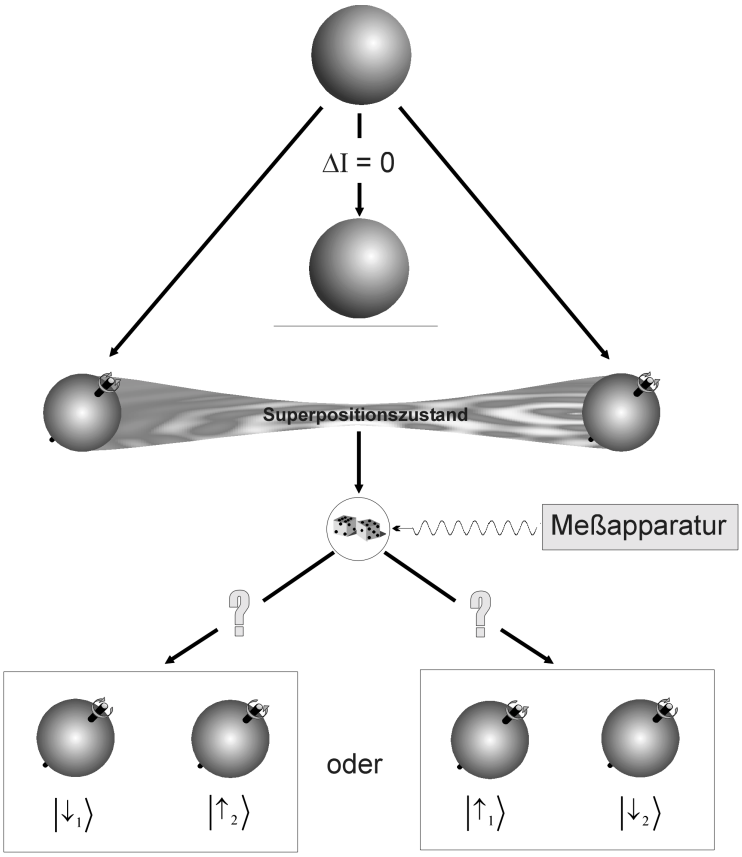


Abb. 6: Werden bei einem drehimpulserhaltenden Zerfall zwei Teilchen emittiert, die über Drehimpuls verfügen, so müssen diese bei einer Messung entgegengesetzt ausgerichtet sein. Da dies jedoch immer auf zwei Arten möglich ist, liegen die beiden Teilchen bis zur Messung in einem Superpositionszustand aller möglichen Endzustände vor. Durch Interaktion mit der Meßapparatur geht das System dann in nur einen der Endzustände über. Welcher Zustand zuletzt angenommen wird kann nicht vorhergesagt werden, es handelt sich bei diesem Vorgang um ein physikalisches Zufallsereignis.

Das EPR-Paradoxon in einer etwas suggestiveren Abwandlung von Bohm [Boh51] beruht auf einem Konflikt, der zwischen wesentlichen Inhalten der speziellen Relativitätstheorie (keine Information kann mit Überlichtgeschwindigkeit propagieren) und nichtlokalen Effekten in der Quantenmechanik zu bestehen scheint.

Man betrachtet hierzu den Zerfall eines beliebigen Teilchens, das zwei Partikel emittiert, die einen Spin jeweils gleichen Betrags transportieren sollen. Es sei der Endzustand des zerfallenen Teilchens hinsichtlich des Drehimpulses derselbe wie der Anfangszustand. Aufgrund des Drehimpulserhaltungssatzes folgt dann, daß die Spins der beiden emittierten Partikel bei einer Messung in entgegengesetzte Richtungen zeigen müssen, um sich gegenseitig zu kompensieren.

Die Quantenmechanik besagt nun aber, daß die Spinrichtung eines einzelnen Partikels nicht von vornherein feststehen kann, da die quantenmechanische Unschärfe eine Eigenschaft der Objekte selbst ist und nicht die Abwesenheit von Wissen, also die Unkenntnis eines, eigentlich schon vor einer Messung fest vorliegenden Zustands.

Wenn aber die Drehimpulserhaltung gültig ist, der Spin eines einzelnen Teilchens jedoch unscharf sein soll, bedeutet dies, daß die beiden Partikel nicht isoliert voneinander betrachtet werden können, sondern als ein zusammenhängendes nichtlokales quantenmechanisches Objekt betrachtet werden müssen, so daß auch für das unscharfe System der Erhaltungssatz seine Gültigkeit behält. Eine Messung der Spinrichtung eines Teilchens muß dann zu einer entsprechenden Ausrichtung des Spins des anderen führen, so daß die Drehimpulserhaltung erfüllt ist. Bemerkenswert ist die Tatsache, daß die Spinrichtung eines individuellen Teilchens nicht im voraus festgelegt ist und im Zuge der Messung völlig zufällig festgelegt wird (vgl. Abb. 6).

Ob man nun eine Interpretation derart vornimmt, daß man die beiden Teilchen als ein nichtlokales Objekt betrachtet oder als zwei getrennte Objekte, die in der Lage sind über eine wie auch immer geartete Wechselwirkung instantan Informationen über vollzogene Zustandsänderungen auszutauschen, es erscheint nur natürlich, daß in beiden Fällen ein gewisses Unbehagen zurückbleibt. Es wurden daher zahlreiche Versuche unternommen quantenmechanische Effekte mit Hilfe klassischer mechanistischer Modelle zu erläutern, wonach z.B. im Falle des EPR-Paradoxons der Spin quasi bis zur Messung in einem komplizierten inneren Mechanismus eines jeden einzelnen der Teilchen versteckt, nichtsdestotrotz aber die Information von Anfang an in jedem Teilchen enthalten wäre (Theorie verborgener Parameter, vgl. Abb. 7).

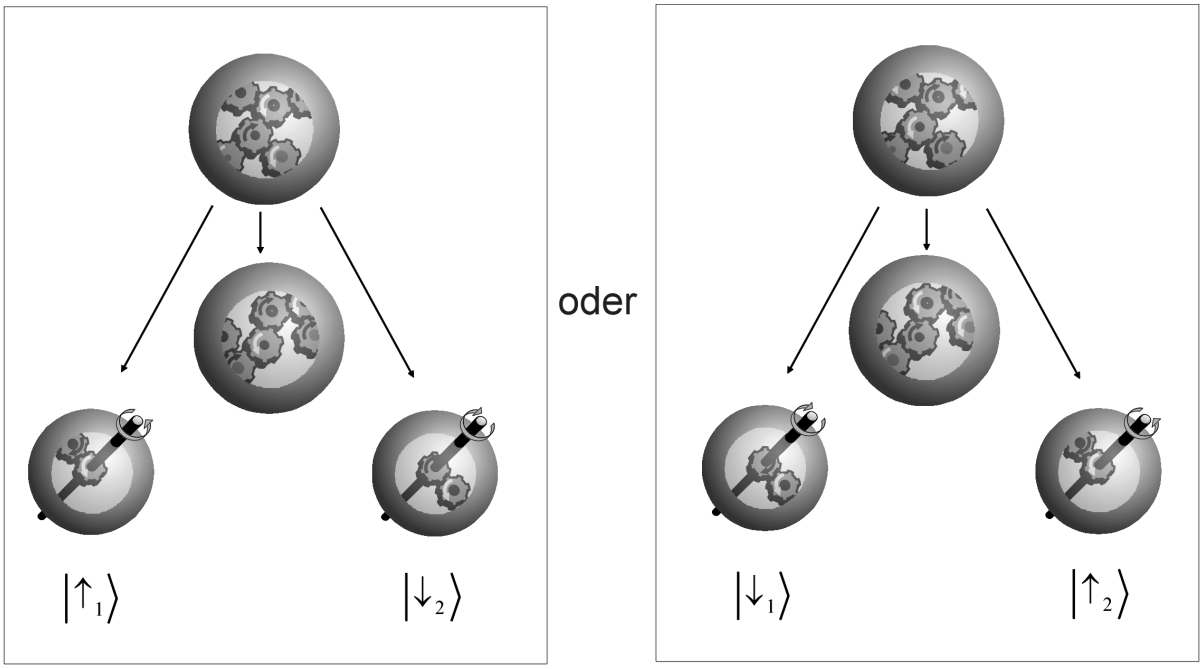


Abb. 7: Nach der Theorie verborgener Parameter sind die individuellen Spins der Teilchen, die beim Zerfall entstehen bereits vor dem Zerfall festgelegt. Die beiden möglichen Endzustände können hier also nicht auf den gleichen Anfangszustand zurückgeführt werden, da sich dieser für die beiden Fälle in seinen verborgenen Parametern unterscheiden muß. Jede Eigenschaft läßt sich nun wieder in deterministischer Weise auf eine spezifische Ursache zurückführen, Zufallselemente kommen nicht vor. In diesem Modell existiert kein Quanten-parallelismus und damit auch keine Möglichkeit einen Quantencomputer zu realisieren.

John Bell konnte jedoch zeigen, daß es bei EPR-Experimenten zu unterschiedlichen Ergebnissen führen muß, je nachdem welche Theorie man zur Vorhersage heranzieht.
Konkret zeigt sich ein Unterschied bei sogenannten Korrelationsmessungen. Dabei wird zunächst der Spin eines der beiden Teilchen in einer definierten Raumrichtung ermittelt und danach der Spin des zweiten Teilchens in Richtung einer, in einem bestimmten Winkel zur ersten Meßrichtung geneigten Achse festgestellt.
Läßt sich zwischen den Resultaten der beiden Messungen ein Zusammenhang finden, so sind die Messungen offensichtlich korreliert. Unter Nutzung der jeweiligen Theorien lassen sich diese Korrelationen als Funktion des Zwischenwinkels quantifizieren.
Man erhält nun als prinzipielles Resultat in Form der sogenannten Bellschen Ungleichung [Bel64], daß bestimmte Korrelationswerte für Theorien, die auf verborgenen Parametern beruhen, verboten sind, während die Quantenmechanik solche Werte zuläßt.
Experimentell konnte durch Messung dieser Korrelation die Quantenmechanik bestätigt werden (Abb. 8).

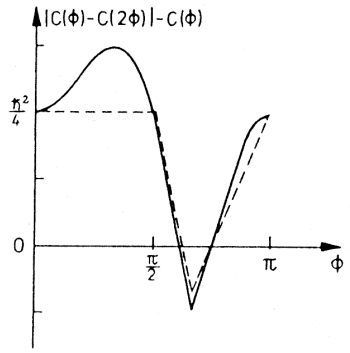


Abb. 8: Die durchgezogene Kurve gibt eine Korrelationsfunktion entsprechend der Quantenmechanik wieder, die gestrichelte Linie stellt die gleiche Korrelation für Theorien verborgener Parameter dar. Man erkennt, daß für bestimmte Winkel Φ beträchtliche Unterschiede auftreten, die sich auch im Experiment überprüfen lassen.

Es muß jedoch hinzugefügt werden, daß bei diesen Experimenten eine Vielzahl von möglichen Einwänden zu berücksichtigen sind. Insbesondere die Möglichkeit der klassischen, kausalen Kommunikation zwischen den beiden Teilchen, so daß sich das Ergebnis einer Messung in Übereinstimmung mit den Gesetzen der speziellen Relativitätstheorie dem anderen Teilchen mitteilt, muß durch raffinierte experimentelle Anordnungen ausgeschlossen werden können [Asp82, Wie98]. Hier wurde vor kurzem wieder ein bedeutender Fortschritt erzielt [Wei98], so daß man die Gültigkeit der Quantenmechanik, auch unter strengen Anforderungen an die sogenannte Einstein-Separation, heute als gültig ansehen muß.

Eine letzte Lücke in der Beweiskette zur Nichtlokalität der Quantenmechanik findet sich im wesentlichen nur noch im Signal zu Rausch Verhältnis der EPR-Experimente. Hier ist es bislang noch nicht möglich tatsächlich alle verschränkten Photonenpaare zu detektieren. Man setzt bislang voraus, daß die gemessenen Paare eine repräsentative Auswahl aller erzeugten Paare darstellen. Es ist jedoch denkbar, daß aufgrund eines nicht erkannten systematischen Einflusses nur bestimmte Paare detektiert werden können, die für sich betrachtet eine Verletzung der Bellschen Ungleichung ergeben, während bei Betrachtung aller erzeugten Teilchenpaare, was eben bislang experimentell nicht möglich ist, zumindest bislang rein rechnerisch die Möglichkeit besteht, daß das Bellsche Limit nicht überschritten wird.

Absehbare Fortschritte in der Technologie der verwendeten Apparaturen werden hier jedoch über kurz oder lang die Effizienz auf ein Niveau anheben, von dem aus eindeutige und belastbare Aussage möglich sein wird.

5.3.5 Verschränkung und Quantenparallelismus

Ein EPR-Teilchenpaar, wie es im vorherigen Abschnitt beschrieben wurde, wird in der Quantenmechanik zweckmäßigerweise als ein einzelnes zusammenhängendes System behandelt. Solche Teilchen, die nicht isoliert voneinander betrachtet werden können, werden als verschränkt bezeichnet. Man hat es also im Fall der Verschränkung mit einer Art von physikalischem Holismus zu tun.
Werden die Teilchen einer Messung unterworfen, so verlieren sie ihre Verschränkung und können in Folge als unabhängige Objekte angesehen werden.
Was bei diesem Prozeß der Messung im Detail passiert ist noch nicht völlig geklärt. Es gibt jedoch Interpretationen dahingehend, daß bei einer Messung das untersuchte Teilchen über die Meßapparatur mit seinem gesamten Umfeld verschränkt wird und dabei jede Art von Kohärenz verloren geht [Cer96].
Solange die beiden Teilchen jedoch verschränkt sind, muß jedes mögliche Ergebnis, welches das Resultat einer zukünftigen Messung sein könnte, in irgendeiner Art und Weise bereits in diesem verschränkten Zustand enthalten sein. Man bezeichnet dies als auch als Quantenparallelismus.
Dieser Parallelismus ist die physikalische Grundlage des Funktionsprinzips eines Quantencomputers. Unterschiedliche Zustände sind in einem Register verschränkter Quantenobjekte (bei meist unterschiedlicher Gewichtung) gleichzeitig physikalisch real. Das bedeutet, sie können gleichzeitig verarbeitet werden. In einem klassischen Computer muß der Prozessor die entsprechenden Zustände nacheinander annehmen, was zu einer Verzögerung des Algorithmus führt.
Die parallel vorhandenen quantenmechanischen Zustände sind allerdings nicht vollständig unabhängig voneinander, d.h. es ist keineswegs von vornherein als selbstverständlich anzunehmen, daß die parallel vorliegenden physikalischen Zustände bei der Bearbeitung eines konkreten Problems alle benötigt werden. Es gilt also, Algorithmen zu finden, die aus dem physikalischen Vorteil der Quantenparallelität einen Nutzen ziehen können.
Für eine Rechnung, die auf dem Prinzip des Parallelismus fußt, ist es natürlich auch unabdingbar, daß die Verschränkung der Zustände erhalten bleibt. Eine Messung beispielsweise würde die Superposition und damit auch die Verschränkung zerstören und das System in einen sogenannten Eigenzustand überführen, mit der Folge, daß die Bestandteile des

Quantengatters als voneinander getrennt angesehen werden müßten. Dann würde das System nur noch einen einzigen Zustand besetzen, der Vorteil wäre verloren.
Da dies nicht nur für Messungen gilt, sondern für jede Art der unkontrollierten Wechselwirkung dieser verschränkten Zustände mit der Umgebung, läßt sich hierbei auch schon erahnen, welche Anforderungen an die praktische Realisierung komplizierter verschränkter Zustände, getragen von bis zu mehreren hundert Teilchen, wie sie für einen anwendbaren Quantencomputer gebraucht würden, gestellt werden. Jegliche Einwirkung von außerhalb muß abgeschirmt werden um die Kohärenz des Systems möglichst lange aufrecht zu erhalten. Selbst die Wechselwirkung mit der auch im Vakuum immer vorhandenen sogenannten Nullpunktsenergie des elektromagnetischen Feldes kann ausreichen, um ein verschränktes Quantensystem in einen neuen, unerwünschten Zustand zu überführen.

Anhand des einfachsten Falls eines 2-Niveau-Systems soll die Problematik der Superposition und der Messung noch einmal verdeutlicht werden.
Betrachtet man ein Teilchen, dessen Spin nur in zwei verschiedenen Zuständen auftreten kann (2-Niveau-System), so würde man zunächst vermuten, daß sich im Spin auch lediglich nur ein Bit an Information codieren läßt. (Spin auf/ab entsprechend 0/1).
Dies ist jedoch bei genauerer Betrachtung nicht der Fall. Die Quantisierung bezieht sich nämlich tatsächlich nur auf die Messung einer Eigenschaft. Dies bedeutet, daß die Resultate des Meßprozesses nur bestimmte diskrete Werte sein können, das beobachtete Objekt selbst aber durchaus vorher auch in Zwischenzuständen vorgelegen haben kann.
Allerdings muß man bei der Interpretation eines solchen Zwischenzustandes wiederum sehr vorsichtig vorgehen. Der Zwischenzustand bedeutet nicht etwa, daß zum Beispiel ein Spin in irgendeine beliebige Richtung zwischen den beiden, bei der Messung möglichen Werten zeigt und durch den Vorgang der Messung dann in einen der beiden Endzustände ausgerichtet wird. Gerade eine solche Analogie zu klassischen Effekten liegt nicht vor. Der Spin des Teilchens befindet sich quasi in beiden Zuständen gleichzeitig und wird dann bei der Messung auf nur eine, die diskrete beobachtbare Richtung reduziert.
Es ist dabei aus prinzipiellen Gründen nicht möglich den Meßvorgang als Projektion im klassischen Sinne zu deuten. Die Messung dreht weder einen vorhandenen Spin, noch liefert sie die, mit der Meßanordnung korrespondierende Komponente eines beliebig im Raume ausgerichteten Spins.

Tatsächlich läßt sich zeigen, daß durch keinen noch so raffinierten Mechanismus das Resultat einer Messung präzise erklär- und vorhersehbar ist. Dies wäre eben wieder eine Theorie verborgener Parameter, wie sie ja durch die Experimente zum EPR-Paradoxon ausgeschlossen werden konnte.

Erstreckt sich der Superpositionszustand über mehrere Teilchen, so sind diese bezüglich der mit diesem Zustand verbundenen Eigenschaft miteinander verschränkt, und können daher nicht mehr isoliert voneinander betrachtet werden. Erst durch die Messung gewinnen solche verschränkten Teilchen ihre Individualität zurück (vgl. Abb. 6).

Dadurch, daß das Endresultat der Messung nicht festliegt und auch nicht auf einen tieferliegenden Mechanismus (verborgene Parameter) zurückgeführt werden kann, liegt hier zum ersten Mal eine Situation in der Natur vor bei der ein physikalischer Prozeß ein objektiv zufälliges Element enthält. Das bedeutet die Nichtvorhersagbarkeit eines bestimmten Ereignisses geht nicht, wie zum Beispiel bei einem klassischen chaotischen System, auf die Unkenntnis aller Parameter eines Systems bzw. einen nicht zu bewältigenden Rechenaufwand zurück, sondern sie ist ein nicht zu umgehendes Element der Realität selbst. Dies hat unter anderem zur Folge, daß sich unter Nutzung von Quanteneffekten auch ideale Zufallsgeneratoren konzipieren lassen, was auf der Ebene der klassischen Physik nicht möglich war.

Wenn aber ein Ereignis aufgrund eines zufälligen Mechanismus eintritt, so bedeutet dies, daß Information entsteht. Tatsächlich gilt für Information in der Natur kein Erhaltungssatz, wie etwa für Energie oder Ladung, was keineswegs als selbstverständlich vorausgesetzt werden kann. Bei dem in Abb. 6 skizzierten Prozeß würde ein Bit an neuer Information entstehen. Man würde also zur Beschreibung des Endzustandes des Systems nach der Messung ein Bit mehr Information benötigen als zur vollständigen Beschreibung des Ausgangszustands.

Ein ungestörtes quantenmechanisches Zweiniveausystem in einem Zwischenzustand enthält also dadurch, daß zwei verschiedene Resultate aus ihm hervorgehen können, mehr als nur ein Bit an Information. Dieser Zustand stellt sozusagen die Vorstufe des neuentstehenden Bits dar.

Das Problem liegt darin, daß es nicht möglich ist, diese Information auszulesen, da hierfür eine Messung notwendig ist und eine solche lediglich einen der beiden Eigenzustände erzeugen kann.

Die Frage ist, ob es auf andere Weise als über den direkten Zugriff gelingen kann, sich den höheren Informationsgehalt eines quantenmechanischen Zweiniveausystems, man bezeichnet diesen im allgemeinen als Qubit, nutzbar zu machen.

Dies kann man tun, indem man mehrere Qubits, d.h. von der Umgebung isolierte und damit nicht einer Meßwechselwirkung unterworfene Quantensysteme, miteinander verschränkt. Durch kohärente Überlagerung der Zustände wächst die Menge an gespeicherter Information dabei dramatisch an und zwar nach einem Exponentialgesetz in Bezug auf die Anzahl der verwendeten Qubits (Abb. 9).

Läßt man dieses System verschränkter Quantenobjekte sich nun in der Zeit entwickeln, so findet quasi eine parallele Verarbeitung der gesamten enthaltenen Information statt.

Man kann sagen, daß in einem System, das aus vielen miteinander verschränkten Qubits besteht, zu jeder Zeit die Information über jeden möglichen Endzustand tatsächlich physikalisch enthalten ist. Ein klassischer Computer kann dagegen zu einer bestimmten Zeit nur einen einzigen aller möglichen Zusände tatsächlich physikalisch annehmen.

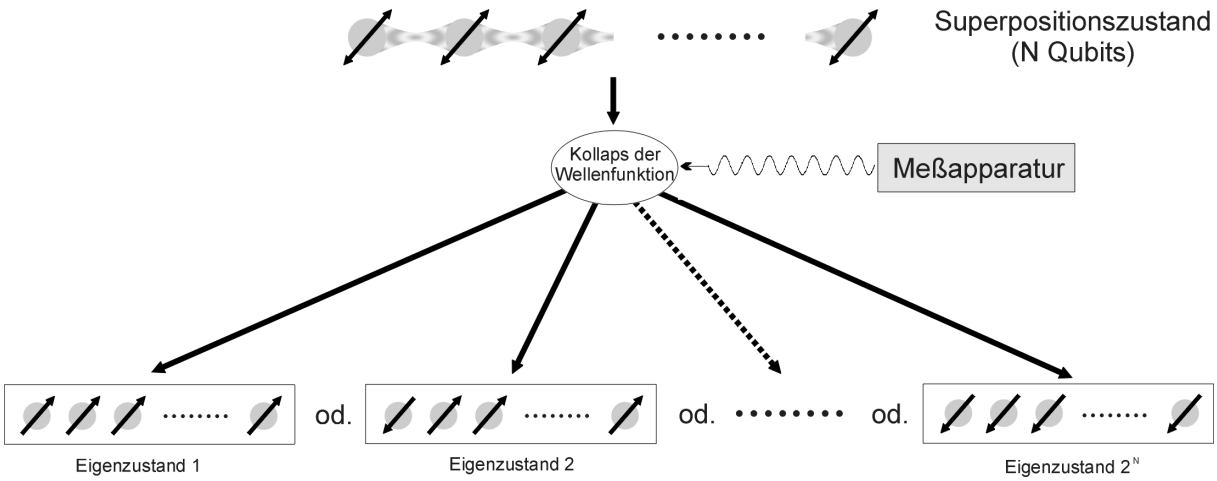


Abb. 9: Der Superpositionszustand enthält die Information über alle 2^N möglichen Endzustände. Nach der Messung kollabiert der Superpositionszustand jedoch in einen von 2^N möglichen Eigenzuständen und enthält dann nur noch die Information über den angenommenen Endzustand selbst.

In diesem Faktum erkennt man nun auch den Zusammenhang zwischen Rechenzeit und Parallelismus. Da die Anzahl der gleichzeitig enthaltenen Zustände des Quantencomputers exponentiell mit der Zahl der Qubits ansteigt, ein klassischer Computer diese aber alle nacheinander abarbeiten muß, wäre umgekehrt für eine Rechnung die auf einem geeigneten Algorithmus beruht eine exponentielle Beschleunigung bei beim Übergang von einem klassischen auf einen Quantenprozessor denkbar.

Ein kritischer Punkt ist also auch die Suche nach geeigneten Algorithmen, die den physikalischen Vorteil des Quantenparallelismus zu nutzen imstande sind. Dies kann keineswegs als trivial vorausgesetzt werden.
Die experimentelle Herausforderung besteht jetzt darin, den Prozeß so zu steuern, daß eine gewollte und kontrollierbare Entwicklung des quantenmechanischen Systems stattfindet, ohne daß dazu ein externer Eingriff erforderlich wäre, der das System in einen Eigenzustand überführen würde.

5.3.6 Rechnen mit dem Quantencomputer

Um einen Quantencomputer eine Rechnung durchführen zu lassen, sind im Prinzip drei Schritte notwendig. Zuerst muß der Ausgangszustand präpariert werden. Dieser läßt sich mit der Software eines klassischen Computers vergleichen als diejenige Menge von Daten, die von der Hardware des Rechners derart manipuliert wird, daß das Resultat eine Lösung der gestellten Aufgabe ist. Die Propagation dieses Anfangszustandes wird bestimmt durch den apparativen Aufbau des Computers und entspricht der Hardware der klassischen Maschine. Schließlich muß das Ergebnis durch eine Messung des erhaltene Endzustands ausgelesen werden.
Wie beim konventionellen, binären Rechner formuliert man die zu lösende Aufgabe in einem Algorithmus als Abfolge logischer Operationen.
Hier wird man damit konfrontiert, daß die gewöhnliche binäre Logik nicht ohne weiteres auf die Situation der Quantenmechanik übertragen werden kann. Bestimmte elementare logische Operationen sind durch Quantengatter verhältnismäßig aufwendig zu realisieren, während andere, wie das Controlled NOT auf sehr simple Weise umzusetzen sind.
Dies führt direkt zur Frage nach den Möglichkeiten eines, auf einem quantenmechanischen Algorithmus basierenden Computers. Da die Implementation logischer Operationen in ein Quantenrechenwerk sehr viel mühsamer ist, als es bei einem klassischen Rechner der Fall ist, ist es sehr schwierig, konkrete Beispiele an Rechenoperationen zu benennen, die von einem Quantencomputer besser, was gleichbedeutend ist mit schneller, bearbeitet werden können. Man kann nicht einfach einen vorhandenen klassischen Algorithmus nach einer festen Vorgehensweise in einen Quantenalgorithmus umwandeln und auf diese Weise eine

exponentielle Beschleunigung der Bearbeitungszeit erhalten. Eine solche Übersetzungsvorschrift gibt es nicht, man muß vielmehr unter Nutzung anderer mathematischer Prinzipien von vornherein der physikalischen Verschiedenheit des Quantencomputers von der klassischen, binären Maschine Rechnung tragen, allein dann läßt sich der grundlegende Vorteil auch ausnutzen.

Mit dieser Problematik beschäftigt sich die Theorie der Quantenalgorithmen, die nach Vorgehensweisen sucht, mit Hilfe derer sich bestimmte Probleme signifikant schneller bearbeiten lassen, d.h. daß mit dem Umfang einer gestellten Aufgabe der Rechenaufwand weniger stark anwächst als dies bei einem klassischen Computer der Fall wäre.

Dadurch, daß beim Quantencomputer Superpositionen zur Anwendung kommen, werden quasi mehrere binäre Zustände gleichzeitig parallel verarbeitet (Quantenparallelismus). Dieser Quantenparallelismus ist der Grund dafür, daß man überhaupt eine Verbesserung gegenüber klassischen Rechnern erwartet. Man erhält die Parallelität hier also nicht durch Verwendung einer räumlich und materiell immer begrenzten parallelen Architektur, sondern durch die Ausnutzung eines hochparallelen, prinzipiell nicht limitierten physikalischen Phänomens.

Da hier eigentlich die physikalischen Prinzipien der Quantenionformationsverarbeitung behandelt werden sollten, sei die Umsetzung auf konkrete Probleme der klassischen Informationsverarbeitung nur im Anhang (B) kurz am Beispiel des Auffindens der Periode einer Funktion dargestellt werden [Ste98].

Zusammenfassung: Die klassischen physikalischen Prinzipien, gemäß denen alle heute in Benutzung befindlichen gewöhnlichen Rechnersysteme arbeiten, basieren auf noch fundamentaleren Naturgesetzen. Auf einer solchen grundlegenderen Ebene stehen zusätzliche Naturphänomene für den Bau eines Rechners zur Verfügung, die man aus dem klassischen, dem Menschen zugänglichen Erfahrungsraum nicht kennt, es sind dies die „verschränkten quantenmechanischen Zustände“.
Die Existenz und Verfügbarmachung dieser Verschränkung ist in der Vergangenheit bereits vielfach experimentell gezeigt worden.
Der Quantenparallelismus, als ein zentraler Punkt dieser Art von Physik, bildet die Grundlage für ein dem klassischen Rechner mathematisch beweisbar überlegenes Computerparadigma („Quanten-Turing-Maschine“).
Die praktische Anwendbarkeit dieser physikalischen Überlegenheit ist bereits für einige bislang nicht effizient berarbeitbare Problemstellungen gezeigt worden.

5.4 Einsatzmöglichkeiten des Quantencomputers

Bei der Frage, ob es sich lohnt, die enormen apparativen Probleme, mit den zwangsläufig damit verbundenen Kosten anzugehen, die mit dem Bau eines Quantencomputers verbunden sind, ist es zunächst einmal wesentlich festzustellen, welche Vorteile eine solche Maschine gegenüber einem klassischen Computer mit sich bringt.

Zwar hat der Quantencomputer aufgrund seiner Funktionsweise Zugriff auf elementarere physikalische Prinzipien zur Ausführung seiner Rechenoperationen, er definiert also eine Art Obermenge zu den klassischen Computern, es ist aber noch keineswegs gewährleistet, daß die zusätzlichen Fähigkeiten auch mit einer prinzipiell verbesserten Rechenleistung einhergehen. Damit ist gemeint, daß beispielsweise eine bloße Verdopplung der Rechengeschwindigkeit bei gleichen Schaltzeiten (Taktfrequenzen) von klassischem und Quantencomputer sicher nicht als Motivation dafür angesehen werden kann, letzteren zu bauen, da es kostengünstiger ist, die klassische Maschine zu verbessern, oder einfach den entsprechenden Zeitverlust in Kauf zu nehmen.

Gesucht wird also nach Problemen, die auf einem klassischen Computer generell als nicht bearbeitbar gelten, da der Rechenaufwand mit zunehmender Größe des Problems entweder exponentiell oder nach einem sehr starken Polynomialgesetz ansteigt.

Die Bedeutung des Unterschiedes zwischen exponentiellem und polynomialem Anstieg kann man sich am besten anhand eines konkreten Beispiels illustrieren:

Würde man mit einem heute verfügbaren Computer eine Verschlüsselung nach dem RSA (Rivest, Shamir, Adleman)-Verfahren (vgl. Kap. **6.6.1** und [Riv78]) durchführen und eine zu faktorisierende Zahl von zweitausend Stellen generieren, dann würde man für die Entschlüsselung der Zahl, die die Zerlegung in die größten Primfaktoren erfordert, bei Nichtverfügbarkeit des Schlüssels selbst dann nicht zu einer Lösung gelangen, wenn jedes Atom des Universum ein Hochleistungsrechner wäre und all diese Rechner seit der Entstehung des Kosmos an dem Problem gearbeitet hätten.

Dieses Faktorisierungsproblem kann man sich leicht klar machen, wenn man selbst beispielsweise versucht die Zahl 221 in ihre Primfaktoren zu zerlegen. Man sieht sofort ein, daß diese Aufgabe deutlich schwieriger ist, als die Umkehroperation, die einfache Multiplikation von 17 mit 13.

Tatsächlich existieren mehrere Problemklassen, für deren Bearbeitung auf klassischen, sogenannten Turing-Rechnern bislang kein polynomialer Algorithmus gefunden werden konnte, obwohl kein Beweis vorliegt, daß ein solcher generell unmöglich sein muß.
Für eines dieser nichtbearbeitbaren Problem, die oben angesprochene Faktorisierung in Primzahlen, die vor allem in der Kryptographie eine beträchtliche Rolle spielt, konnte gezeigt werden (Algorithmus von Shor [Sho94]), daß auf einem Quantencomputer eine exponentiell schnellere Bearbeitung verglichen mit den klassischen Vorgehensweisen, möglich ist. Die praktische Realisierung dieses Verfahrens würde insbesondere die Entschlüsselung des RSA-Codes ermöglichen, auf dem zahlreiche in letzter Zeit häufig diskutierte Kryptographie-verfahren (Public Key) für den Datenaustausch zwischen Computern basieren [Riv78].
Die Funktionsweise dieses Algorithmus beruht zum einen auf der Nutzung der Superposition der Zustände. Dies bedeutet, daß man alle möglichen Lösungen des Problems gleichzeitig zur Verfügung hat und diese nicht nacheinander austesten muß. Die Schwierigkeit besteht nun allerdings darin, unter der Vielzahl der in Frage kommenden Kandidaten, die richtige Lösung herauszufinden. Hierzu bedient man sich der Interferenz (vgl. Kap. **5.3.3**). Man präpariert den Ausgangszustand und die Parameter, die die Zeitentwicklung des Ausgangszustandes bestimmen in der Weise, daß die falschen Antworten durch destruktive Interferenz immer stärker unterdrückt werden (wie die Orte minimaler Lichtintensität beim Doppelspaltversuch), während die richtige Lösung durch konstruktive Interferenz immer weiter verstärkt wird (Intensitätsmaximum im Interferenzmuster), bis sie alle anderen Möglichkeiten deutlich überragt und ausgelesen werden kann. Gerade auch die Interferenz ist es, die nur in der Quantenmechanik existiert und in klassischen Computern nicht zur Verfügung steht.

Ein anderer Algorithmus für den Quantencomputer bringt eine weniger deutliche Ver-besserung gegenüber herkömmlichen Rechnern mit sich, dafür liegt in diesem Fall ein Beweis dafür vor, daß das klassische Verfahren grundsätzlich langsamer als der Quantenalgorithmus ist. Beim sogenannten Groverschen Algorithmus [Gro96] steigt der zum Durchsuchen einer Datenbank mit N Elementen notwendige Rechenaufwand nur mit $\sqrt{N}$ an, während klassisch hierfür N Rechenschritte notwendig sind.
Man kann hier nicht von einer echten qualitativen Verbesserung, sondern eher von einer Eingrenzung des Suchraumes sprechen. Allerdings ist dieser Algorithmus auf eine wesentlich breitere Klasse von Problemen anwendbar als die Faktorisierung in Primzahlen.

Eine spezielle Klasse von mathematischen Aufgabenstellungen, die sogenannten nichtdeterministisch polynomialen (NP) Probleme, gelten als derzeit mit einem klassischen Computer nicht exakt lösbar. Es werden beträchtliche Anstrengungen unternommen, um für diese NP-Probleme effiziente Algorithmen für einen Quantencomputer zu finden, bislang ist dies jedoch noch nicht zufriedenstellend gelungen. Die Lösung derartiger Aufgaben hätte insbesondere auch eine explizite ökonomische Bedeutung, da solche NP-Probleme in der Wirtschaft sehr häufig auftreten und bislang nur mit Näherungsmethoden angegangen werden können.
Ein konkretes Beispiel wäre das sogenannte "Travelling Salesman"-Problem [Suy98]. Es wird dabei der kürzeste Weg gesucht, entlang dem ein Handelsreisender eine bestimmte Anzahl von Städten besuchen kann. Diese Aufgabe erfordert von einem gewöhnlichen Rechner bei einer zunehmenden Anzahl von Städten sehr schnell einen enormen Rechenaufwand und kann derzeit nur bis ca. auf 95 % des Optimalwerts gelöst werden.
Auch für die Bilderkennung bzw. generell für die Bearbeitung von hochgradig korrelierten Daten verspricht man sich erhebliche Vorteile bei der Nutzung von Quantenalgorithmen [Hat98].

Ein besonders wichtiger Punkt bei der Frage nach der praktischen Anwendbarkeit eines Quantenrechner ist die Fehlertoleranz. Da es weder möglich ist, Zwischenschritte auszulesen und im Falle eines Fehlers zum vorherigen Rechenschritt zurückzukehren noch bestimmte, besonders fehleranfällige Zustände einfach kopiert und mehrfach verarbeitet werden können, ist man auf völlig neue Vorgehensweisen bei der Korrektur von Fehlern angewiesen. Mit dieser Frage befaßt sich ein weiteres wichtiges Teilgebiet der Quanteninformationsverarbeitung. Bisherige Erkenntnisse lauten dahingehen, daß die Berücksichtigung bzw. die Korrektur möglich ist, allerdings zu einem erhöhten Rechenaufwand führen. Der grundsätzliche durch den Quantenparallelismus erhaltene Vorteil geht allerdings durch die Implementation fehlerkorrigierender Codes nicht verloren.

Da im Rahmen dieser Technologieanalyse der Schwerpunkt auf der physikalischen Realisierung der Quanteninformationstechniken liegen soll, wird auf Detail der Algorithmen und der Fehlerkorrektur an dieser Stelle nicht näher eingegangen. Es sei hier auf eine Machbarkeitsstudie der DLR (Deutsches Zentrum für Luft- und Raumfahrt e.V.) verwiesen, die im Laufe des Jahres 1999 im Auftrag des BMBF-Referats 524 „Informatiksysteme“ durchgeführt werden soll.

Fazit: Bislang sind nur wenige Algorithmen bekannt, die die physikalische Vorteile des Quantenparallelismus ausnutzen können. Die wichtigsten sind der Faktorisierungsalgorithmus von Shor und der Algorithmus von Grover. Ersterer, weil er tatsächlich eine exponentielle Beschleunigung gegenüber jedem bekannten klassischen Algorithmus aufweist und letzterer, weil seine Überlegenheit mathematisch beweisbar ist, also heute schon ausgeschlossen werden kann, daß jemals ein gleich schnelles Verfahren für einen klassischen Computer gefunden werden wird.
Der Gebiet der Quantenalgorithmen ist ein eigenständiger Forschungsbereich, und das Auffinden passender Algorithmen für den Quantencomputer ist ein wesentlicher Punkt bei der Frage nach dem Nutzen eines solchen Geräts.

5.5 Experimentelle Techniken

5.5.1 Allgemein

Die drei wesentlichen Grundanforderungen an ein quantenmechanisches Rechenwerk sind [Jam98b]:

1.) Die Fähigkeit einen Satz von verschränkten Zwei-Niveau-Quantensystemen so von der Umgebung zu isolieren, daß während des Rechenvorganges die Kohärenz erhalten bleibt. Dennoch muß die Möglichkeit gewährleistet sein, so mit dem System wechselwirken zu können, daß die gezielte Präparation von Zuständen möglich ist.

2.) Ein Mechanismus, der zur Durchführung logischer Operationen die einzelnen Qubits miteinander verknüpft, eine Art Datenbus. Die Verknüpfung muß dabei wiederum in Form einer Verschränkung erfolgen.

3.) Eine Technik, die das Auslesen des Quantenzustandes am Ende der Berechnung erlaubt.

5.5.2 Ionenfallen

Eines der vielversprechendsten Konzepte zur praktischen Realisierung eines Quanten-computers ist das der Ionenfallen [Cir95, Mon95b].
In einer solchen Falle werden Ionen durch geschickt angeordnete elektrische, magnetische (Penning) oder elektromagnetische (Paul) Felder an ihrem Ort festgehalten. In der Mitte der Falle ist die Amplitude des einfangenden elektromagnetischen Wechselfeldes Null, und das Ion erfährt keine Kraft [Pau53, Gho95].
Für einen anwendbaren Quantencomputer müssen die Geometrien der Falle und der einfangenden elektrischen und elektromagnetischen Felder so beschaffen sein, daß die Möglichkeit besteht, mehrere Ionen in symmetrischer Weise anzuordnen. Diese Eigenschaft besitzen lineare Ionenfallen (Abb. 10). Bei diesen erzeugen vier parallel angeordnete

Elektroden, die sich in etwa einem Millimeter Abstand voneinander befinden, ein elektromagnetisches Quadrupolwechselfeld, das dafür sorgt, daß sich die Ionen entlang der Symmetrieachse in der Mitte der Anordnung ansammeln. Damit die Ionen nicht in Längsrichtung aus der Apparatur austreten können, werden an den Enden der Elektroden abstoßende Felder erzeugt, so daß die Ionen zur Mitte der Falle hin abgedrängt werden und sich dort aufgrund ihrer gegenseitigen elektrostatischen Abstoßung in Form einer Kette aufreihen [Win98, Hug98].

Dagegen ist die klassische Paul-Falle mit Ringelektroden für die Speicherung von mehreren Ionen kaum geeignet, da hier das elektromagnetische Wechselfeld nur an einem einzigen Punkt verschwindet. Werden in einer solchen Anordnung mehr als ein Ion eingefangen, dann befinden sich diese aufgrund ihrer elektrostatischen Abstoßung an Orten, an denen sie durch das dort nicht verschwindenden Wechselfeldes aufgeheizt werden.

Die ersten erfolgreichen Versuche zur Präparation verschränkter ionischer Zustände bis zu drei Qubits wurden in elliptischen Ionenfallen durchgeführt. Dabei wurden in einem Experiment jeweils ein innerer elektronischer Zustand eines von zwei Ionen und ein Vibrationszustand benutzt, während ein anderer Versuch auf der Verschränkung zweier Vibrationszustände mit einem elektronischen Zustand eines einzelnen Ions beruht.

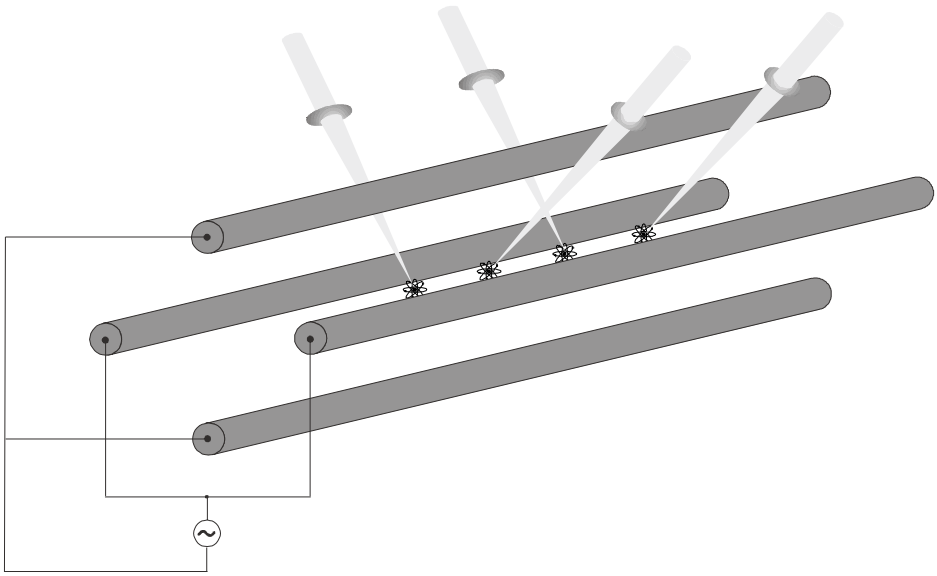


Abb. 10: In einer linearen Ionenfalle werden einzelne Ionen durch ein Quadrupolwechselfeld an ihrem Ort festgehalten. Die Adressierung der einzelnen Ionen soll durch Fokussierung von Laserlicht erfolgen.

Wesentlich ist, daß die Ionen, die später das Herz des Computers bilden, so vollständig wie nur möglich von ihrer Umgebung abgeschirmt werden, da jede unbeabsichtigte Wechselwirkung mit der Außenwelt den quantenmechanischen Superpositionszustand sehr stark beeinträchtigt. Es wird daher für eine solche Falle ein Ultrahochvakuum benötigt, so daß Stoßprozesse so weit wie möglich ausgeschlossen werden können.

Weiterhin müssen die Ionen sehr weit abgekühlt werden, damit sie bezüglich der Eigenschaften, die für die quantenmechanische Informationsverarbeitung Verwendung finden, den jeweiligen quantenmechanischen Grundzustand der Bewegung annehmen. Gerade auf der gezielten Manipulation dieser quantisierten Zustände beruht je die Funktionsweise des Quantencomputers. Da die Unterscheidbarkeit und der individuelle Zugriff auf die quantenmechanischen Zustände dabei um so einfacher werden, ja näher man dem Grundzustand kommt, muß man gezielt die Niveaus in diesem Bereich bevölkern. Umgekehrt rücken bei immer höheren Energien die Zustände zum quasiklassischen Kontinuum zusammen und sind somit nicht mehr in kontrollierter Weise experimentell zugänglich.

Bei der Ionenfalle handelt es sich hierbei konkret um elektronische und vibronische Zustände der Ionen.

Die Kühlung der Ionen stellt eine besondere experimentelle Herausforderung dar. Es gibt verschiedenste Techniken, mit deren Hilfe die Kühlung vorgenommen werden kann und die oftmals auch parallel, für jeweils unterschiedliche Temperaturbereiche optimiert, verwendet werden. Für Ionen handelt es sich dabei um unterschiedlichste Methoden der Laserkühlung [Win75b, Mon95a, Die89, Win78, Neu78, Ita95, Bir94, Esc95].

Das Grundprinzip der Laserkühlung besteht darin, das Ion in einer solchen Weise mit Laserlicht anzuregen, daß Absorptions- und Emissionsprozeß zu einem Impulsverlust des Ions oder Atoms führen. Dies erreicht man z.B., indem man das eingestrahlte Licht in Relation zur internen Resonanz des Atoms zu niedrigeren Energien hin, d.h. in Richtung kleinerer Frequenzen, verstimmt. Man regt dann vom elektronischen Grundzustand des gegenwärtigen Vibrationsniveaus aus den angeregten elektronischen Zustands des nächstniedrigen Vibrationszustands an, was eine Verlangsamung der mechanischen Ionenschwingung bedeutet (Abb. 11). Bildlich gesprochen könnte man sagen, daß das eingestrahlte Photon das schwingende Ion von vorn, gegen dessen Bewegungsrichtung trifft und die Absorption des Photons daher zu einer Abbremsung des Ions führt.

Mit Hilfe der sogenannten Dopplerkühlung ist es prinzipiell möglich, eine Konfiguration der Ionen zu erreichen, in der diese wie in einer Perlenkette aufgereiht sind. Durch alternierende

Anwendung zweier Kühlprozesse die jeweils auf der Nutzung von Zuständen unterschiedlicher Lebensdauer beruhen, kann für einzelne Ionen bereits die 95 %-ige Besetzung des Schwingungsgrundzustands erreicht werden [Die89].
Der elektronische Grundzustand eines Ions kann durch optisches Pumpen besetzt werden, indem durch geeignet gewählte, laserinduzierte Absorption und Emission gezielt der Grundzustand des Ions bevölkert und in der Gesamtbilanz damit Energie abgeführt wird. Der elektronische Grundzustand ist damit im Vergleich zum vibronischen sehr leicht zu kontrollieren.

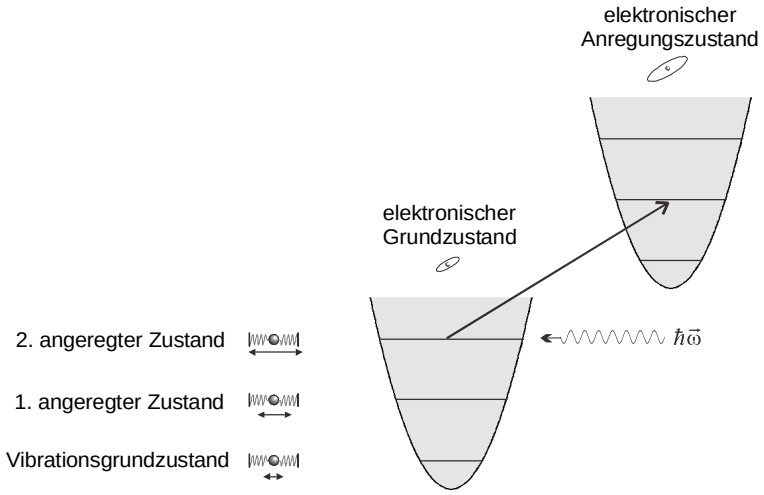


Abb. 11: Grundprinzip der Laserkühlung: Durch Einstrahlung von Licht ($\hbar\vec{\omega}$) -geringerer als der Übergangsenergie zwischen elektronischem Grund- und Anregungszustand werden gezielt niedrigere Vibrationszustände bevölkert. Die fehlende Energie für die elektronische Anregung wird quasi der kinetischen Energie des Ions entnommen.
Man erkennt an diesem Kühlmechanismus auch das Wechselspiel zwischen elektronischer und vibronischer Anregung, wie es für die Verschränkung von Qubits, die auf diesen unterschiedlichen Eigenschaften basieren, genutzt wird.

Durch Abstimmung der elektrostatischen Coulomb-Abstoßung der Ionen mit dem elektromagnetischen Feld der Ionenfalle kann der Abstand zwischen den Ionen auf bis zu 30 µm eingestellt werden, wobei dieser Abstand allerdings um so geringer wird, je mehr Ionen sich in der Falle befinden [Ste87, Jam98c]. In diesem Zustand müssen die einzelnen Ionen dann von Lasern zwecks Präparation des Ausgangszustandes individuell adressiert werden können

(vgl. Abb. 10). Auch diese Aufgabe ist keineswegs trivial. Der Laser muß extrem genau auf das einzelne Ion fokussiert werden und dabei eine hohe Stabilität aufweisen, da bei geringen Schwankungen, bedingt durch die extreme Fokussierung, bereits unerwünschte, starke Intensitätsgradienten auftreten können. Für die Adressierung der Ionen wurden neben der gewöhnlichen räumlichen Fokussierung eines Laserstrahls bereits eine Vielzahl von Alternativmethoden vorgeschlagen, von denen sich einige als besonders geeignet für den Umgang mit Ionenpaaren erwiesen haben. Die Anwendung auf ein Register aus vielen Ionen hingegen ist jedoch in der Regel mit erheblichen Problemen verbunden [Win97, Cir97, Enk97].

Jedes Ion in der Falle bildet zunächst ein Qubit, bestehend aus elektronischem Grund- und einem energetisch höher liegenden Zustand, sowie der Superposition dieser Zustände. Die höheren Zustände liegen dabei sehr nahe am Grundzustand und unterscheiden sich von diesem nur durch sogenannte Hyperfein- oder Zeeman- Aufspaltungen. Beide Eigenzustände und die Superposition dieser Zustände entsprechen dann einem Qubit.
Es wird nun noch eine Art von Datenbus benötigt, der die Verschränkung, d.h. den quantenmechanischen Datenaustausch der Ionen untereinander, ermöglicht. Hierzu benutzt man den kollektiven Vibrationsgrundzustand der eingefangenen Ionen. Kollektiv wird diese Vibration jedes Ions aufgrund der elektrostatischen Abstoßung zwischen den Ionen, die dazu führt, daß diese sich nicht unabhängig voneinander im Raum bewegen können.
Dieser Vibrationszustand kann als ein zusätzliches Qubit betrachtet werden, das mit sämtlichen Ionen in direkter Verbindung steht, wohingegen die individuellen Ionenqubits, die über den elektronischen Grund- und einen metastabilen Anregungszustand definiert sind, zunächst nicht direkt miteinander in Wechselwirkung treten und damit auch nicht direkt sondern nur mittels des Vibrationszustands miteinander verschränkt werden können.
Zum Auslesen des Endzustandes und damit des Ergebnisses einer Rechnung bedient man sich einer Streumethode [Nag86, Sau86, Ber86]. Man bestrahlt die Ionen mit Licht, das gerade der Übergangsfrequenz zwischen dem Grundzustand und einem virtuellen angeregten Zustand entspricht. Von diesem erfolgt dann ein Übergang in den Qubit-Zustand. Streut daraufhin das Ion, so muß es sich im Grundzustand befunden haben und damit in der Lage gewesen sein, das eingestrahlte Photon zu absorbieren und zu streuen, geschieht nichts, so war das Ion im höheren Zustand. Es handelt sich bei diesem Verfahren um sogenannte Raman-Streuung. Der indirekte Weg über den virtuellen angeregten Zustand ist notwendig, da der Energieunter-

schied zwischen den beiden Zuständen des Qubits (Grund- und Hyperfeinzustand) viel zu gering ist um optisch angeregt werden zu können. Die Energiedifferenz entspricht hier einer hohen Radiofrequenz, die optisch nur indirekt als Differenz zweier optischer Photonen (unter Nutzung des virtuellen Anregungszustands) adressiert werden kann.

Man kann für eine solche Falle nicht jedes beliebige Ion benutzen. Die zur Anwendung kommenden Ionen müssen bestimmte Grundanforderungen hinsichtlich der praktischen Anwendung der diversen Kühltechniken, wie auch im Hinblick auf den laseroptischen Präparations- und Ausleseprozeß der für eine Quantenrechnung in Frage kommenden Zustände erfüllen. Außerdem müssen die quantenmechanischen Zustände auf deren Basis Quantenrechnungen durchgeführt werden sollen, eine genügend hohe Lebensdauer aufweisen, so daß die Kohärenz während der Dauer der Rechnung erhalten bleibt.
Hinsichtlich der Lebensdauer sind z.B. Hg^+, Ca^+, Ba^+ oder auch Yb^+ geeignet [Jam98c, Rob97]. Das Ca^+ hat im besonderen den Vorteil, daß die Übergänge zwischen den Zuständen mit heute verfügbaren Titan-Saphir- oder Diodenlasern gesteuert werden können.

Die wesentlichste fundamentale Einschränkung beim Versuch einen funktionierenden Quantencomputer zu bauen, ist die Dekohärenz. Sogar wenn alle äußeren Störungen, wie Fluktuationen im einfangenden Feld, unstabile Laser, etc., erfolgreich abgeschirmt wurden, kann ein quantenmechanischer Zustand immer noch durch spontane Übergänge zerstört werden. Dieser Einfluß läßt sich niemals ganz ausschließen, da er durch elektromagnetische Fluktuationen des Vakuums verursacht wird. Solche Fluktuationen koppeln in unterschiedlicher Weise an angeregte Zustände der Ionen und führen zu spontanen Emissionen, die mit einem Übergang des betreffenden Ions wieder zurück in den Grundzustand verbunden sind [Ple96, Ple97].
Die wirksamste Methode die daraus resultierenden Fehler zu minimieren, liegt zuallererst in der Auswahl möglichst langlebiger Anregungszustände. Diese erhält man insbesondere bei Energieniveaus, die aus dem Grundzustand durch Hyperfein- oder Zeemannaufspaltung hervorgehen, spontane Emission kann für solche Übergänge dann praktisch vernachlässigt werden. Auch metastabile angeregte Zustände mit hohem Drehimpuls, die nur durch Emission von Quadrupol- oder sogar Oktupolstrahlung in den Grundzustand übergehen können, erwiesen sich als außerordentlich langlebig und damit als geeignet für einen Quantencomputer.

Wesentlich bedeutender ist die Dekohärenz für den gemeinsamen Vibrationszustand, der bei der überwiegenden Mehrzahl der Vorschläge für Quantengatter auf Ionenfallenbasis als Datenbus fungieren soll [Mon95a, Mon95b].
Für diese Dekohärenz des Vibrationszustandes gibt es zahlreiche Ursachen: Aufheizung durch elektromagnetische Strahlung [Wal93], Stöße mit Gasatomen, unstabile Potentiale der Elektroden [Win75a, Ang97]. Diese Einflüsse sind jedoch nicht fundamental, d.h. es besteht die Möglichkeit, durch fortgeschrittenere experimentelle Methoden diese Probleme beherrschbar zu machen.
Dennoch muß man feststellen, daß derzeit zwar einzelne auf internen elektronischen Zuständen basierende Qubits über sehr lange Zeit gespeichert werden können, ein aus mehreren verschränkten Ionen bestehender, komplizierter Superpositionszustand in einer linearen Falle, wie er für eine Quantenrechnung notwendig wäre, aber bislang nicht gelungen ist.
Folgerichtig haben die gegenwärtigen Forschungsaktivitäten vor allem auch die Lösung des "Datenbus-Problems" zum Ziel. Hierzu wurden bereits mehrere Konzepte entworfen, deren Umsetzung allerdings bislang nicht erreicht wurde [Sch98, Poy97, Kin98, Jam98b]. Einen beachtlichen Fortschritt stellt hier das NIST- Experiment mit zwei eingefangenen Beryllium - Ionen dar, bei dem eine Verschränkung über Relativbewegungen der beiden Ionen herbeigeführt wird.

Zusammenfassend läßt sich sagen, daß obwohl diese Technik scheinbar auf überschaubaren physikalischen Prinzipien beruht, die experimentellen Schwierigkeiten nicht unbeträchtlich sind. Die Dekohärenzzeiten solcher Systeme liegen derzeit im Bereich von Millisekunden. Dies ist allenfalls zur Durchführung von sehr einfachen Rechenoperationen, basierend auf der Verwendung von weniger als 10 Qubits, ausreichend. Um jedoch in ernsthafte Konkurrenz zu klassischen Computern treten zu können sind mindestens 100 Qubit große Rechenwerke notwendig.
Die Verschränkung von zwei Ionen in einer Falle ist vor kurzem erstmals gelungen [Tur98]. Um ein Gatter von noch mehr Ionen experimentell realisieren zu können, ist, wie bereits angesprochen, der Wechsel auf lineare Ionenfallen notwendig. Die Speicherung von einigen zehn Ionen in einer linearen Falle stellt heute kein Problem mehr dar, die Demonstration von verschränkten Zuständen in linearen Fallen steht allerdings noch aus.

Ob die Technik der Ionenfalle der richtige Weg zu einem anwendbaren kommerziellen Quantencomputer ist, darf aufgrund des beträchtlichen apparativen Aufwands, der für die Realisierung selbst einfacher Quantenschaltung notwendig ist, bezweifelt werden. Da es sich bei den Ionenfallen aber um physikalisch sehr reine Systeme handelt, wäre die Realisierung eines aus ca. zehn Ionen bestehenden Quantengatters zum genaueren Verständnis der relevanten Mechanismen und zur ersten experimentellen Durchführung etwas komplexerer logischer Operationen und Fehlerkorrekturmechanismen von sehr hohem Wert. Andere, beispielsweise auf Festkörpern basierende Ansätze (Kap. **5.5.8 - 5.5.10**) könnten dann auf den Resultaten solcher Funktionsmodelle aufbauen. Gerade für die Realisierung solcher Funktionsmodelle stellt die Ionenfalle derzeit das am weitesten fortgeschrittene experimentelle Konzept und eine solide Basis für zukünftige Weiterentwicklungen dar.
Der wesentliche Vorteil der Ionenfalle ist die Tatsache, daß derzeit keine fundamentalen Probleme einer Verwirklichung dieses Konzepts entgegenstehen und bei nur hinreichend konsequenter Weiterentwicklung der vorhandenen Verfahren in absehbarer Zeit vorzeigbare Ergebnisse möglich sein sollten.

5.5.3 Kernspinresonanz (NMR)

Zu den jüngsten Techniken, die eine mögliche Realisierung eines Quantenrechenwerks versprechen, zählt die Kernspinresonanz (NMR) [Cor97, Ger97, Cor98]. Die NMR wird seit langem als zuverlässige Analysemethode vor allem in Chemie und Medizin eingesetzt. Entsprechend weit entwickelt sind die technische Performance wie auch das zugehörige Fachwissen auf diesem Gebiet. Dennoch entstand erst 1996 die Idee, Kernspinresonanz zur Realisierung der elementaren Operationen eines Quantencomputers heranzuziehen. Der prinzipielle Unterschied zu anderen Vorgehensweisen liegt bei dieser Technik darin, daß nicht ein einzelnes Quantengatter manipuliert wird, sondern jedes Molekül einer flüssigen Probe als ein solches Register fungiert.
Durch diese Vorgehensweise vermeidet man es, mit hohem Aufwand einzelne Teilchen, wie etwa in der Ionenfalle, gezielt in bestimmten, niederenergetischen Zuständen präparieren zu müssen. Dadurch, daß man eine sehr große Zahl von Molekülen zur Verfügung hat, die, in Abhängigkeit von der Temperatur, einer bestimmten statistischen Verteilung folgend sehr viele unterschiedliche Zustände bevölkern, kann man damit rechnen, daß der benötigte Ausgangszustand ebenfalls von einer endlichen Anzahl der Moleküle in der Flüssigkeit angenommen wird. Es besteht in diesem Sinne eine Analogie zum DNA-Computer mit dem Unterschied, daß beim NMR-Quantenrechner nur das Problem der Präparation durch Heranziehen einer großen Zahl von Molekülen gelöst wird, während es beim DNA-Computer die Rechnung selbst ist, die auf diese Weise durchgeführt wird. Dennoch ergeben sich für beide Techniken aufgrund dieser Vorgehensweise relativ starre Begrenzungen hinsichtlich der prinzipiellen maximalen Rechenkapazität.

Zur Erleichterung des Verständnisses des NMR-basierten Quantencomputers soll kurz die Funktionsweise der Kernspinresonanz beschrieben werden [Ern94].
Die NMR mißt die magnetischen Eigenschaften der Atomkerne von Molekülen. Das magnetische Moment des Kerns wird über seine Zusammensetzung aus den Nukleonen (Protonen und Neutronen) bestimmt. In einem äußeren Magnetfeld ergeben sich dann, je nach der relativen Ausrichtung des magnetischen Moments, unterschiedliche quantisierte Energiezustände.

Bestrahlt man die Kerne mit elektromagnetischen Wellen, so kann man Übergänge zwischen verschiedenen Energieniveaus induzieren (Abb. 12), sofern die Energie des eingestrahlten Photons der Energiedifferenz zwischen zwei Niveaus entspricht und die Drehimpulserhaltung gewährleistet ist (erlaubte Übergänge). Die eingestrahlten elektromagnetischen Wellen würden beim Durchgang durch die Probe also eine Schwächung erfahren die sich experimentell nachweisen läßt. Der von der Probe in andere Richtungen gestreute Anteil der Strahlung wird demzufolge im Resonanzfall maximal.

Da nun selbst kleinste Verschiebungen der Lage dieser Energieniveaus auch durch sehr schwache Wechselwirkungen, sowohl durch die Elektronen der benachbarten Atome im Molekül, als auch durch die noch schwächere Wechselwirkung mit benachbarten Atomkernen, mit der Methode der Absorption von Radiowellen immer noch meßbar sind, eignet sich die NMR hervorragend zur Ermittlung chemischer Strukturen oder auch in der Medizin zur Bildgenerierung von Gewebebereichen, die bestimmte Substanzen enthalten, die mit NMR nachgewiesen werden können.

Einflüsse durch Atome aus benachbarten Molekülen in der flüssigen Probe können vernachlässigt werden, da sich diese aufgrund der statistischen Bewegung der einzelnen Moleküle in guter Näherung wegmitteln.

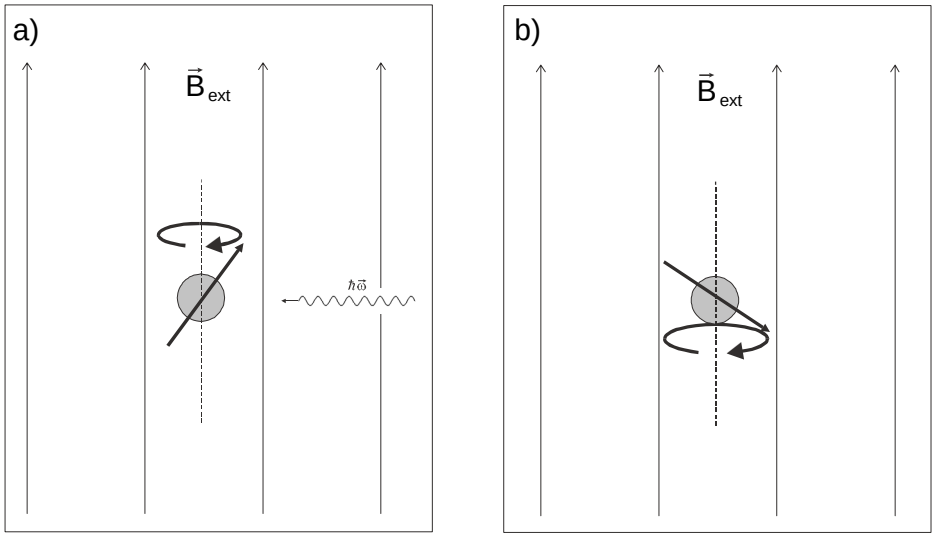


Abb. 12: Grundprinzip der NMR: Das magnetische Moment eines Atomkerns rotiert in einem externen Magnetfeld (B). Es sind quantenmechanisch jedoch nur bestimmte Rotationszustände erlaubt. Strahlt man elektromagnetische Wellen (Photonen) ein, so kommt es zu Übergängen zwischen solchen erlaubten Rotationszuständen, wenn die Energiedifferenz der Zustände gerade der Energie eines Photons entspricht, wobei noch zusätzliche Bedingungen erfüllt sein müssen. Der Kern ändert nach Absorption des Photons dann seinen Zustand. Makroskopisch macht sich dies bemerkbar durch die Schwächung der eingestrahlten elektromagnetischen Pulse beim Durchgang durch die Probe.

Bei der Nutzung der NMR für eine Quantenrechnung bedient man sich der quantisierten Energiezustände der Kernspins im externen Magnetfeld und der Superposition dieser Zustände. Zwei magnetische Niveaus eines Kerns würden dann in diesem Fall ein Qubit definieren. Eine Verschränkung mehrerer Qubits erfolgt innerhalb eines Moleküls über eine direkte magnetische Wechselwirkung zwischen den Atomkernen dieses Moleküls. Die Anzahl der Qubits des gesamten Quantenprozessors wird dann durch die Zahl der NMR-tauglichen Atome im vorliegenden Molekül festgelegt (z.B. H, C^{13}).
Die Kernspins sind in einem solchen Molekül in sehr guter Weise von störenden Einflüssen aus der Umgebung abgeschirmt. Man beobachtet daher in der NMR Kohärenzzeiten in der Größenordnung von Sekunden.
Durch die unterschiedlichen Positionen der Atome im Molekül und die daraus resultierende unterschiedliche Beeinflussung der Kernspins durch die Umgebung, können über eine Feinabstimmung der Radioeinstrahlung gezielt nur bestimmte Atome im Molekül adressiert und somit für eine Quantenrechnung präpariert werden [Bar95c, Llo95, Vin95b]. Die Frequenzabstimmung ersetzt also die räumliche Fokussierung der eingestrahlten Wellen, die bei Kernabständen von nur wenigen Ångström derzeit ohnehin nicht realisierbar wäre.
Im Unterschied zur Ionenfalle läuft der Datenaustausch zwischen den unterschiedlichen Kernspins im Molekül über eine direkte Wechselwirkung der Spins, man benötigt also keinen zusätzlichen quantenmechanischen Zustand als Daten-Bus.

Eigentlich sollte nun die Durchführung einer Quantenrechnung keine Probleme bereiten, jedoch erweist sich der Hauptvorteil der NMR, einfache Präparation durch massive Redundanz, auch als ein schwerwiegender Nachteil, denn bei Zimmertemperatur besetzen die Kernspins der Moleküle entsprechend der Boltzmann-Verteilung eine große Anzahl von Energiezuständen in beinahe gleicher Weise. Es liegt also kein reiner Grundzustand vor, wie bei der Ionenfalle, sondern man muß unter der Vielzahl der in der Probe vorhandenen Moleküle experimentell diejenigen erfassen können, die sich in Zuständen befinden, die für die Quantenrechnung geeignet sind.
Die Wahrscheinlichkeit, das dieses der Fall ist nimmt nun mit dem Komplexitätsgrad des quantenmechanischen Zustand ab, so daß ab etwa 70 Qubit sich in einer Probe von einigen Gramm im Zeitmittel überhaupt kein Molekül mehr im vorgesehenen Ausgangszustand aufhält, geschweige denn experimentell nachweisbar wäre [War97]. Die Raumtemperatur-

NMR ist also wie der DNA-Computer letztlich dadurch beschränkt, daß man die Probenabmessungen nicht beliebig groß wählen kann.
Für einfache Demonstrationsversuche mit wenigen Qubits ist die NMR allerdings sehr gut geeignet.

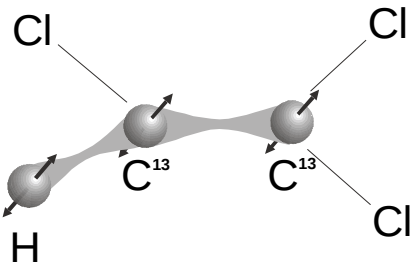


Abb. 13: Durch die Verschränkung dreier Kernspins konnten mit der NMR bei Benutzung des Trichloräthylen-moleküls bereits ein einfaches Quantengatter bestehend aus drei Qubits realisiert werden. Die Verschränkung erfolgt über die magnetischen Dipolmomente der Kerne, weshalb anstelle des natürlichen C^{12}- Kohlenstoff-isotops auf das C^{13} zurückgegriffen werden muß. Die beiden Kohlenstoffkerne können anhand einer gering-fügigen Energieverschiebung der Spinzustände unterschieden werden, die aus der unterschiedlichen elektronischen Umgebung der beiden Atome herrührt.

Die Verwendung von Molekülen mit bis zu zehn NMR-tauglichen Atomen ist durchaus denkbar. Die Präparation dreier verschränkter Qubits wurde an einem Trichlorethylen (C_2HCl_3)-Molekül bereits demonstriert (Abb. 13, [Laf97]). Einfachste Algorithmen konnten auf Basis zweier Qubits durchgeführt werden [Chu98, Jon98]. Als Moleküle wurden hierbei Chloroform und Cytosin benutzt. Damit übertrifft die NMR in diesem Punkt die Ionenfallen-technik, mit der die Verschränkung dreier Qubits erst später gelungen ist.

5.5.4 Josephson-Junctions

Josephson Junctions sind Supraleiter, die durch eine sehr kleine Barriere voneinander getrennt sind. Diese Barriere ist so dimensioniert, daß klassisch kein Strom mehr durch sie hindurch fließen kann, quantenmechanisch aber aufgrund des Tunneleffekts immer noch die Ladungsträger der Supraleitung (sogenannte Cooperpaare, die aus zwei gekoppelten Elektronen entstehen) auf die andere Seite gelangen können. Diese Verbindung ermöglicht also eine quantenmechanische (weil supraleitende) Kopplung der beiden Supraleiter.
Die Anzahl der Cooper-Paare in den beiden supraleitenden Bereichen kann durch eine geeignet gewählte externe elektronische Regelung festgelegt werden [Maa91a, Maa91b, Tuo92, Sie96]. Stellt man die Bedingungen so ein, daß in jedem Bereich eine ungerade Anzahl von Elektronen vorhanden ist, so kann man mit Hilfe der Tunnelbarriere folgendermaßen einen Superpositionszustand und damit ein Qubit erzeugen:
Entfernt man die Barriere, so bilden die beiden Elektronen ein Cooper-Paar, isoliert man die Bereiche vollständig voneinander, ist die Cooperpaarbildung verhindert. Es läßt sich also nun durch gezielte Variation der Tunnelbarriere ein Zustand herbeiführen, bei dem die Wahrscheinlichkeit der Paarbildung gerade 50% beträgt. Man hätte dann eine Superposition zwischen zwei Niveaus der gesamten supraleitenden Anordnung (also beide Bereiche zusammengenommen) vorliegen, die sich um ein Cooperpaar unterscheiden [Shn97].
Für ein ganzes Quantenregister müssen nun solche einzelnen Josephson Junctions nochmals untereinander gekoppelt werden.

Vor kurzem ist die experimentelle Realisierung eines Qubits in einer Josephson-Anordnung erstmals gezeigt worden [Nak97, Nak99].
Im Experiment von Nakamura et al. wurde eine supraleitende Insel mit einem ebenfalls supraleitenden Reservoir zu einer Josephson-Verbindung gekoppelt (Abb. 14). Bekanntermaßen stellen supraleitende Zustände makroskopische Quantenphänomene dar. Die zunächst getrennten Wellenfunktionen der Zustände der Insel und des Reservoirs haben an der Josephson-Verbindung eine bestimmte Phasenbeziehung. Zwischen der Phasendifferenz an dieser Verbindung und der Anzahl der supraleitenden Ladungsträger (Cooper-Paare) innerhalb der supraleitenden Insel besteht in analoger Weise zur Ort-Impuls-Beziehung eine Heisenbergsche Unschärferelation.

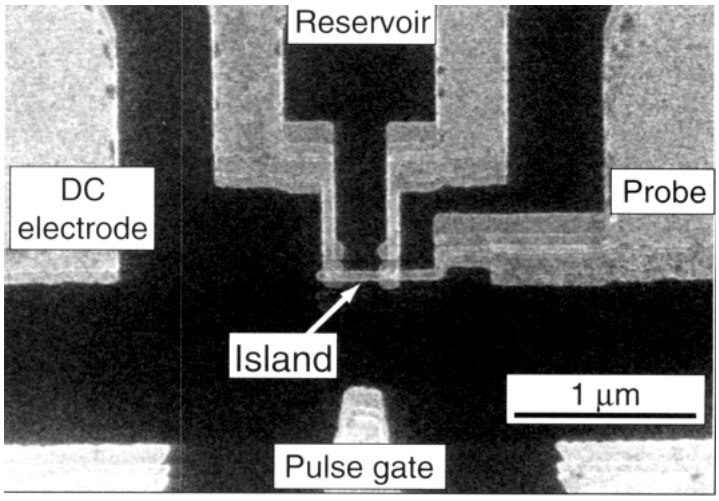


Abb.14: Josephson-Junction, gebildet durch eine sehr kleine Insel (ca. 100 nm) und ein makroskopisches Reservoir. Beide Domänen werden bei Abkühlen (30 mK) supraleitend. Der Quantenzustand, der die Anzahl der supraleitenden Ladungsträger (Cooper-Paar) beschreibt kann in einer solchen Struktur einen Superpositionszustand annehmen, der als Qubit betrachtet werden kann (Abb. aus [Nak99]).

Bei einer hinreichend kleinen Inselstruktur kann diese Unschärfe bezüglich der Anzahl der Cooperpaare zum Tunneln kleinster Ladungen bis hin zu einzelnen Cooper-Paaren führen. Nakamura et al. konnten zeigen, daß sich in gezielter Weise ein Zustand präparieren läßt, bei dem ein einzelnes Cooper-Paar zwischen dem Reservoir und der Insel hin und her oszilliert. Diese Oszillation ist dabei wiederum nicht als eine physikalische Bewegung der Ladungsträger zu verstehen, sondern als ein ein quantenmechanischer Interferenzeffekt. Das System befindet sich damit in einem Superpositionszustand zwischen zwei unterschiedlichen Ladungsniveaus der supraleitenden Insel, die sich um genau ein Cooper-Paar unterscheiden. Dieser Superpositionszustand ist in völlig analoger Weise als Qubit zu betrachten wie etwa die verschränkten Ionen in einer Falle oder die wechselwirkenden Kernspins der NMR.
Damit stellen die Josephson-Junctions den bislang einzigen bereits im Experimentierstadium befindlichen Ansatz für einen festkörperbasierten Quantencomputer dar. Der nächste Schritt ist nun die Verschränkung zweier Qubits und die Demonstration einfacher quantenlogischer Operationen (z.B. C-NOT).

5.5.5 Weitere Entwürfe für die Realisierung eines Quantencomputers

Für die folgenden Vorschläge für die praktische Realisierung von Quantencomputern ist die experimentelle Realisierung zumindest eines Qubits bislang nicht gelungen. Es existieren also lediglich theoretische Überlegungen und Abschätzungen inwieweit diese Ansätze für die Verwirklichung von Quantenschaltungen geeignet sind. Allerdings besteht die berechtigte Annahme, daß insbesondere die festkörperbasierten Konzepte die realistischsten Chancen auf eine technische Umsetzung haben, da die Nutzung der NMR oder der Ionenfalle für große Quantengatter als wenig praktikabel erscheint.

5.5.6 Elektronenspinresonanz (ESR)

Das primäre Problem des Ansatzes, einen Quantencomputer auf Grundlage der NMR realisieren zu wollen, basiert auf der unzureichenden Besetzung der Niveaus, die zur eigentlichen, kontrollierten Quantenrechnnung herangezogen werden.
Für große Quantenregister von etwa 100 Qubits ist eine sehr viel höhere Polarisation des Systems notwendig als dies mit NMR bei Raumtemperatur erreicht werden kann.
Eine Alternative bietet hier die Elektronenspinresonanz. Kommerzielle Spektrometer, betrieben bei Temperaturen von etwa einem Kelvin und bei Feldern von drei Tesla, stellen eine hinreichend vollständige Besetzung des Grundzustandes als Ausgangszustand für eine Rechnung, auch mit hohen Qubitzahlen, sicher.
Die Kohärenzzeit der Tieftemperatur ESR ist deutlich höher als bei der gewöhnlichen Raumtemperatur-NMR [Bar98].
Experimentelle Realisierungen eines ESR-Computers stehen allerdings noch aus. Bisher wurden lediglich Abschätzungen vorgenommen, inwiefern die Verwendung von ESR prinzipielle Vorteile mit sich bringt.

5.5.7 NMR im Festkörper

Bloßes Abkühlen ist nicht geeignet die Probleme der NMR zu lösen, da die flüssige Probe bei geringen Temperaturen amorph erstarrt und damit eine Verbreiterung des Signals auftritt, wie sie beispielsweise auch für NMR an Pulvermaterialien typisch ist [Sli80]. Diese Verbreiterung könnte verhindert werden, wenn die Erstarrung in Form eines Einkristalls stattfinden würde, dies ist jedoch sehr unwahrscheinlich und kaum zu kontrollieren. Besser erscheint es, von vornherein eine einkristalline Struktur als Ausgangspunkt für NMR bei tiefen Temperaturen zu wählen. In einer solchen erhält man ein für die Realisierung eines Quantenprozessors genügend starkes und ausreichend schmales NMR-Signal [Wie98b].
Über das Einbringen einer Verunreinigung (Dotierung), bei der ein Kern mit verschwindendem Drehimpuls durch einen solchen mit Spin ersetzt wird, kann man eine Art Schnittstelle erzeugen, mit deren Hilfe Informationen in das Quantenregister übertragen werden können. Dieses eigentliche Register würde dann aus dem Untergitter bestehen, das die künstliche Fehlstelle umgibt und bis zum nächstgelegenen Dotierungsatom reicht (Die Dotierungsdichte definiert also die Dichte und Größe der elementaren Quantengatter). In diesem Untergitter würde die eigentliche Quantenrechnung ablaufen. Informationen werden von und zu der Schnittstelle mit Hilfe des sogenannten Entanglement Swapping (vgl. Kapitel **6.2**) transportiert. Dies bedeutet, daß eine Verschränkung zwischen zwei Qubits durch eine geeignet gewählte Messung an bestimmter Stelle auf ein anderes Teilchenpaar übertragen werden kann [Llo93, Bar95b]. Allerdings ist das Entanglement Swapping bislang experimentell nicht verifiziert. Derzeitige Versuche zielen darauf ab, diesen Effekt mit verschränkten Photonen zu demonstrieren. Wie ein derartiger Mechanismus aber in einem Festkörper praktisch umgesetzt werden könnte, ist derzeit noch völlig offen.

5.5.8 Magnetresonanzspektroskopie an einzelnen Spins

Der wesentlichste Vorteil der NMR im Vergleich zu allen anderen experimentellen Techniken liegt in der sehr langen Kohärenzzeit. Dies beruht auf der sehr guten Abschirmung des Kernspin von seiner Umgebung. Die relevanten Wechselwirkungen, die für die Dekohärenz die wesentlichsten Beiträge liefern, verlieren mit zunehmender Distanz sehr schnell an Stärke,

so daß bei den üblichen Abständen wie sie zwischen den Kernen unterschiedlicher Moleküle auftreten, nur sehr geringe Störungen zu beobachten sind.
Das unvorteilhafte Signal zu Rausch Verhältnis der Raumtemperatur-NMR, das aus der statistische Messung und der damit verbundenen Mittelung über eine Vielzahl unterschiedlich besetzter Zustände resultiert, stellt den wesentlichen Nachteil dieses Verfahrens dar.
Dieses Problem läßt sich jedoch vermeiden, wenn es gelingt, den Spin eines einzelnen Kerns gezielt zu präparieren und zu messen [Wie98a]. Im Prinzip hätte man dann wieder eine ähnliche Situation vorliegen, wie bei der Ionenfalle, nur daß man nicht den elektronischen Zustand eines Atoms, sondern den Kernspin zu manipulieren hätte und auch nicht auf den experimentell problematischen kollektiven Vibrationszustand als Datenbus angewiesen wäre, mit dem Vorteil deutlich längerer Kohärenzzeiten.
Der Nachteil einer Nutzung einzelner Kernspins liegt im extrem schwierigen Nachweis der entsprechenden magnetischen Kernmomente [Vin95a]. Die Einzelspindetektion wurde bereits mit den Methoden der optischen Spektroskopie versucht [Wra95, Gru97]. Für Kernspins ist insbesondere die Magnetresonanzkraftmikroskopie eine interessante neue Nachweismethode [Rug92, Rug94, Sid95]. Mit den bislang zur Verfügung stehenden Mitteln ist die Messung eines einzelnen Kernspins jedoch noch nicht gelungen.
In diesem Zusammenhang wurde die Verbringung eines einzelnen (geladenen) Moleküls in eine Ionenfalle vorgeschlagen. Hier wären Korrekturen zu den dort herrschenden sehr kleinen elektromagnetischen Kräften durch einen veränderten Kernspin nachweisbar. Zusätzlich hätte man eine nochmals verbesserte Isolation des Systems von der Umgebung.
Kleinere Moleküle konnten bereits in Ionenfallen gespeichert werden [Deh67, Deh69, DiF94, Wue59].

5.5.9 Quantenrechnung in Halbleiter Quanten-Dots

Schwerwiegendstes Problem bei dem Versuch einen Quantencomputer auf Festkörperbasis zu realisieren, ist die Dekohärenz. Aufgrund von Elektron-Phonon-Streuprozessen, die die primäre Ursache für Dekohärenz in Halbleitern darstellen [Sha96], aber auch Elektron-Elektron-Wechselwirkungen, sind die Kohärenzzeiten in solchen Systemen naturgemäß sehr gering.

In sogenannten Quanten-Dots unterscheiden sich die elektronischen Zustände allerdings von denen eines gewöhnlichen Halbleiters. Als Quantendots bezeichnet man kleine Inseln bestehend aus wenigen Atomen. In diesen Inseln haben die Elektronen eine sehr viel geringere, in allen drei Raumrichtungen eingeschränkte Beweglichkeit als im ausgedehnten Festkörper. Durch diese Einschränkungen bilden sich diskrete elektronische Zustände aus, ähnlich den quantisierten Elektronenbahnen im Atom.

Für spezielle Anordnungen von Quantendots konnte gezeigt werden, daß sich die durch Elektron-Phonon Streuung bedingte Dekohärenz stark unterdrücken läßt. Idee hierbei ist es, die unterschiedliche Wirkung des Umgebungsrauschens auf verschiedene quantenmechanische Zustände der Anordnung in der Weise zu nutzen, daß versucht wird, nur diejenigen quantenmechanischen Zustände des Systems zu verwenden, die durch das Rauschen nur schwach gestört werden und mit Hilfe von Fehlerkorrekturmechanismen kompensiert werden können [Zan98]. Voraussetzung hierfür ist daher, daß das Rauschen nicht vollständig statistisch erfolgt, sondern ebenfalls in gewisser Weise kohärent abläuft, also auf unterschiedliche Zustände unterschiedlich stark wirkt. Man kann durch Ausnutzung dieser Rauscheigenschaften theoretisch zu Kohärenzzeiten kommen, die vergleichbar sind mit den Zeiten der Femtosekundenlaserspektroskopie. Es liegt dann also eine experimentelle Adressierung und Manipulationen dieser Zustände prinzipiell im Bereich des technisch machbaren [Heb95].

Eine alternative Methode der Umsetzung eines Quantencomputers mit Hilfe von Quantendots beruht auf dem Vorschlag, gezielt die Tunnelbarriere zwischen Einzelelektronenquantendots zu manipulieren [Los97]. Eine solche Manipulation konnte experimentell bereits vorgenommen werden [Liv96, Wau96, Wau95].

Ist die Tunnelbarriere hoch eingestellt, so sind die Qubit-Zustände der einzelnen Quantendots voneinander isoliert. Bei niedriger Spannung an der Barriere hingegen findet eine Kopplung zwischen den Elektronenspins statt. Man hätte hier also eine sehr elegante Möglichkeit zur Verfügung, den Informationstransfer zwischen den einzelnen Qubits zu manipulieren.

Es muß allerdings beachtet werden, daß die Realisierung selbst eines Demonstrationsexperiments mit wenigen Qubits noch in weiter Ferne liegt. Die Probleme durch Dekohärenz in Festkörpern sind enorm und zur Verwirklichung des vorgeschlagenen Konzepts müssen insbesondere auch im Bereich der Herstellung möglichst perfekter Anordnungen von Quantendots noch erhebliche Fortschritte gemacht werden. Es ist hier also speziell auch die Nanotechnologie gefordert, die notwendigen Vorrichtungen zur Verfügung zu stellen.

Ein interessanter Schritt auf dem Weg zur Beherrschung von Quantendots gelang kürzlich mit der Methode der kohärenten optischen Wechselwirkung [Bon98]. Mit dieser Technik konnte ein angeregter Zustand eines Quantendots gezielt manipuliert werden. Die Kohärenzzeit dieses Zustandes betrug 40 ps ($4 \cdot 10^{-11}$ s). Dies ist zwar deutlich länger als in einem ausgedehnten (bulk) Halbleiter (1 ps), aber immer noch sehr viel weniger als bei atomaren Systemen. Jedoch konnten auch bereits verhältnismäßig lange Kohärenzzeiten von Elektronenspins in Halbleitern beobachtet werden [Kik97].

5.5.10 Quanten-Hall-Systeme

Ein weiterer Vorschlag für einen Festkörper-Quantencomputer beruht auf Hyperfein-Wechselwirkungen zwischen Leitungselektronen und Kernspins in einem zweidimensionalen Elektronensystem bei dem sich das Elektronengas im sogenannten Quanten-Halleffekt-Regime befindet [Kli80, Tsu82]. In diesen speziellen Zustand der Materie, in dem wiederum fundamentale quantenmechanische Phänomene eine tragende Rolle spielen, gelangt man bei sehr tiefen Temperaturen und hohen Magnetfeldern. Die Dynamik der Kernspins wird dann dominiert von sogenannten kohärenten Austauschprozessen die von den Elektronen getragen werden [Bye95, Vag95].
Die praktische Realisierbarkeit eines solchen Systems liegt gleichwohl noch in weiter Ferne. Die Art und Weise, wie in einer solchen Anordnung die Kernspins einzeln adressiert werden könnten, ist bislang weitgehend unklar.

5.5.11 Atomresonatoren

Es ist heute nicht nur möglich Ionen in einer Falle zu speichern, sondern es ist mittlerweile auch Routine, Atomfallen zu bauen mit denen neutrale Atome eingefangen werden können.
Sowohl Atome als auch Ionen können in speziell ausgelegten Fallen kontrolliert an elektromagnetische Feldzustände gekoppelt werden [Bar95b, Bar94, Bru94, Ber94]. Dies liegt daran, daß man die Fallen so konstruieren kann, daß sich ähnlich wie in Mikrowellen - Hohlleitern nur bestimmte elektromagnetische Moden ausbilden. Sind aber bestimmte elektromagnetische

Übergänge des eingefangenen Atoms mit elektromagnetischen Moden verbunden, die nicht kompatibel mit der Geometrie des Resonators sind, so sind auch die entsprechenden Übergänge unterdrückt [Pur46, Hin].
Durch geschickte Wahl des Resonatordesigns läßt sich sogar erreichen, daß überhaupt nur ein oder zwei Moden mit dem im Resonator befindlichen Atom wechselwirken können.
Solche diskreten elektromagnetischen Moden können zur Verschränkung verschiedener Atome oder Ionen benutzt werden [Pel95]. Der Datenbus für einen Quantenprozessor aus mehreren Atomen ist dann kein kollektiver Vibrationszustand mehr, sondern ein erlaubter elektromagnetischer Zustand des Resonators. Das im Resonator befindliche diskrete elektromagnetische Feld kann an den gleichen Übergang verschiedener Atome ankoppeln und auf diese Weise eine Superposition der Anregungszustände unterschiedlicher Atome herbeiführen, was eine Verschränkung der Atome bewirkt.
Nach diesem Prinzip konnten bereits EPR-Atompaare präpariert werden. Diese befanden sich allerdings nicht in einer Falle, sondern durchflogen in kurzem Abstand einen Resonator und wechselwirkten jeweils mit ihren gleichen elektronischen Niveaus mit demselben elektromagnetischen Strahlungsfeld des Resonators, so daß hierdurch eine Verschränkung der Atome selbst zustande kam [Hag97].
Es ist aber auch möglich die Information, die im Lichtfeld des Resonators steckt, mittels eines optischen Signals auf einen anderen, ev. weit entfernten Resonator zu übertragen [Cir97]. Damit wäre die Verschränkung von massiven Teilchen möglich, die sich an ganz verschiedenen Orten befinden, d.h. die Ionen oder Atome als Grundelemente bzw. Qubits eines Quantenprozessors müßten sich nicht räumlich eng beieinander befinden.
Die Verbindung kann dabei sogar auf eine Weise erfolgen, bei der sich die Resonatoren in einem sogenannten dunklen Zustand befinden, d.h. obwohl über das elektromagnetische Feld Informationen ausgetauscht werden, befindet sich im Idealfall niemals ein Photon im Resonator [Enk98]. Es ist sogar möglich, die gesamte Übertragung einschließlich des Lichtfeldes so zu gestalten, daß der Photonenzustand nicht voll besetzt ist, also weniger als ein Photon zur Übertragung verwendet wird. Somit genügt eine derartige Quantenkommunikation mit dunklen Zuständen auch den Prinzipien der Quantenkryptographie.
Größtes experimentelles Hindernis ist beim Resonatorkonzept ebenfalls die Dekohärenz. Die Resonatoren haben nach wie vor zu hohe Strahlungsverluste um die Kriterien erfüllen zu können, die für die Durchführung komplizierterer Quantenalgorithmen notwendig wären. Da dieser Ansatz außerdem ebenfalls auf der Speicherung von Ionen oder Atomen beruht, ist er

auch von den diesbezüglichen experimentellen Einschränkungen betroffen. Die Lokalisierung eines einzelnen Atoms erweist sich dabei als noch komplizierter als die Speicherung eines Ions. Letztlich bedeutet dies, daß der resonatorgestützte Quantencomputer experimentell noch aufwendiger zu realisieren ist, als das gewöhnliche Ionenfallenprinzip. Mit schnellen Fortschritten kann hier deshalb zur Zeit nicht gerechnet werden. Zum Verständnis des Phänomens der Verschränktheit, insbesondere zwischen massiven Teilchen und elektromagnetischen Feldern sowie zur Untersuchung der Dekohärenz können Resonatorexperimente allerdings wesentlich beitragen.

5.5.12 Gefangene Atome in einem optischen Gitter

Diese Vorgehensweise besitzt eine gewisse Analogie zu der Methode der Atomfallen. Man benutzt zur Lokalisierung der neutralen Atome ein mehrdimensionales Kreuzgitter aus Laserstrahlen [Fri98]. Diese bilden für die Atome ein periodisches Potential in dessen Minima sich die Atome dann jeweils anordnen. Die Wechselwirkung mit dem Licht erfolgt dabei über das Dipolmoment der Atome.
Da Kräfte, die das Lichtfeld auf die Atome ausübt außerordentlich gering sind, müssen die Atome extrem abgekühlt werden, man spricht hier von ultrakalten Atomen, damit sie nicht aufgrund ihrer thermischen Energie aus dem Lichtpotentialtopf entweichen.
Durch die bloße Besetzung der Gitterplätze erhält man allerdings noch keine Verschränkung der Atome, da diese für eine direkte kohärente Wechselwirkung zunächst zu weit voneinander entfernt sind.
Durch Verändern des Lichtgitters kann man die Atome jedoch gegeneinander verschieben [Jak98a]. Steuert man diese Verschiebung so, daß die Atome übereinander zu liegen kommen, so stoßen die Atome in kohärenter Weise miteinander, d.h. sie können durch diesen Stoßprozeß miteinander verschränkt werden. Da dies in kontrollierter Weise möglich ist, kann man mit einer solchen Technik quantenlogische Operationen umsetzen [Jak98b].
Dieses Verfahren wurde jedoch noch nicht experimentell durchgeführt. Bislang wurden theoretische Untersuchungen bezüglich der Machbarkeit eines solchen Ansatzes durchgeführt, die praktische Realisierung wird vorbereitet [Bri99].

Fazit: Die Herstellung eines funktionierenden Quantencomputers steckt noch in der frühen Anfangsphase. Experimentelle Realisierungen der grundlegenden quantenlogischen Komponenten liegen bislang nur im Bereich der Ionenfallen, der NMR und der Josephson-Junctions vor. Es existieren zwar bereits eine Vielzahl von Vorschlägen für alternative Methoden, die praktischen Probleme einer experimentellen Umsetzung dürfen hierbei allerdings nicht unterschätzt werden.
Nichtsdestotrotz konnte bereits demonstriert werden, daß Verschränkung im Prinzip beherrschbar ist. Die Herausforderung besteht nun darin, die Systeme so hochzuskalieren, daß komplexe Aufgaben, die für die Anwendung interessant sind, berechnet werden können. Ob dies auf Grundlage der gegenwärtig untersuchten Technologien möglich sein wird, ist jedoch noch offen.

6 QUANTENKOMMUNIKATION

6.1 Quantenkryptographie

Kryptographieverfahren sind seit einiger Zeit Gegenstand heftiger kontroverser Diskussionen. Einerseits bereitet die Industriespionage vielen Unternehmen schwerwiegende Probleme, so daß ein Mindestmaß an Datensicherheit zur Sicherung der Marktstellung unerläßlich ist, andererseits wird von seiten staatlicher Stellen regelmäßig auf die Gefahren abhörsicherer krimineller Kommunikationslinien hingewiesen.
Unabhängig von den Vor- und Nachteilen des sicheren Datentransfers soll hier die Methode der Quantenkryptographie, die auf einer Idee Wiesners [Wie70] von 1970 basiert, erläutert werden.
Zum Vergleich wird zuerst eines der herkömmlichen, als sicher geltenden Verschlüsselungsverfahren (RSA), das auf einem mathematischen Prinzip beruht, beschrieben [Riv78]. Diese Methode findet bereits für die Datenübermittlung via Internet eine breite Anwendung und geriet vor allem in Zusammenhang mit US-Exportrestriktionen für kurze Zeit in den Blickpunkt der Öffentlichkeit. Es wird eine mögliche Schwäche dieses Systems benannt und dann die Verbesserung der Sicherheit mit der Methode der Quantenkryptographie dargestellt.

6.1.1 Klassische Verfahren

Bei klassischer Kryptographie wird ein Text mittels einer Übersetzungsvorschrift (ein Algorithmus) in eine Abfolge von Zahlen, Buchstaben oder Symbolen umgewandelt. Diese Übersetzungsvorschrift wird als Schlüssel bezeichnet. Ziel ist es, die Ermittelung des ursprünglichen Textes bei Nichtverfügbarkeit des Schlüssels so weit wie möglich zu erschweren. Die theoretische Möglichkeit dieses zu tun besteht allerdings immer, d.h. es kann nur versucht werden den praktischen Aufwand so weit wie möglich in die Höhe zu treiben. In diesem Sinne würde man ein Verfahren dann als sicher bezeichnen, wenn es selbst mit den schnellsten heute vorhandenen Rechner Jahre dauern würde, den Code zu brechen.

Bei gewöhnlichen Verschlüsselungsverfahren beruht die Sicherheit der übermittelten Daten also darauf, daß der Empfänger einen Schlüssel zur Verfügung hat, mit dem es ihm möglich ist, die empfangene Nachricht bei relativ geringem Rechenaufwand zu decodieren, ein potentieller Lauscher, der nicht im Besitz des Schlüssels ist, jedoch eine Entschlüsselung nur mit einem sehr hohen Rechenaufwand durchführen kann.

Eine weiter Erhöhung der Sicherheit erhält man für sogenannte „Public Key“-Verfahren, wie zum Beispiel die RSA (Rivest, Shamir, Adleman)-Methode [Riv78]. Die Vertraulichkeit wird hier dadurch gewährleistet, daß die Ver- und Entschlüsselung mit zwei verschiedenen, jedoch miteinander in Zusammenhang stehenden Schlüsseln durchgeführt wird. Nach einem Verfahren, daß auf der Multiplikation zweier großer Primzahlen basiert, werden zwei Schlüssel, ein öffentlicher und ein geheimer, generiert. Der öffentliche Schlüssel wird an alle diejenigen verschickt, von denen man eine geheime Botschaft zu erhalten wünscht. Unter Benutzung dieses öffentlichen Schlüssels kann dann jede Nachricht derart codiert werden, daß nur der Empfänger, der über den geheimen Schlüssel verfügt, die Botschaft decodieren kann. Die Sicherheit liegt hier darin begründet, daß die Umkehrung des auf dem öffentlichen Schlüssel basierenden Codierungsprozesses zwar möglich, aber mit einem ungeheuren Rechenaufwand verbunden ist, so daß derzeit existierende Computer damit überfordert wären. Konkret würde man heute eine 150stellige Zahl als mit gegenwärtig zur Verfügung stehenden Mitteln nicht bearbeitbar ansehen. Die Anzahl der Rechenoperationen, die zur Lösung des Problems notwendig ist, steigt dabei nach einem Exponentialgesetz in Bezug auf die zu faktorisierenden Zahl an [Leu93].

Die Sicherheit der Übertragung beruht hier also letztlich darauf, daß der eigentliche Schlüssel, der zur Decodierung benötigt wird, niemals den Ort des Empfängers verlassen muß.

Ein derzeitiger Schwachpunkt dieses Verfahrens liegt darin, daß kein mathematischer Beweis dafür vorliegt, daß es nicht doch einen Algorithmus gibt mit dem das Faktorisierungsproblem effizienter, bei einem nur polynomialen Anstieg des Rechenaufwands, gelöst werden kann. Das Auffinden eines solchen effizienten Algorithmus für die Faktorisierung würde alle auf RSA gestützten Kryptographieverfahren praktisch über Nacht entwerten.

Eine generelle Unsicherheit stellt das sogenannte "Man in the Middle"-Problem dar. Dabei setzt sich ein Lauscher zwischen die kommunizierenden Parteien und fängt jeweils die öffentlichen Schlüssel ab, um sie durch solche zu ersetzen, zu denen er selbst den geheimen Code besitzt.

Der Transport der Nachrichten vom Sender zum Lauscher fände also immer im Code des Lauschers statt. Für den Weitertransport zum eigentlichen Empfänger, kann der Lauscher die Nachricht dann wieder mit dem Originalschlüssel des Empfängers verschlüsseln, so daß dieser die Nachricht problemlos decodieren könnte und der Lauschangriff damit unbemerkt bliebe.
Einfacher gesagt liegt das Problem in der Unkenntnis der Identität des Empfängers begründet. Diese Unsicherheit haben alle Kryptographieverfahren gemein und ein kritischer Punkt ist daher immer die zweifelsfreie Identifizierung des Kommunikationspartners.
Grundsätzlich vorteilhaft ist es, den Schlüssel persönlich zu übergeben. Die Datensicherheit hängt empfindlich davon ab, wie zuverlässig man über die Identität des Empfängers Kenntnis besitzt. Am sichersten ist die persönliche Schlüsselübergabe an eine Person, die man bereits persönlich kennt, am unsichersten das Versenden über Email an jemanden, dem man nie zuvor begegnet ist. Je weniger Informationen einem hinsichtlich der Identität eines Adressaten zur Verfügung stehen, desto verwundbarer ist eine Kommunikationslinie in Bezug auf einen "Man in the Middle"-Angriff.

Ein weitere Verbesserung der Datensicherheit erhält man durch die Verwendung eines nicht kopierbaren Schlüssels. Der Besitz desselben würde dann garantieren, daß niemand sonst eine Nachricht decodieren kann. Umgekehrt würde die Tatsache, daß ein Lauscher über den Schlüssel verfügt bedeuten, daß der eigentliche Empfänger diesen nur verstümmelt vorliegen hat, so daß dieser die für ihn bestimmte Nachricht nicht erhalten würde und daraufhin das Abbrechen der Kommunikation oder den Wechsel des Übertragungskanals veranlassen könnte. Dies führt auf die Quantenkryptographie.

6.1.2 Grundprinzip der Quantenkryptographie

Diese Grundidee des nicht kopierbaren Schlüssels läßt sich mit Hilfe der Quantenmechanik realisieren [Ben92a].
Für einen beliebigen Quantenzustand gilt, daß er bei einer Messung in einen Eigenzustand überführt wird. Hat er sich vor der Messung nicht bereits in einem solchen Zustand befunden, so ist dies gleichbedeutend mit einer Veränderung des Zustands. Liegt außerdem keine Kenntnis darüber vor, wie der ursprüngliche Zustand präpariert wurde (in welcher Basis), so ist es durch das Meßergebnis allein nicht möglich, die gesamte Information, die zum

Wiederherstellen des vermessenen Zustandes notwendig wäre, zu erhalten. Das Meßergebnis ist also auch eine Projektion des tatsächlichen physikalischen Quantenobjekts auf die von der Meßanordnung vorgegebenen Bedingungen. Die Messung selbst liefert daher nur eine Information über das projizierte physikalische Objekt, nicht über den ursprünglichen Zustand Kennt man die Basis nicht, in welcher der zu vermessende Zustand präpariert wurde, so hat man keinerlei Möglichkeit, eine Manipulation des Objekts durch die Messung zu erkennen, und es ist daher auch nicht möglich eine Messung rückgängig zu machen.
Zwar könnte man meinen, daß durch mehrere verschiedene Messungen an einem Objekt genügend Informationen erhalten werden können, um daraus das gesamte Quantenobjekt zu rekonstruieren, dies ist jedoch nicht möglich. Vielmehr wird durch die erste Messung der Zustand des Meßobjekts verändert, so daß jede weitere Messung nur Informationen über den jetzt vorliegenden und nicht den ursprünglichen Zustand liefert.
Einen Ausweg aus diesem Dilemma würde die Möglichkeit bieten, an mehreren identischen Kopien des ursprünglichen Objekts jeweils einmalige Messungen der unterschiedlichen Parameter vorzunehmen, so daß man auf diese Weise zu der gesuchten Gesamtinformation käme.
Es gilt in der Quantenmechanik jedoch das damit zusammenhängende sogenannte No-Cloning-Theorem [Ben89, Woo82]. Dieses besagt, daß es grundsätzlich nicht möglich ist, einen unbekannten Quantenzustand zu duplizieren. Dieser relativ einfache Sachverhalt ist wiederum von fundamentaler Bedeutung, heißt dies doch, daß der Ausweg der Mehrfachmessung zur Ermittlung der vollständigen Information eines unbekannten Quantenzustands aufgrund eines Naturgesetzes nicht gangbar ist.
Könnte man also einen Quantenzustand mit einem Verschlüsselungscode identifizieren, dann würde dieser die oben genannte Forderung bezüglich der prinzipiellen Einmaligkeit bzw. Nichtkopierbarkeit erfüllen.

Eine physikalisch-technische Realisierung dieses Prinzips soll im folgenden kurz dargestellt werden.
Ein experimentell gut zugänglicher Quantenzustand ist beispielsweise die Polarisation von Licht.
Was versteht man unter Polarisation ?
Physikalisch ist Licht eine elektromagnetische Welle, die sich im Raum ausbreitet. Bei linear polarisiertem Licht ist das elektrische Feld der Welle dabei nicht rotationssymmetrisch bezüglich der Ausbreitungsrichtung, sondern maximal in einer bestimmten Polarisationsebene

und Null in einer senkrecht dazu stehenden Ebene. Das magnetische Feld steht senkrecht auf dem elektrischen, d.h. es ist maximal in der Nullebene des elektrischen Feldes und verschwindet in der Ebene des maximalen elektrischen Feldes. Die Schnittgerade zwischen den beiden Maximal- (oder Null-) Ebenen definiert dabei die Achse entlang der sich die Welle ausbreitet.

Die Polarisationsrichtung erhält man dann, nach Konvention, indem man durch die Ebene des maximalen elektrischen Feldes eine Gerade legt, die senkrecht auf der Ausbreitungsrichtung steht.

Dreht sich diese Polarisationsachse im Verlaufe der Ausbreitung, so spricht man von zirkular polarisiertem Licht, was hier jedoch weiter keine Rolle spielen soll.

Für linear polarisiertes Licht ist nun wichtig zu wissen, daß jeweils nur senkrecht aufeinanderstehende Polarisationsrichtungen gleichzeitig gemessen werden können. Das bedeutet, daß eine Meßanordnung, die die Polarisation in eine bestimmte Richtung (dies sei die z-Achse) ermittelt nur solche Zustände nicht verändert, deren Polarisation in die z-Richtung oder exakt senkrecht dazu gerichtet ist. Irgendwelche Zustände mit dazwischenliegenden Polarisationen würden durch die Messung verändert werden.

Möchte man mit solcherart polarisiertem Licht eine abhörsichere Übertragung realisieren, so muß noch sichergestellt werden, daß der gewählte Polarisationszustand tatsächlich auch physikalisch einmalig ist. Damit ist gemeint, daß es im Übertragungskanal nur ein Quantum (Photon) mit der gleichen Information geben darf, ansonsten könnte ein potentieller Lauscher zwei Photonen abfangen und mit Hilfe zweier Messungen den exakten Polarisationszustand ermitteln und diesen anschließend selbst präparieren und an den eigentlichen Empfänger der Nachricht weiterleiten, ohne daß dieser den Lauschangriff erkennen könnte.

Dazu muß darauf geachtet werden, daß man nicht bei der Präparation mehrere identische Zustände herstellt (was natürlich möglich ist, da der Quantenzustand demjenigen, der ihn erzeugt, bekannt ist). Man muß das Signal soweit minimieren, daß tatsächlich nur jeweils ein Lichtquant pro Informationseinheit (Bit) verwendet wird. Die Nachricht darf also zur Übertragung nur die mindestens notwendige Anzahl physikalischer Informationsträger (hier: Photonen) benutzen, da jedes, beispielsweise zur Verbesserung des Signal / Rausch - Verhältnisses vorhandene zusätzliche Lichtteilchen die Gefahr des unbemerkten Abhörens, durch die nicht feststellbare Entnahme überzähliger Photonen, erhöht. Für den Empfänger wäre der Lauschangriff dann immer schwerer zu entdecken, da er selbst ja immer noch die vollständige Nachricht erhielte.

Man erkennt hier also bereits die Notwendigkeit, daß die technische Realisierung einer derartigen Übertragung so dissipationsarm wie möglich zu erfolgen hat, um überhaupt mit einzelnen Photonen operieren zu können.
Ein technischen Problem dabei ist auch die Bereitstellung der notwendigen geringen Intensitäten. Es ist tatsächlich derzeit nicht möglich, kontrolliert einzelne Photonen zu einem bestimmten Zeitpunkt zu erzeugen. Daher wurde bei den bisherigen Quantenkryptographie-verfahren immer auf konventionelle Weise eine Lichtstrahl soweit abgeschwächt, daß man davon ausgehen konnte, daß sich im Mittel immer wesentlich weniger als ein Photon im Übertragungskanal aufhielt.
Derzeit ist von mehreren Gruppen der Bau einer Ein-Photonen-Quelle geplant [Rem98]. Dies wäre ein erheblicher Fortschritt für eine ganze Reihe von Experimenten, insbesondere auch mit verschränkten Photonenzuständen.

6.1.3 Codierung der Information mit Hilfe der Polarisation [Ben89, Ben92d, Ben92b]

Bei diesem Verfahren wird die Information in der Polarisation der Photonen codiert. Für die Polarisation von Photonen gelten ebensolche Unschärferelationen, wie für Ort und Impuls. Legt man die Polarisationsebene von Photonen mit Hilfe eines Polarisators fest, so bedeutet dies einen Eigenzustand bezüglich dieser Ebene und der darauf senkrecht stehenden. Die Polarisation in einer um 45° dazu geneigten Ebene ist jedoch entsprechend den Gesetzen der Quantenmechanik dann vollständig "unscharf", d.h. bei einer Präparation der Polarisation in Richtung der 0°-Achse beträgt die Wahrscheinlichkeit einer Detektion in den beiden um 45° und um 135° dagegen geneigten Ebenen jeweils 50% und ist damit nicht vorhersagbar. Bei der Wahl von anderen Zwischenwinkeln liegen entsprechend mehr oder weniger starke Korrelationen zwischen den Meßergebnissen vor.
Zur Übertragung eines Codes wählt man nun folgende Vorgehensweise (Abb. 15 u. 16):

1.) Sender (Alice) und Empfänger (Bob) einigen sich auf eine 0°-Richtung und vereinbaren dann, daß nur die Polarisationen in 0°/90°-Richtung oder in 45°/135°-Richtung vermessen werden, was für den Empfänger zwei um 45° gegeneinander geneigten Meßanordnungen eines Strahlteilers entspricht.

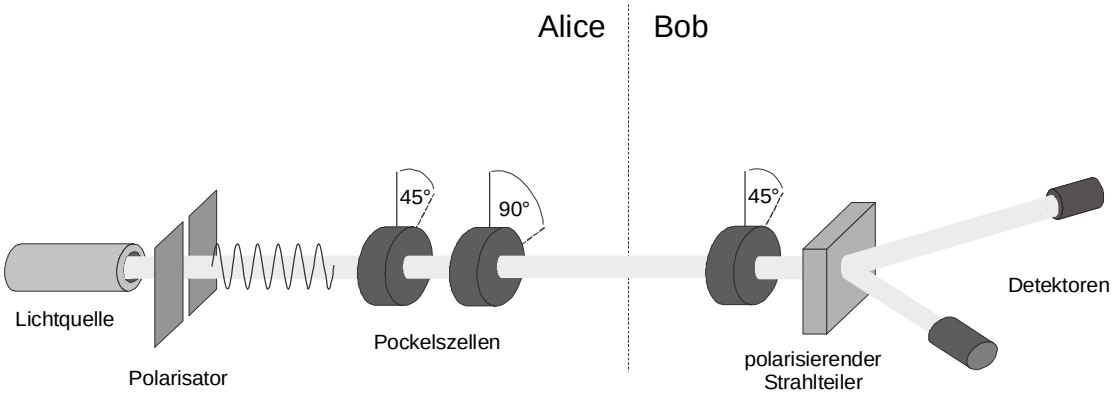


Abb. 15: Schematischer Versuchsaufbau für die Quantenkryptographie auf Basis des Polarisationsprotokolls: Sender Alice schickt linear polarisiertes Licht durch zwei Pockelszellen, von denen die eine 45°- und die andere 90°-Drehungen der Polarisationsebene erzeugen kann. Damit kann Alice vier Polarisationsrichtungen (0°, 45°, 90° und 135°) präparieren. Empfänger Bob kann unter Benutzung des Strahlteilers, der senkrecht zueinander polarisiertes Licht in unterschiedliche Richtungen bricht, immer nur zwei Richtungen unterscheiden, 0° und 90°, oder 45° und 135°. Welches Paar er im Einzelfall untersucht, kann Bob ebenfalls mit Hilfe einer Pockelszelle festlegen.

2.) Alice schickt Bob eine Abfolge von Photonen, die jeweils zufällig in einer der vier Richtungen 0°, 45°, 90°, 135° präpariert werden.

3.) Bob empfängt die Photonen, wobei er vor der Ankunft jedes einzelnen aufs neue, z.B. mit Hilfe einer Pockelszelle, in zufälliger Weise den Strahlteiler in 0° oder in 45° Richtung umorientiert.

4.) Nach der Übermittlung der Photonen tauschen Alice und Bob über eine gewöhnliche, ungesicherte Kommunikationsverbindung Informationen darüber aus, in jeweils welchem System (0°/90° oder 45°/135°) sie ihre Photonen erzeugt bzw. detektiert haben. Für 50% der Fälle erhalten sie dabei Übereinstimmung.

5.) Alice und Bob übernehmen nur diejenigen Ereignisse, bei denen sie beide im gleichen System gemessen haben und generieren daraus ihren Schlüssel.

6.) Alice und Bob überprüfen einen zufällig ausgewählten Teil des ausgetauschten Schlüssels auf einen möglichen Lauschangriff. Der restliche Teil wird zum Übertragen der eigentlichen Nachricht benutzt.

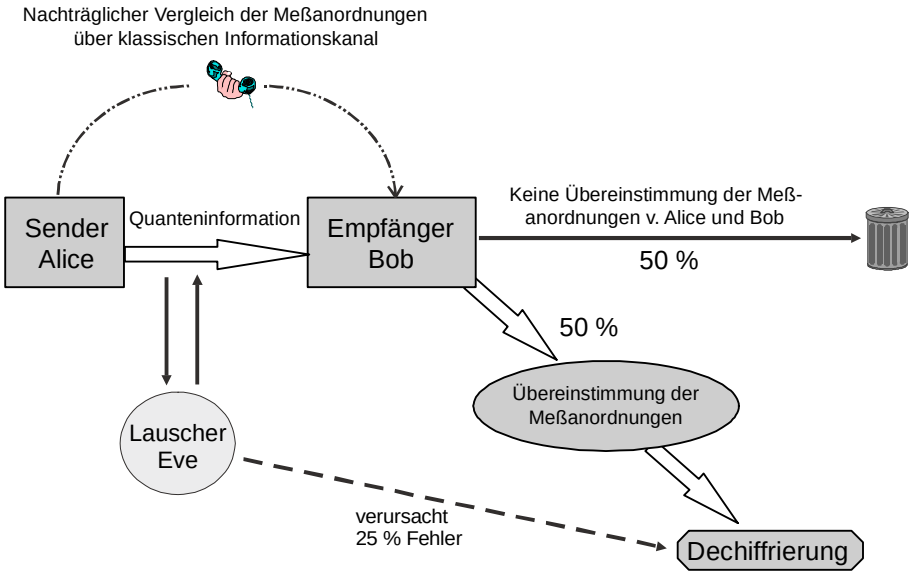


Abb. 15: Vereinfachtes Schema der Quantenkryptographie: Die Anwesenheit des Lauschers Eve führt zu einer Änderung von 50% der übertragenen Zustände. Die Hälfte dieser Änderungen wird vom Empfänger nicht bemerkt, so daß letztlich 25% der Datenbits von Bob falsch aufgezeichnet werden. Die Feststellung dieser Fehlerrate durch Alice und Bob führt dann zur Enttarnung von Eve.

Wie würde sich die Anwesenheit eines Lauschers (Eve) bei einer derartigen Vorgehensweise bemerkbar machen (Abb. 16) ?

Angenommen die Nachricht von Alice würde zunächst von Eve abgefangen werden, wobei vorausgesetzt werden soll, daß sie keine Möglichkeit hat, die apparativen Anordnungen von Alice oder Bob direkt einzusehen. In diesem Fall kann Eve ebenfalls nur mit einer Trefferquote von 50 % die richtige Grundrichtung (0° od. 45°), in dem Alice ihre Zustände jeweils präpariert hat, herausfinden. Eve muß nun allerdings das Signal möglichst korrekt an Bob weiterleiten um unerkannt zu bleiben. Die Photonen, bei denen Eve die Grundrichtung richtig erraten hat, werden von ihr, im Zuge der Übermittlung an Bob, korrekt wiedergegeben. Diejenigen aber, bei denen sie eine falsche Richtung gemessen hat, gibt sie in einem entsprechend veränderten Eigenzustand an Bob weiter.

Welche Folgen hat dieser Eingriff für Bob ?

Er erhält zunächst 50% der Information, denjenigen Teil der von Eve im richtigen System vermessen wurde, in korrekter Weise, so daß hiervon wiederum die Hälfte für den Schlüssel verwendet werden kann. Der von Eve manipulierte Anteil dagegen führt dazu, daß Alice und Bob in diesem Bereich nur eine zufällige Übereinstimmung erhalten. Dies bedeutet, daß von den 0/1-Werten, die Bob denjenigen seiner Messungen entnimmt, die in gemeinsamen

Systemen (50 % der Fälle) stattgefunden haben, nur etwa 75% mit den von Alice tatsächlich präparierten Zuständen übereinstimmen.
Anders ausgedrückt, für jedes Photon, das übertragen wird, beträgt die Wahrscheinlichkeit, daß ein Resultat erzielt wird, das auf eine Manipulation der Übertragung schließen läßt, 25%. Bei der Übertragung von N Bits beträgt die Wahrscheinlichkeit der Entdeckung Eves demzufolge $(1 - 0{,}75^N)$. Mit zunehmender Länge der Nachricht steigt die Wahrscheinlichkeit einer Enttarnung Eves also sehr stark an (Abb. 17).

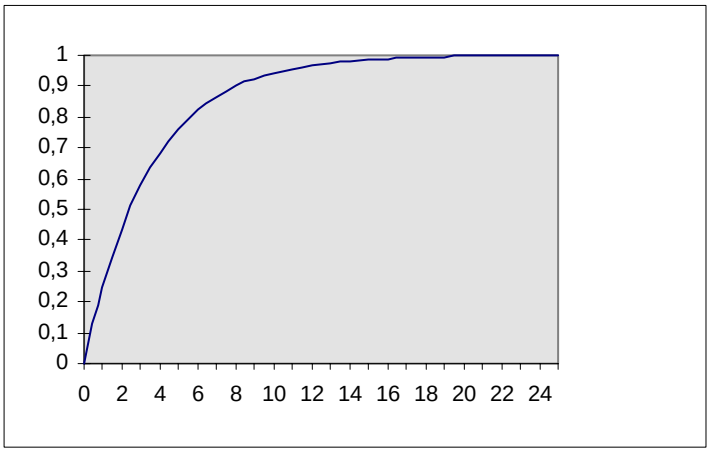


Abb. 17: Wahrscheinlichkeit der Entdeckung eines Lauschers (y-Achse) in Abhängigkeit von der Anzahl der übertragenen Bits (x-Achse).

Die technische Herausforderung liegt bei diesem Verfahren darin, daß die Signalübertragung polarisationserhaltend durchgeführt werden muß, gleichzeitig aber nur eine sehr geringe Intensität verwendet werden darf, so daß im Mittel nie mehr als ein Photon pro übertragenem Bit verwendet wird.

Die polarisationserhaltende Datenübertragung ist in konventionellen Glasfaserkabeln bereits auf Distanzen von über 20 km gelungen [Mul97].
Auf direktem Wege durch die Luft konnte auf einer Distanz von knapp einem Kilometer ein quantenkryptographisch gesichertes Datenpaket übertragen werden [But98]. Dies ist insofern interessant, als dadurch auch die Möglichkeit der abhörsicheren Kommunikation mit Satelliten näher rückt.

6.1.4 Verschlüsselung durch Phasencodierung [Tow93a, Tow93b]

Die Nutzung der Polarisation stellt nicht die einzige Möglichkeit dar, eine abhörsichere Quantenübertragung zu realisieren. Ein weiteres mögliches Protokoll beruht auf der Phasenmodulation.

Die Phase der Photonen, also eine Größe, die mit der Periodizität der elektromagnetischen Welle zusammenhängt, stellt ein Unterscheidungskriterium dar, das durch eine bloße Messung ohne zusätzliche Informationen über die Art der Präparation nicht vollständig reproduziert werden kann. Der Absolutwert der Phase ist hierbei nicht von Bedeutung, da er keiner realen physikalischen Eigenschaft entspricht (vgl. Aharonov-Bohm-Effekt). Wichtig ist immer nur die Phasendifferenz zwischen verschiedenen Zuständen bzw. Meßanordnungen. Diese bestimmt beobachtbare physikalische Quantenphänomene wie beispielsweise die Interferenz.

Die experimentellen Realisierung der Phasencodierung basiert auf einer Mach-Zehnder-Anordnung (Abb. 18). Man teilt dabei zuerst einen Laserpuls in einem Strahlteiler bzw. einem Faserkoppler (bei Übertragung in Glasfasern) in zwei gleich starke Pulse auf, die man auf den unterschiedlichen Wegen eines beim Sender befindlichen Mach-Zehnder-Interferometers weiterleitet. In einem der Wege, befindet sich ein Phasenmodulator mit dem die Phase des Pulses variiert werden kann. Im anderen Arm des Interferometers wird der Puls durch eine längere Laufstrecke verzögert, so daß beide Pulse am Ausgang des Interferometers zeitverschoben eintreffen und somit die eigentliche Übertragungsleitung nacheinander durcheilen. Dies ist notwendig um unerwünschte Interferenzen zwischen den Pulsen während der Übertragung zu vermeiden.

Der Empfänger leitet das Signal wiederum in ein Mach-Zehnder-Interferometer, an dessen Eingang sich ein polarisierender Strahlteiler befindet, welcher sicherstellt, daß die beiden unterschiedlich polarisierten Pulse tatsächlich auch in unterschiedliche Interferometerarme eingespeist werden. In einem Arm befindet sich wieder ein Phasenschieber, während der andere Arm den Laufzeitunterschied und den Polarisationsunterschied, die jeweils vom Sender eingestellt wurden, rückgängig macht, so daß beide Pulse gleichzeitig mit identischer Polarisation am Ausgang des Interferometers ankommen und daher auch miteinander interferieren können. Der resultierende Puls tritt dann wieder in einen Strahlteiler und je nachdem, in welchem der beiden Wege ein Photon gezählt wird, registriert der Empfänger eine Null oder eine Eins.

Ob der ankommende Puls nun tatsächlich in deterministischer Weise in einen der beiden Zählarme geleitet wird oder ob sich ein nicht vorhersagbares, völlig zufälliges Resultat ergibt, hängt empfindlich von der Phasenbeziehung dieser beiden Pulse vor dem Strahlteiler ab. Nur wenn die durch Alice und Bob verursachten Phasenverschiebungen in der Summe 0° oder 180° ergeben, ist das Zählresultat verwertbar. Sofern sich Alice und Bob darauf einigen, nur Winkel von -45°, +45°, -135°, +135° (Alice) bzw. -45°, +45° (Bob) einzustellen, ist dies automatisch für 50 % aller möglichen Kombinationen der Fall. Welche Pulse diese Bedingung erfüllen, wird im nachhinein von Alice und Bob durch eine gewöhnliche Datenübertragung geklärt.

Die Entscheidung, ob Bob eine Null oder eine Eins detektiert, ist also für den Fall, daß die Gesamtphasenverschiebung 0° oder 180° beträgt durch die von Alice gewählte Polarisation eindeutig bestimmt. Für die anderen Phasenverschiebungen ist das Resultat dagegen zufällig und für eine Codierung daher unbenutzbar.

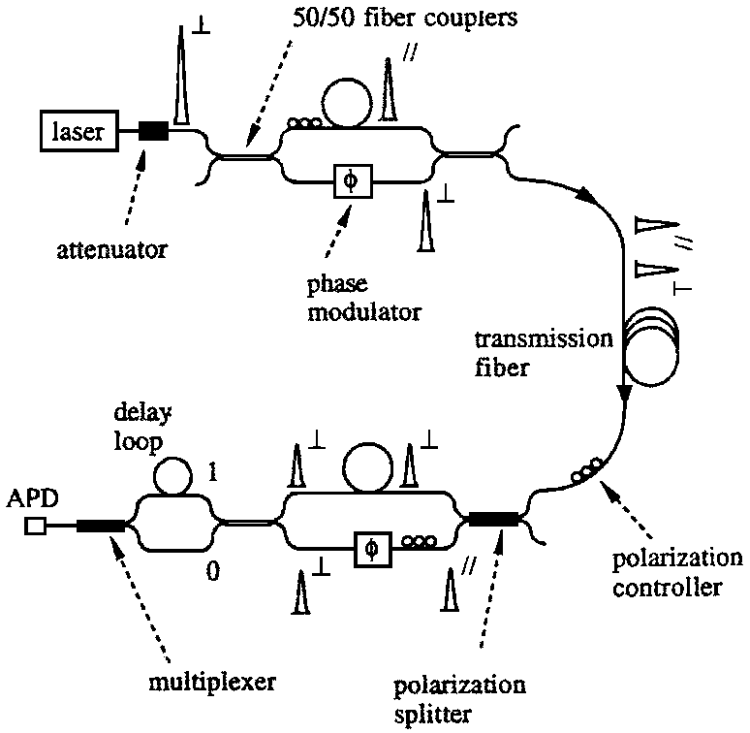


Abb. 18: Schematische Darstellung der experimentellen Anordnung zur Quantenkryptographie mittels Phasen-protokoll. In den beiden Mach-Zehnder-Interferometern wird die Information mittels der Phasenmodulatoren codiert (Sender) bzw. ausgelesen (Empfänger).

Die Schlüsselübertragung erfolgt nun wieder in mehreren Stufen:

1.) Zuerst müssen die Interferometer von Alice und Bob abgeglichen werden. Hierzu werden beiderseits die Phasenmodulatoren ausgeschaltet. Alice verändert dann physisch (nicht über einen Modulator) die tatsächliche Weglänge eines der Interferometerarme, während Bob die Zählraten seiner 0 und 1 Ausgänge beobachtet. Ist die Zählrate der Eins(1)-Ereignisse minimal, dann übermittelt Bob ein Signal an Alice. Die Initialisierung ist damit abgeschlossen.

2.) Alice beginnt nun eine Folge von Pulsen zu senden, von denen sie jeden mit Hilfe des Phasenmodulators um -45°, +45°, -135° oder +135° in der Phase verschiebt.

3.) Bob empfängt die Pulse von Alice, stellt seinen Phasenmodulator in zufälliger Weise auf +45° oder -45° ein und zählt die Nullen und Einsen.

4.) Nach dem Ende der Übertragung vergleichen Alice und Bob über einen konventionellen Übertragungskanal bei welchen Pulsen sich ihre Phasenmodulatoren in derselben Basis befanden.

5.) Es findet eine Überprüfung statt, ob tatsächlich ca. 50 % aller Pulse in der richtigen Basis gemessen wurden, ein Lauschangriff also weitgehend ausgeschlossen werden kann.
Die zur gemeinsamen Basis gehörigen Bits werden dann als Schlüssel benutzt und die sichere Datenübertragung kann beginnen.

Der Vorteil dieser Methode liegt in der relativ geringen Störungsanfälligkeit der Signalübertragung durch die zeitliche Trennung der beiden unterschiedlichen Pulse. Es konnten mit diesem Verfahren bereits bis zu einer Entfernung von 30 km Codes mit einer Übertragungsrate von ca. 1 kBit/s erreicht werden [Mar95]. Nachteil dieser Technik ist die Notwendigkeit, die Interferometer regelmäßig abzugleichen, um thermische Drifts zu kompensieren.
Eine Verbesserung der Handhabung der Kryptographiesysteme, insbesondere die Vermeidung des ständigen Abgleichens der Interferometer bzw. der Polarisatoren, ist durch die Verwendung von Faraday-Spiegeln gelungen [Mul97, Bre92, Zbi98]. Hierbei bestehen Sender und Empfänger im wesentlichen aus Michelson-Morley-Interferometern in deren Seitenarmen

sich Faraday-Spiegel befinden. Mit einem solchen experimentellen Aufbau konnten bereits quantenkryptographische Übertragungen in gewöhnlicher Telekommunikationsglasfaser vorgenommen werden. Es wurden dabei Daten über eine Entfernung von 20 km übertragen und eine Transferrate von ca. 1 kBit/s erzielt [Mul96].

Bei allen der oben vorgestellten Übertragungsverfahren, der Polarisations- und der Phasencodierung liegt die Sicherheit darin begründet, daß Information minimalisiert und gegen Vervielfältigung gesichert wird, d.h. es werden nur so viele physikalische Objekte benutzt, wie zur Speicherung und Übertragung der Information mindestens notwendig sind und die darüber hinaus die Eigenschaft aufweisen, durch eine Messung verändert zu werden, so daß die enthaltene Information nicht unbemerkt abgefangen und vervielfältigt werden kann.
Obwohl es sich bei beiden Eigenschaften um inhärent quantenmechanische Phänomene handelt, werden in keinem der Fälle verschränkte Zustände zur Datenübertragung benutzt. Dies wird in einem anderen Ansatz für die Quantenkryptographie versucht, der Phasenmessung an verschränkten Photonenpaaren.

6.1.5 Phasenmessung an verschränkten Photonenpaaren [Eke92, Rar94]

Ein Ansatz der den Anforderungen der Quantenkryptographie ebenfalls genügt, ist die Benutzung von verschränkten Photonen, wie sie in einer EPR-Quelle (vgl. Kapitel **5.3.4**) entstehen. Man sendet dann jeweils eines dieser Lichtquanten an Alice und Bob, wobei die Paarerzeugung zweckmäßigerweise von Alice selbst durchgeführt wird.
Über die beiden Photonen weiß man nun, daß sie entgegengesetzten Drehimpuls tragen. Mißt also der Sender Alice eine bestimmte Richtung, so wird der Empfänger Bob die entgegengesetzte detektieren. Der Schlüssel selbst stellt also eine vollständig zufällige Folge von Nullen und Einsen dar. Alice und Bob haben nach der Messung jeweils invertierte Zahlenfolgen vorliegen, so daß nur noch einer von beiden die Nullen und Einsen miteinander vertauschen muß, um den gemeinsamen Zufallscode zu erhalten.
Der Code selbst entsteht also als Zufallszahl in einer EPR-Quelle und nutzt so direkt den fundamentalen Zufallsmechanismus aus, der für die Nichtdeterminiertheit der Natur verantwortlich ist. Dadurch, daß jeweils nur zwei Teilchen entstehen, die diese Information tragen

und diese Teilchen auch nicht vervielfältigt werden können, kann ausgeschlossen werden, daß eine dritte Person Kenntnis des Schlüssels hat, wenn Alice und Bob diesen besitzen.
Bei der Kryptographie mit verschränkten Photonen handelt es sich also um eine reine EPR-Anordnung in der Abwandlung von Bohm, wie sie in ähnlicher Weise auch für die Grundlagenexperimente zur Überprüfung der Theorie verborgener Parameter verwendet wurde.

6.1.6 Zusammenfassung

Die Quantenkryptographie befindet sich im Vergleich zum Quantencomputer in einem deutlich fortgeschritteneren Entwicklungsstadium. Dadurch, daß die Sicherheit der Information auf einem fundamentalen physikalischen Naturgesetz beruht, ist sie außerdem bezüglich der Datensicherheit derzeit von keinem anderen System zu übertreffen. Insbesondere da für die sogenannten Public-Key-Verfahren noch kein Beweis dafür vorliegt, daß sich nicht doch ein effizienter Algorithmus finden läßt, können diese nicht als uneingeschränkt sicher eingestuft werden, wenn auch de facto derzeit keine Möglichkeit der Decodierung absehbar ist.
Der wesentliche Nachteil der Quantenkryptographie ist zweifellos der apparative Aufwand. Selbst mit der fortgeschrittensten Variation (Faradayspiegel) sind noch sehr kostenintensive Maßnahmen erforderlich, um einen Übertragungskanal einzurichten. Das z.B. eine Mischung aus verschiedenen Übertragungsleitern (Kupferkabel, Glasfaser) derzeit noch undenkbar ist, versteht sich von selbst.
Weiterhin ist zu beachten, daß bei realen Systemen eine gewisse Fehlerrate durch Rauschen vorhanden ist. Fehler durch einen Lauschangriff wären von Fehlern, die durch Rauschen verursacht werden nicht zu unterscheiden. Die erforderliche weitestmögliche Verminderung des Rauschens, als notwendige Bedingung für ein sicheres, reales Quantenkryptographiesystem würde den apparativen Aufwand und damit die Kosten weiter erhöhen.
Eine breite Anwendung dieser Verfahren ist daher für die nahe Zukunft, insbesondere solange die etablierten konventionellen Methoden noch tragen, nicht absehbar.
Für eine Informationsübertragung von höchster Sicherheitsanforderung ist die Quantenkryptographie allerdings durchaus geeignet. Gerade der „Man in the Middle“-Angriff, der bei keiner Kryptographiemethode auszuschließen ist, erfordert immer einen ähnlichen Aufwand, wie die verwendete Kryptographiemethode ihn vorgibt. D.h. insbesondere bei der Quanten-

kryptographie könnte es sich für eine Vielzahl potentieller Lauscher als unmöglich erweisen, die notwendigen technischen Mittel für das Anzapfen der Übertragung aufzubringen.
Für höchste Sicherheitsansprüche in militärischen oder geheimdienstlichen Belangen ist daher die Quantenkryptographie durchaus in der Diskussion.
Auch kommerzielle Hersteller von Hochleistungskryptographiesystemen erachten die Forschung an dieser neuen Methode für wünschenswert, da die Sicherheit der heutigen Systeme zwar gegenwärtig nicht in Frage steht, diese für die Zukunft aber aus prinzipiellen Gründen nicht unbefristet garantiert werden kann.
Die Bereitstellung einer, im Hinblick auf den zugrundeliegenden Mechanismus abgesicherten Methode als jederzeit verfügbare, wenn auch heute noch kostenintensive Alternative wäre daher durchaus sinnvoll.
Es herrscht in vielen internationalen Arbeitsgruppen auf diesem Gebiet noch eine rege Forschungstätigkeit. Insbesondere eine vereinfachte Anwendung und die weitere Verbesserung der Sicherheit steht hierbei im Vordergrund. Aber auch Anwendungsmöglichkeiten für Kryptographienetze mit mehreren Benutzern sind Gegenstand derzeitiger Experimente.

6.2 Quantenteleportation

Die Quantenteleportation beschreibt ein Verfahren, mit dessen Hilfe man quantenmechanische Zustände instantan von einem Teilchen auf ein anderes, möglicherweise weit entferntes, übertragen kann. Da der Transport hierbei nicht im klassischen Sinne durch das Bewegen von Materie von einem Ort zum anderen erfolgt, sondern mit Hilfe der extremen Nichtlokalität verschränkter Quantenzustände durchgeführt wird, wurde dafür in Anlehnung an, in ähnlicher Weise "nicht-suggestive" Transportmethoden des Science-Fiction-Genres der etwas irreführende Name Teleportation gewählt.

Tatsächlich hat man es bei der Quantenteleportation nicht mit dem Transport massiver Objekte zu tun, sondern lediglich der quantenmechanische Zustand, also bestimmte Eigenschaften des Objekts, werden von einem Teilchen auf ein anderes übertragen. Da hierbei der Zustand des ersten Teilchens verändert wird, kann man davon sprechen, daß alle diejenigen Eigenschaften, die das Teilchen (z.B. ein Photon) von anderen unterschieden und damit seine Individualität definiert haben (z.B. eine bestimmte Polarisationsrichtung), auf ein anderes Teilchen übertragen wurden, so daß ein unabhängiger Beobachter nicht in der Lage wäre zu entscheiden, ob tatsächlich nur der Quantenzustand teleportiert, oder ob das Teilchen selbst an den neuen Ort bewegt wurde. D.h. alle diejenigen Eigenschaften, die einen individuellen Charakter aufweisen, werden mittels der Teleportation übermittelt, die materielle Grundsubstanz jedoch, die alle Objekte dieser Sorte gemeinsam haben, wird nicht übertragen, sondern von einem am Zielort befindlichen Teilchen übernommen [Ben93].

Eine vielleicht bessere Interpretation der Quantenteleportation erhält man, wenn man das verschränkte Teilchenpaar, mit dem die Teleportation durchgeführt wird, als ein einziges sehr ausgedehntes quantenmechanisches Objekt betrachtet. Wird dieses Objekt nun an einer Stelle durch eine Wechselwirkung verändert, so geht es im selben Moment in einen neuen Zustand über, so daß eine Messung "am anderen Ende" des Objekts eine, mit der lokalen auslösenden Wechselwirkung korrelierte Änderung des Quantenzustand ergibt.

Der nichtlokalisierte physikalische Zustand, der den beiden, bei den Messungen nachzuweisenden individuellen Teilchen vorausgeht (vgl. Abb. 6), ändert seine Eigenschaft also überall gleichzeitig.

Obwohl die Teleportation nach heutigem Kenntnisstand instantan abläuft, ist es dennoch nicht möglich, auf diese Weise überlichtschnell Informationen zu übertragen. Um einen Quanten-

zustand vollständig charakterisieren zu können, ist es unabdingbar die Bedingungen (die Basis) zu kennen, unter welchen der Zustand präpariert wurde (vgl. Quantenkryptographie). Die Information über die Basis muß aber zusätzlich auf konventionellem Wege und damit nicht schneller als das Licht, an den Zielort übertragen werden.

Dies liegt wiederum daran, daß identische Quantenzustände unterschiedliche Meßergebnisse (Eigenzustände) ergeben können, wenn sie mit unterschiedlichen apparativen Anordnungen (entsprechend unterschiedlicher Basen) gemessen werden. Hinter dieser Tatsache verbirgt sich die fundamentale Erkenntnis, daß eine Messung in der Quantenmechanik mit einem wesentlichen Eingriff in das gemessene System verbunden ist. Die Messung führt dabei zum sogenannten Kollaps der quantenmechanischen Wellenfunktion.

Das eigentlich Neue bei der Quantenteleportation ist, daß es möglich ist einen Quantenzustand zu übertragen ohne daß es notwendig wäre, das Teilchen selbst zu transportieren. Der teleportierte Quantenzustand kann dabei auch völlig unbekannt sein, für eine Teleportation ist die Kenntnis des zu teleportierenden Zustandes nicht erforderlich und für den Fall, daß es sich nicht um einen Eigenzustand (d.h. ein mögliches Meßergebnis) handelt, auch nicht zugänglich.

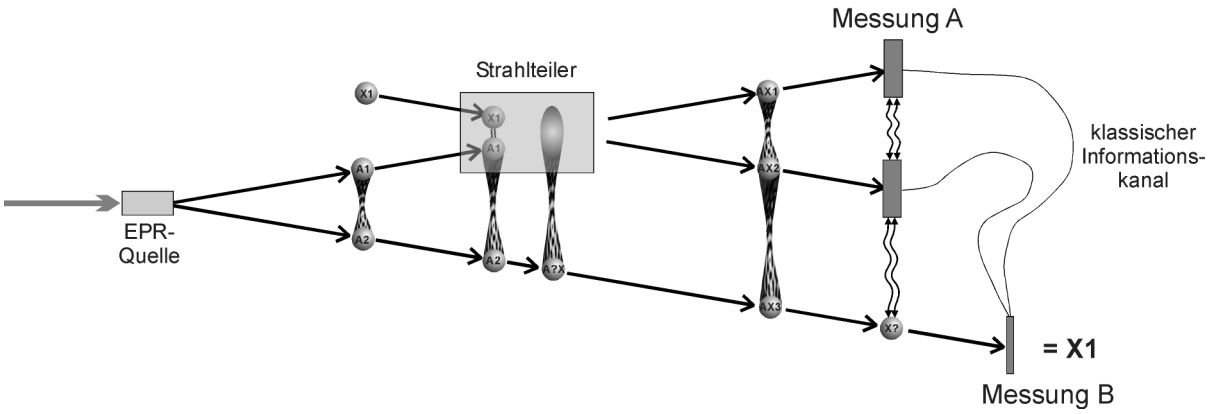


Abb. 19: Prinzip der Quantenteleportation: In einem doppelbrechenden Kristall wird ein verschränktes Photonenpaar (A1 und A2) erzeugt. Eines dieser Photonen wird in einem Strahlteiler mit dem zu teleportierenden Lichtquant (X1) verschränkt. Durch die Messung (A) an diesen beiden Photonen (A1 und X1) geht das Gesamtsystem in einen neuen Zustand über. Das Zielphoton (A2) der Teleportation muß jetzt nur noch eine Meßapparatur (B) durchlaufen um den Zustand des zu teleportierenden Photons anzunehmen. Dazu muß die Meßanordnung B allerdings geeignet eingestellt werden, wozu Informationen bezüglich der Resultate der Messung A unabdingbar sind.

Experimentelle Realisierung der Teleportation [Bou97] (vgl. Abb. 19):

Ausgangspunkt ist ein verschränktes Teilchenpaar, daß durch die sogenannte "Down Conversion" gewonnen wird. Bei diesem Prozeß wird ein einzelnes Photon bestimmter Frequenz in einen nichtlinearen, doppelbrechenden, optischen Kristall eingestrahlt und dabei in zwei Photonen mit jeweils der halben Frequenz konvertiert.

Die beiden erzeugten Photonen können dadurch miteinander verschränkt werden, daß man sie in einem bestimmten, der Ortsunschärfe der Photonen entsprechenden Raumbereich zusammenführt. Die Photonen sind dann physikalisch ununterscheidbar, d.h. sie haben jegliche Individualität verloren. Würde man an einem solchen Ort eine Messung durchführen und ein Photon registrieren, so wäre es prinzipiell nicht möglich zu sagen, um welches der beiden es sich dabei handelt. Ununterscheidbar gemachte identische Teilchen sind, nachdem sie sich wieder getrennt haben und solange keinerlei Wechselwirkung mit anderen Objekten stattfindet, miteinander maximal verschränkt.

Bei der hier genutzten "Down Conversion" werden die beiden niederenergetischen Photonen auf Kegeloberflächen emittiert, wobei die Spitze der Kegel im Kristall liegt. Die beiden Kegel schneiden sich und die dabei entstehenden zwei Schnittgeraden definieren Zustände, in denen die beiden Photonen nicht unterscheidbar sind, da es nicht möglich ist, sie einem bestimmten der beiden Kegel zuzuordnen.

Man erzeugt kurz nacheinander zwei dieser verschränkten Photonenpaare und führt die Strahlen jeweils so, daß sich ein Photon des ersten Paares mit einem des zweiten in einem Strahlteiler trifft, so daß diese beiden nicht unterscheidbar und damit verschränkt werden.

Wie eine kurze Rechnung zeigt, wird dabei der Zustand desjenigen Photons, das mit einem der im Strahlteiler befindlichen Lichtquanten verschränkt ist, auf das andere im Strahlteiler anwesende Photon übertragen.

Diese Übertragung wird durch ein nachgeschaltetes Interferenzexperiment, das auf die übertragenen Eigenschaften empfindlich ist, experimentell nachgewiesen.

Beim ersten Teleportationsexperiment war es noch nicht möglich, jeden der möglichen Zustände des verschränkten Photonenpaars experimentell nachzuweisen, so daß der Nachweis der Teleportation nur für bestimmte Ausgangszustände erfolgen konnte (vgl. auch Quantendatenkompression) [Bou97]. Neuere Versuche haben hier jedoch Fortschritte ergeben [Bos98, Fur98]. Im Rahmen der Experimente zum NMR-Quantencomputer [Bra98] ist nun auch die Teleportation eines quantenmechanischen Zustand innerhalb eines Moleküls

gelungen, also auch für "massive" Materie im Unterschied zu den vorhergehenden Experimenten, die ausschließlich auf verschränkten Photonen basierten [Nie98].

Eine Weiterentwicklung der Teleportation ist das sogenannte "Entanglement Swapping" [Yur92a, Yur92b, Zuk93]. Hierbei wird nicht ein individueller quantenmechanischer Zustand übertragen, sondern die Eigenschaft der Verschränkung zweier Teilchen auf ein anderes Teilchenpaar übertragen. Es wird also der Gesamtzustand eines Teilchenpaars, daß in dieser Hinsicht als ein einziges, ausgedehntes Objekt zu betrachten ist, auf ein anderes Teilchenpaar übertragen.
Bisher wurde das "Entanglement Swapping " nicht experimentell realisiert. Allerdings scheint eine erfolgreiche experimentelle Verifizierung dieses Phänomens für die nähere Zukunft durchaus greifbar.

Mögliche Anwendungen der Quantenteleportation liegen in der Quantenkryptographie, da ein externer Eingriff auch hier mit einer Zerstörung des quantenmechanischen Zustandes verbunden ist, so daß der Empfänger einen starken Anstieg der Fehlerrate feststellen würde.
Wichtiger ist die Fähigkeit Verschränkung transportieren zu können natürlich für den Quantencomputer, da dieser ja gerade mit hochgradig verschränkten Zuständen operiert. Verschiedene Atomresonatoren oder Ionenfallen könnten auf diese Weise zu einem Quanten-register zusammengeschaltet werden.
Die Idee, nach dieser Methode makroskopische Gegenstände oder gar Personen transportieren zu wollen, kann dagegen nicht Gegenstand einer seriösen Abschätzung der Anwendungs-gebiete dieses physikalischen Effekts sein und gehört bis auf weiteres in den Bereich des Science-Fiction.

Die Quantenteleportation ermöglicht die Übertragung von Materieeigenschaften auch über große Distanzen zwischen verschränkten Objekten. Für die Quantenteleportation ist bislang kein eigenständiges Anwendungsgebiet erkennbar. Sie kann aber sowohl für die Quantenkryptographie, als auch den Datentransport innerhalb eines Quantenprozessors genutzt werden. Mit Hilfe der Teleportation und des „Entanglement Swapping“ ließe sich ein Netzwerk von Quantengattern aufbauen.

6.3 Quantendatenkompression

Das sogenannte "Quantum Dense Coding" nutzt nichtlokale EPR-Zustände zur Übertragung von in besonderer Weise komprimierten Informationen [Ben92c, Bar95a].
Klassisch gilt, daß man an einen binären physikalischen Zustand nicht mehr als ein Bit Information koppeln kann. Beispielsweise kann der Spin eines Fermions bei einer Messung nur die Werte $\pm\hbar/2$ annehmen, die dann mit den binären Werten 0 und 1 identifiziert werden können. Aus zwei binären Systemen kann man vier Zustände (2^2) bilden und somit zwei Bits an Information übertragen.
Für ein quantenmechanisches Vierniveausystem, wie ein EPR-korreliertes Teilchenpaar gilt dann in gleicher Weise, daß es insgesamt zwei Bits an Information enthält.
Für die Möglichkeit durch den physischen Transport nur eines physikalischen Teilchens, das selbst nur ein Zwei-Niveau, also 1-Bit-System darstellt, mehr als nur dieses eine intrinsische Bit übertragen zu können, spielt nun wieder die Nichtlokalität eines quantenmechanischen Systems die tragende Rolle.
Man versendet beim "Dense Coding" nicht ein einzelnes isoliertes Teilchen, sondern eines, das zusammen mit einem anderen ein EPR-Teilchenpaar bildet, also mit einem zweiten Teilchen verschränkt ist.
Wie bei der Quantenkryptographie und der Quantenteleportation betrachtet man wieder einen Sender Bob und einen Empfänger Alice, die jeweils ein Teilchen eines EPR-Teilchenpaars erhalten. Das verschränkte Teilchenpaar, als nichtlokales quantenmechanischen Objekt, kann bei einer Messung nur einen von vier möglichen Zuständen (Eigenzustände) einnehmen.

Der Ablauf der verdichteten Informationsübertragung ist nun wie folgt (Abb. 20):

1.) Alice generiert ein EPR-Teichenpaar und schickt eines davon an Bob.

2.) Bob kann nun auf vier unterschiedliche Arten eine Manipulation bzw. Messung an seinem Teilchen vornehmen. Obwohl er bei einer Messung an seinem eigenen Teilchen immer nur zwei unterschiedliche Werte erhalten kann, führen die unterschiedlichen Messungen am quantenmechanischen Objekt (Teilchenpaar) zu vier verschiedenen Zuständen. Wichtig ist hierbei, daß die möglichen Zustände nicht eine zufällige Folge der Messung Bobs sind,

sondern von diesem gezielt durch die Manipulation an seinem Teilchen herbeigeführt werden können [Ben92c].

3.) Bob sendet sein Teilchen (klassisch 1 Bit) an Alice.

4.) Alice ermittelt durch Messung an dem von Bob erhaltenen und ihrem eigenen Teilchen den, von Bob durch seine Messung präparierten, quantenmechanischen Zustand des EPR-Paares und registriert auf diese Weise, welchen der vier möglichen Zustände die Manipulationen Bobs ergeben haben.

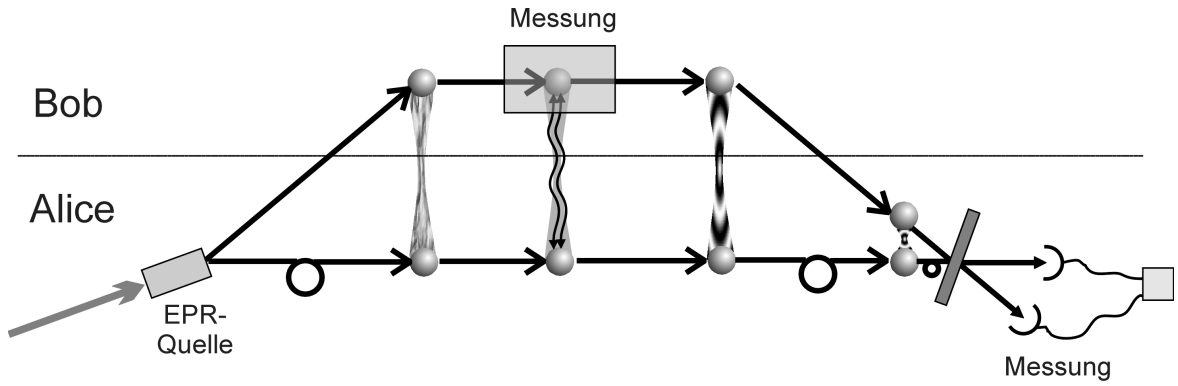


Abb. 20: Schema der Quantendatenkompression: Alice generiert ein EPR-Teilchenpaar, von denen sie eines an Bob schickt. Bob führt eine von vier verschiedenen Operationen (Messsungen) an seinem Teilchen durch, was das Gesamtsystem (also das Teilchenpaar) in einen neuen Zustand überführt. Danach schickt Bob sein Teilchen zurück an Alice, die eine interferometrische Messung an den beiden Teilchen vornimmt um festzustellen, in welchem Zustand sich das Teilchenpaar befindet.

Durch die gezielte Messung an seinem Teilchen und der damit verbundenen Rückwirkung auf das gesamte nichtlokalisierte, quantenmechanischen System sowie der anschließenden Übersendung seines Teilchens überträgt Bob zwei Bit, obwohl physisch tatsächlich nur ein Teilchen bewegt wurde, das für sich alleine betrachtet maximal ein Bit transportieren könnte.
Dies muß dahingehend interpretiert werden, daß der restliche Informationsfluß in irgendeiner Art und Weise über die quantenmechanische Verbindung zwischen den EPR-Teilchen zustande kommt.

Im Experiment ist mit dieser Technik bereits die Übertragung von einem "Trit" (1,58 Bit) gelungen [Mat96]. Dies liegt darin begründet, daß zwei der vier Eigenzustände nicht experimentell unterschieden werden konnten, demnach also nur drei statt vier unterschiedliche Meßergebnisse für Alice identifizierbar sind. Der Informationsgehalt liegt damit jedoch immer noch deutlich über dem klassisch möglichen Wert von einem Bit.

Die Anwendungsmöglichkeiten dieser Methode sind sicherlich nicht in der Telekommunikation zu suchen, wie man sie heute kennt. Von einer Effizienz, die pro übertragenem Bit nur ein Photon nutzt, ist man bei der konventionellen Datenübertragung noch viele Größenordnungen entfernt. Die Quantendatenkompression (wie auch die Teleportation) könnten sich eher als hilfreich für den Datentransfer innerhalb eines Quantencomputers erweisen, wo ein effizienter Übertragungsmechanismus bei möglichst geringer Störung des Systems von Vorteil ist.
Eine weiteres potentielles Einsatzgebiet ist die Quantenkryptographie, für die eine Implementation solcher Verfahren aufgrund der ohnehin schon sehr ähnlichen Anforderungen an den apparativen Aufbau mit einem deutlich geringeren Aufwand möglich wäre, als bei kommerziellen Glasfaserübertragungssystemen.

6.4 Quantenzufallsgeneratoren

Eines der ältesten Probleme von Naturwissenschaft und Philosophie, das auch für bestimmte Anwendungen von beträchtlicher Bedeutung ist, stellt die Frage nach zufälligen Prozessen in der Natur dar.

Gerade in der Kryptographie ist ein Schlüssel natürlich völlig wertlos, wenn er auf eine einfache Gesetzmäßigkeit, d.h. einen simplen Algorithmus zurückgeführt werden kann.

Die Qualität einer Zufallszahl kann man mittels des Arguments der Komprimierbarkeit quantifizieren [Cha77]. Danach gilt eine Zufallszahl dann als ideal, wenn sie nicht auf ein einfacheres System reduzierbar ist. Dies bedeutet, der elementarste Algorithmus der eine Abfolge ideal zufälliger (Binär-) Zahlen beschreibt, ist die Zahlenfolge selbst.

Es ist nun keinesfalls trivial, eine solche nicht komprimierbare Zahlenfolge technisch zu generieren. Dies soll anhand eines klassischen Würfels erläutert werden.

Aus persönlicher Erfahrung weiß man, daß die Zahlen Eins bis Sechs beim Würfelwurf in offensichtlich zufälliger Weise aufeinander folgen. Die Ursache hierfür liegt in der extremen Empfindlichkeit mit der das Resultat (die oben liegende Augenzahl des Würfels) von den Anfangsbedingungen (Ort, Haltung und Geschwindigkeit der Hand, Position des Würfels in/auf der Hand) abhängt. Systeme, bei denen kleinste Unterschiede in den Anfangsbedingungen über kurz oder lang zu sehr großen Differenzen in der Entwicklung des Systems führen, nennt man in der Physik auch chaotische Systeme. Man darf nun allerdings derartiges chaotisches Verhalten nicht mit Zufallsereignissen verwechseln. Das Chaos beruht in der klassischen Physik lediglich auf einem Mangel an Information bezüglich des Anfangszustands und/oder der praktischen Unmöglichkeit eine entsprechend große Menge an darin enthaltener Information hinreichend genau (analytisch oder mittels Computer) zu verarbeiten. Die Abläufe selbst sind jedoch deterministisch. Würde man demnach ein solches Verfahren zur Generierung eines kryptographischen Schlüssels benutzen, so wäre ein offensichtlicher Angriffspunkt zur Dechiffrierung des Codes das genauere Verständnis des verwendeten chaotischen Systems durch die abhörende Partei. Man sieht sich bei klassischen Verfahren also mit einer Art „Wettbewerb des Wissens“ konfrontiert.

Beim Würfelwurf würde man bei der Verfolgung der Ursachen beispielsweise die menschliche Physiologie genauer untersuchen. Wie sehr zittert die Hand und worauf ist dieses

Zittern zurückzuführen? Finden sich in der Zitterbewegung Regelmäßigkeiten, spielen bewußt gesteuerte Bewegungsabläufe eine Rolle etc.?
Eine solche Kausalkette läßt sich sehr weit fortsetzen und die Frage lautet nun, ob dies so weitergeht bis hin zu einer einzigen, alles umfassenden deterministischen Gesetzmäßigkeit, oder ob auf irgendeiner Ebene der Natur ideale Zufallsereignisse stattfinden, die nicht weiter zurückverfolgt werden können.
In der Tat enthält die Quantenmechanik solche ideal probabilistischen Elemente. Man erkennt sie in der Entstehung bzw. der Messung EPR-korrelierter Teilchenpaare (vgl. Kap. **5.3.4**, Abb. 6), aber auch radioaktiver Zerfall, der ebenfalls ein elementarer quantenmechanischer Effekt ist, weist eine „intrinsische“ Zufälligkeit auf.
Wie bereits ausgeführt können bei diesen Prozessen aus identischen Anfangsbedingungen unterschiedliche Endzustände entstehen. Eine Rückführung auf eine direkte, die Endzustände exakt vorhersagende Ursache (dies wäre ein verborgener Parameter, vgl. Kap. **5.3.4**) ist nicht möglich. In diesem Zusammenhang äußerte Einstein, der die Quantenmechanik in dieser Form ablehnte, seinen bekannt gewordenen Ausspruch: „Gott würfelt nicht.“
Tatsächlich werden radioaktive Präparate, mit allen Nachteilen in Bezug auf die Sicherheitsanforderungen, die bei Umgang mit dem entsprechenden Material zu berücksichtigen sind, bereits zur Generierung von Zufallszahlen benutzt.
An der Universität Genf wurde hingegen eine Methode entwickelt, die auf der Nutzung photonischer Zustände beruht und technisch nach ähnlichen Prinzipien funktioniert, wie die Quantenkryptographie. Dabei wird ein photonischer Quantenzustand mit jeweils fünfzigprozentiger Wahrscheinlichkeit in zwei unterschiedliche Endzustände geschalten. Bei der Deutschen Telekom wird beabsichtigt solche Vorrichtungen in naher Zukunft zur Generierung besonders sicherer Schlüssel einzusetzen [Las99]. Entsprechende Apparaturen wurden teilweise selbst hergestellt, sollen jedoch auch zusätzlich eingekauft werden. Somit ist diese Anwendung, die einen Spin-Off der Quantenkommunikation darstellt, als mit den heute zur Verfügung stehenden Mitteln realisierbar anzusehen.

Als Randnotiz sei an dieser Stelle angemerkt, daß die Grundsatzfrage nach der Determiniertheit der Natur selbstverständlich eine eminente weltanschauliche Bedeutung besitzt. Wären tatsächlich alle Geschehnisse in eindeutiger Weise auf eine einzige fundamentale Ursache bzw. eine Gesetzmäßigkeit zurückzuführen, so wäre jede Art der Handlungs-, Entscheidungs-, oder Willensfreiheit lediglich eine Illusion.

Die Quantenmechanik deckt also ein probabilistisches Prinzip in der Natur auf, das besagt, daß die zukünftige Realität nicht exakt festgelegt sein kann. Daraus läßt sich zwar noch in keiner Weise etwa eine Willensfreiheit ableiten und man sollte dies daher auch nicht tun, es wird jedoch eine zwingend notwendige Bedingung für eine solche Möglichkeit erfüllt.
Es ist durchaus denkbar, daß derartigen Erkenntnissen bei zukünftigen Versuchen ethische wie auch rechtliche Normen auf einer weltanschaulich neutralen Basis zu formulieren, eine verstärkte Bedeutung zukommen wird.

7 NICHT QUANTENZERSTÖRENDE MESSUNG (QND)

Bei klassischen Messungen wird die Wechselwirkung des Meßapparates mit dem zu untersuchenden Objekt vernachlässigt. Wird beispielsweise bei einer Geschwindigkeitskontrolle im Straßenverkehr ein Radarstrahl auf ein Fahrzeug gerichtet, so überträgt diese Mikrowellenstrahlung zwar einen gewissen Impuls auf das Fahrzeug und ändert damit natürlich auch dessen Geschwindigkeit, der Effekt ist jedoch so gering, daß er um viele Größenordnungen unterhalb der Nachweisgrenze der verwendeten Apparatur liegt.
Die Situation ändert sich jedoch, wenn man sich auf die Ebene der Quantenmechanik begibt. Dies liegt nicht nur daran, daß die Meßsonden jetzt im Vergleich zu den Meßobjekten vergleichbare Masse bzw. Impuls u.a. besitzen und daher schon durch quasiklassische Wechselwirkungen zu einer Veränderung des untersuchten Objekts führen.
Die quantenmechanische Unschärfe ist nicht ein meßtechnisches Unvermögen, Kenntnis über bestimmte zwar mikroskopische aber dennoch präzise vorhandene physikalische Größen eines Objekts zu erlangen. Die Unschärfe ist eine Eigenschaft des physikalischen Zustands selbst. Der Versuch einen solchen zu messen führt daher nach heutigem Kenntnisstand immer, auch bei tatsächlich sehr geringer "mechanistischer" Einwirkung auf den Zustand, zu einer minimalen, durch die Eigenarten der quantenmechanischen „Meßwechselwirkung“ und die quantenmechanischen Eigenschaften des Objekts selbst verursachten Veränderung.
Letztlich wesentlich bei der Frage ob ein quantenmechanisches Objekt durch eine Messung verändert wird, scheint allein die Tatsache zu sein, ob und welche Information dem Objekt entzogen wird [Boh51, Scu78]. Die Art und Weise wie eine Informationsextraktion geschieht ist dagegen für die quantenmechanische Störung (Kollaps der Wellenfunktion, Übergang in neuen Eigenzustand) des Zustands von untergeordneter Bedeutung [Dür98], lediglich für die klassischen Rückwirkungen (z.B. Impulsübertrag durch Stoß) spielt dies die zentrale Rolle.
Weiterhin können Meßapparatur und Meßobjekt auch nicht mehr als voneinander unabhängig betrachtet werden. Ein Meßergebnis ist nur reproduzierbar in Bezug auf eine bestimmte Meßanordnung mit der die ursprüngliche Messung vorgenommen wurde. Das Quantenobjekt befindet sich dann in einem Eigenzustand in Bezug auf die gemessene Größe. Hat sich das Objekt zuvor nicht in einem Eigenzustand befunden, so wird es in einen solchen überführt, man spricht hierbei vom Kollaps der Wellenfunktion. Wiederholtes gleichartiges Messen verändert das untersuchte Objekt dann nicht mehr.

Wurde durch eine Messung ein entsprechender Eigenzustand erzeugt, so bedeutet dies insbesondere auch, daß alle mit der betreffenden Eigenschaft über die Unschärferelation verbundenen Größen unscharf werden. Allgemein bekannt ist dieser Zusammenhang insbesondere für Ort und Impuls die sich nicht beide gleichzeitig in einem Eigenzustand befinden können, wie dies in der Heisenbergschen Unschärferelation in ihrer bekanntesten Formulierung auch zum Ausdruck kommt.
Man kann durch Messungen also die Unschärfe nicht beseitigen, sondern nur von einer Eigenschaft auf eine andere quasi "umlagern".

Von einer idealen QND (quantum non demolition)-Messung erwartet man, daß ihre Wechselwirkung auf das Meßobjekt eben auf jene Umlagerung beschränkt ist und klassische Störungen etwa durch gewöhnliche Stoßprozesse gänzlich vermieden werden [Bra80].
Heute praktisch durchführbare Messungen erreichen sind von diesem Ideal der nur noch quantenmechanisch limitierten, minimalen Meßwechselwirkung noch weit entfernt.
Eine gewöhnliche Energiemessung von Licht mit einem Photodetektor ist beispielsweise in der Regel mit der vollkommenen Absorption (demolition) der Lichtquanten und nicht nur der Zerstörung ihres Quantenzustandes (destruction) verbunden.
Ziel der QND-Meßverfahren ist es, die gewünschten Informationen über den Gegenstand der Messung zu gewinnen, dabei jedoch die Störung des betrachteten Objekts auf das physikalische, durch die Quantenmechanik vorgegebene Mindestmaß zu beschränken. Dadurch lassen sich bis heute unerreichte Meßgenauigkeiten erzielen.
Experimentell liegt eine QND-Messung dann vor, wenn man wiederholt einen Eigenzustand nachweisen kann, ohne diesen in irgendeiner Art und Weise zu verändern. Man muß also mehrmals nacheinander dasselbe (nicht ein identisches) Objekt untersuchen können. Insbesondere bedeutet dies natürlich, daß man das zu untersuchende Objekt nicht einfach absorbieren kann, um an die gesuchte Information zu gelangen.
Erste Vorschläge für QND-Messungen betrafen die Registrierung der Bewegungsabläufe mechanischer Oszillatoren [Car80], speziell in Zusammenhang mit den ersten Versuchen der Gravitationswellendetektion auf Basis von Weber-Zylindern. Später wurde jedoch erkannt, daß eine Realisierung von QND-Messungen in der Optik einfacher zu realisieren wäre [Lev86, LaP89, Gra90].
Ein Prinzip, gemäß dem optische Messungen versucht werden, beruht auf der Kopplung zweier elektromagnetischer Feldmoden [Roc97].

Die Signalmode, die es zu messen gilt, tritt mit der "Meter"-Mode in Wechselwirkung und überträgt die gewünschte Information. Im Idealfall geht die Signalmode dabei lediglich in einen Eigenzustand hinsichtlich der zu untersuchenden Eigenschaft über. Die Meter-Mode kann hernach auf konventionelle Weise analysiert werden (Abb. 21).
Bis heute sind solche vollständig idealen Messungen allerdings praktisch nicht durchführbar.
Die meisten Experimente bedienen sich eines nichtlinearen Prozesses der die Information vom Signal auf den Sondenzustand überträgt. Dabei werden Die beiden quantenmechanischen Zustände miteinander verschränkt. Es liegt hier bezüglich des informationsextrahierenden Mechanismus also eine Ähnlichkeit zur Quantenteleportation vor.

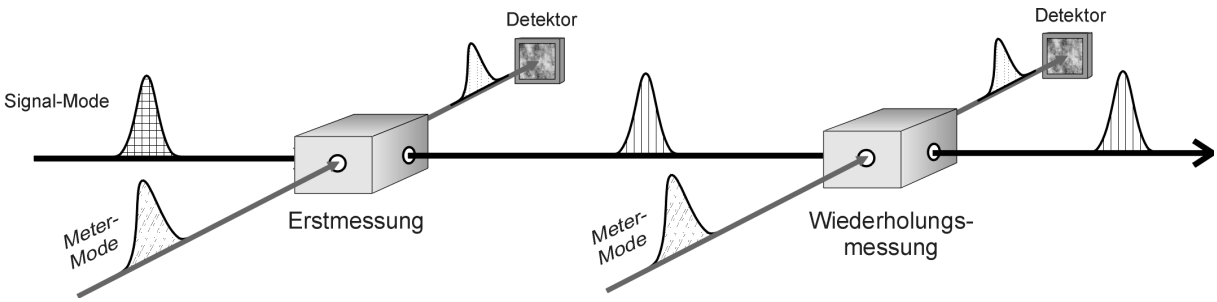


Abb. 21: Prinzip der QND-Messung: Das ankommende Signal wird mit der Meter-Mode in der Meßapparatur verschränkt und geht dabei bezüglich der extrahierten Information in einen Eigenzustand über. Das Signal wird dabei zwar verändert (sofern es sich noch nicht im Eigenzustand befunden hat), jedoch nicht absorbiert. Über eine klassische (quantenzerstörende) Messung der Meter-Mode wird die Information über das Signal dem System entnommen. Eine Wiederholungsmessung mit einer identischen apparativen Anordnung ändert den Zustand des Signals nicht mehr.

Die Systeme, an denen solche QND-Experimente durchgeführt werden sind teilweise sehr unterschiedlich.
Roch et al. [Roc97] benutzten ^{87}Rb Atome in einer magnetooptischen Falle, um die Intensität eines schwachen Signals, das ein wenig gegenüber der Resonanzfrequenz des Rubidiums verstimmt war, zu messen. Durch den geringen Frequenzunterschied tritt dabei eine Absorption nur sehr schwach in Erscheinung.
Die Wechselwirkung des Signals mit dem Rubidium führt nun dazu, daß die Atome in den Grundzustand übergehen. Für einen Sonden-Lichtstrahl ändert sich dadurch der Brechungsindex des Rubidiums, was sich in einer Phasenverschiebung der Lichtwelle äußert.

Die Information über die Intensität des Signals kann also aus der Phasenverschiebung des Sondenlichts abgelesen werden, ohne daß der Signal-Lichtstrahl absorbiert wird (Verluste bei ca. 10 %).
Die Wiederholbarkeit einer QND-Messung am selben Objekt konnte von Bruckmeier et al. sowie Bencheikh et al. gezeigt werden [Bru97, Ben95].
Die Verwendung von optischen Solitonen für QND-Messungen verspricht eine noch bessere Verwirklichung der QND-Idee, da diese über wohldefinierte Teilchen- und optische Eigenschaften verfügen [Bru93, Spä97, Cou98].
Für eine Messung läßt man zwei Solitonen in einer Glasfaseranordnung miteinander kollidieren. Die Meßgröße ist die Anzahl der Photonen, aus denen das Signal-Soliton besteht. Die Information über diese Teilchenzahl wird bei der Kollision auf das Meter-Soliton übertragen. Die unvermeidliche quantenmechanische Meßwechselwirkung äußert sich darin, daß die Phase des Signal-Solitons durch den Informationsübertrag unscharf wird. Bemerkenswert ist diese Messung deshalb, weil ein Soliton als ganzes durch eine quantenmechanische Wellenfunktion dargestellt werden kann und daher den Charakter eines Quasi-Teilchens hat. Man kommt mit diesem Schema dem Idealbild einer QND-Messung daher schon sehr nahe. Jedoch bestehen auch Solitonen noch aus ca. 10^5 bis 10^8 einzelnen Photonen, so daß die beobachteten quantenmechanischen Zustandsänderungen nicht wirklich solche eines individuellen Teilchens sind, sondern noch bis zu einem gewissen Grade einen statistischen Charakter aufweisen.
Was bislang noch aussteht, ist eine Messung, die die Wellenfunktion eines einzelnen Teilchens in einen Eigenzustand überführt und die das erste Ergebnis bei wiederholter Messung reproduziert (entsprechend Abb. 21).

Die Anwendungen der QND wurden anfangs vor allem in der Detektion von Gravitationswellen gesehen [Bra80]. Gravitationswellen, die von bestimmten astronomischen Ereignissen (z.B. Supernovas) erzeugt werden bewirken bei heute bestehenden Detektoren Auslenkungen, die mit der Größenordnung von Quantenfluktuationen dieser Systeme vergleichbar sind. Eine optimal präzise Messung bei minimaler Rückwirkung auf das Meßobjekt, wie es mit einem QND-Verfahren realisierbar wäre, würde daher einen wichtigen Schritt auf dem Weg zu einem Nachweis von Gravitationswellen darstellen.
Von besonderer Bedeutung ist eine minimale Rückwirkung aber auch im Fall des Quantencomputers. Mit einer QND-Messung wäre es hier möglich beispielsweise unerwünschte

Quantensprünge im Register des Computers festzustellen [Chu96], ohne das dieses seine Kohärenz verliert, die ja für eine Quantenrechnung unabdingbar ist.

Ebenso ist für die Kontrolle des Rechenablaufs ein Mechanismus notwendig, der die nachfolgenden Rechenschritte nicht beeinträchtigt. Um Feststellen zu können, ob ein Algorithmus bereits abgearbeitet ist, bedarf es einer Methode, die die Kohärenz des Quantenprozessors nicht zerstört. Gerade dies kann eine geeignete QND-Messung leisten [Oza98].

Weitere Anwendungen liegen in der ultrapräzisen Meßtechnik. Das QND-Verfahren zeigt hier die heute bekannte Grenze für Messungen auf und weist den Weg, wie diese Grenze technisch erreicht werden kann.

Eine weitere Anwendungsmöglichkeit liegt in der optischen Datenübertragung. Mit Hilfe der QND-Technik wäre es hier möglich "quantum repeater" zu bauen, die es erlauben würden, wiederholt Signale zu vermessen, ohne daß sich dabei das ursprüngliche Signal zu Rausch Verhältnis des Strahls ändern würde [Gra98].

Generell kann man sagen, daß je mehr sich Meß- und Kommunikationstechnologien im Zuge fortschreitender Miniaturisierung dem Quantenlimit nähern, desto wichtiger werden fundamentale quantenmechanische Grenzen und ihre optimale Annäherung.

Die nicht quantenzerstörende Messung hat eine Meßgenauigkeit zum Ziel die nur noch über das durch die Heisenbergsche Unschärferelation festgelegte physikalische Mindestmaß limitiert ist. Die Anwendungen liegen sowohl im Bereich der Ultrapräzisionsmeßtechnik (z.B: Gravitationswellenastronomie), als auch im Quantencomputer, für den ein möglichst wechselwirkungsarmer Kontroll- und Auslesemechanismus erforderlich ist.

8 ZUSAMMENFASSUNG

Das aktuelle Gebiet der Quanteninformationsverarbeitung, das auf den Prinzipien der Physik verschränkter Zustände beruht, öffnet die Tür zu einer völlig neuen Technologie.
Man hat nun nicht länger die Möglichkeit, in gewohnter Weise mit den Mitteln der vertrauten mechanistischen Denkweisen bekannte etablierte Prinzipien etwa durch bloße Miniaturisierung weiter zu vervollkommnen, um auf diese Weise zu neuen Entwicklungen zu gelangen, sondern man ist gezwungen, sich in einen abstrakteren Bereich der Natur hineinzudenken und wird dabei nicht nur mit neuen überraschenden Phänomen, sondern auch einer herausfordernden Chance der Realisierung bislang nicht für möglich gehaltener Anwendungen konfrontiert.
Nachdem die Grundlagenforschung erst seit relativ kurzer Zeit überhaupt den experimentellen Nachweis der Existenz dieser „Phänomene“ erbracht hat, befindet man sich derzeit im frühesten Anfangsstadium bei der Entwicklung eines Quantenprozessors. Es ist heute klar und auch *mathematisch beweisbar,* daß ein Quantencomputer in der Lage ist, bestimmte Aufgaben mit einer Effizienz zu lösen, die von allen Computerkonzepten, die sich nicht des Quantenparallelismus bedienen, prinzipiell nicht erreichbar ist. Die Quanten-Turing-Maschine definiert also eine Art Obermenge zu den klassischen Rechnern. Was derzeit noch weitgehend ungeklärt ist, ist die Frage, wie groß die Bandbreite der Einsatzbereiche tatsächlich ist, für die der Quantencomputer eine wesentliche Verbesserung gegenüber klassischen Maschinen anzubieten hat. Insbesondere deshalb kann daher auch noch nicht entschieden werden, ob die gemachten Entdeckungen über kurz oder lang die Grundlage einer neuen Schlüsseltechnologie bilden werden, oder ob sich letztlich dieses Feld aufgrund des beträchtlichen Bedarfs an wissenschaftlich-technischem Equipment und Know-How, bei möglicherweise stagnierenden Anwendungsoptionen, nur als eine für Physik und Philosophie interessante Nische der Naturwissenschaft erweisen wird. Dann wären andere Computerkonzepte, wie beispielsweise Neuro- oder DNA-Rechner dem Quantencomputer möglicherweise aus Gründen der Wirtschaftlichkeit letztendlich überlegen (Tab. 1).
Gleichwohl gelten die geäußerten Bedenken natürlich auch für die alternativen Technologien wie optische und biologische CPUs, wobei diese Herangehensweisen als weniger fundamental hinsichtlich der zugrundeliegenden Paradigmen anzusehen sind.

	Technologischer Aufwand	Anwendungs-breite	Entwick-lungszeit	Paralleles Rechnen	kurzfristiger Nutzen	langfristiges Potential
Weiterentwicklung klassischer Systeme	mittel	klassische Probleme	kurz	sehr stark begrenzt	hoch	gering
DNA-Rechner	gering	noch offen (< 70 Bit)	mittel	bis 70 Bit parallel	gering	mittel
Neuro-Hardware	sehr hoch	Neuroinformatik	lang	begrenzt	gering	hoch
Nanoelektronik (SET)	hoch	klassische Probleme	lang	wie klassisch	mittel	mittel
Quantencomputer	sehr hoch	noch offen	lang	unbegrenzt	gering	hoch

Tab. 1: Potential unterschiedlicher Ansätze für zukünftige Computertechnologien.

Ebenso ist es denkbar, daß sich zwischen den besprochenen Teilbereichen der Quanten-informationsverarbeitung eine starke Heterogenität bezüglich zukünftiger Anwendungen ausbilden wird. Beispielsweise könnte es in in einigen Jahren üblich sein, daß in der Telekommunikation auch verschränkte photonische Zustände wie selbstverständlich genutzt werden, wohingegen ein Quantencomputer vielleicht niemals zur Serienreife gelangt.
Gerade solche Unwägbarkeiten in einem Entwicklungsstadium, wie es hier vorliegt, führen natürlich zu einem recht hohen Risiko für ein Industrieunternehmen, das als potentieller Nutzer der neuen Technologien in Frage käme. Es verwundert daher nicht, daß der überwiegende Anteil industrieller Forschungsaktivitäten auf dem Gebiet der Quanteninformations-verarbeitung von Großbetrieben durchgeführt wird, die traditionsgemäß immer auch grundlagennahe Forschung in ihren Unternehmen praktiziert haben, wie beispielsweise IBM, HP, Lucent (Bell-Labs) oder auch die British Telecom.

Eine interessante historische Parallele, was die Realisierung neuartiger Rechenwerke betrifft, ist bei der Frage nach zukünftigen Computerprinzipien die Tatsache, daß die Entwicklung leistungsfähiger klassischer Rechenmaschinen in England und den USA eng zusammenhing mit der Notwendigkeit die Codes der Achsenmächte im zweiten Weltkrieg zu entschlüsseln. Gerade bei einer solchen Aufgabe ist die Zeit, die zur Bearbeitung eines Problems notwendig ist offensichtlich von zentraler Bedeutung. Die Eignung dieses Prinzips zur vereinfachten Textverarbeitung oder Verbesserung der Telekommunikation war dabei freilich noch nicht abzusehen. Daß es nun wieder die Entschlüsselung von Codes ist, in dem sich das neue als

dem alten Prinzip überlegen erweist, könnte als Hinweis für eine bevorstehende, ähnliche Entwicklung gedeutet werden.

Abschließend soll zu der Frage nach zukünftigen Computersystemen Joel Birnbaum, Direktor der Hewlett-Packard Laboratorien und Senior Vice-President für Forschung und Entwicklung mit dem Auszug aus einer Rede, gehalten während der ACM97 am 3. März, 1997, San Jose, California, zitiert werden [Bir97]:

> *In considering the three alternatives that I have touched on today -- quantum computing, DNA-based computing, and optical computing -- I'm led to propose a tentative conclusion: Communicate with photons, but compute with electrons.*
> *I think this is true because of the great disparity in the coupling forces between charged particles and photons. It seems to me that computing, which involves changes of state and switching, is best done with stronger forces, such as the Coulomb forces among electrons, and that the opposite is true for communications, in which the far weaker interaction among photons is a decided advantage. For that reason, I think that quantum computing has the best long-term chance of becoming a widespread, general-purpose computing technology. Optical and biological computing, I think, will exist in hybrid forms with electronic controllers and memories and will probably find their best application as niche computers for specific large-scale problems in signal processing, pattern recognition, or optimization.*
> *Of course, breakthroughs may occur in the biological and optical realms that could change this conclusion, but I am placing my personal bet on some form of electronic computing being the most prevalent. I particularly like quantum computing because it offers the tantalizing opportunity of an exponentially more powerful form of logic than we have used in the last half century.*

9 ENTWICKLUNGS- UND UMSETZUNGSHEMMNISSE

Das derzeit führende Land auf dem Gebiet der Quanteninformationsverarbeitung sind die Vereinigten Staaten. Insbesondere dem Konzept des Quantencomputers wurde dort wesentlich früher Beachtung geschenkt als dies in Europa der Fall war. Mittel für die Forschung werden in den USA insbesondere von der DARPA (Defense Advanced Research Projects Agency), also aus dem Verteidigungshaushalt zur Verfügung gestellt. Dies ist einsichtig, da sämtliche kryptographischen Anwendungen sowohl des Quantencomputers als auch der Quantenkommunikation eine beträchtliche sicherheitspolitische Relevanz aufweisen. Es ist daher nicht überraschend, daß auch auf der experimentellen Ebene (Ionenfallen und NMR) die USA einen Vorsprung gegenüber Europa und der Bundesrepublik besitzen.
Weil allerdings auch in Deutschland und Europa hervorragende Kompetenzen auf allen Gebieten bestehen, die derzeit hinsichtlich der möglichen Realisierung eines Quantenprozessors in der Experimentierphase oder auch erst in der Diskussion sind, ist der amerikanische Vorsprung als aufholbar einzustufen.

Das derzeitige Ziel der F+E - Aktivitäten beruht kurzfristig nicht so sehr auf der Notwendigkeit, marktfähige Produkte zu entwickeln, dies ist derzeit tatsächlich kaum abzusehen, sondern es kommt darauf an, diese Technologien auf ihre Anwendbarkeit hin zu überprüfen und vor allem bezüglich der personellen Kompetenz und der technischen Leistungsfähigkeit zumindest solange die Konkurrenzfähigkeit sicherzustellen, bis eindeutige Aussagen über die Anwendbarkeit und die zukünftige Marktrelevanz von - auf verschränkten physikalischen Zuständen basierenden - Technologien, gemacht werden können. Gerade das mutmaßliche Potential der Quanteninformationsverarbeitung erweist sich als Dreh- und Angelpunkt bei jeder Überlegung hinsichtlich eines verstärkten Forschungsengagements. Weil die genannten physikalischen Grundprinzipien einen völlig neuartigen Raum für zukünftige technologische Entwicklungen eröffnen und dadurch eine Schlüsselstellung definieren, besteht ein hoher Bedarf an belastbaren umfassenden Aussagen bezüglich der gesamtgesellschaftlichen Tragweite dieses unkonventionellen und schwer einschätzbaren Segments der Physik.
Eines der wesentlichen Entwicklungshemmnisse im Informationsdefizit bezüglich des tatsächlichen Entwicklungspotentials der Quanteninformationsverarbeitung. Schlüsselfrage hierbei ist: Werden sich Quanteninformationstechniken ein breites Anwendungsfeld

erschließen und einen entsprechend hohen Grad der Durchdringung konventioneller Technologien erzielen, wie dies im Fall des klassischen binären Rechners geschehen ist, oder werden verschränkte Zustände nur eine Lösung für spezielle, eng begrenzte technische Fragestellungen sein?

Die Beantwortung dieser Frage ist natürlich für die Industrie von besonderer Relevanz, sofern es Entscheidungen bezüglich eines Forschungsengagements auf diesem Gebiet betrifft.

Neben den rein experimentellen Schwierigkeiten, wie etwa Beherrschung von Verschränkung und Unterdrückung bzw. Kompensation von Dekohärenz ist also die Anwendbarkeit ein wichtiger Punkt der durch die Forschung geklärt werden muß, bevor abschließende Beurteilungen auf diesem Gebiet getroffen werden können.

10 ANHANG A

10.1 Literatur zur Quanteninformationsverarbeitung

Um eine Aussage über gegenwärtige Tendenzen im Bereich Quanteninformation machen zu können, wurden entsprechende Literaturrecherchen in der Datenbank INSPEC durchgeführt. Die Resultate sind unten graphisch dargestellt und erlauben eine erste Einschätzung der Dynamik der diesbezüglichen Forschungsaktivitäten sowohl im nationalen Vergleich als auch weltweit.

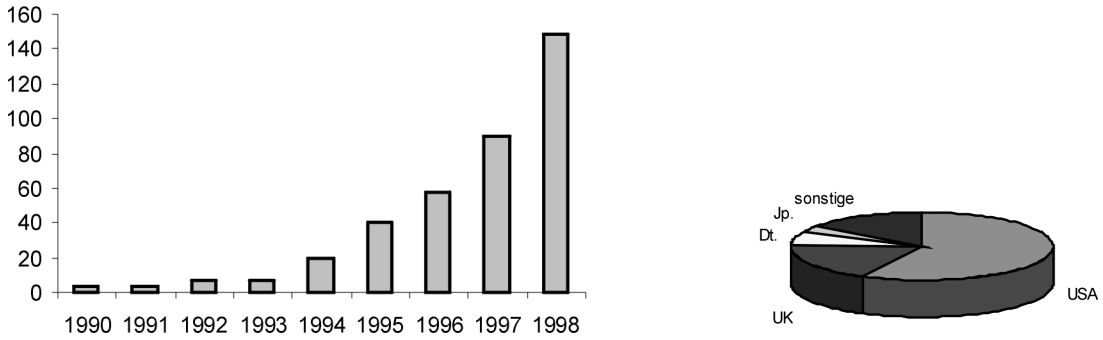


Abb. 22: Links: Anzahl der weltweiten Publikationen pro Jahr auf dem Quanteninformations-Teilgebiet des „quantum computing“ seit 1990. Rechts: Jeweiliger prozentualer Anteil der führenden Industrienationen an den Veröffentlichungen auf dem Gebiet des Quantencomputers.

Seit dem Jahr 1994 ist weltweit ein sehr starker Anstieg der Aktivitäten auf dem Gebiet der Quanteninformationsverarbeitung und hierin insbesondere im Teilbereich des Quantencomputers zu verzeichnen. Dies liegt vor allem auch an der Entdeckung des Quantenalgorithmus von Shor zur effizienten Faktorisierung von Primzahlen. Damit wurde ein wichtiger Schritt weg vom bloßen Quantensimulator hin zum universell einsetzbaren digitalen Quantencomputer vollzogen.
Mit der sich dadurch abzeichnenden Möglichkeit bislang als sicher angesehene Kryptographieverfahren entschlüsseln zu können, wurden in Folge des Shorschen Algorithmus in den USA auch erhebliche Geldmittel von seiten des Militärs aufgewendet.

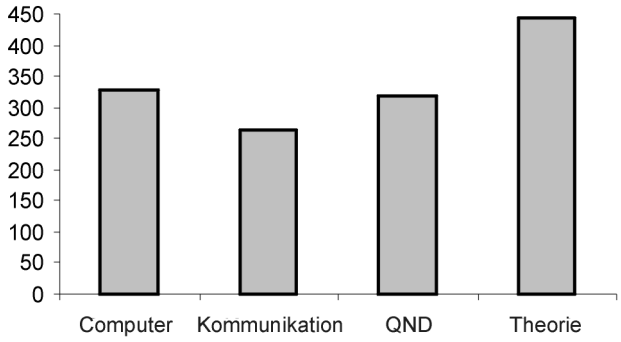


Abb. 23: Aufteilung der Publikationen in die unterschiedlichen Teilaspekte der Quanteninformationsverarbeitung.

10.2 Patente im Bereich Quanteninformationstechniken

Die Recherchen wurden in den internationalen Patentdatenbanken WPINDEX und INPADOC durchgeführt. Es wurden getrennte Recherchen für die Bereiche quantum computing, quantum cryptography und quantum non-demolition vorgenommen.

10.2.1 Quantencomputer

Quantum computer
INVENTORS: Bruce Kane
ASSIGNEES: Unisearch Limited
ISSUED: Sept 17, 1997
SERIAL NUMBER: WO 9914858

Three dot computing elements
INVENTORS: David P. DiVincenzo, Chappaqua, NY
ASSIGNEES: International Business Machines Corporation
ISSUED: June 25, 1996
SERIAL NUMBER: US291306

Method for reducing decoherence in quantum computer
INVENTORS: Peter W. Shor, New Providence, NJ
ASSIGNEES: Lucent technologies Inc., Murray Hill, NJ
ISSUED: June 16, 1998
SERIAL NUMBER: US548923

Parallel architecture for quantum computers using ion trap arrays
INVENTORS: Ralph Godwin Devoe
ASSIGNEES: IBM
ISSUED: Aug. 11, 1998
SERIAL NUMBER: US5793091

10.2.2 Quantenkryptographie

Interferometric quantum cryptographic key distribution system
INVENTORS: Charles H. Bennett
ASSIGNEE: IBM
ISSUED: April 26, 1994
SERIAL NUMBER: US5307410

Quantum key distribution using non-orthogonal macroscopic signals
INVENTORS: Charles H. Bennett, Stephen J. Wiesner
ASSIGNEE: IBM
ISSUED: Mai 07, 1996
SERIAL NUMBER: US5515438

System and method for key distribution using quantum cryptography
INVENTORS: Paul David Townsend
ASSIGNEE: British Telecomm
ISSUED: Oct. 07, 1997
SERIAL NUMBER: US5675648

System and method for key distribution using quantum cryptography
INVENTORS: Paul David Townsend, Keith James Blow
ASSIGNEE: British Telecomm
ISSUED: June 25, 1998
SERIAL NUMBER: US693109

Key distribution in a multiple access network using quantum cryptography
INVENTORS: David W: Smith, Paul D. Townsend
ASSIGNEE: British Telecomm
ISSUED: June 16, 1998
SERIAL NUMBER: US5768378

Method for key distribution using quantum cryptography
INVENTORS: Simon J. Phoenix, Stephen M. Barnett
ASSIGNEE: British Telecomm
ISSUED: June 9, 1998
SERIAL NUMBER: US5764765

System and method for quantum cryptography
INVENTORS: Keith J. Blow
ASSIGNEE: British Telecomm
ISSUED: May 26, 1998
SERIAL NUMBER: US5757912

Quantum cryptography device and method
INVENTORS: Nicolas Gisin, Bruno Huttner, Antoine Muller, Beat Perny, Hugo Zbinden
ASSIGNEE: Telecom PTT
ISSUED: March 12, 1998
SERIAL NUMBER: WO9810560

Method for key distribution using quantum cryptography
INVENTORS: Stephen M. Barnett, Simon J.D. Phoenix
ASSIGNEE: British Telecomm
ISSUED: June 9, 1998
SERIAL NUMBER: US5764765

Quantum cryptography
INVENTORS: Paul D. Townsend
ASSIGNEE: British Telecomm
ISSUED: June 4, 1998
SERIAL NUMBER: EP0776558

Method and apparatus for polarisation-insensitive quantum cryptography
INVENTORS: Paul D. Townsend
ASSIGNEE: British Telecomm
ISSUED: Nov. 27, 1997
SERIAL NUMBER: WO9744936

Improved detector for quantum cryptography
INVENTORS: George L. Morgan, Richard J. Hughes, Gabriel G. Luther
ASSIGNEE: George L. Morgan, Univ. California, Gabriel G. Luther, Richard J. Hughes
ISSUED: Nov. 20, 1997
SERIAL NUMBER: WO9743840

Polarisation Modulation
INVENTORS: Stephen V. Kershaw, Paul D. Townsend
ASSIGNEE: Stephen V. Kershaw, Paul D. Townsend, British Telecomm
ISSUED: March 14, 1996
SERIAL NUMBER: WO9607951

Quantum Cryptography using discarded data
INVENTORS: Simon J.D. Phoenix, Stephen M. Barnett
ASSIGNEE: British Telecomm, Simon J.D. Phoenix, Stephen M. Barnett
ISSUED: April 14, 1994
SERIAL NUMBER: WO9408409

Quantum cryptographic system with reduced data loss
INVENTORS: Lo; Hoi-Kwong ,Chau; Hoi Fung
ASSIGNEE: none
ISSUED: March 24, 1998
SERIAL NUMBER: US5732139

Method and apparatus for quantum communication employing nonclassical correlations of quadrature-phase amplitudes
INVENTORS: Kimble; Harry J.; Ou, Zhe-Yu; Pereira; Silvania E.
ASSIGNEE: California Institute of Technology, Pasadena, CA
ISSUED: Aug. 16, 1994
SERIAL NUMBER: US5339182

Apparatus and method for quantum mechanical encryption for the transmission of secure communications
INVENTORS: Franson; James D.
ASSIGNEE: The Johns Hopkins University, Baltimore, MD
ISSUED: Sept. 7, 1993
SERIAL NUMBER: US5243649

10.2.3 Quantum nondemolition

Device and method for quantum nondemolition measurements using parametric oscillation
INVENTORS: Harry J. Kimble, Silvania F. Pereira, Daniel F. Wallis
ASSIGNEE: Univ. Texas
ISSUED: July 31, 1990
SERIAL NUMBER: US4944592

Quantum non-demolition optical tapping
INVENTORS: Keith J. Blow, Brian P. Nelson, Nicholas J. Doran
ASSIGNEES: British Telecomm
ISSUED: July 26, 1994
SERIAL NUMBER: US5333220

10.3 Internationale Institute mit Aktivitäten auf dem Gebiet der Quanteninformationsverarbeitung

Diese Auflistung erhebt keinen Anspruch auf Vollständigkeit, außerdem ist die Reihenfolge der Aufzählung zufällig und nicht als Wertung zu verstehen

Aktivitäten in Europa:

Belgien

Universite Libre de Bruxelles
Dr. N. Cerf
Tel.. +32-2-6505535
Fax.: +32-2-6505767
Email: ncerf@ulb.ac.be

Riverland Research
Dr. W. v.d. Velde
Dr. A. Karlson
Tel.: +32 2 721 5454
Fax.: +32 2 721 5380
Email: wvdv@riv.be
akarlson@riv.be

Finnland

Universität Helsinki
Dr. K.-A. Suominen (Theorie)
Tel.: +358-9-1918530
Fax.: +358-9-1918458
Web: http://www.physics.helsinki.fi/~kasuomin/AMO.html

Frankreich

Departement de Physique de l´ENS
Prof. Serge Haroche
Tel.: +33-1-44-32-3420
Fax.: +33-1-45-87-34-89
Email: serge.haroche@physique.ens.fr
Web: http://www.phys.ens.fr/

Universite Paris Sud
Prof. M. Santha
Tel.: +33-1-69156599
Fax.: +33-1-69156587
Email: miklos.santha@lri.fr

Großbritannien

Centre for Quantum Computation, Oxford
Prof. Artur Ekert (Theorie)
Prof. Andrew Steane (Ionenfallen)
Tel.: ++44 1865-282 202
Fax.: ++44 1865-272 387
Mail: enquiries@qubit.org
Web: http://www.qubit.org

University of Plymouth
Prof. R. Jozsa
Tel.: +44 1752 232734
Fax.: +44 1752 232780
Email: rjozsa@plymouth.ac.uk

Prof P.L. Knight (Quantenoptik - Theorie)
Tel.: ++44 171 5947727
Fax.: ++44 171 8238376
Mail: p.knight@ic.ac.uk
Web: http://www.lsr.ph.ic.ac.uk/TQO/index.html

Univ. of Cambridge
Dr. S. Popescu
Tel.: +44-1223-330543
Fax.: +44-1223-330508
Email. sp230@netwon.cam.ac.uk

DERA Malvern
Dr. J.G. Rarity
Tel.: +44 1684 895031
Fax.: +44 1684 896270
Mail: rarity@dera.gov.uk
Web: http://www.lsr.ph.ic.ac.uk/TQO/EPSRC/DRA/index.html

Hewlett-Packard Laboratories
Dr. T.P. Spiller
Tel.: +44 117 9229280
Fax.: +44 117 9228924
Email: ts@hplb.hpl.hp.com

University of Wales
Prof. Dr. Samuel Braunstein
Fax.: ++44 1248 36-1429
Mail: schmuel@sees.bangor.ac.uk
Web: http://www.sees.bangor.ac.uk/~pieter/group.html

Italien

Dipartimento di Scienze Fisiche ed Astronomiche
Dr. M. Palma
Tel.: (0)91-617 1579
Fax.: (0)91-617 1617
Email: palmagm@mildred.physics.ox.ac.uk

Universita´di Pavia
Prof. G.M. D´Ariano
Tel.: +39 382 507484
Fax.: +39 382 507563
Email: darianopv.infn.it

Institute for Scientific Interchange Foundation, Turin
Prof. Mario Rasetti
Tel.: ++39-011-6603090
Fax.: ++39-011-6600049
Mail: isi@isi36a.isi.it
Web: http://www.isi.it/

Irland

The Ntl. Univ. of Ireland, Maynooth
Dr. J.M. Twamley
Tel.: +353 1 708 3553
Fax.: +353 1 708 3967
Email: jtwamley@hphys.may.ie

Niederlande

TU Delft Applied Physics
Prof. J. E. Mooij
Lorentzweg 1
2628 CJ Delft
Tel: +31 15 278 6153
Fax: +31 15 278 3251
Email: mooij@qt.tn.tudelft.nl
Web.: http://qt.tn.tudelft.nl/

Quantum Computing and Advanced System Research, CWI
Prof. P. Vitanyi
Tel.: (+)31 20 5924124
Fax.: (+)31 20 5924199
Email: paulv@cwi.nl

Österreich

Universität Innsbruck
Prof. Peter Zoller (Theorie)
Prof. Ignacio Cirac (Theorie)
Tel.: ++43-512-507-6200
Fax.: ++43-512-507-2919
Web: http://info.uibk.ac.at:/c/c7/c705/qo/#info
Mail: peter.zoller@uibk.ac.at
ignacio.cirac@uibk.ac.at

Prof. Anton Zeilinger
Tel.: ++43-512-507-6300
Fax.: ++43-512-507-2921
Mail: anton.zeilinger@uibk.ac.at
Web: http://info.uibk.ac.at/c/c7/c704/qo/

Prof. Rainer Blatt
Tel.: ++43-512-507-6350
Fax.: ++43-512-507-2952
Mail: rainer.blatt@uibk.ac.at
Web: http://heart-c704.uibk.ac.at/rb.html

Polen

University of Gdansk
Dr. R. Horodecki
ul. Wita Stwosza 57
80-952 Gdansk
Email: fizrh@univ.gda.pl

Schweiz

Universität Genf
Prof Nicolas Gisin
Tel.: ++41 22 702 6595
Fax.: ++41 22 781 0980
Mail: nicolas.gisin@physics.unige.ch
Web: http://www.unige.ch/gapoptic/

Spanien

Univ. de Barcelona
Prof. R. Tarrach
Tel.: 343-4021180
Fax.: 343-4021198
Email: tarrach@qubit.ecm.ub.es

Univ. de Cantabria
Prof. E. Santos
Tel.: +34 42 201451
Fax.: +34 42 201402
Email. santos@besaya.unican.es

Im Zuge des **5. EU-Rahmenprogramms** wurde 1999 ein Europäisches Förderprogram zur Quanteninformationsverarbeitung begonnen.
Diese Aktivitäten sind dem Bereich **FET** (Future and Emerging Technologies) des **IST** (Information Society Technologies) - Programms zugeordnet.
Der Bereich FET ist speziell auf die Förderung von Projekten mit visionären und weitreichenden Ansätzen, bei hohem Risiko und relativ langer Zeitdauer bis zur praktischen Umsetzung, zugeschnitten.
Weiter Informationen finden sich auf der FET-Homepage:
http://www.cordis.lu/ist/fetintro.htm

Aktivitäten außerhalb Europas:

Japan

NTT Basic Research Laboratories
3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa
243-0198 JAPAN
Tel +81 462 40 3405
Fax +81 462 40 4726
E-mail nobu@will.brl.ntt.co.jp
http://www.brl.ntt.co.jp/physics/butsusei-g/index.html

Kanada

Laboratory for Theoretical and Quantum Computing
Université de Montréal
C.P. 6128 succursale Centre-ville
Montréal (Québec) H3C 2J7 Canada
Tel (514) 343-6111 ext: 3514
Fax (514) 343-5834
Email utheorie@IRO.UMontreal.ca

USA

National Institute of Standards and Technology
Time and Frequency Division
Dr. David. J. Wineland
325 Broadway, Boulder, Colorado 80303, USA
Fax: (303) 497-7375 or 497-6461
wineland@boulder.nist.gov
http://www.bldrdoc.gov/timefreq/ion/index.htm

MIT
Physics and Media Group
Prof. Neil Gershenfeld
77 Massachusetts Avenue
Cambridge, MA 02139-4307 USA

University of California, Berkeley
EECS Electrical Engineering and Computer Science
Computer Science Division, Administrative Office
387 Soda Hall, UC Berkeley
Berkeley, CA 94720-1776
Tel.: 642-1042, Fax: 642-5775
http://hera.eecs.berkeley.edu/Brochure/Areas/theory.html
vazirani@cs.berkeley.edu

Los Alamos National Laboratory
Neutron Science and Technology Group
TA-53, MS-H803
Los Alamos, New Mexico 87545
http://p23.lanl.gov/Quantum/quantum.html

University of Southern California - ISI
Advanced Computer Architecture Laboratory
4676 Admiralty Way, #944
Marina Del Rey, CA 90292-6695
Tel.: (310) 822-1511 x268
Fax.: (310) 823-6714
despain@usc.edu
http://www.isi.edu/acal/

AT&T Labs - Research
Dr. Peter Shor
180 Park Avenue
P.O. Box 971
Florham Park, NJ 07932-0971
Email: shor@research.att.com
Tel: 973 360 8443; Fax: 973 360 8178

Caltech
Prof. Jeff Kimble
Norman Bridge Laboratory of Physics
California Institute of Technology 12-33
Pasadena, CA 91125
Tel: (626) 395 8342, Fax (626) 793 9506
http://www.caltech.edu/subpages/pmares.html

IBM Research Division
Thomas J. Watson Center
Dr. David P. DiVincenzo
P.O. Box 218
Yorktown Heights
NY 10598 USA

10.4 Aktivitäten in Deutschland

Prof. Thomas Beth
Institut für Algorithmen und kognitive Systeme
Universität Karlsruhe
Tel.: 0721/608-4205
Fax: 0721/696893
http://avalon.ira.uka.de/Iaks-beth/iaks-beth.html

Prof. Wolfgang Elsäßer
TU Darmstadt
Tel.: +49 6151 / 16 - 2222
Fax: +49 6151 / 16 - 3022
elsaesser@physik.tu-darmstadt.de
http://www.physik.tu-darmstadt.de/hlo/

Prof. Wolfgang Ertmer
Universität Hannover
Telefon: 0511/762-2231/-2589
Telefax: 0511/762-2211
EMail: ertmer@mbox.iqo.uni-hannover.de
http://www.iqo.uni-hannover.de

Prof. Peter Hänggi
Universität Augsburg
Tel.: +49 +821-598-3249
Fax: +49 +821-598-3222
E-mail: Hanggi@Physik.Uni-Augsburg.DE
http://www.physik.uni-augsburg.de/theo1/

Prof. Theodor W. Hänsch
LMU München
++49-89/2180-3212
++49-89/285192
t.w.haensch@physik.uni-muenchen.de
http://www.mpq.mpg.de/~haensch/haensch.html

Prof. Andreas Hemmerich
Institut für Laserphysik
Hamburg
Telefon : (49) (0)40-4123 2501
Fax : (49) (0)40-4123 6571
email: hemmerich@physnet.uni-hamburg.de

Prof. Gerd Leuchs
Universität Erlangen
09131/85-28371
09131/13508
leuchs@physik.uni-erlangen.de
http://www.physik.uni-erlangen.de/optik/main_d.html

Prof. Günter Mahler
Universität Stuttgart
Tel.: ++49 (0)711 685-5101
Fax: ++49 (0)711 685-4909
mahler@theo.physik.uni-stuttgart.de
http://tutnix.theo1.physik.uni-stuttgart.de/mahler/

Prof. Werner Martienssen
Physikalisches Institut
Robert-Mayer-Str. 2-4
Universität Frankfurt
http://www.rz.uni-frankfurt.de/~kasieber/quanten_html/quantin.html

Prof. Wolfgang Mathis
Universität Magdeburg
Phone: (0391) 67-18862
Fax: (0391) 67-11230
mathis@ipe.et.uni-magdeburg.de
http://pmt05.et.uni-magdeburg.de/elektronik/main.html

Prof. Michael Mehring
Tel.: +49 (0)711-685-0
Fax: +49 (0)711-685-5285
Email: m.mehring@physik.uni-stuttgart.de
http://www.physik.uni-stuttgart.de/ExPhys/2.Phys.Inst./Uebersicht.html

Prof. Dieter Meschede
Universität Bonn
Telefon: +49-228-73-3478 o. -3477 (Büro)
Fax: +49-228-73-3474
E-mail: meschede@iap.uni-bonn.de
http://ibm.rhrz.uni-bonn.de/iap/arb_m.html

Prof. Gerhard Rempe
Universität Konstanz
Tel.: 07531/88-3820
Fax: 07531/88-3072
e-mail: gerhard.rempe@uni-konstanz.de
http://ag-rempe.physik.uni-konstanz.de/cgi-bin/rempe

Prof. Hartmut G. Roskos
Universität Frankfurt
Telefon 069/798-22616
Fax 069/798-28448
roskos@physik.uni-frankfurt.de
http://www.rz.uni-frankfurt.de/piweb/femto/femto_no_frames/index.html

Prof. Axel Schenzle
LMU München
Phone +49/89/2394-4556
Fax +49/89/2805248
Axel.Schenzle@physik.uni-muenchen.de
http://tqo.hep.physik.uni-muenchen.de/index.html

Prof. Peter Schleich
Universität Ulm
Telefon: +49 (731) 50-23080
FAX: +49 (731) 50-23086
E-mail: Wolfgang.Schleich@physik.uni-ulm.de
http://www.physik.uni-ulm.de/quan/quanphys.html

Prof. Gerd Schön
Universität Karlsruhe
Telefon: ++49-721-6083361
Fax: ++49-721-698150
gerd.schoen@phys.uni-karlsruhe.de
http://www-tfp.physik.uni-karlsruhe.de/

Prof. Peter E. Toschek
Institut für Laser-Physik
Hamburg
Telefon : (49) (0)40-4123 2380
Fax : (49) (0)40-4123 6571
E-Post: toschek@physnet.uni-hamburg.de
http://www.physnet.uni-hamburg.de/home/vms/group_a/index.html

Prof. Alexey Ustinov
Universität Erlangen
+49(0)9131 8527268
ustinov@physik.uni-erlangen.de
http://www.physik.uni-erlangen.de/PI3/Ustinov/ind_news.html

Prof. Herbert Walther
Max-Planck Institut für Quantenoptik, Abt. Laserphysik
Tel.: ++49 - (0)89 - 3 29 05 - 704
Fax: ++49 - (0)89 - 3 29 05 - 200
E-Mail: Herbert.Walther@mpq.mpg.de
http://www.mpq.mpg.de/mpq/laserphysics.html

Prof. Harald Weinfurter
Institut für Experimentalphysik
Technikerstr. 25
Universität Innsbruck
Phone: +43-512-507-6316
E-Mail: Harald.Weinfurter@uibk.ac.at

Prof. Reinhard F. Werner
Universität Braunschweig
Tel.: +49-531-391-5200
Fax: +49-531-391-8183
R.Werner@tu-bs.de
http://134.169.50.208/qi/qi.html

Prof. Günther Werth
Universität Mainz
Tel.: +49 6131 39 2883
Fax: +49 6131 39 5169
Email: werth@dipmza.physik.uni-mainz.de
http://dipmza.physik.uni-mainz.de/~www_werth/welcome.html

Prof. Dr. Jörg P. Kotthaus
Sektion Physik der LMU, Geschwister Scholl Platz 1
D-80539 München, Germany
Tel: +49-89-2180-3737
Fax: +49-89-2180-3182
Email: jorg.kotthaus@physik.uni-muenchen.de

1998 wurde ein Schwerpunkt (1078) der DFG (Deutsche Forschungsgemeinschaft) zum Thema „Quanteninformationsverarbeitung“ neu eingerichtet.

Kontakt über Referat IIC9 (Dr. Albrecht Szillinsky),
Kennedyallee 40, 53175 Bonn
Tel.: 0228/885- 2477, Fax: 0228/885-2777
E-Mail: szillinsky@iic9.d400.de.

11 ANHANG B

11.1 Auffinden der Periode einer Funktion

Das Auffinden der Periode einer Funktion spielt für zahlreiche Algorithmen, z.B. auch die Faktorisierung nach Shor, eine zentrale Rolle und soll hier kurz erläutert werden [Ste98].

Gegeben sei eine Funktion *f(x)* mit Periode *r*, d.h. *f(x+r) = f(x)*
Für gegebenes *x* sei die Berechnung von *f(x)* ein effizient lösbares Problem. Die Periodozität *r* soll nicht analytisch ableitbar sein, sich jedoch innerhalb eines vorgegebenen Intervalls $N/2 < r < N$ befinden.
Klassisch muß für jeden der *N/2* Werte *x* innerhalb des Intervalls der Funktionswert *f(x)* gebildet und überprüft werden, wann ein Funktionswert reproduziert wird.
In Abhängigkeit von der Anzahl Bits *z = log N*, die als Eingabeinformation für *N* die Größe des Intervalls und damit den Umfang des Problems spezifizieren, steigt der Aufwand der Berechung der Periodizität *r* nach einem Exponentialgesetz an.
Für die Lösung des Problems mit Hilfe eines Quantencomputers werden *n = 4z = 4logN* Qubits benötigt. Diese werden in zwei Register *a* und *b* unterteilt. Beide Register seien zu Beginn im Ausgangszustand $|0\rangle$ präpariert.
In einem nächsten Schritt wird jedes Qubit des Registers *a* einer Operation *H* unterzogen, so daß der Gesamtzustand

$$\frac{1}{\sqrt{w}}\sum_{a=0}^{w-1}|a\rangle|0\rangle$$ entsteht, mit $w = 2^n$.

Danach wird über die Anwendung eines Netzwerkes logischer Operationen die unitäre, weil reversible Operation $U_f|a\rangle|0\rangle = |a\rangle|f(a)\rangle$ durchgeführt. Man erhält dann für den Gesamtzustand:

$$\frac{1}{\sqrt{w}}\sum_{a=0}^{w-1}|a\rangle|f(a)\rangle$$

Es sei hier betont, daß dieser letzte Schritt durch die physikalische Manipulation von *4z* Qubits erreicht wurde, wohingegen klassisch $w = 2^{4n}$ Werte für *f(a)* einzeln berechnet werden

müßten. In der Superposition der physikalischen Zustände, die von verschränkten physikalischen Objekten gebildet werden, ist damit *gleichzeitig* die gesamte notwendige Information enthalten, die zur Darstellung und Bearbeitung des Problems benötigt wird. Die Eigenzustände, die allein einem direkten Zugriff zugänglich sind, stellen somit eine Art Eckpfeiler dar, die den gesamten Raum der, auf dem Weg der Verschränkung quantenmechanischer Objekte entstehenden, für die Rechnung notwendigen Zwischenzustände aufspannen.

Zwar liegen jetzt alle 2^n Funktionswerte *f(a)* physikalisch vor. Da sie dies jedoch in Form von Superpositionen tun, ist ein direkter Zugriff auf jeden einzelnen Wert, etwa zum Zwecke des Vergleichs nicht möglich, da der Gesamtzustand in einem solchen Fall in eine Superposition derjenigen Zustände kollabiert, die Eigenzustände $|u\rangle$ zu dem gemessenen Eigenwert *u* sind. Nach einer solchen Messung befindet man sich dann im Zustand:

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |d_u + j \cdot r\rangle |u\rangle$$

wobei d_u+jr, für $j = 0,1,2,...,M-1$ alle diejenigen Werte *a* bezeichnet für die $f(a) = u$ wird.

Die Messung des Registers *b* hat also den Gesamtzustand in einen reduzierten Superpositionszustand überführt, der aus einer Überlagerung von $M \cong w/r$ Zuständen mit Werten von *a*, die durch die Periode *r* separiert sind, besteht. Die physikalische Selektion der entsprechenden Zustände ist dabei als ein Interferenzeffekt aufzufassen dessen Parameter von der Wechselwirkung bestimmt werden, die mit der Messung des Registers *b* verbunden ist.

Um die Periodizität zu erhalten, unterwirft man den Gesamtzustand nun einer Fouriertransformation:

$$U_{FT} |a\rangle = \frac{1}{\sqrt{w}} \sum_{k=0}^{w-1} e^{i 2\pi k a / w} |k\rangle$$

und erhält:

$$U_{FT} \frac{1}{\sqrt{w/r}} \sum_{j=0}^{w/r-1} |d_u + j \cdot r\rangle = \frac{1}{\sqrt{r}} \sum_k \tilde{f}(k) |k\rangle$$

mit

$$|\tilde{f}(k)| = \begin{cases} 1, \text{ falls } k \text{ Vielfaches von } w/r \\ 0, \text{ sonst} \end{cases}$$

Eine Messung des Registers *a* ergibt nun einen Wert, der ein Vielfaches von *w/r* sein muß. Daraus läßt sich schließlich die Periodizität *r* ableiten.

An diesem Beispiel wird deutlich, wie durch die Nutzung von Superpositionen, die durch verschränkte Quantengatter realisiert werden, eine hochgradige Parallelisierung eines klassisch seriellen Rechenprozesses erfolgen kann. Es ist jedoch zu beachten, daß die parallel verarbeiteten Daten miteinander korreliert sind. Ein exponentieller Geschwindigkeitsvorteil für nicht korrelierte Daten läßt sich mit dieser Art von Quantenparallelismus nicht erreichen. Dennoch gibt es mehrere Quantenalgorithmen, die diese effiziente Art der Ermittelung der Periodizität einer Funktion für eine Reihe von Anwendungen nützen. Der bekannteste dieser Algorithmen ist die Faktorisierung in Primzahlen nach Shor.

12 ANHANG C

12.1 Literaturverzeichnis

(Zitate der Form „quant-ph/.....“ verweisen auf Vorveröffentlichungen die unter der jeweils angegebenen Nummer im Internet vom Los-Alamos-Preprint-Server unter der Adresse *http://xxx.lanl.gov* abgerufen werden können)

[Adl94] L. Adleman, Science, 266, 1021, (1994)

[Ang97] J.R. Anglin, J.P. Paz, and W.H. Zurek, Phys. Rev. A, 55, (1997), 4041

[Asp81] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett., 47, 460, (1981)

[Asp82] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett., 49, 1804, (1982)

[Bar95a] A. Barenco and A. Ekert, J Mod Optic, 42, 1253-1259, (1995)

[Bar95b] A. Barenco, D. Deutsch, and A. Ekert, R. Josza, Phys. Rev. Lett., 74, 4083, (1995)

[Bar95c] A. Barenco et al., Phys. Rev. A, 52, 3457, (1995)

[Bar98] S.E. Barnes, "Efficient quantum computing on low temperature spin ensembles", quant-ph/9804065

[Bel64] J.S. Bell, Physics (Long Island City, New York), 1, 195, (1964)

[Ben80] P. Benioff, J. Stat. Phys., 22, 563, (1980)

[Ben89] C. Bennett, and G. Brassard, SIGACT News, Vol. 20, pp. 78 - 82, Fall (1989)

[Ben92a] C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, Journal of Cryptology, Vol. 5, pp. 3 - 28, (1992)

[Ben92b] C. Bennett, Phys. Rev. Lett., 68, 3121, (1992)

[Ben92c] C.H. Bennett and S. Wiesner, Phys. Rev. Lett., 69, 2881, (1992)

[Ben92d] C. Bennett, G. Brassard, and A. Ekert, Scientific American, 267, 26, Oct (1992)

[Ben93] C.H. Bennett et al., Phys. Rev. Lett. 70, 1895, (1993)

[Ben95] K. Bencheikh, J.A. Levenson, Ph. Grangier, O. Lopez, Phys. Rev. Lett. 75, 3422, (1995)

[Ber86] J.C. Bergquist, R.G. Hulet, W.M.Itano, and D.J. Wineland, Phys. Rev. Lett., 57, (1986), 1699

[Ber94] P. Berman (Ed.), Cavity QED, Advances in Atomic, Molecular, and Optical Physics, (Academic Press, New York, 1994)

[Bir94] G. Birkl, J.A. Yeazell, R. Rückerl, and H. Walther, Europhys. Lett., 27, (1994), 197-202

[Bir97] J. Birnbaum, ACM97, Rede abrufbar unter *http://www.hpl.hp.com/speeches/acm97.html*

[Bit98] W.T. Bittler et al., Phys. Rev. Lett. 81, 3283, (1998)

[Boh51] D. Bohm, "Quantum Theorie", Prentice-Hall, Englewood Cliffs, N.J., (1951)

[Bon98] N.H. Bonadeo, J. Erland, D. Gammon, D. Park, D.S. Katzer, D.G. Steel, Science, 282, 1473, (1998)

[Bou97] D. Bouwmeester et al., Nature 390, 575-579, (1997)

[Bos98] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett., 80, 1121-1125, (1998)

[Bra80] V.B. Braginsky, Y.I. Vorontsov, K.S. Thorne, Science, 209, 547, (1980)

[Bra98] G. Brassard, S. Braunstein, and R. Cleve, Physica D, 120, 43-47, (1998)

[Bre92] J. Breguet, and N. Gisin, Opt. Lett., 68, 3121 (1992)

[Bri99] H.-J. Briegel, T. Calarco, D. Jaksch, J.I. Cirac, and P. Zoller, Preprint, quant-ph/9904010

[Bru94] M. Brune, P. Nussenzveig, F. Schmidt-Kaler, F. Bernadot, A. Maali, J.-M. Raimond, and S. Haroche, Phys. Rev. Lett., 72, 3339, (1994)

[Bru97] R. Bruckmeier, H. Hansen, S. Schiller, Phys. Rev. Lett., 79, 1463, (1997)

[Byc95] Y.A. Bychkov, T. Maniv, and I.D. Vagner, Solid State Commun. 94, 61, (1995)

[Cav80] C.M. Caves, K.S. Thorne, R.W.P. Drever, V.D. Sandberg, M. Zimmermann, Rev. Mod. Phys., 52, 341, (1980)

[Cer96] N.J. Cerf, C. Adami, „Quantum Mechanics of Measurements“, bei Phys. Rev. A eingereicht, preprint quant-ph/9605002

[Cha77] G. Chaitin, IBM Journal of Research and Development, Vol. 21, July (1977), 116-119

[Chu96] I.L. Chuang, and Y. Yamamoto, Phys. Rev. Lett., 76, 4281, (1996)

[Chu98] I.L. Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd, Experimental realization of a quantum algorithm, quant-ph/9801037

[Cir95] J.I. Cirac and P. Zoller, Phys. Rev. Lett, 74, (1995), 4090-4097

[Cir97] J.I Cirac, P. Zoller, H.J. Kimble, and H. Mabuchi, Phys. Rev. Lett, 78, (1997), 3221

[Cla76] J.F. Clauser, Phys. Rev. Lett., 36, 1223, (1976)

[Cor97] D.G. Cory, A.F. Fahmy, and T.F. Havel, Proc. Natl. Acad. Sci. USA, 94, (1997), 1634-1639

[Cor98] D.G. Cory, M. Price, A.F. Fahmy, and T.F. Havel, Nuclear magnetic resonance spectroscopy: an experimentally accessible paradigm for quantum computing, Physica D, in press

[Cou98] J.-M. Courty, S. Spälter, F. König, A. Sizmann, and G. Leuchs, Phys. Rev. A, 58, 1501, (1998)

[Dal98] F. Dalfovo et al., cond-mat/9806038

[Dav94] L. Davidovich, N. Zagury, M. Brune, J.-M. Raimond, and S. Haroche, Phys. Rev. A, 50, R895, (1994)

[Deh67] H.G. Dehmelt, Advances in Atomic and Molecular Physics, 3, 53 (1967)

[Deh69] H.G. Dehmelt, Advances in Atomic and Molecular Physics, 5, 109 (1969)

[Deu85] D. Deutsch, Proc. Roy. Soc. London, A400, 97, (1985)

[Die89] F. Diedrich, J.C. Bergquist, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett., 62, (1989), 403

[DiF94] F. DiFilippo et al. Phys. Rev. Lett., 73, 1481, (1994)

[Dru93] P.D. Drummond, R.M. Shelby, S.R. Friberg, Y. Yamamoto, Nature, 365, 307, (1993)

[Dür98] S. Dürr, T. Nonn and G. Rempe, Nature, 395, 33, (1998)

[Ein35] A. Einstein, B. Podolsky, N. Rosen, Phys. Rev., 47, 777, (1935)

[Eke92] A. Ekert, Phys. Rev. Lett., 67, 661-663, (1992)

[Enk97] S.J. van Enk, J.I. Cirac, and P. Zoller, Phys. Rev. Lett., 78, (1997), 429

[Enk98] S.J. van Enk, H.J. Kimble, J.I. Cirac, and P. Zoller, Quantum Communication with Phantom Photons, quant-ph/9805003

[Ern94] R.R. Ernst, G. Bodenhausen, and A. Wokaum, Principles of Nuclear Magnetic Resonance in One and Two Dimensions, (Oxford University Press, Oxford, 1994)

[Esc95] J. Eschner, B. Appasamy, and P.E. Toschek, Phys. Rev. Lett., 74, 2435, (1995)

[Fey82] R. Feynman, Int. J. Theo. Phys., 21, 467, (1982)

[Fri98] S. Friebel et al., Phys. Rev. A 57, R20, (1998)

[Fre72] S.J. Freedman and J.F. Clauser, Phys. Rev. Lett., 28, 938, (1972)

[Fur98] A. Furusawa, J.L. S rensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Science, 282, 706-709, (1998)

[Ger97] N.A. Gershenfeld and I.L. Chuang, Science, 275, (1997), 350-356

[Gho95] P.K. Ghosh, Ion Traps, Clarendon Press, (1995)

[Gra90] P. Grangier, J.F. Roch, G. Roger, Phys. Rev. Lett., 66, 1418, (1990)

[Gra98] P. Grangier, J.A. Levenson , and J.-P. Poizat, Nature, 396, 537, (1998)

[Gro96] C. Grover, Proc. 28th Ann. ACM Symp. Th. Comp., 212, (1996)

[Gru97] A. Gruber et al., Science, 276, 2012, (1997)

[Hag97] E. Hagley, X. Maître, G. Nogues, C. Wunderlich, M. Brune, J.M. Raimond, and S. Haroche, Phys. Rev. Lett., 79, (1997)

[Hat98] T. Hattori, and K. Takeda, „Search and Recognition of Image Data in Quantum Computer“, 1998 Int. Symp. on Nonl. Theo. Appl. (NOLTA98)

[Heb95] A.P. Heberle, J.J. Baumberg, and K. Kohler, Phys. Rev. Lett., 75, 2598, (1995)

[Hin] E.A. Hinds, Advances in Atomic, Molecular and Optical Physics

[Hug98] R. Hughes et al., Fortschr. d. Phys., 46, (1998)

[Ita95] W.M. Itano, J.C. Bergquist, J.J. Bollinger, and D.J. Wineland, Physica Scripta, T 59, (1995), 106

[Jak98a] D. Jaksch et al. Phys. Rev. Lett., 81, 3108, (1998)

[Jak98b] D. Jaksch, H.-J. Briegel, J.I. Cirac, C.W. Gardiner, and P. Zoller, quant-ph/9810087

[Jam98a] D.F.V. James et al., "Trapped Ion Quantum Research at Los Alamos" quant-ph/9807071

[Jam98b] D.F.V. James, Phys. Rev. Lett., 81, (1998), 317

[Jam98c] D.F. James, Appl. Phys. B (in press)

[Jon98] T.F. Jones and M. Mosca, eigereicht bei J. of Chem. Phys. (1998), quant-ph/9801027

[Kik97] J.M. Kikkawa, I.P. Smorchkova, N. Samarth, D.D. Awschalom, Science 277, 1284, (1997)

[Kik98] J.M. Kikkawa and D.D. Awschalom, Phys. Rev. Lett., 80, 4313, (1998)

[Kin98] B.E. King et al, Phys. Rev. Lett., in press (1998), quant-ph/9803023

[Kli80] K. von Klitzing, G. Dorda, and M. Pepper, Phys. Rev. Lett., 45, 494, (1980)

[Laf97] R. Laflamme, E. Knill, W.H. Zurek, P. Catasti, and S.V.S. Mariappan, quant-ph/9709025

[LaP89] A. LaPorta, R.E. Slusher, B. Yurke, Phys. Rev. Lett., 62, 28, (1989)

[Las99] Dr. Lassman, Dt. Telekom Technologiezentrum Darmstadt, persönliche Mitteilung

[Len93] A. Lenstra, and H. Lenstra, Lecture Notes in Mathematics 1554, Springer-Verlag, New York, (1993)

[Lev86] M.D. Levenson, R.M. Shelby, M. Reid, D.F. Walls, Phys. Rev. Lett., 57, 2473, (1986)

[Liv96] C. Livermore et al., Science, 274, 1332, (1996)

[Llo93] S. Lloyd, Science, **261**, 1569, (1993)

[Llo95] S. Lloyd, Phys. Rev. Lett., 75, 346, (1995)

[Los97] D. Loss, and D.P. DiVincenzo, Quantum Computation with Quantum Dots, quant-ph/9701055

[Maa91a] A. Maassen v.d. Brink, G. Schön, and L.J. Geerligs, Phys. Rev. Lett., 67, 3030, (1991)

[Maa91b] A. Maassen v.d. Brink et al., Z. Phys. B, 85, 459, (1991)

[Mar95] C. Marand, and P. Townsend, Optics Letters, Vol. 20, No. 16, 1695, (1995)

[Mat96] K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, Phys. Rev. Lett., 76, 4656, (1996)

[Mon95a] C. Monroe, D.M. Meekhof, B.E. King, S.R. Jefferts., D.J. Wineland, and P. Gould, Pys. Rev. Lett., 75, (1995), 4011

[Mon95b] C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett., 75, (1995), 4714-4717

[Mul96] A. Muller, H. Zbinden, N. Gisin, Europhys. Lett., 33 (5), 335-339, (1996)

[Mul97] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. 70 (7), 1997

[Nag86] W. Nagourney, J. Sandberg, and H.G. Dehmelt, Phys. Rev. Lett, 56, (1986), 2797

[Nak97] Y. Nakamura, C.D. Chen, and J.S. Tsai, Phys. Rev. Lett., 79, 2328, 1997

[Nak99] Y. Nakamura, Yu. A. Pashkin, and J.S. Tsai, Nature, zur Veröffentlichung eingereicht, 1999

[Neu78] W. Neuhauser, M. Hohenstatt, P. Toschek, and H. Dehmelt, Phys. Rev. Lett., 41, (1978), 233

[Nie98] M.A. Nielsen, E. Knill, and R. Laflamme, Science, 52-55, (1998)

[Oza98] M. Ozawa, Phys. Rev. Lett., 80, 631, (1998)

[Pau53] W. Paul und H. Steinwedel, Z. Naturforsch., A 8 (1953), 448

[Pel95] T. Pellizzari, S.A. Gardiner, J.I. Cirac, and P. Zoller, Phys. Rev. Lett., 75, 4714, (1995)

[Ple96] M.B. Plenio, and P.L. Knight, Phys. Rev. A, 53, (1996), 2986

[Ple97] M.B. Plenio, V. Vedral, and P.L. Knight, Phys. Rev. A, 55, (1997), 67

[Poy97] J. F. Poyatos, J.I. Cirac, and P. Zoller, submitted to Phys. Rev. Lett., quant-ph/9712012

[Pur46] E.M. Purcell, Phys. Rev., 69, 681, (1946)

[Rai92] M.G. Raizen, J.M. Gilligan, J.C. Bergquist, W.M. Itano, and D.J. Wineland, Phys. Rev. A, 45, (1992), 6493-6501

[Rar94] J. Rarity, P. Ownes, and P. Tapster, J. Mod. Opt., 41, 2435-2444, (1994)

[Rem98] persönliche Mitteilung

[Riv87] R. Rivest, A. Shamir, L. Adleman, Communications of the ACM, Vol. 21 (1987), pp. 120-126

[Rob97] M. Roberts, P. Taylor, G.P. Barwood, P. Gill, H.A. Klein, and W.R.C. Rowley, Phys. Rev. Lett., 78, (1997), 1876-1879

[Roc92] J.F. Roch, G. Roger, P. Grangier, J.-M. Courty, and S. Reynaud, Appl. Phys. B, 55, 291-297, (1992)

[Roc97] J.-F. Roch et al., Phys. Rev. Lett., 78, 634, (1997)

[Rug92] D. Rugar, C.S. Yannoni, and J.A. Sidles, Nature, 360, 563 (1992)

[Rug94] D. Rugar et al., Science 264, 1560, (1994)

[Sau86] Th. Sauter, R. Blatt, W. Neuhauser, and P.E. Toschek, Phys. Rev. Lett, 57, (1986), 1696

[Sch98] S. Schneider, D.F.V. James, and G.J. Milburn, quant-ph/9808912

[Scu78] M.O. Scully, R. Shea, J.D. Mc Cullen, Phys. Rep., 43, 486, (1978)

[Sha96] J. Shah, Ultrafast Spectroscopy of Semiconductors and Semiconductor Nanostructures (Springer, Berlin, 1996)

[Shn97] A. Shnirman, G. Schön, and Z. Hermon, Phys. Rev. Lett., 79, 2371, (1997)

[Sho94] P. Shor, Proc. 35th Ann. Symp. Found. Comp. Sci., 124, (1994)

[Sid95] J.A. Sidles, Rev. Mod. Phys., 67, 249, (1995)

[Sie96] J. Siewert, and G. Schön, Phys. Rev. B, 54, 7421, (1996)

[Sli90] C.P. Slichter, *Principles of Magnetic Resonance*, (Springer-Verlag Berlin 1990)

[Spä97] S. Spälter, P. van Loock, A. Sizmann, G. Leuchs, Appl. Phys. B, 64, 213, (1997)

[Ste97] A. Steane, Appl. Phys. B, 64, (1997), 623

[Ste98] A. Steane, Rpt. Progr. Phys., 61, (1998), 117

[Suy98] H. Suyari, and Y. Uesaka, „On a Quantum Computation for Solving TSP within Polynomial Time“, 1998 Int. Symp. on Nonl. Theo. Appl. (NOLTA98)

[Tow93a] P. Townsend, J. Rarity, and P. Tapster, Electronics Letters, 29, 634-635, (1993)

[Tow93b] P. Townsend, J. Rarity, and P. Tapster, Electronics Letters, 29, 1291-1293, (1993)

[Tsu82] D.C. Tsui, H.L. Störmer, and A.C. Gossard, Phys. Rev. Lett., 48, 1559, (1982)

[Tuo92] M.T. Tuominen, J.M. Hergenrother, T.S. Tighe, and M. Tinkham, Phys. Rev. Lett, 69, 1997, (1992)

[Tur98] Q. A. Turchette, C. S. Wood, B. E. King, C. J. Myatt, D. Leibfried, W. M. Itano, C. Monroe, and D. J. Wineland, Phys. Rev. Lett., 81, 3631, (1998)

[Vag95] I.D. Vagner, and T. Maniv, Physica B, 204, 141 (1995)

[Vin95a] D. DiVincenzo, Quantum Computation, Science, 270, 257, (1995)

[Vin95b] D.P. DiVincenzo, Phys. Rev. A, 51, 1015, (1995)

[Wal93] H. Walther, Adv. At. Mol. Phys. 31, (1993), 137

[War97] W.S. Warren, Science, 277, (1997), 1688

[Wau95] F.R. Waugh et al., Phys. Rev. Lett., 75, 705, (1995)

[Wau96] F.R. Waugh et al., Phys. Rev. B, 53, 1413, (1996)

[Wei98] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. 81, 5039, (1998)

[Wie70] Wiesner, (1970), unveröffentlicht

[Wie98a] H. Wie, X. Xue, and S.D. Morgera, Single Molecule Magnetic Resonance and Quantum Computation, quant-ph/9807057

[Wie98b] H. Wie, X. Xue, and S.D. Morgera, NMR Quantum Automata in Doped Crystals, quant-ph/9805059

[Win75a] D.J. Wineland, and H.G. Dehmelt, J. Appl. Phys., 46, (1975), 919

[Win75b] D.J. Wineland, and H.G. Dehmelt, Bull. Am. Phys. Soc., 20, (1975), 637

[Win78] D.J. Wineland, R.E. Drullinger, and F.L. Walls, Phys. Rev. Lett., 40, (1978), 1639

[Win97] D.J. Wineland et al., quant-ph/9710025

[Win98] D.J. Wineland, C. Monroe, W.M. Itano, B.E. King, D. Leibfried, D.M. Meekhof, C. Myatt, and C. Wood, Fortschritte der Physik, 46, (1998), 363

[Woo82] W.K. Woo and W.H. Zurek, Nature, 299, 802, (1982)

[Wra95] J. Wrachtrup et al., Detection of a single electron spin, in O. Marti and R. Möller (eds.), Photons and Local Probes, (Kluwer Academic Publishers, 1995)

[Wue59] R.F. Wuerker, H. Shelton, and R.V. Langmuir, J. Appl. Phys., 30, 342, (1959)

[Yur92a] B. Yurke, and D. Stoler, Phys. Rev. A, 46, 2229, (1992)

[Yur92b] B. Yurke, and D. Stoler, Phys. Rev. Lett, 68, 1251 (1992)

[Zan98] P. Zanardi, and F. Rossi, Quantum Information in Semiconductors: Noiseless Encoding in a Quantum-Dot Array, quant-ph/9804016

[Zbi98] H. Zbinden, A. Muller, B. Huttner, and N. Gisin, J. Cryptology, zur Veröffentlichung eingereicht

[Zuk93] M. Zukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, Phys. Rev. Lett., 71, 4287, (1993)

12.2 Worterklärungen

Alice	In der Quantenkommunikation Synonym für den Sender einer Information.
Bell-Basis	Basis von Zuständen aus denen alle anderen möglichen Zustände des Systems durch Überlagerung erhalten werden können. Die Bell Basis besteht dabei speziell aus Zuständen die eine maximale Verschränkung der Teilchen des Systems beinhalten.
Bellsche Ungleichung	Die Bellsche Ungleichung ist eine Bedingung, die von jeder lokalen deterministischen Theorie erfüllt werden muß. Eine Verletzung dieser Ungleichung bedeutet, daß für den diesbezüglichen Sachverhalt keine lokale, deterministische Erklärung, wie zum Beispiel die Theorie verborgener Parameter eine ist, möglich sein kann.
Bob	In der Quantenkommunikation Synonym für den Empfänger von Informationen.
Boltzmann Verteilung	Die Boltzmann Verteilung beschreibt die Wahrscheinlichkeit *p*, mit der sich ein System bei einer bestimmten Temperatur *T* im Energiezustand *E* befindet: $p(E,T) \propto e^{-\frac{E}{kT}}$, mit der Boltzmannkonstanten *k*.
Controlled Not (C-NOT)	Logische Operation im Sinne einer bedingten Verneinung: $00 \rightarrow 00$; $01 \rightarrow 01$; $10 \rightarrow 11$; $11 \rightarrow 10$.
Dekohärenz	Bezichnet den Verlust an Kohärenz, d.h. das Verschwinden einer festen Phasenbeziehung zwischen unterschiedlichen Wellen. Die Dekohärenz stellt ein wesentliches Problem bei der Realisierung eines Quantenrechners dar.
Dense-Coding	Mit Hilfe der quantenmechanischen Verschränkung ist es möglich mehr Information an physikalische Objekte zu koppeln, als dies ohne Verschränkung möglich wäre.
Doppelbrechung	Ein Kristall ist im allgemeinen bezüglich seiner optischen Eigenschaften nicht isotrop. Unterschiedlich polarisiertes Licht pflanzt sich daher (abhängig von der Orientierung zwischen der Polarisationsebene des Lichts und den Symmetrieachsen des Kristalls) mit verschiedenen Geschwindigkeiten im Material fort. Licht in einem Polarisationsmischzustand wird dadurch in seine Komponenten zerlegt, die dann räumlich getrennt aus dem Kristall austreten können.
Dopplerkühlung	Bei der Dopplerkühlung wird das zu kühlende Atom oder Ion mit Licht bestrahlt, dessen Energie etwas geringer ist, als diejenige, die zu einer elektronischen Anregung des bestrahlten Atoms notwendig wäre. Die Energiedifferenz wird bei hinreichend schnellen Atomen der kinetischen Energie entnommen, so daß diese durch die Absorption langsamer und damit kälter werden.
Down-Conversion	In einem nichtlinearen optischen Kristall wird ein Photon in zwei Photonen mit jeweils der halben Frquenz konvertiert. Diese Photonen sind insbesondere auch bezüglich ihrer Polarisationseigenschaften sehr stark korreliert und unter bestimmten Umständen sogar verschränkt.
DNA	Desoxyribonukleinsäure, trägt die Information, die zum Aufbau der vielfältigen Proteinstrukturen im Körper notwendig ist.
Drehimpuls	Gerichtete Größe, die den Impuls, der einer Drehbewegung innewohnt, beschreibt. Je nach Umlaufsinn des bewegten Objekts zeigt der Drehimpuls in eine der beiden, durch die Drehachse definierten Richtungen.
Eigenzustand	Quantenmechanischer Zustand, der bei der Messung von Objekteigenschaften angenommen wird. Meßresultate sind immer Eigenzustände des untersuchten Systems und außerdem stabil, d.h. nochmaliges Messen verändert einen Eigenzustand nicht. Da jede Art der menschlichen Beobachtung in diesem Sinne eine Messung darstellt, teilt sich uns die Realität nur in Form von Eigenzuständen mit.
Einstein-Separation	Diese bezeichnet eine spezielle räumliche Trennung von Ereignissen oder Objekten. Es soll dabei ausgeschlossen sein, daß zwischen den Orten während eines bestimmten Zeitintervalls eine klassische Nachricht mit maximal Lichtgeschwindigkeit ausgetauscht werden kann. Die Einstein-Separation ist eine wichtige Bedingung bei der Durchführung eines einwandfreien EPR-Experiments.
Entanglement Swapping	Durch Verschränkung jeweils eines Teilchens zweier verschränkter Teilchenpaare (beispielsweise durch Zusammenführung und Ununterscheidbarmachung in einem Strahlteiler) werden auch die unter Umständen räumlich weit voneinander entfernten anderen beiden Teilchen miteinander verschränkt.

Eve	Synonym für einen potentiellen Lauscher bei Quantenkryptographieverfahren.
Faraday-Spiegel	Spiegel, bei dem die Polarisationsrichtung des Lichts vor und nach der Reflexion mittels eines Magnetfelds (Faraday-Effekt) gedreht wird.
Fehlerkorrektur	Spezielle Protokolle zur Kompensation von Fehlern, die bei der zeitlichen Entwicklung des Zustandes eines Quantenprozessors, beispielsweise durch Dekohärenz, auftreten.
Hyperfeinaufspaltung	Die elektronischen Niveaus des Atoms können durch den Einfluß von Magnetfeldern in energetisch verschiedene Unterniveaus aufgespalten werden. Der, im Vergleich zu anderen Beiträgen, sehr geringe Einfluß des magnetischen Kernmoments führt zur Hyperfeinaufspaltung.
Interferenz	Bezeichnet hier die Effekte, die bei der direkten Überlagerung von (quantenmechanischen) Wellen auftreten. Im einfachsten Fall beispielsweise die Entstehung von Intensitätsmaxima und -minima bei Beugung von Lichtwellen am Spalt.
Intensitätsgradient	Bezeichnet die im allgemeinen räumliche Änderung der Intensität. Der Gradient als gerichtete Größe zeigt dabei in die Richtung des stärksten Anstiegs der Intensität.
Kohärenz	Damit Wellen bei einer Überlagerung Interferenzeffekte zeigen, müssen sie zumindest auf der Zeit- bzw. Längenskala auf der der Interferenzeffekt auftritt, über eine feste Phasenbeziehung verfügen. Man bezeichnet sie dann als kohärent.
Korrelationsexperiment	Ein Experiment, bei dem überprüft wird, ob zwischen bestimmten Ereignissen eine mehr als nur zufällige Beziehung besteht. Insbesondere bei Einstein-separierten Ereignissen weist eine solche Korrelation auf eine überlichtschnelle (nicht notwendig akausale) Rückwirkung hin.
Korrelationsfunktion	Gibt den Grad einer Korrelation zwischen Ereignissen an. Wird im allgemeinen so gewählt, daß sie bei unabhängigen, nur zufällige Übereinstimmung zeigenden Ereignissen verschwindet.
Mach-Zehnder-Interferometer	Interferometer bei dem der einfallende Strahl mittels eines Strahlteilers in zwei Teilstrahlen aufgespalten wird die sich nach Durchlaufen unterschiedlicher Wege (Interferometerarme) wieder in einem Strahlteiler treffen, wo es zur Interferenz kommt.
Maxwellsche Gleichungen	Grundgleichungen der elektromagnetischen Wechselwirkung
Michelson-Morley-Interferometer	Interferometer, bei dem ein Lichtstrahl mit Hilfe eines zentral angeordneten, teilverspiegelten Strahlteilers in zwei senkrecht zueinander stehende Teilstrahlen aufgespalten wird, die in sich selbst reflektiert, auf den Strahlteiler zurückgeworfen und in einem ausgehenden, zur Einfallsrichtung senkrecht stehenden, Lichtstrahl vereinigt werden.
nichtdeterministisch-polynomial (NP)	Bezeichnet ein Problem, bei dem der Rechenaufwand zur exakten Lösung des Problems in Abhängigkeit von der Komplexität der Ausgangssituation (beim → TSP die Anzahl der Städte) stärker als nach einem Polynomialgesetz ansteigt.
NMR	Nuclear Magnetic Resonance = Kernspinresonanz: Verfahren, das über die Messung der Wechselwirkung elektromagnetischer Wellen mit magnetischen Kernmomenten Aussagen über die Materialzusammensetzung von Substanzen macht.
NP-vollständig	Klasse von NP-Problemen die jeweils auf ein gemeinsames Prinzip zurückgeführt werden können. Die effiziente Lösung eines Problems dieser Klasse bedeutet die effiziente Lösung aller dieser NP-vollständigen Probleme.
Phase	Eine einfache periodische Schwingung erhält man, indem man eine Kreisbewegung auf ein fortlaufendes Band projiziert. Einer Umdrehung des Kreises entspricht dabei eine Periode der Schwingung. Der Winkel der Drehung wird als Phase der Schwingung übernommen.
Phasenmodulator	Gerät zur Veränderung der Phase einer Schwingung. Im Idealfall bleiben dabei die Form der Wellengruppe und die Wellenfront unverändert.
Phononen	Quanten der mechanischen Gitterschwingungen im Festkörper.
Photonen	Quanten des Lichts (elektromagnetische Wellen). Der Impuls des Photons ist eindeutig durch die Wellenlänge des Lichts bestimmt.
Pockelszelle	Erlaubt eine elektrisch gesteuerte Drehung der Polarisationsrichtung von Licht.
Polarisation	Licht ist eine Welle die aus transversalen Schwingungen von elektrischen und magnetischen Feldern besteht. Die Schwingungsrichtung des elektrischen Feldes zeichnet eine Ebene senkrecht zur Ausbreitungsrichtung aus. Die Richtung, in die das elektrische Feld zeigt bezeichnet man als Polarisationsrichtung des Lichts. Dreht sich diese Richtung während der Ausbreitung des Lichts, so spricht man von zirkularer, bleibt sie erhalten von linearer Polarisation.

Public Key	Kryptographieverfahren, das auf der Verwendung zweier Schlüssel beruht, eines öffentlichen, der jedermann zugänglich sein kann und der zur Verschlüsselung benutzt wird, und eines privaten, der geheim ist und zur Entschlüsselung benötig wird.
polynomial (P)	Nach einem Polynomialgesetz von der freien Variablen x abhängig: $f(x) \propto ax^m + bx^n + \ldots$
Primfaktoren	Ganzzahlige Faktoren in die sich eine Zahl zerlegen läßt und die Primzahlen sind.
Quadrupol	Vierpol, Anordnung aus vier elektrisch geladenen Objekten (Elementarladungen, geladene makroskop. Körper etc.)
Quantenparallelismus	Eigenschaft eines verschränkten Quantensystems gleichzeitig die Information über mehrere, physikalisch verschiedene Endzustände zu enthalten.
Quanten-Turing-Maschine	Turing-Maschine, die nicht nur klassische Operationen und Elemente verwendet, sondern auch quantenmechanische Effekte wie Superposition und Interferenz zuläßt.
Ribonukleinsäure	Makromolekül, das eine wichtige Rolle bei der biologischen Sysnthese von Eiweissen spielt. Enthält wie die DNA die Erbinformation biologischer Systeme.
Watson-Crick-komplementär	Invertierter Nukleinsäurestrang derart, daß sich der ursprüngliche und der invertierte, Watson-Crick komplementäre Strang zu einer Doppelhelix verbinden können.
RSA	Kryptographieverfahren nach dem „Public-Key"-Schema bei dem die Ver- und Entschlüsselung auf der Multiplikation von bzw. Zerlegung in Primzahlen beruht.
Superposition	Überlagerungszustand diskreter quantenmechanischer Zustände.
Travelling Salesman Problem (TSP)	Aufgabe, die darin besteht, für einen Handlungsreisenden die kürzeste Verbindung durch eine vorgegebene Anzahl von Städten zu finden. Diese Aufgabenstellung zählt zur Klasse der NP-vollständigen Probleme.
Turing-Maschine	Universelles Modell für einen Rechner. Anschaulich besteht die TM aus einem unendlich langen Band, auf dem sich unterschiedliche Zeichen befinden und einem Lese-/Schreibkopf. Dieser Kopf befindet sich jederzeit in einem Zustand, der ihm vorgibt, an welche Stelle des Bandes er eine Information abfragen soll und was danach zu tun ist. Jeder reale Rechner kann auf eine solche Maschine zurückgeführt werden.
Verschränkung	Korrelation mehrerer, in einem gemeinsamen Superpositionszustand befindlicher quantenmechanischer Objekte derart, daß eine Manipulation eines der Teilchen über den damit verbundenen Kollaps der Wellenfunktion zur einer Veränderung des anderen Teilchens führt.
Wahrscheinlichkeits-amplitude	Quantenmechanische Objekte werden über eine Wellenfunktion beschrieben. Die Wahrscheinlichkeit ergibt sich aus dem Quadrat der Wahrscheinlichkeitsamplitude. Es reicht jedoch nicht aus, die Realität nur über Wahrscheinlichkeiten zu beschrieben, da dann wichtige Informationen hinsichtlich physikalischer Phänomene nicht berücksichtigt werden.
Zeemannaufspaltung	Die unterschiedlichen elektronischen Niveaus eines Atoms sind mit verschiedenen magnetischen Momenten verbunden. Bringt man ein Atom in ein externes Magnetfeld, so kann sich dieses magnetische Moment in unterschiedlicher Weise relativ zum externen Feld einstellen. Die verschiedenen Orientierungen sind dabei mit unterschiedlichen Anregungsenergien verbunden. Die entsprechende energetische Aufspaltung des elektronischen Niveaus wird als Zeemann-Aufspaltung bezeichnet.