Gösta Fürnkranz

Vision Quanten-Internet

Ultraschnell und hackersicher

EBOOK INSIDE

Springer

Vision Quanten-Internet

Gösta Fürnkranz

Vision Quanten-Internet

Ultraschnell und hackersicher

Springer

Gösta Fürnkranz
Hinterbrühl, Österreich

ISBN 978-3-662-58452-1 ISBN 978-3-662-58453-8 (eBook)
https://doi.org/10.1007/978-3-662-58453-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Einbandabbildung: © AndSus/stock.adobe.com
Planung/Lektorat: Lisa Edelhäuser

Springer ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Einleitung

Die Digitalisierung ist längst zum bestimmenden Element unserer Zeit geworden. Ihre zukünftige Entwicklung bietet vielfältige Chancen und Potenziale, die es zu realisieren gilt. Eine sichere digitale Kommunikation ist dabei ein besonders wichtiger Faktor. Um deren Sicherheit langfristig zu gewährleisten, können innovative Technologien eine wesentliche Rolle spielen. Wir beobachten heute eine rasant steigende Zahl unautorisierter Zugriffe und Manipulationen in Kommunikationsnetzen mit wachsendem Schaden für Einzelpersonen, Gesellschaft und Wirtschaft. Die vermehrte Nutzung des Internets öffnet ein gewaltiges Bedrohungspotenzial hinsichtlich krimineller und terroristischer Zugriffe. Vor allem in Hinblick auf die stete Zunahme von Online-Geschäften, die immer stärker voranschreitende systemische Vernetzung sowie den Ausbau des Internets der Dinge werden Fragen der Datensicherheit und -integrität immer wichtiger. Bereits heute diskutierte Schlagworte wie Industrie 4.0,

autonomes Fahren, Wearables oder Smart City sind Vorboten einer voll vernetzten digitalen Gesellschaft, in der es zu einer explosiven Zunahme an Datenmaterial kommen wird. Dieser Entwicklung kann längerfristig gesehen nur mit völlig sicheren Technologien begegnet werden. Die bisherige Sicherheitstechnologie setzt dabei fast ausnahmslos darauf, den Datenzugang bloß zu erschweren. Es gibt jedoch eine Alternative, welche den unbefugten Zugang zu Daten und Informationen aus inhärent physikalischen Gründen komplett unmöglich machen kann: die Quantenkommunikation.

Im Zentrum dieser Entwicklung steht der Begriff Quanteninformation, welcher einen völlig neuen Zugang zur Informationstheorie eröffnet. In der aktuellen IT erfolgen Datenverarbeitung und Transfer ausschließlich auf Basis von Bits und Bytes, also Folgen von Binärzahlen, die definitionsgemäß nur die Ziffern 0 und 1 enthalten. Die Quanteninformation definiert dagegen als Elementareinheit das Quantenbit (Qubit), welches einer Art gleichzeitige Überlagerung von 0 und 1 entspricht. Damit ergeben sich gegenüber dem klassischen Informationsbegriff zwei wesentliche Vorteile: Zum einen können Quantenbits viel mehr Informationen speichern und übertragen als herkömmliche Bits. Zum anderen beinhalten Qubits einen inhärenten Sicherheitsaspekt, der es unmöglich macht, Quanteninformation abzuhören beziehungsweise zu hacken. Dies ist eine völlig neue Funktionalität, die es in der klassischen IT nicht gibt. Klassische Information kann beliebig kopiert und vervielfältigt werden und ist somit automatisch der unautorisierten Weitergabe preisgegeben. Im Fall von Quantenbits ist dies nach heutigem Wissen aus physikalischen Gründen unmöglich.

In den letzten Jahren sind in der Grundlagenforschung eine Reihe wichtiger Prinzipien demonstriert worden, die das hohe Potenzial dieser Technologie unterstreichen.

Die bahnbrechenden Ergebnisse aktueller Experimente stellen einen Meilenstein in der Entwicklung der Quantenkommunikation dar. So konnten beispielsweise Quantenkanäle bereits auf Entfernungen von bis zu 1203 km erfolgreich realisiert werden. Erste Geräte zur Quantenkryptografie werden von einschlägigen Firmen angeboten. Weltweit werden daher erhebliche Anstrengungen unternommen, um die technischen Voraussetzungen für eine globale Verbreitung schaffen zu können Alle diese Maßnahmen zielen darauf ab, die Quantenkommunikation auch über große Entfernungen zu ermöglichen. In letzter Konsequenz ist dafür ein spezielles Quantennetzwerk erforderlich, das als erste Prototypen in Europa; Asien und den USA implementiert wurde. In China und Europa existieren hierzu erste Fördermaßnahmen, welche einschlägig aktive Forschungseinrichtungen und Unternehmen unterstützen. In Fachkreisen wird dieser Entwicklung eine große Zukunft vorhergesagt. Gerade auch der europäischen Forschung (wo diese Technik ihre Wurzeln besitzt) ist es ein zentrales Anliegen, die abhörsichere Quantenkryptografie marktfähig zu machen.

Eine weitere Triebfeder für die Ausbildung eines Quantennetzwerks liegt in der aktuellen Computerentwicklung, welche aus physikalischen Gründen in absehbarer Zeit an eine Grenze stoßen wird. Hinzu kommt die Schwierigkeit, dass es heute schon EDV-Probleme gibt, die selbst von Supercomputern entweder viel zu langsam oder gar nicht sinnvoll bearbeitet werden können. Die Suche nach innovativen Konzepten hat daher in der Computerwelt längst eingesetzt. Der revolutionärste Ansatz besteht im Konzept des Quantencomputers. Das ehrgeizigste Ziel der Quanteninformatik ist die Entwicklung eines technisch nutzbaren Quantencomputers. Das große kommerzielle Interesse der Industrie, allen

voran klangvolle Namen wie Google, IBM oder Microsoft, lassen dieses Ziel realistisch erscheinen. Studien von Morgan Stanley räumen dem Quantencomputer mittlerweile einen hohen Stellenwert ein, selbst Kritiker wie der Informatiker Scott Aaronson stimmen dem zu. Obwohl gegenwärtig noch im juvenilen Stadium, sind die Quantenrechner der möglicherweise einzige Hoffnungsträger, der imstande wäre, die Computerleistung klassischer Rechner noch erheblich zu toppen. Sollte der Quantencomputer einst die Schwelle zur technischen Nutzbarkeit überwinden, stellt er eine umso faszinierendere Vision in Aussicht: Die Kombination aus inhärenter Datensicherheit und der potenziellen Vernetzung von Quantencomputern könnte eines Tages ein Quanteninternet entstehen lassen, das in punkto Sicherheitsaspekt und Verarbeitungsgeschwindigkeit zu einem völligen Paradigmenwechsel führt. Durch die theoretische Fähigkeit von Quantenrechnern, bestimmte Problemstellungen zu bewältigen, die selbst für Supercomputer unlösbar sind, könnte ein solches Quantenhypernet noch ungeahnte Möglichkeiten der zukünftigen Informationswelt bereithalten.

Zur Auslegung des Buchs möchte der Autor folgendes bemerken: Der Autor bedient sich einer bewusst optimistischen Sprechweise, weil die Forschung bereits wichtige Erfolge zu verbuchen hat und es sich lohnt, die Perspektiven und Potenziale des noch so jungen Gebiets der Quanteninformationstechnologie einer breiten Öffentlichkeit aufzuzeigen. Immerhin basieren diese auf wissenschaftlichen Erkenntnissen von fundamentaler Tragweite. Freilich ist die Quantenphysik bis heute eine kontroversiell diskutierte Thematik, die selbst von ihren profundesten Kennern nicht immer verstanden wurde und wird. Gerade in der populärwissenschaftlichen Darstellung stellt es eine besondere Herausforderung dar,

den Drahtseilakt zwischen fachlicher Genauigkeit und Simplifizierung zu meistern. Um Missverständnissen und Fehlinterpretationen vorzubeugen, sei dem Leser empfohlen, das Buch in seiner Chronologie zu lesen, da es eine beinahe durchgängige didaktische Struktur enthält. So werden zahlreiche Begriffe zunächst nur erwähnt, danach immer wieder aufgegriffen und weiter vertieft. Bereits in Teil 1 werden Versuchsanordnungen diskutiert, die eine wichtige Grundlage für spätere experimentelle Anordnungen und Prinzipdarstellungen in Teil 2 und Teil 3 bilden. In manchen Aspekten weicht der Autor bewusst von üblichen Erklärungsmodellen ab, indem er das heute verstärkt diskutierte Konzept Information (im Sinne einer tiefer gehenden physikalischen Entität) explikativ einbringt. Damit nimmt er Anteile an Positionen, wie sie von Instanzen (wie beispielsweise Anton Zeilinger) vertreten werden. In diesem Sinne möchte der Autor umfassend über den aktuellen Stand der Forschung zum Thema Quanteninternet informieren und sich gemeinsam mit dem Leser auf eine faszinierende Zukunftsreise begeben als Vorgeschmack auf eine neue technologische Ära, die einst Realität werden könnte.

Inhaltsverzeichnis

1

Die quantendigitale Zukunft

1.1 Digitale Visionen

Als vor gut 200 Jahren die industrielle Revolution einsetzte, bedeutete sie weltweite Veränderungen. Damit verbunden war eine tief greifende Umgestaltung der wirtschaftlichen und sozialen Verhältnisse, was die Entwicklung von Produktivität, Technik und Wissenschaft stark beschleunigte. Im Nebenaspekt ergaben sich aber auch eine Reihe von gesellschaftlichen Problemen, verbunden mit Arbeiterunruhen, die Regulierungen und soziale Reformen notwendig machten. Nun, im 21. Jahrhundert, steht der Mensch vor einer ähnlich epochalen Veränderung. Während damals die Muskelkraft durch die Dampfmaschine ersetzt wurde, lebt der Mensch nunmehr im digitalen Zeitalter, wo der Mikrochip sich anschickt, die geistige Arbeit zu substituieren. Was in den 1940ern mit der Entwicklung des Computers begann, später die erste Mondlandung ermöglichte, Taschenrechner zum

G. Fürnkranz, *Vision Quanten-Internet,*
https://doi.org/10.1007/978-3-662-58453-8_1

Massenprodukt machte und die ersten Home-PCs boomen ließ, findet seinen aktuellen Höhepunkt in der Ausbildung des Internets und seiner mobilen Endgeräte. Dies markiert gleichzeitig das Informationszeitalter, dessen zukünftige Zielrichtung die totale Vernetzung von jedem mit allem vorsieht. Aktuell verbindet das Internet Milliarden Menschen miteinander, und es soll bald rund 40 Mrd. vernetzte Geräte umfassen. Mit ungeheurer Dynamik öffnet die Digitalisierung ein neues Kapitel der menschlichen Entwicklung. Digitale Infrastrukturen, Produkte und Dienstleistungen verändern Gesellschaft und Wirtschaft. Dieser Übergang zu einer neuen Moderne wird gemeinhin als digitale Revolution bezeichnet – ein Prozess, der längst als nicht abgeschlossen zu betrachten ist. Zumal auch für das Internet der Dinge, wo Zukunftsforscher großes Potenzial in tragbarer Elektronik, Assistenzsystemen, Robotik und Künstlicher Intelligenz sehen. Damit verbunden sind moderne, systemisch vernetzte Produktionsverfahren zur Steigerung von Effizienz und Innovation. Weitere große Umbrüche zeichnen sich in der Mobilität ab, wo die digitale Vernetzung öffentlicher Verkehrsmittel sowie das autonome Fahren im Mittelpunkt stehen.

Wie die Geschichte lehrt, können technologische Entwicklungen ein starker Motor für gesellschaftliche Veränderungen sein – im Positiven wie im Negativen. Neue Technologien haben die Menschheit immer schon vor Herausforderungen gestellt, ihre Handlungsspielräume im Guten wie im Bösen erweitert, das Leben erleichtert wie auch vernichtet. Von der neolithischen bis zur industriellen Revolution war dies das Ergebnis von Fortschritt durch technischen Wandel, wie die Erfindung des Buchdrucks, welche die Wissenschaft und Weltbilder verändert hat. Der digitale Wandel bedeutet erneut Herausforderungen und Gefahren: Lückenlose Überwachung und Einschränkung der persönlichen Freiheit müssen ebenso beachtet werden

wie der Schutz vor Cyberkriminalität oder ethische Fragen rund um den Einsatz von Künstlicher Intelligenz. Dass eine neue Technik massenweise Arbeitskräfte ersetzt, hat bislang jeden technologischen Wandel begleitet. Aber andererseits entstehen auch laufend neue Tätigkeitsfelder. Viele Unternehmen werden sich verändern müssen, um nicht ein Opfer der digitalen Disruption zu werden (Verdrängung bestehender Produkte und Strukturen durch neue Technologien und Systeme). Im Lastenheft der Politik stehen demnach gesetzliche Regulierungen, die moderne Rahmenbedingungen setzen und für soziale Absicherungen sorgen, damit Arbeitnehmer die positiven Potenziale realisieren können.

Der stete Fortschritt in Mikroelektronik und Kommunikationstechnik erweckt die Vision einer umfassenden Vernetzung unzähliger Sensoren und Computer, eingebettet in die persönliche Umgebung. Winzigste Prozessoren, Speicherbausteine und Sensoren mit minimalen Produktionskosten können in viele alltägliche Gegenstände und Geräte implementiert werden. Nicht nur Mikroprozessoren wurden über Jahrzehnte immer kleiner, leistungsfähiger und preiswerter, sondern auch Funksensoren ermöglichen es, Systeme aus der Ferne schnell und billig zu überwachen und zu diagnostizieren. Sie können in großer Anzahl installiert und adaptiert werden, vermeiden teure Kabelverbindungen und lassen sich unsichtbar in Objekte integrieren, die vorher nicht netzwerkfähig waren. Zusammen mit Fähigkeiten zur Ortserkennung erlangen solche drahtlosen Devices eine nie da gewesene Qualität. Die allgegenwärtige Smartphone-Kultur, aber auch Funketiketten oder Chips in Ausweisen und Kreditkarten sind Vorboten einer neuen Ära des „Ubiquitous Computing" („Überallrechnens"). Bereits um 1990 orakelte der Informatiker und Kommunikationswissenschaftler Mark Weiser: „In the 21st century the

technology revolution will move into the everyday, the small and the invisible“ (https://de.wikipedia.org/wiki/Ubiquitous_computing). Als Reaktion wurde in Europa der Begriff „Ambient Intelligence“ geprägt, welcher die digitale Kommunikation alltäglicher Objekte zur Entlastung und Erleichterung des Lebens in den Vordergrund stellt. Dahin gehende Forschungen verfolgen das Ziel, Prozessoren, Sensoren und Funkmodule in einer Weise zu vernetzen, dass sie adaptiv auf die Bedürfnisse der Nutzer reagieren. Dabei soll sich die sichtbare Technik jedoch zurückziehen und nur noch auf unmerkliche Weise wirken. So wird die Anwesenheit verschiedener Personen von Systemen in der räumlichen Umgebung erkannt, um daraufhin individuell und unaufdringlich zu reagieren. Alltagsgegenstände sollen sich so von passiven zu aktiven Objekten verändern und adaptiv auf die Menschen einwirken. Neuartige Schnittstellen wie Sprach- oder Gestenerkennung leisten maßgebliche Unterstützung. Langfristig soll Ambient Intelligence alle Lebensbereiche umfassen. Ein damit ausgestattetes Smart Home der Zukunft erhöht Komfort, Sicherheit und trägt zur automatischen Energieeinsparung bei. Im Bürobereich wird die Arbeitseffizienz verbessert und durch lernfähige Assistenz gesteigert. Im Feld der intelligenten Transportmittel macht Ambient Intelligence den Verkehr sicherer und Ressourcen schonender, ebenso können Sensornetze umfassende Überwachungsaufgaben übernehmen. Freilich gilt es hier das Augenmaß zu bewahren, sonst ist der Normalbürger am Ende dem totalen Monitoring preisgegeben.

Die 5. Generation von Mobilfunkstandards (5G-Ausbau) ist von zentraler Bedeutung für die zukünftige Nutzung des Internets. Datenraten bis zu 10 Gbit/s sowie geringe Latenzzeiten erlauben eine hohe Dichte mobiler Endgeräte. Damit eröffnet sich eine Vielzahl neuer Geschäftsmodelle und Applikationen. Diese „hypervernetzte 5G-Ära“ soll

bereits in den 2020er Jahren über 40 Mrd. vernetzte Endgeräte ermöglichen. Dies schafft eine wesentliche Basis für das Internet der Dinge, welches Ambient Intelligence unterstützt: Geräte stellen demnach Zusatzinformationen im Internet zur Verfügung und kommunizieren miteinander. Kombiniert mit den Bedürfnissen der NutzerInnen können diese Devices automatische Unterstützung leisten. Die Industrie profitiert von besserer Instandhaltung der Maschinen, indem etwa Zustandsinformationen automatisch kommuniziert werden. Eine andere Kategorie betrifft tragbare Geräte am Körper (Wearables); sie können zum Beispiel Vitalparameter aufzeichnen (wie etwa Herzschlag oder Blutdruck) und die Daten an Ärztezentren funken und so die Überwachung des Gesundheitszustands des Patienten aus der Entfernung gestatten. Ebenso können erweiterte und virtuelle Realitäten ungeahnte Impulse vermitteln: Man blendet etwa via Brille visuelle Zusatzinformationen oder Objekte in Echtzeit ein und schafft damit eine interaktive virtuelle Umgebung. Dies bietet theoretisch beliebig viele Anwendungsmöglichkeiten, vom Tourismus über Bildung bis hin zu Handwerk und Bauindustrie. So kann in der Zukunft ein Projekt vor Baubeginn bereits virtuell besichtigt werden oder es werden Arbeitsanweisungen direkt am Objekt eingespielt.

Das Internet der Dinge bildet ebenso die Basis für das autonome Fahren. Eine besondere Challenge, die immer mehr in den Fokus der Fahrzeugindustrie rückt. Es ermöglicht neue Konzepte zur Vernetzung und Optimierung des öffentlichen und Individualverkehrs. Damit verbindet sich mehr Komfort bei gleichzeitig verringerter Umweltbelastung. Unfälle könnten vermieden und Parkplatzprobleme gelindert werden, Staus ließen sich umgehen, nicht zuletzt könnte auch die Zahl aktiver Fahrzeughalter drastisch sinken. Im Moment vorwiegend als Assistenzsystem realisiert, wird sich diese Technologie einst zum

vollautonomen Fahren weiterentwickeln. Der 5G-Ausbau spielt hier eine große Rolle, da sehr viele Fahrzeugdaten in Sekundenbruchteilen übertragen und verarbeitet werden müssen, was die Mobilfunkbetreiber vor gewaltige Herausforderungen stellt. Benötigt wird zentimetergenaues und stets aktualisiertes Kartenmaterial zusätzlich zur simultanen Erfassung der eigenen Position. Weiteres Datenmaterial betrifft etwa Streckenverlauf, Fahrbahnzustand, aktuelle Verkehrssituation, Wetterlage, Fahrmanöver anderer Autos und vieles mehr. Damit entsteht unmittelbar auch ein Kompetenzproblem: Wem gehören diese Daten eigentlich und was darf mit ihnen geschehen? Ein anderer Aspekt betrifft selbstredend Hacker- und Software-Security, welche hier naturgemäß einen sehr fortschrittlichen Standard erreichen muss. Ebenso stellen sich völlig neue juristische Fragen, wie etwa Rechtsansprüche beim Eintreten des Versicherungsfalls. Wäre der „Fahrer" dann von Sanktionen und Haftung gänzlich entbunden? Wer wäre stattdessen verantwortlich?

Mit dem Schlagwort „Industrie 4.0" verbindet man die industrielle Nutzung moderner Informations- und Produktionstechniken, die auf diese Weise verbunden werden sollen. Als Grundlage dafür dienen intelligente und digital vernetzte Systeme. Dies soll eine weitgehend selbstorganisierte Produktion ermöglichen. Menschen, Maschinen, Anlagen und Logistik sowie Produkte kooperieren und kommunizieren dabei direkt miteinander. Diese Vernetzung soll es gestatten, nicht nur einen Produktionsschritt, sondern eine ganze Wertschöpfungskette zu optimieren, wobei alle Phasen im Lebenszyklus des Produkts mit eingeschlossen sind – inklusive Recycling. Oft wird Industrie 4.0 auch als Zukunftsprojekt verstanden, das auf folgenden Prinzipien beruht: einerseits der Vernetzung von Maschinen mit Sensoren, andererseits der Funktionstransparenz, das heißt einer

Erweiterung durch Sensordaten, technische Assistenz und dezentrale Entscheidungen. Dazu sind allerdings viele Herausforderungen zu bewältigen. Grundziel ist dabei, die IT und die Produktionstechnologie miteinander zu verschmelzen. Im Zentrum steht ein sogenanntes cyberphysisches System, das heißt ein Verbund softwaretechnischer Komponenten mit mechatronischen Teilen, die über eine Infrastruktur (zum Beispiel das Internet) miteinander kommunizieren. Auf Basis von Standards und Normen verspricht man sich davon innovative Produkte und Leistungen. Dabei erhalten Daten als „neuer Rohstoff" eine besondere Bedeutung, womit Datensicherheit und Eigentum selbstredend eine Schlüsselrolle spielen.

Die bisherigen Fortschritte in der Computertechnologie sowie die explosiv zunehmende Informationsmenge durch Vernetzung schaffen neue Gesichtspunkte für weitere Fortschritte in der Künstlichen Intelligenz (KI). Längst ist KI ein Thema, das immer mehr in den Fokus von Firmen und Öffentlichkeit rückt. Die Einsatzgebiete sind vielfältig und betreffen u. a. Fertigung, Instandhaltung, Logistik, Vertrieb, Marketing und Controlling, aber auch Suchalgorithmen und vieles mehr. Schon heute sind Computer dazu in der Lage, zusätzlich zu strukturierten Daten auch unstrukturierte Informationen wie Sprache oder Fotos zu verarbeiten. Damit können Zusatzdaten generiert und verarbeitet werden, die bislang nicht zugänglich waren. Zudem gewinnt der Bereich Machine Learning zunehmend an Bedeutung. Computer lernen dabei an jedem einzelnen Fall, was die Fehlerwahrscheinlichkeit immer weiter reduziert und Handlungsabläufe optimiert. Abseits der industriellen Verwendung kann ein Roboter dann auch in wenigen Minuten eine Tumordiagnose stellen. Eines Tages sollen auch Neuroprothesen möglich werden, das heißt, neuronale Teile ersetzen motorische, sensorische oder kognitive Fähigkeiten, die

durch Verletzung oder Krankheit beeinträchtigt wurden. Abseits der klassischen Informatik könnten in der Zukunft innovative Konzepte, wie beispielsweise der Quantencomputer, zu völlig neuen Möglichkeiten und Sichtweisen beim Machine Learning führen. Einige Experten sind der Ansicht, dass Quantenprozessoren das maschinelle Lernen revolutionieren werden. Firmen wie Google, IBM oder Microsoft investieren heute schon in die Vision der Zusammenführung von KI mit Quantencomputing. Auch hier werden natürlich zunehmend ethische Fragen virulent, die bei einer disruptiven Technologie automatisch zu stellen sind. Bei der Einführung von KI in Unternehmen fühlen sich heute schon Mitarbeiter mit der Sorge belastet, dass durch den technischen Fortschritt Arbeitsplätze verloren gehen. Hier ist die Überzeugungsarbeit vom Management gefragt, dass KI in den meisten Fällen erst durch das Zusammenwirken mit dem Menschen ihr volles Potenzial entfalten kann.

Mit intelligenten Stromnetzen und Smart Grids wird zukünftigen Anforderung nach ökonomisch-ökologischer Optimierung Rechnung getragen. Diese erlauben eine direkte Kommunikation zwischen Verbraucher und Netzbetreiber, was für einen Ausgleich von Angebot und Nachfrage im Verteilernetz sorgt sowie den nachhaltigen Umstieg auf erneuerbare Energien fördert. Ein Beispiel ist etwa die Erzeugung von Elektrizität aus Windkraft oder Fotovoltaik, welche natürlichen Schwankungsbreiten unterliegt. Das intelligente Stromversorgungsnetz reagiert darauf adaptiv, indem es das Zusammenspiel von Verbraucher, Erzeuger und Speicher durch digitale Kommunikation so koordiniert, dass die bestmögliche Effizienz gewährleistet ist. Damit wird eine wichtige Voraussetzung für die Vision einer zukünftigen Smart City erfüllt, welche den Einsatz digitaler Technologien für die Nutzung nachhaltiger Quellen in den Vordergrund stellt. Als weitere Maßnahme zur

langfristigen Energie- und Ressourcenschonung wird der 3D-Drucktechnologie eine große Zukunft vorhergesagt. Dieses auch von Konzernen unterstützte Feld wird immer interessanter für komplexe Anwendungen und könnte einst den klassischen Fertigungsprozess ersetzen. Schon heute werden in Asien Häuser gebaut, welche direkt dem 3D-Drucker entstammen. Produktionssysteme werden dadurch dezentral gestellt, wodurch Fertigung und Verbrauch am selben Ort stattfinden. Diskutabel bleibt, welche genauen Auswirkungen dies bei größerer Verbreitung auf Verkauf, Distribution und Transport hätte. Die Steigerung der Wirtschaftlichkeit gilt andererseits gegenüber so manch konkurrierendem Herstellungsverfahren als erwiesen und wächst zudem mit steigender Komplexität der Bauteilgeometrie. Schlagworte wie „Bioprinter" oder „Digital Food" stellen in Aussicht, dass es auf diesem Wege eines Tages zu markanten Innovationen im Gesundheitswesen wie auch in der Nahrungsmittelproduktion kommen mag. Gut vorstellbar auch, dass Online-Shops die Technik nutzen werden, indem der Kunde keine physische Ware mehr erwirbt, sondern einen digitalen Konstruktionsplan downloadet und damit den privaten 3D-Drucker füttert. In jedem Fall geht es dabei um äußerst komplexes Datenmaterial, das es entsprechend zu schützen gilt.

Zukunftsware: Datenschutz und Prozessorleistung

Mit Hinblick auf die ubiquitäre Vernetzungstendenz sowie die genannten Visionen (die nicht der Fantasie des Autors entstammen, sondern bereits breit diskutiert werden) muss unmittelbar einleuchten, dass die digitale Sicherheit in der zukünftigen IT noch viel umfassender gedacht werden muss. Dies betrifft nicht nur das Internet der Kommunikation, sondern ebenso das Internet der Dinge, von dessen allmählicher Omnipräsenz viele Experten überzeugt sind. Schon heute prasseln Hacker- und Lauschangriffe

global gesehen zu Millionen im Sekundentakt herein und verursachen einen gewaltigen wirtschaftlichen Schaden. In einer immer stärker vernetzten Welt kann sich dieses Problem nur potenzieren. Man mag sich gar nicht vorstellen, was das erst für einen künftigen vollautonomen Fahrbetrieb bedeuten kann. Ein gut gezielter Cyberangriff auf das zigtausende Autos steuernde Verwaltungssystem könnte die absolute Katastrophe bedeuten. Selbstredend bedürfen kritische Infrastrukturen, speziell auch im Zusammenhang mit modernen Industriekonzepten, besonderer Schutzmaßnahmen. Ein Grundsatzproblem besteht darin, dass die generierte Datenmenge (die jährlich exponentiell wächst) in der Zukunftswelt exorbitante Ausmaße erreichen wird. Damit steigt nicht nur die Gefahr unautorisierter und krimineller Angriffe ebenso rapide an, sondern es erreicht auch die Menge personenbezogener Daten eine schwindelerregende Größenordnung. Die bereits heute im Internet erzeugte Informationsmenge (um 2020 ca. 200 Exabyte pro Monat) ist viel zu groß und komplex, um konventionell bearbeitet zu werden. Deshalb werden oft große Datenmengen zentral erfasst und miteinander verschränkt (Big Data). Dies kann für viele sinnvolle Zwecke genutzt werden, etwa für Wirtschaft, Finanz und Medizin. Auf der anderen Seite macht die Ansammlung immer größerer persönlicher Datenbestände die Sicherung von Privatsphäre und Datensouveränität zunehmend zur Herausforderung. In einer so hoch vernetzten Welt muss „echte Privacy" deshalb als eine der wichtigsten Forderungen der Gesellschaft gelten – sonst droht am Ende der totale Überwachungsstaat (der sich mancherorts schon abzeichnet).

Wie aktuelle Beispiele zeigen, ist die Weitergabe persönlicher Daten ein florierendes Geschäft, was zur Ignoranz gegenüber gesetzlichen Auflagen motivieren kann. Hier ist generell ein langfristig wirkender Schutz gefragt, der jedoch nicht ausschließlich in Regulierungen bestehen

kann, sondern auch technisch gewährleistet sein muss. Weil Daten generell als das Gold der Zukunft anzusehen sind und deren Analyse und Weitergabe Konzernen viel Geld einbringt, werden logischerweise irgendwann konträre Geschäftsmodelle entstehen. Somit müssen umfassender Cyberschutz und Sicherung der Privatsphäre in der Zukunft als wesentlicher Business-Faktor ernst genommen werden. Ganz wichtig auch: zentrale Datenspeicher, digitale Archive und Datenbankensysteme, in denen jetzt schon sehr viel Material abgelegt wird. Was heute als sicher gilt, muss diesen Anspruch auch noch in 20, 50 oder 100 Jahren erfüllen können. Bei Banken und großen Unternehmen herrscht überwiegend die Meinung vor, dass zwar die heutige Sicherheitstechnik als ausreichend zu betrachten ist, die Vorstellung jedoch, dass am Tag X einmal die Technik nicht mehr standhält, ein gewisses Unbehagen erzeugt. Dazu gilt es klar festzuhalten, dass die aktuelle digitale Sicherheitstechnik ausschließlich auf der Annahme beruht, dass die Rechnerleistung des Angreifers nicht ausreicht, um die benutzte Codierung beziehungsweise die bestehende Firewall zu knacken. Für diese Annahme gibt es jedoch keinen direkten wissenschaftlichen Beweis. Ein Schwachpunkt der heute üblichen Public-Key-Algorithmen (wie RSA oder elliptische Kurven), die etwa für digitale Signaturen oder Schlüsselaustausch verwendet werden, besteht darin, dass sie auf der Schwierigkeit mathematischer Probleme beruhen. Durchbrüche in der Forschung sowie die stete Zunahme der Rechnerleistung können jedoch dazu führen, diese Verfahren zu brechen. Die Grundfrage ist daher: Wie kann man einen langfristigen und nachhaltigen Cyberschutz garantieren, der auch zukünftigen Computerentwicklungen von potenziell sehr großer Leistung standhält?

Es muss daher im Sinne der Gesellschaft sein (nicht nur von Regierungen und Eliten), dass die Wissenschaft

neue Konzepte zum Thema digitale Sicherheit bereitstellt. Die Quantenkommunikation bildet hierzu die ideale Voraussetzung. Dabei geht es insbesondere um den innovativen Ansatz der inhärenten Sicherheit, das heißt um ein System, dessen Wirksamkeit nicht eine Variable der Computerleistung des Angreifers ist, sondern einen physikalischen Mechanismus enthält, welcher die Immunität garantiert. Auf Basis der bisherigen Informationstechnik ist ein physikalisch garantierbares Verfahren jedenfalls nicht möglich. Die Quantenkommunikation bietet dagegen einen Weg, um eine ganz wesentliche potenzielle Sicherheitslücke automatisch zu schließen: Die völlig abhörsichere Datenverbindung zwischen zwei entfernten Punkten. Eine solche Hochsicherheitsverbindung kann entweder direkt von Punkt zu Punkt erfolgen oder durch vertrauenswürdige Knotenpunkte verteilt hergestellt werden. Zusammen mit Methoden der klassischen Sicherheitstechnik vermag sie auch einen bis dato unerreichten Schutz gegen Hackerangriffe sowie den unautorisierten Zugriff auf Datenbanken zu gewährleisten. Diese Technik liegt dem Grundprinzip nach schon fix und fertig in den Schubladen, ist der Marktreife schon sehr nah und harrt nur mehr der nötigen großen Investitionen. Sie ist bereits in asiatischen Testnetzwerken im bis dato größten Maßstab implementiert und könnte bereits in den 2020er Jahren überregionale Verbreitung finden. Sie kann eine wichtige Rolle in lokalen Strukturen wie auch in Backbone-Netzwerken spielen. Da hiermit auch viele kommerzielle Anwendungen verbunden sind, wird letztlich ein globales Hochsicherheitsnetz vorstellbar, das permanent weiterentwickelt wird und so den zukünftigen Sicherheitsanforderungen bestens gewachsen wäre. Schon heute bieten Firmen Sicherheitslösungen auf Basis der Quantenschlüsselverteilung (englisch, QKD) an, welche die traditionelle Kryptografie verbessert. Dabei handelt es sich um

Verteilungs-Appliances kombiniert mit Linkverschlüsslern, die durch optische Fasern miteinander verbunden sind. Zu den typischen Anwendungen zählen sichere LAN-Erweiterungen, Unternehmensumgebungen oder Datencenter-Links. Verbindungsbandbreiten bis zu 10 Gbit/s sowie Reichweiten um die 100 km erlauben den Einsatz in metropolischen Quantennetzwerken. Gut vorstellbar, dass in einiger Zeit viele User ein Quantenmodul zur abhörsicheren Kommunikation in ihrem Computer nutzen.

Auf der anderen Seite impliziert die Projektion in die digitale Zukunft rasant steigende Computerleistungen. Dies nicht nur als Folge der angesprochenen exponentiellen Datenzunahme und der dafür benötigten wachsenden Prozessorleistung, sondern auch in Hinblick auf zukünftige Logistik- und Optimierungsaufgaben. Wie man zeigen kann, gibt es zahlreiche Problemstellungen, die von klassischen Computern entweder gar nicht oder jedenfalls in keinem angemessenen Zeitrahmen gelöst werden können. Ein bekanntes Beispiel ist das Problem des Handlungsreisenden: Die Berechnung des optimalen Routenplans, um eine Reisestrecke möglichst kurz zu halten, stellt traditionelle Rechner vor erhebliche Probleme; gilt es doch, aus hunderten Billionen möglicher Varianten (die schon bei weniger als 20 Städten auftreten) die optimale auszuwählen. Ein damit verwandtes Zukunftsproblem betrifft zum Beispiel die Verkehrsflussoptimierung beim autonomen Fahren. Das Erfassen von extrem vielen Daten mithilfe von Sensoren ist zwar technisch kein Problem, sehr wohl aber die anschließende simultane Berechnung der optimalen Fahrmanöver für alle Fahrzeuge. Auf Basis der herkömmlichen EDV benötigen klassische Computer dafür viel zu lange. Wie erste Simulationen von Quantenrechnern bereits nahelegen, können derartige und verwandte Optimierungsaufgaben mit diesem neuen Konzept wesentlich rascher gelöst werden.

Davon abgesehen existieren zahlreiche weitere logistische Herausforderungen, vor allem aber auch wissenschaftliche Problemstellungen, die mit klassischen Computern nicht sinnvoll oder gar nicht zu bewältigen sind. Auch mit Hinblick auf KI und Machine Learning werden neue Computerkonzepte immer wichtiger. Nicht zuletzt auch deshalb, weil die herkömmliche „Silicium-Revolution" in wenigen Jahren ausgereizt erscheint. Das vielversprechendste Konzept ist hier der Quantencomputer, der wahrscheinlich die einzige Möglichkeit darstellt, die Computerleistung noch wesentlich zu verbessern oder sogar in eine neue Dimension zu führen. So können Quantencomputer zum Beispiel im Bereich der KI die dort auftretenden harten kombinatorischen Optimierungsprobleme viel effizienter lösen. Auch vermögen sie Strukturen aus verrauschten Daten viel schneller zu erkennen und liefern entsprechend neue Gesichtspunkte für Machine Learning. Heute schon zeigt sich, dass gleichsam jede digitale Quantensimulation eines komplexen Problems auf einem Quantensimulator durchgeführt werden kann. Das große Marktpotenzial beweisen IT-Riesen wie Google, Microsoft oder IBM, die bereits Milliarden in diese Technologie investiert haben. VW beispielsweise hat eine Kooperation mit Google geschlossen, um auf Basis von Quantenprozessoren Kalkulationen für Akkus und autonome Fahrzeuge erstellen zu lassen. Quantentechnologien werden daher auch von dieser Seite eine wichtige zukünftige Rolle spielen. Unabhängig vom enormen wissenschaftlichen Wert steht demnach die Entwicklung von technologisch nutzbaren Quantencomputern, respektive einer damit verbundenen Netzwerktechnik im Fokus der Forschung. Während ein QKD-Internet bereits ein fassbares Ziel mit klaren Konturen darstellt (Regierungen und Unternehmen haben schon ihr Interesse artikuliert), muss ein Netzwerk leistungsfähiger Quantenprozessoren

hingegen noch als reine Zukunftsvision gesehen werden. Dabei ist noch nicht einmal klar, welche Funktionalitäten damit eigentlich genau verbunden sein können. Ebenso lässt sich noch nicht abschätzen, in welchem Umfang eine Realisierung physikalisch/technologisch überhaupt möglich ist. Die Gesichtspunkte eines Quanteninternets sind vielfältig und für so manchen Forscher überwiegend noch ein Graubereich. Dennoch geben sich einige Experten heute schon der faszinierenden Spekulation hin, dass auf Basis von Quantentechnologien eines Tages ein unsagbar leistungsfähiges Hypernet entstehen wird, welches in den Parametern Prozessorgeschwindigkeit, Datenrate und Sicherheit völlig neue Maßstäbe setzt. Dabei gilt es explizit festzuhalten, dass der Geschwindigkeitsvorteil eines Quanteninternets nicht etwa auf einen überlichtschnellen Transfer von direkt nutzbarer Information zurückzuführen ist, sondern auf die Tatsache, dass Quantenbits viel mehr Information speichern und übertragen können als herkömmliche Bits. Zwar kann auch ein Quanteninternet nicht schneller als das Licht kommunizieren, sehr wohl aber überlichtschnell koordinieren und synchronisieren, was es bezüglich dieser Eigenschaft einzigartig macht (auf derartige und ähnliche Aspekte wird später noch ausführlich eingegangen). Schließlich würde ein Quanteninternet nicht nur vom Speed-up seiner Quantenprozessoren profitieren, sondern es könnte bei entsprechender Konfiguration auch dazu beitragen, Quantencomputer skalierbar (das heißt um beliebige Qubits erweiterbar) zu machen. Mit Hinblick auf die Anforderungen des Internets der zukünftigen Welt gilt es festzuhalten: Wenn die angedachten Visionen der klassischen IT (die sich ja nicht sofort, sondern in einer schleichenden Revolution vollziehen würden) langfristig sinnstiftend sein sollen, so ist jedenfalls eine „quantendigitale" Begleitung dieser Entwicklung nicht wegzudenken. Nicht zuletzt auch deshalb,

weil Quantencomputer eine theoretische Gefahr für die traditionelle Sicherheitstechnik darstellen und daher auf längere Sicht besondere Verfahren notwendig machen. Ironischerweise beruhen diese Maßnahmen wiederum erheblich auf der Quantentheorie.

1.2 Revolutionäre Quantenphysik

Es war bereits Thema der Alpbacher Technologiegespräche Schon seit vielen Jahrzehnten hat die Quantentechnologie eine revolutionäre Auswirkung auf die Menschheit. Errungenschaften wie Laser, bildgebende Verfahren oder Halbleitertechnologie haben ihre Wurzeln in grundlegenden Gesetzen der Quantenmechanik. Insbesondere resultiert daraus die moderne Computerentwicklung, ohne die ein weltumspannendes Netzwerk wie das heutige Internet gar nicht erst möglich wäre. Nicht so bekannt ist in der Öffentlichkeit der Umstand, dass bereits jedes Smartphone, jeder DVD-Player, aber auch jede Badezimmer-LED als Kind der Quantentheorie anzusehen ist. Die wirtschaftlich hohe Bedeutung der Quantentechnik lässt sich daran erkennen, dass heute schon gut ein Drittel des Bruttosozialprodukts eines Industriestaats durch Produkte erwirtschaftet wird, die auf der Quantentheorie beruhen. Forschungsergebnisse in den letzten Jahren und Jahrzehnten geben Anlass zur berechtigten Hoffnung, dass die Quantentechnik noch viele weitere Facetten bereithalten könnte. Quantentechnologien können in unterschiedlichen Bereichen Anwendungen finden und ermöglichen auf vielen Gebieten Verbesserungen von bestehenden technischen Lösungen. Ebenso eröffnen sie fundamental neue Möglichkeiten und Gesichtspunkte. Abseits der Quantenkommunikation und der Quanteninformatik ist etwa die Quantensensorik von besonderem

Interesse. Obwohl die Quantenphysik eine Wissenschaft der Unbestimmtheiten und Wahrscheinlichkeiten ist, kann sie zu einer noch nie da gewesenen Präzision beitragen: Heutzutage werden klassische Sensoren immer kleiner und präziser gebaut. Allerdings ist bereits jetzt abzusehen, dass damit in Zukunft keine entscheidende Verbesserung in den Parametern Empfindlichkeit und Spezifizität zu erreichen sein wird. Originäre Quantenphänomene wie Superposition oder Verschränkung können jedoch dazu genutzt werden, physikalische Größen wie Druck, Temperatur, Zeit, Lage, Beschleunigung oder aber elektrische, magnetische sowie Gravitationsfelder wesentlich präziser zu erfassen. Dies kann zu vielfältigsten Anwendungen führen wie auch zur Untersuchung fundamentaler wissenschaftlicher Fragestellungen.

Um zu verstehen, wie nahe diese „zweite Quantenrevolution" uns heute bevorsteht, drehen wir das Rad der Zeit zurück, um zu sehen, worin die erste Quantenrevolution bestand: Am Ende des 19. Jahrhunderts wurde manchem Studenten (etwa dem jungen Max Planck!) von einem Physikstudium abgeraten, da man der Meinung war, dass es nichts Wesentliches mehr zu entdecken gäbe. Allerdings zogen, wie es Lord Kelvin (William Thomson) ausdrückte, alsbald „dunkle Wolken" am Physikhimmel auf. Eine solche war zum Beispiel die Strahlung, welche von glühenden Körpern emittiert wird, etwa der Sonne, die uns gleißend weiß erscheint, wenn sie im Zenit steht. Doch weiß kaum jemand, dass sie in erster Linie grün leuchtet. Der physiologische Grund liegt darin, dass die Sonne (so wie jeder Stern) Strahlung mit vielen verschiedenen Wellenlängen abgibt und die menschliche Wahrnehmung den sichtbaren Anteil dieser Mixtur als „weißes" Licht interpretiert. Physikalisch steht hinter dem realen „grünen" Strahlungsmaximum das wiensche Verschiebungsgesetz, welches besagt, dass mit zunehmender

Oberflächentemperatur eines Sterns die Wellenlänge der maximal emittierten Strahlung immer kleiner wird. Ein besonders heißer Stern leuchtet demnach in erster Linie blau, unsere mittelheiße Sonne danach grün, ein kühler Roter Riese wie Beteigeuze im Sternbild Orion vorwiegend im roten Spektrum. Will man allerdings nicht nur das Maximum, sondern die gesamte Energieverteilung eines glühenden Körpers erklären, stößt man mit der klassischen Physik an eine Grenze. Es ist im Rahmen der klassischen Physik nicht möglich, eine Formel zu finden, die mit den ermittelten Messdaten übereinstimmt. Insbesondere käme es nach den Vorhersagen der klassischen Physik zu unendlich großen Termen („UV-Katastrophe"), was definitiv nichts mit der Realität zu tun hat. Erst der deutsche Theoretiker Max Planck fand das sogenannte plancksche Strahlungsgesetz, indem er eine der klassischen Physik grundsätzlich fremde Annahme machte: Danach tauscht das Licht seine Energie nicht in beliebig feiner Einteilung aus, sondern in Klumpen oder Portionen, welche er „Quanten" nannte. Allerdings misstraute Planck seinem eigenen Quantenmodell und hoffte noch lange, dass seine Annahme zugunsten der klassischen Physik wieder verworfen werden könnte – eine Hoffnung, die nie erfüllt wurde. Die Quanten erwiesen sich als fundamental. Diese Erkenntnis entstammte dem damals noch völlig unbekannten Albert Einstein, der durch Planck inspiriert 1905 seine nobelpreisgekrönte Lichtquanten-(Photonen-)Hypothese veröffentlichte. Diese Lichtteilchen werden auch in der zukünftigen Quantentechnik eine ganz entscheidende Rolle spielen. Im Unterschied zu Planck, der zunächst nur den Energieaustausch zwischen Atomen als quantisiert annahm, erweiterte Einstein diese Vorstellung auf das Licht selbst, welches demnach aus diskreten Energiequanten besteht. Auf dieser Basis erfuhr dann erstmals der fotoelektrische

Effekt eine Deutung, welcher heute die Grundlage für Belichtungsmesser in Kameras wie auch die Photovoltaik bildet. Einstein erkannte aber gleichermaßen sofort die Problematik der neuen Quantentheorie, welche sich, wie wir später genauer sehen werden, etwa im Doppelspalt-Experiment äußert (Abschn. 3.1). Die sogenannte Interferenz, die dabei entsteht, ist auf Basis der klassischen Wellenvorstellung des Lichts leicht erklärbar, sorgt aber bei einer Teilchenvorstellung für eine konzeptionelle Schwierigkeit. Einstein hätte vorausgesagt, dass für sehr schwaches Licht, das heißt einzelne Lichtquanten, eine solche Interferenz (salopp: Überlagerung von Lichtwellen) nicht mehr auftreten darf. Alle Experimente beweisen jedoch das genaue Gegenteil. Damit werden der menschliche Verstand und seine Vorstellungskraft auf eine harte Probe gestellt. Denn wie kann ein einzelnes Teilchen gleichzeitig durch zwei Spalte treten, wenn es per se als unteilbar angenommen wird? Das widerspricht dem gesunden Menschenverstand. Derartige und ähnliche Fragen wurden immer drängender, als die Quantenmechanik einige Zeit später unter anderem durch Werner Heisenberg und Erwin Schrödinger mathematisch ausformuliert wurde. Dies war die erste Quantenrevolution, mit ihr gelang es, eine ungeheure Vielzahl von Phänomen zu verstehen, die im Rahmen der klassischen Physik völlig unerklärlich bleiben. Nicht nur die Strahlung glühender Körper, sondern generell die Entstehung von Licht als quantisierter Übergang von Atomspektren (Quantensprung) konnte erstmals erklärt werden. Vor allem aber führte das moderne Verständnis von Atomen und Molekülen nicht nur zur Quantenchemie, sondern ebenso zur Festkörperphysik, welche die unmittelbare Basis der Halbleitertechnik und somit die Grundlage aller heutigen Computer liefert. Neben einer Vielzahl weiterer Entwicklungen sind vor allem wichtige Anwendungen

in der Medizin zu nennen (etwa Magnetresonanz- oder Positronenemissions-Tomografie), und natürlich auch die weiße LED, welche eine Revolution in Sachen Leuchtmittel einläutete. Mithin hat die Quantentechnik unseren heutigen Alltag also längst durchdrungen.

Trotz ihrer gewaltigen Erfolge steht die Quantenphysik in dem Ruf, ein rätselhaftes Gebiet mit verwirrenden Grundannahmen zu sein, welche den menschlichen Verstand in extremer Weise herausfordern. Solche Positionen entstehen aber vor allem dann, wenn man sie nicht als fundamentale Wissenschaft akzeptieren will und ihr Denkweisen der klassischen Physik künstlich aufprägt. Ebenso war und ist sie Gegenstand zahlreicher Interpretationen und philosophischer Betrachtungen, die bis heute umstritten sind. Viele Physiker folgen jedoch der pragmatischen Ansicht von Sir Karl Popper und sind Anhänger einer eher interpretationsfreien Quantenmechanik. Frei nach der Doktrin: „Shut up and calculate!“ rechtfertigt sich dieses Vorgehen durch seine nachhaltigen Erfolge, wovon kein Ende abzusehen ist. In den nächsten Jahren und Dekaden könnte sogar ein weiteres Kapitel dieser Erfolgsgeschichte aufgeschlagen werden. Mit der Bezeichnung „zweite Quantenrevolution“ ist die Wissenschaft allerdings nicht sonderlich glücklich. Getreu dem Motto, man solle den Tag nicht vor dem Abend loben, harrt dieser Begriff noch einer affineren Bezeichnung. Hier wäre es vielleicht angebrachter, vom „Quantenvorteil“ beziehungsweise „Vorsprung durch Quantentechnik“ zu sprechen, zumal viele der neuen Applikationen die Welt nicht neu erfinden werden. Immerhin könnten sie bestehende technische Lösungen ganz erheblich verbessern, was mittel- bis langfristig einen großen Vorteil für Forschung, Wirtschaft und Gesellschaft bedeuten kann. Den allergrößten Vorsprung, um nicht zu sagen technologischen Quantensprung, würde dabei die Entwicklung eines leistungsfähigen

Quantencomputers markieren, dies wäre zweifellos der Gipfelpunkt dieser Entwicklung.

Die Vernetzung von Quantenrechnern durch ein abhörsicheres Quanteninternet könnte als Langzeitziel nicht nur dazu beitragen, deren Potenzial der ganzen Menschheit zur Verfügung zu stellen, sondern auch ihre Leistungsfähigkeit – gleich einem Netzwerk von Supercomputern – in noch unbekannte Regionen vordringen zu lassen. Wohlgemerkt, noch befindet sich die „Quanten-IT" im Anfangsstadium, doch arbeitet die Wissenschaft hart daran, diese Vision in ersten Schritten Wirklichkeit werden zu lassen. Als angepeiltes großes Etappenziel steht dabei die Entwicklung eines regionalen, schließlich auch globalen QKD-Netzwerks für die Quantenkryptografie im Mittelpunkt. Der renommierte Innsbrucker Quantenforscher Rainer Blatt ist davon überzeugt: „Die Quantenkryptografie wird die erste wirtschaftliche Anwendung der zweiten Quantenrevolution werden." Dazu ist ganz essenziell Grundlagenforschung erforderlich, welche in jüngster Zeit einen Meilenstein in Richtung Quanteninternet setzen konnte. Im Nachfolgenden dazu eine eher journalistisch gehaltene Schilderung.

1.3 Der Quantensatellit

China, Wüste Gobi, Weltraumbasis Xingjiang. Man schreibt den 16. August 2016, 1:40 morgens Ortszeit.

„… 3, 2, 1 – Zündung" Die Wüste bebt. Eine viele Meter hohe Rakete vom Typ „Langer Marsch 2d" rüttelt und schüttelt sich, eingehüllt in eine weiße Rauchwolke. Unter den vielen gebannt zusehenden Menschen befindet sich auch ein Mann, der das Spektakel mit besonderer Spannung verfolgt: Jian-Wei Pan, der chinesische Chefwissenschaftler des Projekts. Ihm zur Seite

steht ein Herr von gänzlich anderer Statur. Das Licht des Raketenfeuers wird von seiner Brille reflektiert, verliert sich im Dickicht seines nicht unbeträchtlichen Bartes, der ihm das Aussehen eines bedeutenden Philosophen verleiht. So mag man sich Platon oder Aristoteles vorgestellt haben – allerdings ohne Anzug und Krawatte. Diese eindrucksvolle Persönlichkeit ist der prominente österreichische Physiker Anton Zeilinger.

„Hoffentlich geht jetzt nichts schief!" mögen beide Wissenschaftler unisono gedacht haben. Als die Rakete störungsfrei emporsteigt, immer mehr an Höhe gewinnt, lässt ihre Anspannung allmählich nach. Zunehmend kehrt innere Ruhe ein, ehe sie von den einsetzenden Jubelschreien der Menge abgelöst wird.

Die Rakete steigt und steigt. Schon beginnt sie ihre Triebstufen abzuwerfen, bis sie am Ende aus dem Blickfeld der Zuschauer verschwindet und in die Erdumlaufbahn einschwenkt. Jetzt ist sie keine Rakete mehr, sondern ein gut 600 kg schwerer Forschungssatellit – der das „Quantum Experiment at Space Scale" (kurz QUESS) mit sich trägt. Randvoll mit hochsensiblem Gerät wird er für mindestens zwei Jahre die Erde mit der nicht unbeträchtlichen Geschwindigkeit von gut 27.000 km/h umrunden. Die beiden Forscher können gedanklich gerade noch ein Stoßgebet hinterher in den Himmel schicken, dass die geplanten Experimente auch tatsächlich gelingen mögen. Dabei gilt ihre Sorge weniger der Verlässlichkeit der Quantenphysik, von der sie überzeugt sind, sondern der Frage, ob die hoch komplizierte Technik wie geplant funktioniert und keine Defekte auftreten. Denn Reparaturen am QUESS-Satelliten, soviel dürfte klar sein, wären wohl mit leichten Schwierigkeiten verbunden. Kaum gedacht, werden sie bereits von Journalisten umzingelt, worauf sie geduldig und gebetsmühlenartig immer wieder erklären müssen, worum es bei diesem Projekt überhaupt geht.

Wie kommt es eigentlich zu dieser austro-chinesischen Zusammenarbeit? Immerhin ist der Schauplatz hier China – was hat das vergleichsweise kleine Österreich damit zu tun?

Dafür kann man mehrere Gründe anführen. Zum einen liegt dies daran, dass Österreich auf eine Reihe bedeutsamer Quantenphysiker zurückblicken kann, angeführt von den Nobelpreisträgern Erwin Schrödinger und Wolfgang Pauli- Aber auch die aktuelle Forschung kann sich sehen lassen in Form zahlreicher international anerkannter Institute. Als geografische Hochburg ist dabei die „Quantenhauptstadt" Wien zu nennen. Besonders zu nennen sind hier die herausragenden Leistungen von Anton Zeilinger und seinen Forschergruppen. Öffentlich bekannt wurde „Mr. Beam" vor allem durch die erstmalige Realisierung der Quantenteleportation optischer Zustände, jener nach Science-Fiction klingenden Methode, Information vom Ort A verschwinden zu lassen, um sie daraufhin am Ort B wieder zu replizieren. Mitglied dieser Gruppe (und als Doktorand somit Schüler Zeilingers) war Jian-Wei Pan, der wissenschaftliche Leiter des Quantensatelliten-Projekts. Der hochbegabte und visionäre Forscher ist nicht nur im chinesischen Nationalfernsehen ein sehr gefragter Interviewpartner, sondern hat zudem den imageträchtigen Breakthrough-Preis gewonnen. Dabei steht ihm Zeilinger selbst in punkto medialer Präsenz in nichts nach – schließlich hat die österreichische Politik, welche immer wieder die Wichtigkeit innovativer Forschung als potenziellen Wirtschaftsmotor betont, mit Zeilinger eines ihrer besten Aushängeschilder gefunden. Stichwort Österreich und somit Europa. Natürlich hätte Anton Zeilinger gerne auch ein Satelliten-Projekt mit der ESA, der Europäischen Weltraumorganisation, realisiert, was aber nicht gelungen war. Mithin verbleibt die Zusammenarbeit mit den Chinesen als einzige Option. Dabei besteht der österreichische Beitrag zunächst einmal

darin, dass Bodenstationen in Wien und Graz eingerichtet wurden, welche die vom Satelliten gesendeten Daten auswerten. Konkret handelt es sich dabei um astronomische Observatorien; etwa die „Satellite Laser Ranging Station" in Graz-Lustbühel oder das „Hedy Lamarr Quantum Communication Telescope" auf dem Dach des Instituts für Quantenoptik und Quanteninformation (IQOQI) in Wien-Alsergrund. Die ESA kommt zumindest als optische Bodenstation auf der Urlaubsinsel Teneriffa vor. Wohlgemerkt, der rund 160 Mio. US$ teure Satellit wird ausschließlich von China aus betrieben und finanziert.

Die beiden Starwissenschaftler befinden sich mittlerweile, umringt von Journalisten, in der Rolle von zum Interview genötigten Quantenpredigern. Was sie einerseits erfreut, denn sie wollen ja Werbung für ihre Projekte machen und somit die Hoffnung auf weitere Forschungsmittel nähren. Andererseits versuchen sie die fachlichen Aspekte so einfach wie nur möglich zu halten – was im Falle der Quantenphysik immer eine gute Option darstellt, aber alles andere als einfach ist. Trotz aller gebotener Contenance können sie dabei eines nicht unterdrücken: das Leuchten in ihren Augen, ihre verborgene, jedoch vorhandene Emotion – denn sie sind felsenfest davon überzeugt: Quantenphysik ist die Wissenschaft der Zukunft! Gerade im Zusammenhang mit dem Internet, längst eine der wichtigsten Lebensadern des Menschen geworden, kann dies einmal der ganz große Renner werden. Die beiden Forscher bemühen sich also um eine allgemeinverständliche Darstellung, frei nach dem Motto: Erzähle Geschichten rund um die Quantenphysik möglichst einfach, aber nicht einfacher! Was mögen sie vor diesem Hintergrund wohl erklärt haben? Wieso ist diese Technik so revolutionär? Was ist der eigentliche Clou daran?

QUESS ist ein internationales Forschungsprogramm im Bereich der Quantenoptik. Ein Satellit, kulturbeflissen

nach dem chinesischen Philosophen Micius getauft, der im 5. vorchristlichen Jahrhundert entdeckte, dass sich Licht geradlinig ausbreitet, wird von der Chinesischen Akademie der Wissenschaften sowie von diversen Bodenstationen aus betrieben. Die Universität Wien sowie die Österreichische Akademie der Wissenschaften fungieren gleichsam als Schirmherren der europäischen Empfangsstationen. QUESS ist ein sogenannter Proof of Concept, was bedeutet, dass die Übertragung quantenoptischer Zustände über große Distanzen auf ihre physikalische wie auch technologische Machbarkeit hin überprüft werden soll. Konkret geht es dabei um die Entwicklung der inhärent abhörsicheren Quantenkryptografie sowie der Quantenteleportation. Unter Quantenkryptografie versteht man die Erzeugung eines absolut zufälligen Quantenschlüssels zur anschließenden Datenübertragung via klassischer Verschlüsselungsverfahren über das Internet. Die Quantenteleportation bezeichnet dagegen die Möglichkeit, Quanteninformation am Ort A verschwinden zu lassen und am Ort B eine 100 % exakte Replika davon herzustellen – wiederum völlig abhörsicher. In beiden Fällen bildet die Verschränkung die wesentliche Grundlage. Dabei stellt es ein wichtiges Ziel dar, die Existenz der Verschränkung über eine neue Rekorddistanz nachzuweisen. Die weitere Zielsetzung sieht vor, durch verschränkte Lichtquantenpaare über tausende Kilometer völlig abhörsichere Quantenkanäle zwischen Satellit und Bodenstationen herzustellen. Dabei stellen sowohl die Distanz als auch das Sicherheitslevel ein absolutes Novum dar. Freilich darf man sich mit „QUESS 1“ noch nicht den tatsächlichen Technologieträger vorstellen. So besitzt er einstweilen nur beschränkte Kommunikationsmöglichkeiten und funktioniert wegen sogenannter Infrarotstörungen nur in Abwesenheit von Sonnenlicht. Im Erfolgsfall sind jedoch weitere Micius-Satelliten avisiert, die in einigen Jahren

bereits erste Prototypen einer datensicheren Verbindung zwischen China und Europa bilden könnten. Ein erstes globales Netzwerk, dessen Sicherheit einen gewaltigen Fortschritt gegenüber dem bisherigen darstellt, hält Projektchef Pan bereits um 2030 für vorstellbar.

Allmählich flaut das Gewimmel um die beiden Starwissenschaftler ein wenig ab. Während Jian-Wei Pan immer noch von zahlreichen, vorwiegend einheimischen Menschen umringt steht, die ihn „Vater der Quanten" nennen, vermag sich Zeilinger erstmals mit einiger Zufriedenheit über den Bart zu streichen und sich seiner Begleitung zuzuwenden. Plötzlich stellt sich ihm ein deutscher Journalist in den Weg und beginnt mit investigativen Fragen: „Sie, ich verstehe immer nur Bahnhof! Dieses Quantenlatein ist doch für keinen normalen Menschen begreiflich! Haben Sie nicht eine anschaulichere Erklärung parat? Und außerdem: was soll daran revolutionär sein? Es gibt doch zahllose Möglichkeiten und Unmengen von IT-Fachkräften, welche die Daten im Internet schützen können! Wozu dann überhaupt Quantentechnik? Wollen Sie sich nur profilieren?".

Es geht also um eine allgemeinverständliche Erklärung, die stark vereinfacht das Wesentliche auf den Punkt bringen soll: Der eben gestartete Satellit führt einen speziellen Laser mit sich an Bord, der wie ein Maschinengewehr einzelne Patronen hintereinander abfeuert (Abb. 1.1). Diese Projektile nennen Physiker Lichtquanten (Photonen) – sie sind die kleinsten Partikel des Lichts. Der Laser erzeugt blaues Licht und zielt damit auf einen speziellen nichtlineare Kristall. Am Ziel entsteht aus jedem einzelnen blauen Photon ein Paar infraroter Photonen, welche sich mit Lichtgeschwindigkeit zu den Bodenstationen bewegen. Und jetzt kommt der eigentliche Clou: Obwohl räumlich weit voneinander getrennt, bildet jedes dieser Photonenpaare

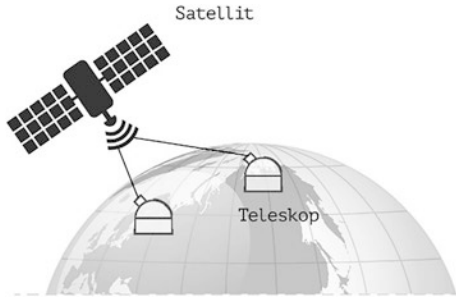

Abb. 1.1 Das QUESS-Experiment

dennoch eine untrennbare Einheit. Sie hängen gewissermaßen wie durch ein unsichtbares Band miteinander zusammen. Dies ist in dem Sinne zu verstehen, dass sie in bestimmten physikalischen Eigenschaften in engstem Zusammenhang stehen – und das ohne Kabel, ohne Signalwirkung, ohne irgendetwas. Einfach so! Diese völlig verrückt scheinende Eigenschaft der Natur wird manchmal auch als „Quantenspuk" bezeichnet. Sie hat aber nichts mit Zauberei zu tun, sondern ist eine Grundeigenschaft der Natur, die man Verschränkung nennt. Die vordergründige Aufgabe von QUESS besteht zunächst einmal darin, zu beweisen, dass der „Quantenspuk" über große Distanzen tatsächlich existiert beziehungsweise technisch aufrechtzuerhalten ist. Der Nachweis geschieht mit Methoden der Statistik. Sobald dies mit ausreichender wissenschaftlicher Signifikanz geschafft ist, kann die Erzeugung eines speziellen Schlüssels für die Quantenkryptografie geprüft werden, was zum Beispiel folgendermaßen geschieht:

Die vom Satelliten erzeugten Infrarot-Photonenpaare sind in einer bestimmten physikalischen Eigenschaft miteinander verschränkt, also gleichsam wie durch Zauberei miteinander verbunden. Das Interessante ist aber die Tatsache, dass völlig unbekannt ist, welche Werte diese

Eigenschaft jeweils annimmt. Um diese Werte herauszufinden, ist eine Messung an den Teilchen nötig, die von den Bodenstationen ausgeführt wird. Nun geschieht abermals etwas sehr Merkwürdiges: jedes Mal, wenn so eine Messung gemacht wird, steht dann zwar der Wert fest, jedoch kann nicht gesagt werden, welchen Wert die nächste Messung ergeben wird. Es könnte sich dabei um denselben, jedoch auch um einen anderen Messwert handeln. Tatsächlich kann auf keine Weise vorhergesagt werden, welchen genauen Wert die einzelne Messung ergibt – das ist völlig zufällig, die Physiker sagen „objektiv zufällig". Insbesondere kann solch ein Zufall von keinem Computer der Welt generiert werden, und zwar deshalb nicht, weil er der Natur selbst entstammt.

Stellt man sich vor, dass man den gemessenen Eigenschaften willkürlich die Zahlen 0 beziehungsweise 1 zuordnet, also ein Bit an Information, so ist die Grundidee zum Quantenschlüssel bereits umrissen: Angenommen, China will eine völlig abhörsichere Datenachse nach Österreich herstellen. Dann könnten in der Zukunft mehrere Satelliten als Quantenrepeater so geschaltet werden, dass verschränkte Photonenpaare erzeugt werden, wovon je ein Photon China, das andere Österreich erhält. Wenn nun die Messwerte der Photonen bestimmt werden, entsteht bei jeder Messung völlig zufällig eine 0 oder 1, bei der nächsten Messung wieder, und so weiter und so fort. In der Praxis werden in Sekundenschnelle Millionen Messungen durchgeführt, wodurch eine absolut zufällige Bitfolge entsteht, die als Quantenschlüssel verwendet werden kann. Dieser lässt sich nach gängigen Verfahren kryptografisch einsetzen und über das normale Internet versenden. Das Entscheidende ist dabei: Durch die besondere Verbindung via Verschränkung erhalten China und Österreich bei bestimmten Einstellungen der Messgeräte

automatisch immer haargenau denselben Schlüssel. Damit entfällt die sicherheitstechnisch bedenkliche Schlüsselverteilung über das Internet völlig, was einen großen Fortschritt darstellt.

Warum kommt diese Technik – falls sie in größerem Maßstab funktioniert – einem Paradigmenwechsel in puncto abhörsicherer Datenübertragung gleich? Zum einen gibt es für etwaige Codeknacker (in der Praxis immer Computer) keine Möglichkeit, den Quantenschlüssel algorithmisch zu generieren, da er objektiv zufällig entsteht, also von der Natur selbst stammt. Es bleibt daher nur die Möglichkeit, alle erdenklichen Kombinationen von Bitfolgen durchzuprobieren, was bei praxisbezogenen Schlüsseln großer Länge selbst für Supercomputer unvorhersehbar lange dauert. Außerdem ist jeder erzeugte Quantenschlüssel ein Original gleicher Qualität und nicht von der verwendeten Kryptotechnik oder der Vertrauenswürdigkeit von Personen abhängig. Sensationell ist zudem, dass ein erfolgter Lauschangriff physikalisch entdeckt werden kann, was mit der bisherigen Technik nicht möglich ist. Der Grund liegt darin, dass potenzielle Hackerattacken den gesamten Quantenzustand automatisch so weit beeinflussen, dass dies statistisch eindeutig erfasst werden kann. Man weiß also immer, ob die Schlüsselverteilung 100 % sicher erfolgt ist oder nicht.

„Äh, gut – alles klar, Professor! War ja nur eine Frage."

Nachdem nun auch ein weiterer Zweifler befriedet erscheint, wiewohl sich Zeilinger nicht sicher ist, ob er den Vondannenschleichenden wirklich überzeugt hat, kann er sich nunmehr seiner Begleitung zuwenden: Heinz Engl, dem Rektor der Universität Wien, der es sich nicht nehmen lassen wollte, diesem Spektakel innovativster Forschungsarbeit schon in seiner ersten Stunde beizuwohnen. Jetzt wird es aber Zeit für ein Gläschen Sekt!

1.4 Interkontinentale Quantentelefonie

Gut ein Jahr später knallen die Sektkorken erneut. Das QUESS-Experiment erweist sich viel rascher als erfolgreich als ursprünglich erwartet. Der große Saal der Österreichischen Akademie der Wissenschaften in Wien ist prallvoll gefüllt. Dicht nebeneinander gedrängt starren Forscher und Journalisten gespannt auf zwei riesige Bildschirme. Was sich hier anbahnt, ist eine wissenschaftliche Sensation: die weltweit erste interkontinentale Videotelefonie mittels abhörsicherer Quantenübertragung, und zwar zwischen China und Europa. „Das ist …", sagt Anton Zeilinger, der die Vorgänge moderiert, „… hier keine Pressekonferenz, sondern eine Live-Demonstration." Der zweite Hauptakteur sitzt im 7600 km östlich entfernten Beijing (Peking): Jian-Wei Pan, der wissenschaftliche Leiter des QUESS-Experiments. Dieses wurde ja im August 2016 gestartet, um die technologische Machbarkeit der neuartigen Quantenkommunikation über große Distanzen zu überprüfen. Zeilinger hält ein kleines Satellitenmodell hoch und erläutert die Vorgänge, die sich gleich abspielen werden. „In China befinden sich fünf Bodenstationen, welche die Satellitendaten empfangen – wir sind die sechste". Die Stationen werden jetzt gleich durch Quantenkanäle miteinander verbunden. Alles wartet gespannt. Die Minuten kreisen ins Leere. Nur der per Live-Videoschaltung anwesende Präsident der Chinesischen Akademie der Wissenschaften, Chunli Bai, trinkt völlig gelassen seinen Tee.

Um die Wartezeit zu überbrücken, bis die Verbindung zustande kommt, beginnt Zeilinger über die Entstehungsgeschichte des Projekts zu erzählen. Dabei moniert er die schneckenartige Entscheidungsfindung der EU in Fragen

wissenschaftlicher Förderungen, lobt hingegen die ungleich rasantere Entscheidungsfähigkeit der Chinesen Will heißen: wenn ihn sein ehemaliger Doktorand Pan nicht aus eigenem Antrieb in das Projekt eingebunden hätte, säßen sie allesamt heute nicht hier. Glücklicherweise fühlt sich Pan der konfuzianischen Tradition verpflichtet, welche eine besondere Lehrer-Schüler-Beziehung pflegt. Und gerade Pan war es auch, welcher wenige Monate zuvor die entscheidende Vorarbeit geleistet hatte. Bereits im Juni 2017 gelang es dem chinesischen Forscher und seiner Gruppe, erstmals einen Quantenlink über 1200 km herzustellen – das war bereits absoluter Weltrekord! Dieser Erfolg ist ein wichtiger Markstein für die Quantenkommunikation. Denn dadurch können zwei Parteien über große Distanzen einen Quantenschlüssel austauschen, welcher absolut sicher ist – einerseits wegen seiner völlig zufälligen Generierung, andererseits weil ein Lauschangriff automatisch die extrem empfindliche nichtlokale Verbindung der Quanten beeinflusst und somit auffällt. Mit nichtlokaler Verbindung meint man konkret die Verschränkung der Teilchen, also den ominösen „Quantenspuk", der hiermit über eine neue Rekorddistanz bestätigt werden konnte. Bislang funktionierte die Quantenkommunikation selbst unter optimalen Bedingungen nur über etwa 100 km, denn sowohl in Glasfaserkabeln wie auch in atmosphärischer Umgebung werden die Photonen stets an Atomen gestreut, wodurch die Verschränkung sukzessive verloren geht. Der bisherige Rekord wurde von Rupert Ursin gehalten. Diesem gelang es bereits 2007, eine Verschränkung über 144 km zwischen den Urlauberinseln La Palma und Teneriffa herzustellen. Viel größere Entfernungen sind auf diese Weise auch nicht möglich, weshalb als nächster Schritt die Satellitenlösung gewählt wurde, wo sich die Lichtquanten in der Hochatmosphäre weitgehend ungestört bewegen können. Dazu wurde eben der Micius-Trabant gestartet, welcher sich in

500 km Höhe nur unwesentlich über der Flugbahn der internationalen Raumstation ISS befindet. Da Satelliten in Erdnähe generell die höchsten Umlaufgeschwindigkeiten aufweisen, steht Micius den Physikern immer nur wenige Minuten lang für Messungen zur Verfügung. Dies ist jedoch ausreichend, um die extrem empfindliche Verschränkung nachweisen zu können. Wenn bei einem Lichtteilchen an einer bestimmten Bodenstation die Polarisation (Schwingungsebene des Lichts, Abschn. 1.5) gemessen wird, besitzt das verschränkte Partnerteilchen an der anderen Station eine dazu fix korrelierte Polarisation. Durch statistische Auswertung, etwa via bellsche Ungleichung (Abschn. 1.8), kann so die Existenz eines Quantenkanals eindeutig nachgewiesen werden.

Es ist nicht ganz einfach, dem Laien begreiflich zu machen, welche unerhörte Leistung die Forscher hier erbracht haben. Schon unter sterilen Laborbedingungen ist für derartige Experimente eine außerordentliche Präzision erforderlich. Auf dem Satelliten befindet sich neben einem Speziallaser und Quantenmodulen auch eine hochgenaue Optik, welche die verschränkten Photonen äußerst exakt zu den Bodenstationen sendet. Die technische Realisierung gestaltet sich vor allem auch deshalb schwierig, weil man auf keine Standardkomponenten zurückgreifen kann. Es ist daher viel Detailarbeit nötig, um den gesamten Aufbau weltraumtauglich zu machen. Abgesehen vom Problem der kosmischen Strahlung, welche die hochempfindlichen Geräte zerstören könnte, ist allein die Steuerung der Optik, welche das Quantensignal zu den Stationen leitet, um vieles akkurater auszuführen als bei üblichen Satelliten. Normalerweise wird bei Satelliten mangelhafte Präzision durch stärkere Sendeleistung ausgeglichen – dies ist jedoch bei QUESS unmöglich. Das Quantensignal kommt nur dann an, wenn die verschränkten Lichtquanten in den 1,2 bis 1,8 m messenden Spiegeln der Empfängerstation

einzeln nachgewiesen werden. Bei Satellitengeschwindigkeiten von über 7,5 km/s eine wahrhaft winzige Spiegelgröße, bei der ständig nachjustiert werden muss. Zur schnellen Übermittlung von Steuersignalen nutzen die Forscher deshalb Laserstrahlen mit anderen Frequenzen, um das Quantensignal nicht zu stören. Micius erfordert also eine hochpräzise Optik, die sowohl heftigen Vibrationen (etwa beim Start der Trägerrakete) als auch großen Temperaturschwankungen standhalten muss. Dies stellt sehr hohe Ansprüche an das Design eines solchen Versuchsaufbaus. Angesichts der nur zum Teil genannten Schwierigkeiten ist es erstaunlich, wie gut die Kopplung zwischen Micius und den Bodenstationen funktioniert. Die Experimente stellen jedenfalls einen Meilenstein in der Entwicklung der Quantentechnik dar. Bislang hat China bereits einen Backbone mit einer Kabellänge von etwa 2000 km zwischen Beijing und Shanghai realisiert. Allerdings sind dazu dutzende Zwischenstationen (sogenannte Trusted Repeater) notwendig, zumal die Quantenkommunikation in optischen Fasern ohne Quantenrepeater eben nur über etwa 100 km möglich ist. Darum wird die quantische Sicherheitskette ständig unterbrochen. Die QUESS-Technik ist dagegen deshalb so revolutionär, weil sie einen direkten Quantenkanal zwischen sehr weit entfernten Punkten herstellt. Allerdings ist der Weg zu einer praktischen Nutzung noch in einiger Entfernung. Wegen Problemen wie dem Überblenden durch Sonnenlicht können Messungen einstweilen nur nachts erfolgen. Und selbst das Mondlicht kann ein Problem sein, das sich jedoch mit einem ausgeklügelten Zeitmodusverfahren kompensieren lässt. Die eigentliche Schwierigkeit liegt im Moment jedoch in der noch viel zu geringen Datenrate – und das, obwohl der Speziallaser beinahe 6 Mio. verschränkte Lichtquanten in der Sekunde erzeugt. Dennoch sind die Forscher optimistisch und versprechen bereits für

die nächsten fünf Jahre eine Steigerung der Datenrate um einen Faktor Tausend.

Mittlerweile ist es ganz still im Saal geworden. Gleich ist es soweit. Die Spannung steigt. Plötzlich tönt es aus Beijing: „Professor Zeilinger, can you hear us?“ Die erste interkontinentale quantensichere Videokonferenz ist eröffnet. Tosender Applaus. Später werden zwei Bilder verschickt, die 100 % quantenkryptografisch verschlüsselt sind. Das von Österreich versendete Bild zeigt ein Foto von Nobelpreisträger Erwin Schrödinger. Das von Beijing übermittelte ziert dagegen der Namenspatron des Satelliten, der Philosoph Mozi (latinisiert Micius). Danach erläutert Rupert Ursin den Journalisten die Funktionsweise der neuartigen Übertragungstechnik: Die vom Satelliten erzeugten verschränkten Photonen werden von den Bodenstationen gemessen, wodurch sich aufgrund der intrinsischen Quantenzufälligkeit eine Folge echter Zufallszahlen ergibt. Der auf diese Weise erzeugte Quantenschlüssel wird sodann für ein Verfahren namens One Time Pad (OPT, Abschn. 2.6.1) verwendet, welches in Kombination mit Quantentechnik nachweislich die völlig abhörsichere Übertragung von Daten über das normale Internet gestattet. Wichtig ist dabei festzuhalten: Nur in Kombination mit Quantentechnik. Das bedeutet einerseits, die Schlüsselverteilung darf nicht über das Internet erfolgen und andererseits, dass es nur dann 100 % sicher ist, wenn der dabei verwendete Schlüssel absolut zufällig ist. Diese Bedingung ist in der normalen IT streng genommen nicht gegeben, da klassische Computer keine echten Zufallszahlen erzeugen können, mit der neuen Quantentechnik dagegen schon. Freilich kann Micius noch keinen direkten Quantenkanal über 7600 km herstellen (aktueller Rekord 1203 km). Deshalb haben die Forscher hier

eine Art Hybridsystem angewandt. Der Satellit sendet zeitversetzt verschränkte Photonen sowohl nach Europa als auch nach China. Die Lichtquanten, deren Polarisationen miteinander verschränkt sind, werden zunächst von der Grazer Bodenstation am Observatorium Lustbühel gemessen, wodurch ein völlig zufälliger Quantenschlüssel entsteht, der bei Micius gespeichert wird. Danach erzeugen die Chinesen auf dieselbe Weise einen zweiten Quantenschlüssel. Beide Schlüssel werden sodann im Orbit mathematisch kombiniert und wieder nach Österreich und China übermittelt. Mit dem jeweils eigenen und dem kombinierten Schlüssel, sozusagen Private Key und Public Key, können beide Bodenstationen einen gemeinsamen Code generieren, der zur eindeutigen Chiffrierung beziehungsweise Dechiffrierung benutzt wird. Der besondere Sicherheitsaspekt der abhörsicheren Quantentelefonie ergibt sich unter anderem daraus, dass jeglicher Lauschangriff den Quantenzustand bei der Erzeugung des Private Key so weit stört, dass dies messtechnisch bemerkt werden kann. Leider sind aufgrund der bescheidenen Übertragungsrate die erzeugten Quantenschlüssel noch zu klein, um die für ein Videotelefonat nötige Datenmenge absolut sicher zu verschlüsseln. Daher hat man einen davon in viele Teile zerlegt und sie mehrfach getauscht. Damit war das Telefonat noch nicht hundertprozentig sicher.

Anton Zeilinger zeigt sich dennoch zufrieden. „Allein das hier …“, gibt er zu Protokoll, „… ist um vieles sicherer gegen Abhören als alles, was derzeit möglich ist.“ Schließlich wendet er sich noch einmal den Journalisten zu. „Was Sie hier gesehen haben, ist für mich ein historischer Moment und ein wichtiger Schritt auf dem Weg zu einem zukünftigen Quanteninternet“ (https://www.oeaw.ac.at/detail/event/pan-jianwei-unter-top-ten-forschern/).

Japans erster Mikro-Quantenstellit

Ganz unabhängig von den chinesischen-österreichischen Arbeiten an der QUESS-Technik hat Japan einen weiteren richtungweisenden Schritt gesetzt: So wurde im Juli 2017 der 50-kg-Mikrosatellit „Socrates" in den Weltraum entsandt, welcher unter anderem zur Quantenkommunikation genutzt werden kann. An Bord befindet sich ein nur 6 kg schwerer Minitransmitter, der einzelne Lichtquanten mit zwei unterschiedlichen Polarisationsrichtungen sendet, welche als 0/1-Bits fungieren. Im Unterschied zur QUESS-Technik sind die Teilchen allerdings nicht miteinander verschränkt. Das aus 600 km Höhe stammende 10-Mbit/s-Signal wurde von Bodenstationen in Koganei (westlich von Tokio) empfangen, anschließend einem Quantenreceiver zugeführt, decodiert und für ein Protokoll zur Quantenkryptografie verwendet. Das vom Nationalen Institut für Informations- und Kommunikationstechnologie (NICT) entwickelte System demonstriert, dass Quantenkommunikation auch in leichtgewichtigen und kostengünstigen Mikrosatelliten implementiert werden kann. Deshalb dürfte es sich hierbei um eine Schlüsseltechnologie für zukünftige Sat-Boden-Netzwerke handeln, mit dem langfristigen Ziel eines globalen Hochsicherheitsnetzwerks auf Basis der Quantenkryptografie. Unterstützt wird diese Einschätzung durch die Tatsache, dass heute schon intensiv an einem globalen Sat-Kommunikationsnetz höchster Bandbreite geforscht wird. Dazu gilt es allerdings eine Technik zu finden, die sehr große Informationsmengen vom Weltall in sehr kurzen Perioden senden kann. Da die bisher verwendeten RF-Bänder von Überlastung bedroht sind, könnte die Zukunftstechnologie der laserbasierten Datenübertragung die Lösung sein. Durch die Verwendung von Lasertechnik arbeitet eine Sat-optische Kommunikation mit einem „festen" Frequenzband (das durch die Frequenz

des Lichts bestimmt ist) und erlaubt bei größerer Leistung und Effizienz den Einbau in kleinere und leichtere Terminals. Bei einer solchen rein optischen Kommunikation kann die abhörsichere Quantenkryptografie direkt implementiert werden (https://www.nature.com/articles/nphoton.2017.107).

1.5 Der objektive Zufall

In der Welt von Casino und Glücksspiel gilt bekanntlich der alte Spruch: „Am Ende gewinnt immer die Bank". Doch ist dieses (notorischen Spielern leider nur allzu vertraute) Faktum alles andere als reiner Zufall, sondern wissenschaftlich begründbar. Und zwar durch Mathematik, konkret durch Wahrscheinlichkeitsrechnung und Statistik. Ein Beispiel: Sie würfeln immer wieder und notieren, wie oft Sie eine „6" erhalten. Sie wiederholen diesen Vorgang viele Male und achten darauf, dass der Würfel nicht gezinkt ist. Wenn man nun die Anzahl aller gewürfelten Sechser durch die Gesamtzahl aller Würfe teilt, so wird man feststellen, dass das Ergebnis umso eher dem Wert $1/6 = 0{,}1666\ldots$ entspricht, je mehr Würfe durchgeführt werden. Das ist kein Zufall, sondern ein fundamentales mathematisches Gesetz, das man das „Gesetz der großen Zahlen" nennt. Dabei macht es für das Gesetz der großen Zahlen überhaupt keinen Unterschied, ob ein Würfel viele Male hintereinander oder viele Würfel gleichzeitig geworfen werden. Entscheidend ist immer nur die Anzahl der „Realisierungen" eines Ereignisses, eine Zahl, welche theoretisch gegen unendlich streben kann. Den oben erhaltenen Wert 1/6 nennt man die relative Häufigkeit des Ereignisses. Unter der *Wahrscheinlichkeit* eines Ereignisses versteht man die zu erwartende relative Häufigkeit seines Eintretens für eine gegen unendlich

strebende Anzahl von Durchführungen. Im obigen Beispiel beträgt demnach die Wahrscheinlichkeit, eine Augenzahl „6“ zu werfen, rund 16,67 %. Genau auf dieser Basis arbeiten auch alle Casino- und Lotteriespiele, denn damit lässt sich eine Gewinnerwartung vorherberechnen, die umso genauer eintreffen wird, je öfter gespielt wird und je mehr Spieler beteiligt sind. Aus diesem Grund wissen auch die Lottogesellschaften ziemlich genau im Voraus, welchen Gewinn sie machen werden. In abgewandelter Form erfolgen so auch statistische Überprüfungen in der Wirtschaft, bei Banken und Versicherungen, aber auch die Wählerstromanalysen der Meinungsforscher kommen so zustande. Im letzteren Fall wird eine Stichprobe entnommen, woraus sich eine Schlussfolgerung für ein größeres Kollektiv ergibt – dies auf Basis von speziellen Verteilungsfunktionen, die angeben, wie groß die durchschnittliche Wahrscheinlichkeit für ein bestimmtes Merkmal ist, einschließlich statistisch abgesicherter Vertrauensintervalle.

Wie zu erkennen ist, kann man dem Zufall mit Wahrscheinlichkeitsrechnung gut beikommen. Aber unterliegen Würfel- und Lotteriespiele (für sich genommen) wirklich dem reinen Zufall? Streng genommen nein, denn welche Augenzahl geworfen wird oder welche Kugeln beim Lotto gezogen werden, ließe sich rein theoretisch durchaus vorherberechnen. Deren genaues Verhalten ist durch sogenannte Anfangs- oder Randbedingungen vorbestimmt, wie zum Beispiel die exakte Position, die Geschwindigkeit, der Luftwiderstand, der Drehimpuls (Drall) usw. In der Praxis scheitert eine mögliche Berechnung jedoch genau daran, dass diese Anfangsbedingungen nicht in ausreichendem Maße bekannt sind – und zwar bei sehr, sehr Weitem. Man spricht vom deterministischen Chaos beziehungsweise in manchen Fällen auch von einem chaotischen System. Letzteres ist dadurch bestimmt, dass

kleinste Unterschiede in den Anfangsbedingungen zu völlig verschiedenen Verhalten führen und langfristig nicht vorhersagbar sind. So ist weder das Wetter langfristig vorhersagbar noch die exakten Bewegungen unserer Planeten im Sonnensystem. Damit gilt es etwas Wesentliches festzuhalten: Diese Art von „Zufallsprinzip" ist gar kein wirklicher Zufall, sondern er erscheint bloß als solcher. In Wahrheit könnte es dafür jedoch eine physikalische Erklärung geben, die uns persönlich nur verborgen ist. Im Sinne von Ursache und Wirkung würde dann auch ein kausaler Zusammenhang bestehen. Selbst wenn man eine Unterscheidung vornimmt bezüglich starker und schwacher Kausalität (im Sinne von: ähnliche Ursachen haben entweder ähnliche oder völlig verschiedene Wirkungen), kann man diese Möglichkeit nicht ausschließen. Die Annahme der Zufälligkeit resultiert also letztlich aus der persönlichen Unkenntnis; es handelt sich daher um einen *subjektiven* Zufall. Von dieser Annahme geht primär auch die klassische Physik aus, wo es demnach keinen echten Zufall gibt. Wenn alle Parameter eines Ausgangzustands (ideal genau) bekannt sind, kann daraus die Zukunft vorhergesagt werden. Daraus entsteht die orthodox klassische Vorstellung, dass alle physikalischen Entitäten, bis hin zu allerkleinsten Teilchen, in dauerhafter Wechselwirkung miteinander stehen. Jede Aktion ruft eine Reaktion hervor, die vorherberechenbar ist. Diesen Ansatz nennt man in der Wissenschaft den Determinismus. Es war das Verdienst Isaac Newtons, die streng deterministische Sicht auf mathematische Weise darzustellen. Aus Newtons Bewegungsgleichung (Kraft = Masse mal Beschleunigung) lässt sich zu jedem kinematischen Vorgang eine Differenzialgleichung formulieren, deren Lösung zunächst eine allgemeine Kurvenschar ergibt, welche der Menge aller möglichen Bewegungszustände eines Körpers entspricht. Durch Vorgabe der Randbedingungen (wie etwa Anfangslage

und Anfangsgeschwindigkeit) wird daraus eine konkrete (sogenannte partikuläre oder spezielle) Lösung, welche den Naturvorgang für alle Zeiten vorherbestimmt. Damit ergibt sich eine Naturbeschreibung, die Vergangenheit, Gegenwart und Zukunft eines physikalischen Vorgangs vollständig determiniert.

In krassem Gegensatz zur deterministischen Position steht hingegen die Auffassung von Zufall in der Quantenmechanik: der Quantenzufall wird in der Tat als „echt" angenommen – Quantenprozesse sind nicht subjektiv, sondern *objektiv* zufällig. Es ist demnach nicht das subjektive Unwissen, das sie zufällig erschienen lässt, sondern es gibt schlichtweg keine Anfangsbedingungen, welche als Ursache gelten könnten. Das bedeutet, dass er keine auch noch so verborgene Erklärung besitzt – der Quantenzufall ist irreduzibel. Dies sieht heute die überwältigende Mehrheit aller Physiker als eine wesentliche Grundeigenschaft der Quantenphysik an. Den Zufall im quantenmechanischen Einzelprozess kann man daher auch nicht weiter begründen. Nach Anton Zeilinger kann man lediglich ein Verständnis dafür bekommen, warum er nicht weiter erklärbar ist. Ein Beispiel ist etwa der radioaktive Zerfall einer Substanz. Es ist üblich, dafür eine Halbwertszeit anzugeben, nach der die Hälfte einer ursprünglich vorhandenen Menge von Atomkernen zerfallen ist – doch ist dies ein rein statistischer Wert. Er gestattet keinerlei Aussage, zu welchem exakten Zeitpunkt ein einzelnes Atom konkret zerfällt. Ein solches Ereignis ist objektiv zufällig, das heißt, es ist von Natur aus in keiner Weise vorherbestimmt, ob ein bestimmter Kern zu einem konkreten Zeitpunkt zerfallen wird oder nicht; es kann entweder geschehen oder auch nicht. Ein anderes Beispiel ist ein Photon, das einen sehr engen Spalt passiert und anschließend auf einem Messschirm registriert wird. Anders als man vielleicht denken mag,

geht das Lichtquant nicht gerade durch, sondern kann an vielen verschiedenen Stellen auf dem Messschirm mit unterschiedlicher Wahrscheinlichkeit registriert werden. Dabei ist es wiederum objektiv zufällig, ob das Photon an einer bestimmten Stelle nachgewiesen wird oder nicht. An manchen Orten ist dieser Nachweis wahrscheinlicher, an anderen wieder nicht. Die Quantentheorie beschreibt deshalb in diesem Fall nicht das Faktische, sondern das Mögliche. Die Menge all dieser Möglichkeiten (= Ereignisse, die mit einer bestimmten Wahrscheinlichkeit gemessen werden könnten) bezeichnet man als Quantenzustand. Er wird mathematisch durch eine sogenannte Wellenfunktion beschrieben. In einem Quantenzustand existieren bis zum Zeitpunkt der Messung alle Möglichkeiten in einer Art Überlagerung gleichzeitig. Erst die Messung erzeugt aus den bestehenden Möglichkeiten ein Faktum. Ein Teilchen „existiert" also (bis zum Zeitpunkt der Messung) überall dort, wo die Wahrscheinlichkeit, es zu messen, ungleich null ist. Die Überlagerung all dieser Möglichkeiten wird manchmal salopp als „Wahrscheinlichkeitswelle" bezeichnet (in Anspielung an den zentralen Begriff Wellenfunktion). Vor dem Zeitpunkt der Messung befindet sich das Teilchen räumlich und zeitlich an keinem bestimmten Ort. Das ist eine ganz wesentliche Eigenschaft der Quantenmechanik, die man *Nichtlokalität* nennt.

Ein Quantenzufallsgenerator

Die besondere Art des quantenmechanischen Zufalls mag einerseits befremdlich anmuten, eröffnet andererseits jedoch vielversprechende Möglichkeiten für die zukünftige Informationstechnologie. Eine wichtige Forderung betrifft dabei die Erzeugung „echter" Zufallszahlen für die abhörsichere Quantenkommunikation, wie sie im QUESS-Experiment demonstriert wurde. Die nächsten

beiden Abschnitte stellen dazu zwei vereinfachte Versuchsanordnungen vor.

Experiment 1 Ein Laserstrahl trifft auf einen Strahlteiler und wird anschließend von zwei Photonendetektoren gemessen, die dahinter angeordnet sind (Abb. 1.2). Bei einem Strahlteiler handelt es sich um ein optisches Bauteil, welches einfallendes Licht in zwei Strahlen auftrennt. 50 % der Lichtintensität werden dabei transmittiert, die andere Hälfte wird im rechten Winkel reflektiert. Ein Photonendetektor ist eine Art hochgenauer Belichtungsmesser, der durch eine ausgeklügelte Multipliertechnik auf Basis extrem empfindlicher Fotodioden einzelne Lichtquanten messen kann. Schaltet man den Laser ein, so sprechen beide Detektoren zu gleichen Teilen an – was angesichts des 50-%-Splittings auch nicht weiter verwunderlich ist. Interessanter (und für die Quantentechnologie relevant) wird die Anordnung dann, wenn der Laser (der Licht aus Abertrillionen von Photonen erzeugt) durch einen speziellen Einzelphoton-Laser ersetzt wird. Dieser gestattet die Erzeugung von Licht der „allerkleinsten Helligkeit", feuert also sozusagen wie eine alte Muskete immer nur einzelne Lichtquanten nacheinander ab.

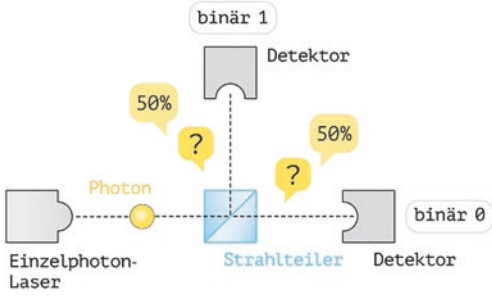

Abb. 1.2 Quantenzufallsgenerator

An dieser Stelle sei bemerkt, dass die Helligkeit (Lichtintensität) im Quantenmodell der Anzahl der Photonen entspricht. Die kleinste Menge Licht ist demnach genau 1 Lichtquant. Darunter gibt es nur noch null, also kein Lichtquant und somit völlige Dunkelheit. Im Unterschied zur klassischen Physik, welche unendlich viele Abstufungen zwischen 0 und 1 erlaubt, gilt in der Quantenphysik also das Motto: „Die Natur macht Sprünge“ (was Max Planck anfangs nicht glauben wollte). Schickt also der Einzelphoton-Laser singuläre Lichtquanten auf den Strahlteiler, so beobachtet man, dass in völlig zufälliger Abfolge einmal der eine, dann wieder der andere Detektor anspricht – niemals jedoch beide gleichzeitig. Ordnet man den beiden Photonendetektoren die Binärzahlen 0 beziehungsweise 1 zu und reiht alle einzelnen Messwerte hintereinander, so entsteht auf diese Weise eine Bitfolge wie zum Beispiel 0101011001… Nun kann man den Versuch wiederholen, führt erneut Einzelmessungen durch und erhält etwa die Bitfolge 1100101011… Diese unterscheidet sich ersichtlich von der ersten. Wenn man nun eine lange Messreihe mit Milliarden einzelner Photonen durchführt und dann die relative Häufigkeit bestimmt, also die Anzahl aller Binärwerte 0 beziehungsweise 1 durch die Gesamtzahl aller Messwerte teilt, so wird man als Schätzwert für die Wahrscheinlichkeit jeweils 50 % erhalten. Diese Wahrscheinlichkeit bleibt konstant für jede Messreihe (vorausgesetzt die Zahl der Messwerte erlaubt die Anwendung des Gesetzes der großen Zahlen).

Interpretation Die beschriebene Anordnung stellt einen Quantenzufallsgenerator dar. Wenn ein einzelnes Lichtquant auf den Strahlteiler trifft, ist es aufgrund des objektiven Quantenzufalls völlig unmöglich, vorherzusagen, ob es transmittiert oder reflektiert wird (und somit als 0

oder 1 gemessen wird). Wohl ergibt sich in der Gesamtstatistik jedes Mal eine 50-%-Verteilung, das quantenmechanische Einzelereignis bleibt jedoch unvorhersagbar zufällig. In der klassischen Physik beziehungsweise bei einem „normalen" Laser bleibt dieser Effekt nur deshalb verborgen, weil sichtbares Licht aus einer astronomischen Anzahl von Photonen besteht. Davon abgesehen weist das Ansprechen von jeweils immer nur einem Detektor darauf hin, dass es sich bei einem Photon um ein unteilbares physikalisches Objekt handeln muss. Freilich würde diese Feststellung allein für keinen wissenschaftlichen Beweis ausreichen. Wie jedoch Einsteins Deutung des Fotoeffekts, später entdeckte Phänomene wie der Compton-Effekt und zahllose weitere Experimente (auch solche in Beschleunigeranlagen wie dem CERN in Genf) beweisen, sind Photonen die unteilbaren Elementarbausteine des Lichts (als auch der sonstigen Strahlung des elektromagnetischen Spektrums).

Experiment 2 Es werde nun an die Stelle des „normalen" Strahlteilers ein spezieller, sogenannter polarisierender Strahlteiler gesetzt. Im Unterschied zu oben hängt hier das Teilungsverhältnis von der Polarisation des eintretenden Lichtstrahls ab. Die klassische, aber auch quantenmechanische Eigenschaft der Polarisation des Lichts muss an dieser Stelle kurz erklärt werden: Es ist dem schottischen Theoretiker James Clerk Maxwell geschuldet, dass man das Licht in der klassischen Physik als elektromagnetische Welle beschreibt (Heinrich Hertz gelang der experimentelle Nachweis). Betrachtet man lediglich die Schwingungskomponente des elektrischen Felds, so kann diese verschiedene Richtungen beschreiben, die sich auch zeitlich ändern können. Ein besonderer Fall liegt bei linear polarisiertem Licht vor, wo die elektrische

Feldstärke immer in derselben Ebene schwingt. Angesichts des teilchenartigen Lichtquanten-Modells erscheint eine solche Vorstellung natürlich grotesk, was auf den problematischen Begriff Welle-Teilchen-Dualismus von Quantenobjekten führt. Wir werden darauf noch später eingehen und vorerst die Tatsache hinnehmen, dass man auch Teilchen die wellenartige Eigenschaft der Polarisation zuordnen kann. Was passiert nun, wenn einzelne Lichtquanten auf den polarisierenden Strahlteiler treffen, der also im Unterschied zum normalen Bauteil auch die Polarisationsrichtung berücksichtigt? Angenommen, der polarisierende Strahlteiler lässt in der Transmissionsrichtung horizontal polarisiertes Licht durch und dahinter sei ein Photonendetektor mit der Aufschrift „0“ platziert. In der Reflexionsrichtung kann dagegen nur vertikal polarisiertes Licht durchtreten, dahinter befinde sich der Detektor „1“. Nun sei noch angenommen, dass das emittierte Licht des Einzelphoton-Lasers linear polarisiert sei. Dann können im Experiment drei Fälle auftreten: falls horizontal polarisiertes Licht eingestrahlt wird, so wird mit Sicherheit, also der Wahrscheinlichkeit 100 %, immer Detektor 0 ansprechen, bei vertikal eingestrahltem Licht dagegen ausschließlich Detektor 1 „klicken“. Ganz anders hingegen, wenn das eingestrahlte Licht eine Polarisation aufweist, die zwischen horizontaler und vertikaler Richtung liegt, beispielsweise im Winkel von 45° zu den Detektorrichtungen steht. Dann wird objektiv zufällig einmal der eine, dann wieder der andere Detektor ansprechen, und es entsteht (wie in Experiment 1) ein Quantenzufallsgenerator. Dieses quantenzufällige Verhalten gilt auch für andere Winkel, zum Beispiel 30° oder 60°, jedoch mit jeweils unterschiedlicher Gesamtstatistik und somit unterschiedlichen Wahrscheinlichkeiten (siehe „Gesetz von Malus“ in Abschn. 2.6.3).

Interpretation Offensichtlich kann die beschriebene Anordnung auch mit dem polarisierenden Strahlteiler als Quantenzufallsgenerator fungieren (sofern das eingestrahlte Licht weder horizontal noch vertikal polarisiert ist). In diesen relevanten Fällen ist das Verhalten des Photons von besonderem quantenmechanischem Interesse. Nachdem das Lichtquant durch den Strahlteiler getreten ist, befindet es sich in einer Überlagerung (Superposition) von zwei Möglichkeiten, nämlich Transmission oder Reflexion. Die abstrakte „Wahrscheinlichkeitswelle" repräsentiert diesen Quantenzustand, welche jedoch keinesfalls als konkrete, räumlich ausgedehnte Welle zu verstehen ist. Ihre Aufgabe besteht lediglich darin, die Wahrscheinlichkeit dafür anzugeben, welche Ereignisse eintreten können. Alle bestehenden Möglichkeiten sind im Quantenzustand bereits enthalten, und zwar gleichzeitig. Da ein Photon jedoch unteilbar ist, kann es, wenn es einmal bei einem der beiden Detektoren gemessen wurde, nicht auch noch beim zweiten Detektor registriert werden. Deshalb muss notwendigerweise die Superposition ab diesem Moment zusammenbrechen (da sie ja die Wahrscheinlichkeit beschreibt und diese also am zweiten Detektor automatisch null sein muss). Im Sinne der Kopenhagener Interpretation der Quantenmechanik (benannt nach dem dänischen Physiker Niels Bohr), spricht man dann von einem „Kollaps der Wellenfunktion". Dass es sich beim vielleicht verstörend wirkenden Superpositionsprinzip definitiv um kein Hirngespinst handeln kann, beweist allein schon die Tatsache, dass man im Experiment die Detektoren entfernen kann und daraufhin die Teilstrahlen in einem zweiten Strahlteiler wieder zusammenführt. Das Ergebnis ist ein Photon mit der ursprünglichen Polarisationsrichtung.

1.6 Quantenverschränkung

Die Quantenverschränkung (englisch: entanglement) zählt als zentrales Element der Quantenmechanik zu den interessantesten Phänomenen der Physik. Auch für ein zukünftiges Quanteninternet bildet sie die wesentliche Ressource. Einerseits gestattet sie einen inhärent sicheren Quantenschlüsselaustausch zwischen Kommunikationspartnern, andererseits repräsentiert sie ein wesentliches Fundament für die Realisierung und Vernetzung von Quantenprozessoren.

Perfekte Korrelationen Im Abschn. 1.5 wurde dargelegt, dass die Kombination von Einzelphoton-Laser, polarisierendem Strahlteiler und Photonendetektoren einen Quantenzufallsgenerator ergibt. Es sei nun eine Anordnung betrachtet, welche durch *zwei* derartige Zufallsgeneratoren repräsentiert sei. Hierbei kommen insbesondere zwei polarisierende Strahlteiler zum Einsatz, die räumlich weit voneinander getrennt sein können. Eine Verschränkungsquelle (zum Beispiel speziell angeregte Calcium-Atome) befindet sich genau in der Mitte und sendet in entgegengesetzte Richtungen jeweils ein Photon aus, die in der Polarisation korreliert seien. Damit meint man, dass die emittierten Photonenpaare in bestimmten physikalischen Eigenschaften in sehr enger Beziehung stehen – in diesem Fall betrifft dieser Zusammenhang die Polarisation des Lichts. Man sagt auch, die Polarisationen der Photonen seien „verschränkt“. Wenn man nun eine Messreihe an einem der beiden Strahlteiler vornimmt, so entsteht, analog zu den beiden Experimenten in Abschn. 1.5, eine objektiv zufällige Folge von Binärzahlen. Das höchst Verblüffende ist aber die Tatsache, dass die parallel durchgeführte Messreihe am zweiten Strahlteiler

exakt dieselbe Binärfolge ergibt! Führt man eine erneute Messreihe durch, so ist zwar die entstehende Bitfolge eine andere – die Messung am zweiten Generator ergibt jedoch wieder haargenau dieselbe Bitreihe wie am ersten Zufallsgenerator. Man kann dieses Experiment in beliebiger Abfolge reproduzieren und stellt (bei ideal kompletter Vermeidung von Messfehlern) stets dieselbe Art von perfekter Korrelation fest.

Interpretation Angesichts der Tatsache, dass die Binärfolgen objektiv zufällig entstehen, zeigen verschränkte Systeme ein höchst bemerkenswertes Verhalten. Da es ja völlig zufällig ist, ob an einem der beiden Zufallsgeneratoren eine 0 oder 1 gemessen wird, ist es umso verblüffender, dass der Messwert am zweiten Generator dann stets exakt dieselbe Binärzahl ergibt. Dies beweist eindeutig, dass bestimmte Observablen (beobachtbare Messgrößen) verschränkter Teilchen statistisch nicht unabhängig sein können, sondern stark korreliert sind. Diese Feststellung fordert den menschlichen Verstand vor allem dann aufs Extremste heraus, wenn man sich vor Augen hält, dass die Verschränkung aktuell durch QUESS bereits auf eine Entfernung von über 1200 km verifiziert wurde. Man könnte also die beiden Zufallsgeneratoren 1200 km voneinander trennen, und sie würden dennoch das beschriebene perfekt korrelierte Verhalten zeigen. Wie unter anderem die Quantenkosmologie nahelegt, sollte dieses bizarr anmutende Phänomen durch das gesamte Universum hindurch Gültigkeit besitzen und sogar den Regelfall darstellen.

Antikorrelationen Im obigen Beispiel treten perfekte Korrelationen auf, das heißt, die Polarisation der beiden verschränkten Teilchen ist bei ihrer Messung exakt die

gleiche. Nun gibt es aber auch verschränkte Systeme, die antikorreliert sind. Beispielsweise können Photonen in einer Weise miteinander verschränkt sein, dass die Messung an einem der beiden Teilchen eine Polarisation in vertikaler Richtung ergibt, die parallele Messung am verschränkten Partnerteilchen dagegen eine horizontale Polarisation. Die beiden Polarisationsebenen sind also um 90° gegeneinander verdreht. In Abb. 1.3 ist eine entsprechende experimentelle Anordnung dargestellt: Ein Einzelphoton-Laser zielt auf einen speziellen Kristall, woraufhin aus jedem einzelnen Lichtquant ein Paar verschränkter Photonen generiert wird. Zur Messung des antikorrelierten Verhaltens der erzeugten Teilchen dienen Polarisationsfilter, welche als Analysatoren wirken. Statistisch gesehen erhält man nur dann 100 % „Klicks" an den beiden Photonendetektoren, wenn die Stellung der Analysatoren

1. genau der Polarisationsrichtung der erzeugten Teilchen entspricht und
2. die Relativposition beider Analysatoren zueinander exakt 90° beträgt.

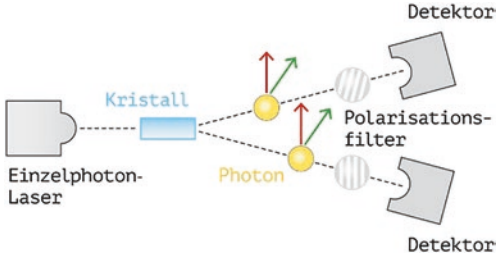

Abb. 1.3 Erzeugung und Messung antikorrelierter Photonen

Wesentlich ist dabei festzuhalten, dass es zwar unvorhersagbar zufällig ist, welche Polarisation an einem einzelnen Lichtteilchen bestimmt wird. Sobald dieser Messwert aber feststeht, ist der zweite Messwert am Partnerteilchen infolge der Verschränkung automatisch vorherbestimmt. In gewisser Hinsicht verhält sich somit die Quantenphysik in diesem Fall dann doch deterministisch, indem zwar Messwerte objektiv zufällig auftreten, das weitere Geschehen jedoch vorherbestimmt ist. Dennoch lässt sich das Phänomen der Verschränkung nicht auf Basis der klassischen Physik erklären, wodurch die Quantenmechanik sich fundamental von klassischen Theorien unterscheidet. Auf der anderen Seite steht die Quantenmechanik allerdings mit der Speziellen Relativitätstheorie in Einklang, die (ihrer kausalen Struktur wegen) ebenso als klassische Theorie gilt. Daraus ergeben sich wichtige Schlussfolgerungen für den Sicherheitsaspekt und die Übertragungsgeschwindigkeit eines Quanteninternets, worauf später noch ausführlich eingegangen wird (Abschn. 3.6).

Ein anderes Beispiel für antikorreliertes Verhalten ist die quantenmechanische Eigenschaft des Spins eines Teilchens. Den Spin kann man sich wie eine Art inneren Drall (Drehimpuls) eines Teilchens vorstellen. Er tritt bei Bosonen (wie dem Photon, wo er der Zirkular-Polarisation entspricht) und Fermionen (wie Elektron oder Proton) gleichermaßen auf, kann jedoch unterschiedliche Werte besitzen. Für Bosonen ist der Spin immer ganzzahlig (zum Beispiel haben Photonen den Spin 1), bei Fermionen immer halbzahlig (Elektronen haben etwa den Spin $1/2$). Wie vielen physikalischen Größen kann man auch dem Spin eine Richtung bezüglich einer gegebenen Achse zuordnen. So kann der Spin eines Elektrons in positive („Spin up“) oder negative Richtung („Spin down“) weisen, also $+1/2$ oder $-1/2$ betragen. Diese Zahlenwerte beziehen sich auf die Proportionalität zum Wirkungsquantum – denn selbstverständlich ist

auch der Spin „gequantelt“. Im Übrigen besteht für den Spin ein Unbestimmtheitsprinzip vergleichbar mit der heisenbergschen Unschärferelation, das besagt, dass man die Komponenten des Spins nicht gleichzeitig bezüglich zweier Raumrichtungen messen kann. Auch die Spins von Quantenteilchen lassen sich experimentell verschränken, wobei sie dann ein antikorreliertes Verhalten zeigen: Eine Verschränkungsquelle, zum Beispiel ein Atom, sendet zwei Spin-$^1/_2$-Teilchen aus, die sich in entgegengesetzter Richtung voneinander fortbewegen. Misst man daraufhin an einem Teilchen „Spin up“, so misst man am verschränkten Partnerteilchen automatisch „Spin down“. Und umgekehrt: Wenn an einem Teilchen „Spin down“ gemessen wird, dann hat das verschränkte Teilchen sicher „Spin up“. Diese Antikorrelation besteht übrigens für jede Richtung. Sie gilt also zum Beispiel auch für die horizontale beziehungsweise vertikale Richtung. Misst man also in horizontaler Richtung „Spin rechts“, so determiniert die Verschränkung am zweiten Teilchen ein „Spin links“. Ebenso verhält sich eine Messung in der dritten Raumrichtung: Hier entstehen zum Beispiel die Messergebnisse „Spin vorne“ am ersten Teilchen beziehungsweise „Spin hinten“ am zweiten Teilchen. Wie bereits dargelegt, unterliegen konkrete Messwerte stets der objektiven Zufälligkeit.

Verschränkte Vielteilchensysteme Die Verschränkung wird üblicherweise als Phänomen zweier eng korrelierter Teilchen dargestellt. Dadurch könnte jedoch der Eindruck entstehen, dass dieses Phänomen auf eine „Zweisamkeit“ beschränkt bleiben muss – das ist keineswegs der Fall. Einschlägige Phänomene wie GHZ-Zustände (GHZ = Zeilinger/Greenberger/Horne) und verwandte Experimente beweisen, dass auch mehrere oder sogar sehr viele Teilchen miteinander verschränkt sein können – auch wenn sie räumlich getrennt sind. Gerade mit Hinblick auf

die in der Zukunft zu erwartenden Entwicklungen der Quanteninformationstechnologie sind komplexe verschränkte Systeme ein zentraler Forschungsansatz. Dabei gilt die Faustregel: je komplexer die Zustände, umso nützlicher sind sie, aber desto schwieriger ist auch der Umgang mit ihnen. Eine Möglichkeit der konkreten Realisierung besteht darin, dass man viele Teilchen miteinander wechselwirken lässt, um auf diese Weise komplexe Verschränkungszustände herzustellen. Dabei geht es nicht nur um tiefere Einblicke in die Quantenmechanik, sondern auch um die Klärung anderer grundlegender Fragen. Von technologischer Bedeutung ist etwa die Frage, ob die Menge an Information, welche verschränkte Quantenobjekte „speichern" können, unbegrenzt ist oder ob hier ein fundamentales Limit existiert. Allerdings ist die Realisierung verschränkter Vielteilchensysteme eine sehr schwierige Aufgabe und stellt die Quantentechnologie vor gewaltige Herausforderungen. Bereits Systeme mit mehr als drei Teilchen erweisen sich als sehr schwer zu handhaben. Wie aktuelle Forschungsergebnisse beweisen, befindet sich aber auch diese Entwicklung auf einem guten Weg: Bei Vielteilchensystemen wird die Verschränkung durch das sogenannte Verschränkungsspektrum beschrieben. Womit sich wichtige Eigenschaften eines kollektiven Quantensystems erfassen lassen, unter anderem auch, wie schwierig es ist, dieses mit einem klassischen Computer zu berechnen. Anstatt mithilfe eines Quantensimulators die Verschränkungseigenschaften des realisierten Zustands zu messen, wird stattdessen der Verschränkungs-Operator direkt simuliert. Diese Methode bietet den großen Vorteil, dass damit das Spektrum viel größerer Quantensysteme gemessen werden kann, was mit herkömmlichen Computern sehr schwierig bis unmöglich wäre.

Quantenmechanische Interpretation Obwohl anfangs als rein statistische Korrelation „verniedlicht" und später von Albert Einstein bespöttelt, erweist sich die Verschränkung als das charakteristische Element der Quantenmechanik schlechthin. Eine Feststellung, die bereits von Erwin Schrödinger um 1935 getroffen wurde, auf den auch der Terminus „Verschränkung" zurückgeht. Charakteristisch ist vor allem, dass die Bestandteile eines verschränkten Systems nicht einzeln lokalisiert sind, sondern sich ihr *gemeinsamer* Zustand räumlich über das gesamte System verteilt. Darum kann dieses Phänomen nur auf Basis einer nichtlokalen Theorie korrekt beschrieben werden. Die Quantenmechanik erklärt die Verschränkung aus dem vorhin dargelegten Superpositionsprinzip, das sich auch auf Zustände zusammengesetzter Systeme bezieht. Nur in dem Spezialfall, wenn der Gesamtzustand gleich dem Produkt seiner Einzelzustände ist, sind Teilsysteme unabhängig voneinander. Im Allgemeinen sind sie es aber nicht – und demnach verschränkt. Sie sind deshalb nur durch einen einzigen Zustand beschreibbar, der das gesamte System darstellt. Anders gesagt, ein verschränkter Zustand ist wie ein abstraktes Gebilde zu sehen, das sich unabhängig von Raum und Zeit, theoretisch über beliebige Distanzen, erstrecken kann (eben nichtlokal ist) und definitiv nicht auf separate Teilsysteme zurückgeführt werden kann. Erst mit diesen nichtlokalen Korrelationen ergibt sich eine quantenmechanisch vollständige Beschreibung des Gesamtsystems. Obwohl sich der Mainstream der Wissenschaft dieser Interpretation anschließt, gibt es selbst heute noch „unverbesserliche Relativisten" (Zitat Rupert Ursin im Gespräch mit dem Autor) welche mit teils haarsträubenden Erklärungen verzweifelt nach einer klassischen Theorie suchen. Die Natur folgt aber offenbar der bekannten Losung: „Das Ganze ist tatsächlich mehr als die Summe seiner Teile".

1.7 „Spukhafte Fernwirkung“

In der Populärliteratur sowie in Medienberichten wird die Verschränkung manchmal als „Quantenspuk“ bezeichnet. Wie kommt es eigentlich zu dieser mystifizierenden Namensgebung? Bloß eine journalistische Plattitüde? In diesem Fall nicht, denn ihr Hintergrund steht eng mit einer Person in Zusammenhang, die wohl jeder kennt: Albert Einstein – neben Stephen Hawking der vermutlich populärste Physiker weltweit.

Jener Einstein also, der gleichermaßen für die Genialität seiner weltberühmten Relativitätstheorie und seine pazifistisch-liberalen Überzeugen steht wie für sein komisch-kauziges Aussehen, das einmal mit einem pensionierten Schäferhund verglichen wurde. Jener Einstein, der bisweilen als Prinzip Hoffnung für schlechte oder faule Schüler herhalten muss, indem er immer wieder (fälschlich) als solcher bezeichnet wurde und wird. Gewiss ist es nutzlos darauf hinzuweisen, dass es nur ganz wenigen Menschen vorbehalten ist, Naturgesetze zu entdecken und im Fall der theoretischen Physik dafür ein außerordentliches Talent für Mathematik und komplex-logisches Denken erforderlich ist. Außerdem ganz wichtig und kennzeichnend für ein Forschergenie: der physikalische Instinkt. Gerade dieser war bei Einstein besonders reichhaltig ausgeprägt. Albert Einstein (1879–1955) wurde als Sohn einer jüdischen Familie in Ulm geboren. Er war somit Deutscher, nahm später aber mehrere andere Staatsangehörigkeiten an. Unter anderem war er für kurze Zeit auch Österreicher. Als aufgeweckter, bisweilen aufrührerischer, aber guter Schüler mit ausgeprägtem Interesse an Naturwissenschaften beschrieben, wurde er dagegen im Studium am Schweizer Polytechnikum von seinem Mathematiklehrer als durch Abwesenheit glänzender „Faulpelz“ bezeichnet. Eine Einstellung, die er später bei der Formulierung der

Allgemeinen Relativitätstheorie noch bereuen sollte. Dazu muss man wissen, dass Einstein als theoretischer Physiker an Mathematik naturgemäß hohes Interesse hatte. Aber eben nur, solange diese eine Hilfe zur Beschreibung physikalischer Modelle darstellt. Der Mathematik per se stand er als höchst abstraktem und unanschaulichem Orchideenfach (was Mathematik dem wahren Wesen nach ist) mit größter Skepsis gegenüber. Umso dankbarer war er später, als er auf maßgebliche Vorarbeiten und die Unterstützung des Mathematikers Hermann Minkowski sowie seines Studienfreunds Marcel Grossmann zurückgreifen konnte. Legendär ist das berühmte Wunderjahr („annus mirabilis“) 1905, als Einstein neben der Speziellen Relativitätstheorie auch die Photonenhypothese einreichte – beide völlig revolutionär zur damaligen Zeit. Anhand der brownschen Molekularbewegung erbrachte er dabei noch quasi nebenher einen Beweis für die Existenz von Atomen (letztere waren damals noch heftig umstritten). Und das als wissenschaftlicher Nobody, der vergebens um eine universitäre Assistenzstelle angesucht hatte, stattdessen bei einem Schweizer Patentamt als „Assistent 3. Klasse“ seine Zeit totschlug. Seine physikalischen Arbeiten waren so innovativ, dass sie anfangs bloßes Kopfschütteln auslösten, heute jedoch als Jahrhundertentdeckungen kopernikanischer Dimension gerühmt werden. Als 1915 noch die Allgemeine Relativitätstheorie mit dem berühmten Konzept der Raumkrümmung folgte (die kurze Zeit später experimentell verifiziert werden konnte), wuchs die Anerkennung der einsteinschen Arbeiten über alle Grenzen hinaus. Es war die Metamorphose zum populärsten Physiker der Welt – zum Forschergenie schlechthin. Noch heute gilt es allerdings als handfester Skandal, dass Einstein nur ein einziges Mal den Nobelpreis erhielt (1921 für die Photonenhypothese), und das, obwohl er mit der Relativitätstheorie ein Teilgebiet der modernen Physik praktisch im völligen Alleingang entwickelte. Über die Gründe darf

spekuliert werden. Lag es etwa an der Inkompetenz des Nobelkomitees oder aber an seiner jüdischen Abstammung? War die Relativitätstheorie noch zu gewagt?

Unmittelbar nach der Machtergreifung der Nazis emigrierte Einstein in die USA, wo er in Princeton eine Gastprofessur bekleidete, die er bis zu seinem Tod innehatte. Als Weltweiser und Pazifist war er auch in politischen wie militärischen Fragen eine gefragte Person. Als „großen Fehler" bezeichnete er später seine Empfehlung an Präsident Roosevelt, die USA sollten ein Programm zur Entwicklung einer Atombombe starten – aus Sorge, dass Hitler-Deutschland unter Werner Heisenberg und anderen eine solche Massenvernichtungswaffe entwickeln könnte. Einstein war allerdings zu keiner Zeit selbst aktiv am „Manhattan-Projekt" beteiligt. Bemerkenswert ist Einsteins ambivalentes Verhältnis zur Quantenphysik: Auf der einen Seite war er ein wichtiger Wegbereiter (nicht Schöpfer), auf der anderen Seite wollte er die erkenntnistheoretischen Konsequenzen nicht mittragen. Auf diese Weise verlor der Genius in späteren Jahren zunehmend die „geistige Führerschaft" in der theoretischen Physik, wie es ein Fachkollege einmal ausdrückte. Während er in der Öffentlichkeit wie ein Volksheld gefeiert wurde, sah die Quantengemeinde ihren einstigen Führer hingegen nicht mehr auf der Höhe der Zeit. Warum nur sträubte sich Einstein so sehr gegen die Konsequenzen der Quantentheorie?

Die Murmelspiel-Analogie

Zwei Personen, nennen wir sie Alice und Bob, welche an zwei verschiedenen Orten wohnen, nehmen an einem besonderen Spiel teil. Jeder von ihnen erhält von der Post ein Paket geschickt, in welches der Absender rote und blaue Murmeln gelegt hat. Die Spielregeln bestehen darin, dass beide zum selben, vorher verabredeten Zeitpunkt ihre

Pakete öffnen. Eine weitere Regel besagt, dass dies mit verbundenen Augen zu geschehen hat. Nachdem jeweils genau eine Murmel aus dem Paket entnommen wurde, wird das Paket wieder geschlossen, ohne hineinzusehen, und anschließend weggeworfen. Das Spiel wird alle drei Tage wiederholt und geht viele Male so dahin. Mit der Zeit fällt Alice und Bob etwas Merkwürdiges auf: Sie ziehen bei jeder Ziehung Murmeln derselben Farbe. Zieht Alice eine rote Murmel, dann hat auch Bob eine rote gezogen. Zieht Alice eine blaue Murmel, dann auch Bob – dabei kommen die Farben aber jeweils ganz zufällig heraus. Die beiden sind völlig verdutzt und machen sich Gedanken, was die Ursache sein könnte.

Jetzt kommen zwei Theoretiker hinzu. Nennen wir sie Niels und Albert. Sie suchen ebenso nach einer Erklärung für das Phänomen. Niels: „Ich komme zu dem Schluss, dass beide versendeten Pakete eine untrennbare Einheit miteinander bilden, auch wenn sie räumlich entfernt sind. Die Farbe der Murmeln ist auf fundamentale Weise unbestimmt. Die Murmeln nehmen erst dann eine konkrete Farbe an, wenn sie von Alice und/oder Bob gezogen werden. Ob sie dann aber rot oder blau sind, ist völlig zufällig – objektiv zufällig. Man kann darüber nur eine Wahrscheinlichkeitsaussage machen." Sofort protestiert Albert: „Was reden Sie für einen Unfug! Es gibt mehrere mögliche Ursachen. Zum Beispiel hat die Post immer nur Murmeln derselben Farbe hineingetan. Oder es war ein Übeltäter in der Nacht, der die Pakete manipuliert hat. Alice und Bob könnten sich auch irgendwie abgesprochen haben. Wir wissen es nur nicht. Ich komme zu dem Schluss, dass es unser bloßes Unwissen ist, dass die Farben zufällig erscheinen lässt. Ihre Wahrscheinlichkeitsannahme resultiert somit aus persönlicher Unkenntnis und kann somit kein Naturgesetz sein."

Die beiden debattieren noch eine ganze Weile so dahin. Nach einiger Zeit stößt ein weiterer Theoretiker dazu: John. Er behauptet, er könne ein Experiment vorschlagen, das eindeutig beweist, wer von beiden recht hat.

Was meinen Sie, wird Johns geheimnisvolle Messung ergeben? Sie würden natürlich auf Albert tippen. Die Ideen von Niels wirken völlig an den Haaren herbeigezogen und widersprechen diametral unserer Alltagserfahrung.

In der Tat ist das „Murmelspiel“ nur eine Karikatur eines der meistzitierten Streitgespräche der Wissenschaftsgeschichte: der berühmt gewordenen Kontroverse zwischen Albert Einstein und dem dänischen Nobelpreisträger Niels Bohr um die sogenannte EPR-Problematik. Wir erinnern uns, dass nach heutiger Auffassung die korrelierten Eigenschaften verschränkter Objekte auf Basis einer nichtlokalen Quantentheorie gedeutet werden. Es ist aber gerade dieser nichtlokale Aspekt, welcher den menschlichen Verstand auf eine umso härtere Probe stellt. Die menschliche Logik vermutet hier automatisch irgendeine Ursache „dahinter“, folgt also dem kausalen Denkansatz, der fest in der menschlichen Vorstellungswelt einzementiert ist. Bereits zu Beginn der Quantentheorie gab es zwei konträre Denkrichtungen: Die Anhänger des klassischen Realismus mit Einstein an der Spitze (aber auch Erwin Schrödinger, Louis de Broglie, David Bohm und John Bell). Im Gegensatz dazu die Vertreter einer eher positivistischen Philosophie, angeführt von Niels Bohr, Werner Heisenberg, Paul Dirac und Wolfgang Pauli. Niels Bohr war mit Sören Kierkegaards Philosophie vertraut und damit wohl auch mit Immanuel Kants Untersuchungen über „das Ding an sich“. Dieser war zu der Überzeugung gelangt, dass man über das Ding an sich nichts aussagen könne, nicht einmal, ob es überhaupt existiert. Unsere Mitteilungen können demnach nur Erfahrungen und Wahrnehmungen betreffen, Beobachtungen und Messungen. So argumentiert auch Bohr in der sogenannten „Kopenhagener Deutung der Quantenmechanik“. Nur das Beobachtbare wäre demnach das einzig Wirkliche, das man über die Welt wissen könne. Die Physik solle demnach von beobachtbaren Größen (Observablen) handeln. Überprüfbare Aussagen seien in aller Regel nur über Wahrscheinlichkeiten möglich. Einstein war hingegen (im Jargon der Philosophen gesprochen) ein Vertreter des „naiven Realismus“.

Seine Überzeugung war es, dass die Dinge auch ohne Beobachtung mit genau festgelegten Eigenschaften existieren und verwehrte sich gegen den Quantenzufall *(„Gott würfelt nicht!")* Er befürwortete stattdessen eine objektive, vollständige und genau determinierte Wirklichkeit. Während Bohr den Grundsatz der Komplementarität postulierte, hielt Einstein hingegen die heisenbergsche Unschärferelation (welche die Komplementarität zweier physikalischer Größen ausdrückt, indem sie die Unmöglichkeit der gleichzeitigen Messung von Ort und Impuls beschreibt) lediglich für ein Manko der Messgenauigkeit. Um 1930 gab es mehrere Kongresse zur Präsentation und Diskussion neuer Entwicklungen der Quantenphysik, dabei fanden auch die berühmt gewordenen Debatten statt, welche am Beispiel der Quantenverschränkung eine besondere Zuspitzung fanden.

Betrachten wir deshalb noch einmal die Quantenverschränkung und überlegen, worin ihre eigentliche Brisanz besteht. Nehmen wir dazu als Beispiel ein System antikorrelierter Spins her, wie vorhin diskutiert. Am Teilchen A wird Spin up gemessen, woraufhin kurze Zeit später am Teilchen B vorherbestimmt Spin down gemessen wird. Dieses Ergebnis für sich wäre nicht weiter spannend, denn die Messergebnisse könnten ja schon bei der Erzeugung der Teilchen festgelegt worden sein. Das Brisante ist aber die Tatsache, dass der Messwert am Teilchen A objektiv zufällig entsteht, er könnte also genauso gut ein Spin rechts an Teilchen A und somit Spin links am Teilchen B ergeben. Oder auch eine entsprechende Spinkorrelation in einer beliebig anderen Raumrichtung. Der Witz an der Quantenverschränkung besteht also darin, dass *trotz* objektiver Zufälligkeit des Messwerts bei Teilchen A der Messwert von Teilchen B stets vorhersagbar ist. In modernen Experimenten ist es zudem möglich, die Messung von A und B schneller vorzunehmen, als das Licht Zeit hätte,

von A nach B zu gelangen. In diesem Sinne ist die Sprechweise gerechtfertigt, dass sich A und B instantan beeinflussen.

Nun versetzen wir uns in die Gesinnung Einsteins und versuchen in der Denkweise der „Realisten" das Phänomen zu erklären. Im Wesentlichen gibt es dann zwei Möglichkeiten:

1. Es könnte ein (noch) unentdeckter Mechanismus existieren, der das Verhalten der verschränkten Teilchen im Vorhinein bestimmt (und somit auch den objektiven Zufall vortäuscht). Dies entspricht nachgerade dem Geist des Determinismus, wie er unter anderem durch Newton so erfolgreich in die klassische Physik eingeführt wurde.
2. Wäre die objektive Zufälligkeit tatsächlich ein Naturgesetz, so müssten die verschränkten Objekte zwangsläufig irgendwie miteinander kommunizieren, also klassische Information austauschen. Letzteres deshalb, weil das verschränkte zweite Teilchen ja „wissen" muss, welcher Messwert am ersten Teilchen vorliegt, um daraufhin den antikorrelierten Spin zu „zeigen". Falls die beiden Teilchen räumlich sehr weit voneinander getrennt wären, stellt sich unmittelbar die Frage, wie schnell diese Signalwirkung erfolgen kann. Gibt es da ein Limit?

Lange Zeit, bevor man entsprechende Experimente (oder gar einen Meilenstein wie QUESS) realisieren konnte, gab Einstein immer wieder Kostproben seines besonderen physikalischen Instinkts und Scharfsinns. So erfasste er als Allererster nicht nur die fundamentale Bedeutung von Plancks Quantenmodell, sondern ebenso die besondere Brisanz der Verschränkung, die er von theoretischen Überlegungen her kannte. Während sie anderswo noch als

statistische Korrelation verharmlost wurde, war für den großen Denker aber bereits klar, dass es sich um ein Phänomen von grundlegender Relevanz handeln musste. Zwar brachte sich das Genie um die eigentliche Frucht seiner Leistung, indem er die falschen Schlussfolgerungen daraus zog, er trug jedoch ganz entscheidend dazu bei, dass diese (ursprünglich rein philosophische) Frage in der Physik überhaupt thematisiert wurde. Es ist nur allzu leicht nachvollziehbar, dass Einstein zu jener Gründerzeit der Quantentheorie naturgemäß dem „gesunden Menschenverstand" vertraute und nach einer Erklärung im obigen Sinne suchte. Zur Erklärung der Verschränkung folgte Einstein also der intuitiven menschlichen Logik und stellte neben dem Unbestimmtheitsprinzip, das er also für ein Manko der Messgenauigkeit hielt, auch die objektive Zufälligkeit infrage. Damit verbinden sich u. a. die inflationär zitierten Worte: *„Gott würfelt nicht!"* Einstein zufolge müsse es für das Phänomen der Verschränkung also eine Ursache geben, welche die Physik einfach noch nicht entdeckt hätte, sogenannte „verborgene Variablen". Einstein argumentierte sinngemäß: Wenn es wirklich völlig zufällig wäre, welche Merkmale die Objekte bei ihrer Messung zeigen, dann müsste das eine Teilchen dem anderen ja eine Mitteilung machen, ein Signal senden – also klassische Information austauschen. Eine derart klassische Signalübertragung müsste jedoch bei entsprechend großer räumlicher Entfernung der verschränkten Objekte überlichtschnell vor sich gehen. Selbstredend sah er darin natürlich den glatten Widerspruch zu der von ihm höchstselbst entdeckten Relativitätstheorie, welche eine überlichtschnelle Informationsübertragung ja ausdrücklich untersagt. Ebenso steht das im Widerspruch zum relativistischen Prinzip der Lokalität. Wenn dies dann doch möglich wäre, so ginge es seiner Meinung nach nicht mit rechten Dingen zu. Einstein sprach von einer *„spukhaften*

Fernwirkung" zwischen den verschränkten Objekten. Selbstverständlich ist diese Metapher im spöttischen Sinne zu verstehen und als Aufforderung an seine Kollegen gerichtet, die Quantenmechanik zu einer vollständigen Theorie weiterzuentwickeln. Laut Einstein wäre die Quantenmechanik entweder nichtlokal oder aber unvollständig. Da er sich mit der Nichtlokalität verschränkter Systeme überhaupt nicht anfreunden konnte, schloss er demnach auf die Unvollständigkeit der Quantenmechanik.

Nun wissen wir also, woher der „Quantenspuk" ursprünglich stammt. Einstein reichte dem Argument noch ein philosophisches nach. Er stellte die Frage nach der Wirklichkeit physikalischer Objekte. Insbesondere suchte er nach physikalischen Entitäten, die er „Elemente der Realität" nannte. Wenn die Objekte nämlich tatsächlich erst bei ihrer Messung zur Realität werden, dann können sie vorher gar nicht existieren. Einstein jedenfalls definierte eine physikalische Größe, deren Wert mit Sicherheit vorhersagbar ist, ohne das System zu stören, als ein Element der Realität. In einer vollständigen Theorie müsse zudem jedes Element der physikalischen Realität eine Entsprechung haben. Um keinen gänzlich falschen Eindruck zu erwecken: Einstein fand die Quantentheorie „sehr achtunggebietend", war er doch höchstselbst an ihrem Aufbau beteiligt. Er musste das auch, weil der Formalismus (bis heute) in bester Übereinstimmung mit den Experimenten steht. Aber er hatte eben große Probleme mit der erkenntnistheoretischen beziehungsweise ontologischen Seite, welche seiner Meinung nach ein ganz wesentliches Fundament einer physikalischen Theorie bildet. So herrschte er einmal schroff den jungen Werner Heisenberg an: „Sie, wenn Sie glauben, Sie können eine Theorie beobachtbarer Größen machen, irren Sie sich!" Damit meinte Einstein sinngemäß, dass erst das philosophische Korsett einer Theorie entscheide, was die

beobachtbaren Größen wären – und das wäre seiner Meinung nach der lokale Realismus.

Wie wichtig ihm das war, erkennt man an der Tatsache, dass er sich mit den jungen amerikanischen Physikern Boris Podolsky und Nathan Rosen Verstärkung holte (wohl auch aus sprachlichen Gründen). Einstein, Podolsky und Rosen (EPR) warfen in einem 1935 in den USA erschienenen Artikel die Frage auf, ob die Quantenmechanik eine vollständige Theorie sei (Einstein et al. 1935). Obwohl Einstein diese Arbeit nicht sonderlich mochte, indem der Hauptteil „.sozusagen durch Gelehrsamkeit verschüttet" sei, wurde er später in *„Quantenmechanik und Wirklichkeit"* in seiner Muttersprache umso deutlicher:

> „Wesentlich für diese Einordnung der in der Physik eingeordneten Dinge erscheint ferner, dass zu einer bestimmten Zeit diese Dinge eine voneinander unabhängige Existenz beanspruchen, soweit diese Dinge in verschiedenen Teilen des Raumes liegen. Ohne die Annahme einer solchen Unabhängigkeit der Existenz (des So-Seins) der räumlich distanten Dinge voneinander, die zunächst dem Alltagsdenken entstammt, wäre physikalisches Denken im geläufigen Sinne nicht möglich" (Einstein 1944).

Diese Position, die man heute den lokalen Realismus nennt, steht natürlich in krassem Widerspruch zu der aktuellen Auffassung von Nichtlokalität in der Quantentheorie. In der besagten Arbeit geben EPR demnach ein Kriterium für Realität und Lokalität an, das man vereinfacht etwa so darstellen kann: Zwei verschränkte Spin-1/2-Teilchen werden von einer Verschränkungsquelle ausgesendet. Falls die Teilchen genügend weit voneinander entfernt sind, sollte es EPR zufolge am ersten Teilchen möglich sein, eine Messung durchzuführen, ohne das zweite Teilchen dabei zu beeinflussen. Da es also keine Beeinflussung gibt, müssen

demnach alle Spinwerte, die man an den Teilchen messen könnte, im Vorhinein bereits festgelegt sein. Wie oben gezeigt, könnte man dann an einem Teilchen zum Beispiel „Spin up“ und am zweiten Teilchen „Spin down“ messen. Dies allerdings auch in verschiedenen Raumrichtungen. Die quantenmechanische Unbestimmtheitsrelation erlaubt es aber nicht, Spinkomponenten verschiedener Richtungen gleichzeitig zu messen. Dadurch ergäbe sich laut EPR ein Widerspruch, woraus folge, dass die Quantenmechanik unvollständig sein müsse. Sie wäre demnach notwendig durch eine fundamentalere Theorie zu ersetzen, welche die gleichzeitige Berechnung aller Spinkomponenten gestatte, wie auch die simultane Bestimmung von Ort und Impuls zulasse (und somit die heisenbergsche Unschärferelation obsolet macht). Da es zur Zeit Einsteins keine moderne Experimentalphysik gab, die eine Entscheidung hätte herbeiführen können, führte das Genie mit dem dänischen Physiker Niels Bohr endlose Debatten auf rein theoretischer Ebene. Berühmt wurden jene Solvay-Konferenzen während der 1930er Jahre, bei denen Einstein ständig die Quantenmechanik zu überlisten versuchte. Der kongeniale Niels Bohr konnte aber jedes Mal die intellektuellen Attacken seines Kollegen kontern. In einem der Fälle schien Bohr schon fast schachmatt, als er im letzten Moment noch Einsteins Allgemeine Relativitätstheorie aus den Ärmel zog und diesen also (gemeinsam mit Heisenberg und Pauli) mit seinen eigenen Waffen schlug.

1.8 Das Bell-Theorem

Wie dargelegt, werfen EPR in ihrer 1935 erschienen Arbeit die Frage auf, ob die Quantenmechanik eine vollständige Theorie sei. Dieses Argument wird gerne auch als EPR-Paradoxon bezeichnet. Damit verbindet sich die

Forderung, die Quantenmechanik durch eine Theorie verborgener Variablen zu ergänzen, da ansonsten die Verschränkung paradox erschiene. Insbesondere trete dabei laut Einstein eine „spukhafte Fernwirkung" auf, was nun wahrhaft kein Ansatz für eine exakte Naturwissenschaft sein könne. Paradoxien entstehen aber nur dann, wenn der Quantenmechanik klassische Denkmuster aufgesetzt werden – wie der lokale Realismus. Wie man heute weiß, ist keine physikalische Theorie verborgener Variablen imstande, die Quantenphysik in allen Vorhersagen zu reproduzieren. Dieses sogenannte Bell-Theorem ist mittlerweile von ganz zentraler wissenschaftstheoretischer Bedeutung, zeigt es doch, dass es diese bizarre Quantenwelt „wirklich" gibt und es sich hierbei um eine Naturbeschreibung von fundamentaler Bedeutung handeln muss. Ganz maßgeblich wird diese Feststellung erhärtet durch die Tatsache, dass sie vollständig auf wissenschaftlichen Beweisen beruht. Für den Laien mag sich allerdings die Frage stellen, wie eine solche Beweisführung überhaupt vor sich geht. Dazu anschließend eine kleine Einführung in Sachen Arbeitsweise der Physik.

Falsifizierbare Hypothesen Zunächst sei ein einfaches Beispiel betrachtet, das durchaus zum Selbstversuch geeignet ist: Sie lassen ein Blatt Papier und eine Münze gleichzeitig aus derselben Höhe zu Boden fallen. Dabei machen Sie die Beobachtung, dass die Münze deutlich schneller fällt. Warum ist das so? im Wesentlichen könnte es zwei Ursachen geben:

1. die Münze fällt deshalb schneller, weil sie schwerer ist, das heißt, weil ihre Masse größer ist,
2. die Münze fällt schneller, weil das Blatt Papier mehr Luftwiderstand aufweist und dadurch eine Kraft (Reibung) entsteht, welche die Fallbewegung abbremst.

Sie haben nun zwei Vermutungen (Hypothesen) gebildet, die wahr oder falsch sein können. Damit wird bereits eine wichtige wissenschaftliche Forderung erfüllt: das Formulieren von *falsifizierbaren* Hypothesen.

Um zu entscheiden, welche der Hypothesen richtig oder falsch ist, muss ein geeignetes Experiment durchgeführt werden, das eine eindeutige Entscheidung herbeiführt. Das Experiment ist in den Worten von Isaac Newton der „höchste Richter" in der Physik. Dazu knüllen Sie das Papier zusammen und lassen erneut beide Körper aus derselben Höhe zu Boden fallen. Ergebnis: beide Körper fallen nahezu gleich schnell – damit wurde automatisch Hypothese 1 widerlegt, Hypothese 2 dagegen ist bestätigt. Der Grund liegt in der ganz einfachen logischen Schlussfolgerung, dass Hypothese 1 annimmt, dass schwere Körper schneller fallen – somit müsste weiterhin die Münze rascher fallen als das Papier, dessen Masse sich durch das Zusammenknüllen nicht verändert hat. Da dies im Widerspruch zum Experiment steht, muss Hypothese 1 verworfen werden. Hypothese 2 wird dagegen eindeutig bestätigt, da eine Reduktion des Luftwiderstands auch die entstehende Reibung reduziert und somit die Papierkugel schneller fällt.

Auf diesem Ergebnis aufbauend können Sie nun eine weitere Hypothese aufstellen: Wenn der freie Fall ersichtlich nicht von der Masse, sondern lediglich vom Luftwiderstand abhängt, dann müssen im Vakuum alle Körper notwendigerweise gleich schnell fallen (da es im Vakuum ja keine Luft gibt). Zur experimentellen Überprüfung dieser Hypothese ist schon ein wenig mehr Etat nötig: zum Beispiel eine lange, evakuierbare Glasröhre, in der sich eine Daunenfeder und eine Münze befinden. Mit einer halbwegs guten Vakuumpumpe lässt sich sodann mit wenig Mühe demonstrieren, dass beide Objekte ganz offensichtlich gleich schnell zu Boden fallen. Und das, obwohl eine Daunenfeder gewiss viel weniger Masse besitzt als eine Münze.

Zusammenfassend bleibt festzuhalten: Physikalische Beweisführung funktioniert in der Weise, dass

1. falsifizierbare Hypothesen formuliert werden, die
2. durch reproduzierbare Experimente überprüft werden müssen.

Aus der Verifikation einer ersten Hypothese können sich Schlussfolgerungen ergeben, die zu weiteren experimentellen Überprüfungen führen. Oftmals findet man auch erst einen interessanten Effekt und formuliert die passende Hypothese hinterher. Man spricht in diesem Fall von einer Deutung – Einsteins Photonenhypothese ist ein berühmtes Beispiel dafür. In jedem Fall gilt aber die goldene Regel: nur experimentell bestätigte Hypothesen haben die Aussicht, als Naturgesetze anerkannt zu werden. Einfacher ausgedrückt, die Physik handelt stets nach der Maxime: „Behauptungen müssen *zwingend* bewiesen werden" (man möchte diesen Ansatz gerne auch der Politik nahelegen). Derartige Spielregeln gelten in sehr viel komplizierterer Form nun auch für das Bell-Theorem. Auch hier müssen geeignete Hypothesen formuliert werden, die anhand von Experimenten zu überprüfen sind. Diese Hypothesen werden in aller Regel mathematisch formuliert, woraus sich konkrete Werte von Messgrößen vorhersagen lassen. Diese Werte werden daraufhin mit den experimentell gewonnen Daten verglichen. Nur wenn hier eine (nach statistischen Regeln definierte) wissenschaftliche Signifikanz (= hinreichend kleine Abweichung) gegeben ist, haben derartige Vermutungen die Chance, als Naturgesetz zu gelten. Im Falle des EPR-Paradoxons dauerte es allerdings bis ins Jahr 1964, bis ein entsprechendes mathematisches Kriterium veröffentlicht wurde (frühere Versuche waren nicht allgemein genug). Das Ergebnis war die sogenannte bellsche Ungleichung. Diese quantitative Darstellung des

EPR-Problems ist einem leider viel zu früh verstorbenen irischen Theoretiker zu verdanken, dem die Grundlagen der Quantentheorie ein ganz besonderes Anliegen waren.

Doktor Bertlmanns Socken Wir erinnern uns, dass in der Murmelspiel-Analogie eine Person namens John vorkommt.

Dieser kam ja zu Niels und Albert hinzu und behauptete, eine Entscheidung herbeiführen zu können. Die Rede ist vom irischen Physiker John Stewart Bell, der sich Jahrzehnte nach den Solvay-Konferenzen in die Debatte einschaltete und das EPR-Paradoxon in eine quantitative Form brachte. Obwohl aus ärmlichen Verhältnissen stammend, schaffte Bell dennoch Abschlüsse in mathematischer und experimenteller Physik, worauf er schließlich als Teilchenphysiker und Feldtheoretiker unter anderem am CERN in Genf arbeitete. Daneben beschäftigte er sich zudem mit Grundsatzfragen zur Quantentheorie, insbesondere auch dem EPR-Argument. Bell verfasste dazu einmal eine berühmt gewordene Analogie („Doctor Bertlmann's socks"), wo er die Thematik humorvoll und für eine breite Öffentlichkeit leicht verständlich auf den Punkt brachte. Im Mittelpunkt der Szene steht dabei Bells damaliger Freund und Mitarbeiter Reinhold Bertlmann.

Der bekannte Wiener Quantenphysiker Reinhold Bertlmann besitzt (auch nach eigener Darstellung) die Gewohnheit, verschiedenfarbige Socken anzuziehen. Ist eine Socke rot, ist die andere vielleicht blau; ist eine Socke pink, ist die andere grün usw. Laut John Bell kann man sich bei Reinhold Bertlmann immer sicher sein, dass die Socken „antikorreliert" sind; das heißt, wenn man die Farbe einer Socke beobachtet, dann zeigt die andere Socke ganz sicher eine andere Farbe, also etwa anti-rot, anti-blau etc. Wenn man somit eine Socke an Bertlmanns Hosenbein beobachtet (welche Farbe auch immer sie dann hat), so ist determiniert, dass die zweite Sockenfarbe ganz sicher

Abb. 1.4 Dr. Bertlmanns Socken. (Karikatur Autor, nach einer Zeichnung von John Bell, dieser im Bild links)

eine andere sein wird (Abb. 1.4). Dies erinnert frappant an die Antikorrelationen bei verschränkten Teilchen, die ein ähnliches Verhalten zeigen. In dieser humorvollen Metapher bringt John Bell die Kernfrage des EPR-Problems auf den Punkt: Wird die Farbe beider Socken im Vorhinein schon von der Natur festgelegt (Position des Realismus) oder aber entsteht die Farbe der Socken objektiv zufällig erst beim Messprozess (der Beobachtung) der Socken selbst? Im Falle von Doktor Bertlmann liegt gewiss die realistische Position vor (die von Bell eigentlich vertreten wurde): Es gibt hier ganz bestimmt eine Ursache für das antikorrelierte Verhalten der Socken – nämlich die, dass sie von Bertlmann in der Früh so angezogen wurden. Würde es sich dagegen um echte Quantensocken handeln, so wäre die Farbe der Socken bis zu jenem Zeitpunkt völlig unbestimmt, an dem sie beobachtet werden.

Hier nun noch einmal die beiden wesentlichen Positionen, zwischen denen Bell eine wissenschaftlich fundierte Entscheidung herbeiführen wollte:

Hypothese 1: Position des lokalen Realismus im Sinne Einsteins Es gibt unbekannte physikalische Größen, welche das Verhalten verschränkter Teilchen im Voraus bestimmen. Das Unschärfeprinzip sowie die Annahme der objektiven Zufälligkeit beruht lediglich auf der subjektiven Unkenntnis dieser Größen und stellt somit kein Naturgesetz dar. In Einsteins bildhafter Sprache: „Gott würfelt nicht!" Die Quantenmechanik muss darum unvollständig sein und durch eine Theorie verborgener Variablen ergänzt werden. Der lokale Realismus zwingt zu der Annahme, dass verschränkte Objekten individuelle Eigenschaften besitzen, die ihr Verhalten steuern. Eine Messung ist daher immer nur das Ablesen einer Eigenschaft, die von der Natur bereits vorherbestimmt ist.

Hypothese 2: Annahme der Nichtlokalität im Sinne Bohrs Obwohl räumlich getrennt, bilden verschränkte Teilchen eine untrennbare Einheit. Bevor ihre Eigenschaften gemessen werden, ist es auf fundamentale Weise unbestimmt, welche Merkmale bei der Messung konkret vorliegen, aber eindeutig festgelegt, dass sie korreliert sind. Messergebnisse sind objektiv zufällig, das heißt, die Natur hat von Haus aus nicht festgelegt, welche Eigenschaften die Teilchen vor der Messung besitzen. Insbesondere zeigt sich dabei ein nichtlokales Verhalten, das heißt, zwei (eventuell räumlich sehr weit getrennte) Objekte können sich instantan beeinflussen- im Unterschied zur lokalen Position, wo dies bestenfalls mit Lichtgeschwindigkeit erfolgen kann. Das ist eine zentrale Aussage der sogenannten Kopenhagener Interpretation der Quantenmechanik, die auch heute noch von vielen Physikern vertreten wird.

Bellsche Ungleichung Um dem Leser die komplizierte Mathematik zu ersparen, wollen wir uns hier darauf beschränken, die bellsche Ungleichung allgemein zu beschreiben. Für ein näheres Durchdringen der Grundgedanken sei der interessierte Leser an die vielen weiterführenden Bücher verwiesen, die es dazu gibt, beispielsweise (Zeilinger 2005). Im Übrigen existieren zahlreiche Derivate wie etwa die verallgemeinernde und leichter überprüfbare CHSH-Ungleichung oder die „pädagogisch wertvolle" Wigner-Ungleichung (Abschn. 2.6.3). Die Überprüfung der originalen Bell-Ungleichung kann anhand der Korrelationen von Messergebnissen (wie in der Polarisation verschränkter Photonen oder im Spin verschränkter Elektronen) vorgenommen werden. Dazu werden extrem viele verschränkte Teilchenpaare bezüglich ihrer jeweils korrelierten Eigenschaft (Spin- beziehungsweise Polarisationsrichtung) gemessen. Dies schafft die Voraussetzung für die anschließende statistische Untersuchung, die nach dem Gesetz der großen Zahlen umso repräsentativer ist, je mehr einzelne Messergebnisse eingehen. Daraus können entsprechende relative Häufigkeiten beziehungsweise Wahrscheinlichkeiten berechnet werden, welche sodann in die Ungleichung eingesetzt werden. Anschaulich gesprochen macht die Bell-Ungleichung also einen Vergleich zwischen Wahrscheinlichkeiten die bei Hypothese 1 auftreten und solchen, die bei Hypothese 2 zu erwarten sind. Dabei besteht das entscheidende Kriterium darin, dass Hypothese 1 in jedem Fall der Ungleichung genügen muss. Falls dies zutrifft, wäre sozusagen der lokale Realismus bewiesen und Einstein hätte recht. Wird sie aber verletzt (zumindest in bestimmten Fällen), so muss Hypothese 1 zugunsten von Hypothese 2 verworfen werden.

Experimente zum Bell-Theorem Interessant ist, dass John Bell die nach ihm benannte Ungleichung unter

anderem deshalb formulierte, weil er ursprünglich Einsteins Position stützen wollte. Dieses Bemühen war umso höher zu bewerten, als die EPR-Problematik Anfang der 1960er Jahre keinen mehr interessierte und als „philosophisches Geplänkel von vorgestern" galt. Eine Einschätzung, die sich heute grundlegend geändert hat. Die EPR-Arbeit ist aktuell das meistzitierte Paper in der Quantenforschung. Deshalb fragte John Bell einen der ersten Experimentalphysiker, welcher die Bell-Ungleichung überprüfen wollte, den Franzosen Alain Aspect, ob er schon eine sichere Anstellung an seiner Uni habe. Erst als dieser bejahte, konnte es losgehen. Im Jahr 1982 gelang Aspect (nach früheren Messungen von Kollegen) eine wissenschaftlich noch signifikantere Überprüfung der Bell-Ungleichung. Ein wichtiger Punkt bei diesem und nachfolgenden Experimenten war es, mögliche „Schlupflöcher" zu schließen. So könnte es etwa sein, dass die Messparameter der einen Messeinrichtung am Ort der anderen bekannt sind. Man muss also sicherstellen, dass die beiden Messungen raumzeitlich voneinander getrennt sind (um im Fachjargon zu sprechen). Ebenso könnte die theoretische Existenz von unter- oder überlichtschnellen Signalen dazu führen, dass es davon abhängt, an welchem Punkt und in welcher Richtung gemessen wird. Schließlich gibt es auch das Nachweisschlupfloch, das durch in der Praxis immer gegebene Messfehler entsteht. Dank Computern und moderner Experimentalphysik ist es heute möglich, ein Schlupfloch nach dem anderen zu stopfen.

Experimentelle Ergebnisse Als die Ergebnisse so weit feststanden, dass sie einer seriösen Beurteilung unterzogen werden konnten, lösten diese einen Ruck in der Fachwelt aus. Unglaublich, aber wahr: die Bell-Ungleichung wurde in allen relevanten Messreihen signifikant verletzt und somit Hypothese 2 im Sinne der Kopenhagener

Interpretation bestätigt. Dies nicht nur in Aspects Pionierversuchen über geringere Distanzen, sondern auch in den sehr medienwirksamen Experimenten von Anton Zeilinger und Rupert Ursin. So wurden unter anderem Quantenkanäle quer durch Wien und sogar unterhalb der Donau eingerichtet, ebenso zwischen den Kanarischen Inseln La Palma und Teneriffa. Damit konnte die Verletzung der Bell-Ungleichung bereits über eine Strecke von 144 km demonstriert werden. Den aktuellen Distanzrekord (1203 km) in Sachen „Quantenspuk" verkörpert das QUESS-Experiment, das bereits eingehend beschrieben wurde. Einen numerischen Rekord stellt der erst jüngst durchgeführte „Big-Bell-Test" dar (siehe unten). Dabei konnte ebenso klar eine Widerlegung festgestellt werden. Eine wichtige Forderung betrifft, wie angesprochen, das Schließen der „Schlupflöcher". Die raumartige Trennung wurde bereits in Versuchen von Alain Aspect und Gregor Weihs (1998) sichergestellt, indem eine extrem schnelle Manipulation der Anordnung eine Informationsübertragung mit Lichtgeschwindigkeit unmöglich macht. Das dabei durch eine zu geringe Zählrate entstehende Nachweisschlupfloch konnte 2001 durch ein Experiment von M. A. Rowe geschlossen werden. Theoretisch wäre zudem auch ein Lokalitätsschlupfloch denkbar, das heißt, ein eventuell noch nicht bekannter physikalischer Mechanismus könnte existieren, der dennoch einen klassischen Infoaustausch zwischen den Messeinrichtungen gestattet. Dafür gibt es jedoch bis dato nicht die geringsten Hinweise. Aktuelle Experimente implizieren, dass es für die sogenannten „Loopholes" keine wirkliche Grundlage gibt. Der angesprochene Big-Bell-Test legt zudem den Ausschluss eines weiteren Schlupflochs nahe: In derartigen Experimenten werden durch Zufallsgeneratoren verschiedene Messanordnungen sehr oft umgeschaltet. Theoretisch könnte das Verhalten dieser Generatoren aber

wieder durch unbekannte Parameter bestimmt sein und somit wäre das Setting der Messung nicht völlig frei und unabhängig. Deshalb wurde die zufällige Entscheidung von über 100.000 Personen herangezogen, welche über 90 Mio. zufällige Bits erzeugten, die in 13 verschiedenen Experimenten an weltweit 12 Instituten für die Einstellung der Messgeräte verwendet wurden. Korrekterweise muss angemerkt werden, dass der Extremfall eines superdeterminierten Universums (in dem alles stringent vorherbestimmt ist und es absolut keinen freien Willen gibt) wissenschaftlich durch solche Tests niemals ganz auszuschließen ist.

Folgerungen und Bedeutung Die experimentellen Befunde zur bellschen Ungleichung legen also vehement nahe, dass Hypothese 1 zugunsten von Hypothese 2 verworfen werden muss. Somit deutet alles darauf hin, dass Einsteins Postulat nicht zutrifft, als er forderte, die Quantentheorie sei unvollständig. Zwar hatte er ganz richtig erkannt, dass die Kopenhagener Deutung definitiv nicht mit der lokal realistischen Vorstellung der klassischen Physik verträglich ist, irrte aber im oben genannten Punkt. Demnach kann es keine Theorie verborgener Variablen geben, welche imstande wäre, die gemessenen Korrelationen (in allen Fällen) zu reproduzieren. Dies ist Inhalt des Bell-Theorems, das heute nach Ansicht der allermeisten Physiker als bewiesen gilt. Als ebenso widerlegt gilt damit auch der lokale Realismus. Wie viele Physiker meinen, muss jedenfalls mindestens eines der beiden Prinzipien aufgegeben werden: entweder die Lokalität und/oder der Realismus. Wie dargelegt, versteht man unter „Realismus“ die Annahme, dass die Messgeräte nur Werte liefern, die bereits im Vorhinein feststehen. Mit „lokal“ verbindet sich vor allem die Annahme, dass die Messung an einem Teilchen den Zustand des anderen

bestenfalls mit Lichtgeschwindigkeit beeinflussen kann. So weit, so gut. Das Experiment – der höchste Richter in der Physik – hat also gesprochen. Man muss sich allerdings erst einmal auf der Zunge zergehen lassen, was das in erkenntnistheoretischer Hinsicht bedeuten könnte. Schon Schrödinger meinte, die Verschränkung sei „… so verrückt, dass sie uns wahrscheinlich zwingt, von unserer liebgewordenen, alltäglichen Vorstellung dieser Welt Abschied zu nehmen". Anton Zeilinger sagt hierzu: „Es stimmt irgendetwas nicht an unserem Weltbild: entweder stimmt unsere Vorstellung von Raum und Zeit nicht, also zwei separierte Orte oder Zeitpunkte sind eventuell gar nicht getrennt. Oder unsere Vorstellung von der Wirklichkeit stimmt nicht" (https://www.youtube.com/watch?v=Pf92k-sfKdk&t=1349s). Im Sinne der Kopenhagener Deutung jedenfalls manifestiert sich die Realität erst durch die Beobachtung (den Messprozess) selbst. John Bell freilich war „Realist" – er konnte es nicht fassen, dass seine eigene Ungleichung offenbar den Realismus aus den Angeln hob. Er äußerte daraufhin immer wieder: „It's a mystery!" Auf der anderen Seite gab er jedoch der Möglichkeit Spielraum, dass das gesamte Universum nichtlokal wäre.

Ganz unabhängig von Interpretationsfragen und Philosophie ergibt sich die einfache, aber weitreichende Schlussfolgerung (welche für die Quantenkommunikation eine Tragweite haben wird): Dass es die Quantenmechanik eben „wirklich" geben muss und sie definitiv keine Theorie ist, die aus der klassischen Physik heraus erklärbar ist. Es handelt sich somit ganz klar um eine nichtklassische Theorie. Diese Abgrenzung umfasst auch die Relativitätstheorie (die ihrer kausalen Struktur wegen ebenso zu den klassischen Theorien gezählt wird). Deren kausaler Charakter ist es aber nachgerade, welcher in der Quantenphysik offenbar zu Grabe getragen wird, wie das Bell-Theorem

beweist. Insbesondere wird hier aufs Neue bestätigt, dass die seltsamen Unbestimmtheiten physikalischer Messgrößen keine persönliche Unkenntnis über deren wahren Wert repräsentieren, sondern die Dinge an sich *(„a priori")* unbestimmt sind. Die Wellenfunktion legt nur die Wahrscheinlichkeit von Messwerten fest, nicht aber, welches konkrete Messergebnis im Einzelfall auftritt. Gerade diese dem menschlichen Verstand völlig zuwiderlaufende Position bildet jedoch die Grundlage von Hypothese 2, die experimentell glänzend bestätigt wird. Ebenso bestätigt wird die Tatsache, dass sich verschränkte Objekte instantan beeinflussen. Je nach Sichtweise kann man das dann mit Einstein als „Quantenspuk" bespötteln. Oder aber – was eher der wissenschaftlichen Position entspricht – man erkennt es als eine Grundeigenschaft der Natur an, die es per se zu akzeptieren gilt. Eben die Eigenschaft der Nichtlokalität, welche kein klassisches Pendant kennt und gerade beim Phänomen der Verschränkung am deutlichsten zutage tritt. Am Ende müsste man sich aber dennoch die philosophische Frage stellen, ob Erklärbarkeit (also Wissen) ein fundamentales Bedürfnis des Menschen ist, das angesichts der modernen Physik offenbar niemals befriedigt werden kann. Denn was ist dann Wirklichkeit an sich? Vielleicht verhält es sich aber gerade so, dass das Wissen selbst, also die Information, die Wirklichkeit abbildet. In der Physik gibt es jedenfalls zahlreiche Hinweise dafür, dass man offenbar die Begriffe Wirklichkeit und Information nicht voneinander trennen darf. Unabhängig davon erweisen sich die Bell-Ungleichung beziehungsweise deren Derivate als äußerst nützlich für ein zukünftiges Quanteninternet. Denn sie stellt ein statistisches Kriterium dar, ob ein Quantenkanal nun intakt ist (zum Beispiel maximal verschränkt) oder ob etwa ein technisches Gebrechen oder eine Manipulation vorliegen. Es lässt sich also auf diese Weise das unautorisierte

Abhören von quantenkryptografisch verschlüsselten Daten direkt feststellen. Ebenso wird der objektive Zufall als elementarstes quantenmechanisches Ereignis bestätigt. Da er deshalb nicht mehr weiter reduzierbar ist, sind die bei QKD-Systemen erzeugten Zufallszahlen die bestmöglichen, die man überhaupt je erzeugen könnte. Neben der fundamentalen Bedeutung für die Grundlagenforschung rückt demnach die technologische Anwendbarkeit verschränkter Zustände aktuell immer mehr in der Vordergrund.

1.9 Quanteninformation

Bevor wir uns mit dem Begriff Quanteninformation näher auseinandersetzen, sei zunächst erklärt, was man unter klassischer Information versteht. Dazu ein bekanntes Beispiel, das auf den Statistiker John Tukey zurückgeht: Sie sitzen in einem Lokal und haben die Auswahl, einen Kaffee auf folgende Arten zu bestellen: heiß oder kalt, groß oder klein, mit oder ohne Koffein. Wie leicht zu überlegen ist, gibt es dafür insgesamt 8 Möglichkeiten. Der Kellner möchte nun wissen, welche Kombination genau serviert werden soll, deshalb fragt er: „Wollen Sie den Kaffee heiß?“ Sie antworten mit ja oder nein. „Hätten Sie gerne einen großen Kaffee?“ Sie sagen erneut ja oder nein. „Möchten Sie koffeinfreien Kaffee? Ja oder nein?“ Es wurden also drei Fragen gestellt mit drei Ja/Nein-Antwortmöglichkeiten. Der Informationswert dieser Bestellung mit $2^3 = 8$ Möglichkeiten ist demnach 3 Bit an Information, was sich als eine dreistellige Binärzahl darstellen lässt. Diese Grundidee, nämlich, dass man Information auf Grundlage von Ja/Nein-Aussagen als Binärzahl symbolisieren kann, bildet die Basis der gesamten heutigen Digitaltechnik; insbesondere auch der aktuellen IT. Dabei wird

die Elementareinheit der klassischen Information durch das Bit (binary digit, Einheitenzeichen „bit“) repräsentiert. Es enthält eine Entscheidung zwischen zwei Aussagen (ja oder nein, wahr oder falsch), als Binärzahl dargestellt 1 oder 0. Bei 2^N Fragestellungen ist der Informationswert demnach N Bit an Information. In der Computerwelt arbeitet man bekanntlich gerne mit Gruppen von 8 Bit, die man dann ein Byte nennt. 1 Byte entspricht demnach 8 Fragestellungen und damit $2^8 = 256$ Antwortmöglichkeiten beziehungsweise Bitfolgen. Das heißt, es sind 8 Bit an Information nötig, um eine der 256 Möglichkeiten zu kennen.

Nun kann man auf diese Weise jede Art von Information beliebig „digitalisieren“, wenn man nur hinreichend viele Fragen stellt und eine dementsprechende Anzahl von Ja/Nein-Aussagen (Bits) erhält. Diese Fragen können die Farbwerte der Bildpunkte einer Datei ebenso betreffen wie den Schalldruck eines Musik-Streams beim Sampling. Allgemein misst ein Sensor eine physikalische Größe (zum Beispiel ein CCD-Chip die Bildhelligkeit) und gibt entweder ein digitales Signal weiter oder ein analoges Signal, das mit einem Analog-Digital-Umsetzer in einen digitalen Wert transformiert wird. Insbesondere können auch Buchstaben und Zahlenwerte in Form von Bitfolgen dargestellt werden, mit denen man nach dem Binärkalkül auch rechnen kann. Dieses Dualsystem (Binärsystem), das unter anderem auf das „letzte Universalgenie“ Gottfried W. Leibniz zurückgeht, bildet heute die Grundlage für die Datenverarbeitung in Computern auf Basis von logischen Grundoperationen (Gatter). Die systeminterne Codierung hängt dann allerdings von der Art der Information und ihrer späteren Nutzung ab. Dabei spielen Dateiformate eine wesentliche Rolle zur Standardisierung. Schließlich können die Binärwerte in Arbeitsspeicher, Datenbanksystemen oder Dateisystemen abgelegt werden.

Insgesamt bietet die Digitaltechnik viele Vorteile, nicht zuletzt auch deshalb, weil hier lediglich zwischen zwei Signalzuständen unterschieden werden muss (0 oder 1). Diese können physikalisch zum Beispiel durch einen niederen beziehungsweise höher liegenden Spannungswert realisiert sein. Von wirtschaftlichem Vorteil ist zudem, dass die Bauteile demnach keine allzu hohe Genauigkeit erfordern, was die Produktionskosten senkt. Davon profitiert auch das klassische Internet: Physikalisch gesehen handelt es sich dabei um ein komplexes Netzwerksystem, wo informationsverarbeitende Systeme wie Computer und mobile Endgeräte klassische Information miteinander austauschen. Neben funkbasierten Systemen werden größere Netzwerkstrukturen interkontinental vorwiegend über Glasfaserkabel miteinander verbunden. Der Grund für den Einsatz von faseroptischen Techniken ist vielfältig, liegt jedoch vor allem in den enormen Übertragungskapazitäten, die sich mit dieser Methodik verbinden. Dieser Vorteil ist primär auf die Tatsache zurückführen, dass Licht eine sehr hohe Schwingungsfrequenz aufweist. Sie liegt „telekomüblich" mit um die 10^{14} Hz im Infrarotbereich, dies bedeutet um die 100 Billionen Schwingungen pro Sekunde. Zu beachten ist, dass faseroptische Systeme ein optisch dichtes Medium bilden und deshalb die Lichtgeschwindigkeit um etwa 1/3 kleiner ist als ihr Wert im Vakuum. Was technisch keine Rolle spielt, da selbst dann immer noch Bitraten im Zig-Tbit-Bereich möglich sind. Pro einzelner Faser versteht sich, mehrere zusammengenommen können Rekordraten von 1 Pbit/s und mehr erreichen. Anschaulich gesprochen, werden die Bits physikalisch also durch sehr schnelle Ein/Aus-Lichtpulse dargestellt. Diese „Hochfrequenztechnik" ist andererseits der Preis für die Digitaltechnik, den es zu zahlen gilt, denn sie setzt naturgemäß sehr hohe Bitraten pro Zeiteinheit voraus. Deshalb nützt man unter anderem

die hohe „Trägerfrequenz“ des Lichts aus, was sich als ideale physikalische Ressource anbietet. Ein technischer Mehraufwand entsteht allerdings durch die Tatsache, dass die Lichtintensität in den Glasfasernetzwerken sukzessive abnimmt, sodass sie spätestens alle 100 km durch sogenannte Repeater gemessen, verstärkt und weitergeleitet werden muss. Trotz der technologisch komplexen Infrastruktur ist die klassische Informationsverarbeitung von der Grundidee sehr einfach und deshalb heute so weit verbreitet, dass sie zur digitalen Revolution geführt hat.

Die fundamentale Andersartigkeit der Quantenmechanik ist nun dazu angetan, den Spielraum der klassischen Informationsverarbeitung maßgeblich zu erweitern. Ein wesentlicher Unterschied liegt im Superpositionsprinzip, das wir schon angesprochen haben. In Abschn. 1.5 haben wir gesehen, dass sich ein Photon, wenn es beispielsweise durch einen polarisierenden Strahlteiler (PST) tritt, in einer Überlagerung zweier möglicher Polarisationsrichtungen befindet, nämlich horizontal oder vertikal. Daraufhin kann es als „0“ oder „1“ gemessen werden – was einem klassischen Bit an Information entspricht. Entscheidend ist aber der wichtige Umstand, dass es sich *vor* der Messung in einem Überlagerungszustand (Superposition) von horizontaler und vertikaler Polarisation befindet, also sozusagen 0 und 1 gleichzeitig abbildet. Dies bildet die Grundlage einer neuen Art von Information, der Quanteninformation. Analog der klassischen Information, deren Grundeinheit das Bit ist, wird die Elementareinheit der Quanteninformation als Quantenbit (Qubit) definiert. Es handelt sich dabei um das einfachste quantenmechanische Zweizustandssystem, das bei seiner Messung nur zwei Werte (Eigenwerte) annehmen kann, die man wiederum 0 oder 1 nennen kann. Eine zentrale Frage, die sich unmittelbar stellt, ist naturgemäß, wie viel Information ein Qubit „speichern“ und übertragen

kann. Obwohl nicht letztgültig geklärt und Gegenstand aktueller Forschung, liegt hier die Vermutung nahe, dass ein Qubit unendlich (!) viel klassische Information enthält. Betrachten wir dazu als Beispiel wieder polarisiertes Licht, das auf den PST trifft (siehe Experiment 2 in Abschn. 1.5). Das Licht kann allgemein linear, rechts- oder linkszirkular oder auch elliptisch polarisiert sein. Das bedeutet, der elektrische Feldstärkevektor einer Lichtwelle kann konstant in einer Ebene verbleiben, jedoch rechtwinklig zur Fortpflanzungsrichtung auch Kreise beziehungsweise Ellipsen beschreiben. Dabei lässt sich zeigen, dass der Feldstärkevektor stets aus einer Überlagerung von horizontal und vertikal polarisiertem Licht (also 0 und 1) zusammensetzt ist. Er stellt somit eine Superposition dieser beiden Basiszustände dar. Da es theoretisch unendlich viele mögliche Richtungen gibt, in die das Licht polarisiert sein kann, würde es demnach auch unendlich viel klassische Information erfordern, all diese Möglichkeiten zu beschrieben. Um den Zustand eines Photons anzugeben, reicht also ein klassisches Bit (Wahl zwischen 0 oder 1) definitiv nicht aus, vielmehr müssen beide Anteile in einer Art Überlagerung (Linearkombination) angegeben werden, was das wesentliche Kennzeichen des Quantenbits darstellt.

Nun besteht das geradezu Fantastische der Quantentheorie aber genau darin, dass sich das Superpositionsprinzip auf beliebige Linearkombinationen der Basiszustände erweitern lässt. Man kann also sozusagen beliebig viele Qubits selbst miteinander in eine Superposition bringen. So ergeben zwei derart überlagerte Qubits bereits 4 Basiszustände (00, 11, 01, 10), drei Qubits dementsprechend 8 Basiszustände, 4 Qubits 16 Zustände usw. Aufgrund der rasanten (exakter exponentiellen) Zunahme der Basiszustände bei wachsender Qubit-Zahl kann eine solche Anordnung erheblich

mehr Information speichern als jeder bekannte Supercomputer (je nach Schätzung ab etwa 50 Qubits). Hierin liegt auch der revolutionäre Grundgedanke des Quantencomputers. Falls dieser zum Beispiel nach dem Prinzip des sogenannten Einweg-Quantencomputers arbeitet (Abschn. 2.5.4), packt er sozusagen alle Lösungsmöglichkeiten eines Problems in einen sehr komplexen Quantenzustand – und das gleichzeitig – woraufhin versucht wird, durch eine geschickte Messreihe an die bereits darin enthalte Lösung heranzukommen. Ganz maßgebliche Unterstützung erfährt der Quantencomputer dabei durch die Verschränkung. Jener „Quantenspuk" also, den Einstein bespöttelte. Dieser erlaubt nicht nur die Entwicklung neuartiger Fehlerkorrektur- und Redundanzverfahren (die sich von klassischen Pendants maßgeblich unterscheiden), sondern ebenso die Erzeugung ganz neuer Quantenzustände, die nicht aus einzelnen Subzuständen zusammengesetzt werden können. Dies hat neben dem Einweg-Quantencomputer vor allem auch bei denjenigen Konzepten eine besondere Bedeutung, die – ähnlich wie beim klassischen Computer – auf schaltkreisartigen Modellen (unter Einsatz von Quantengattern) beruhen. Klassische Computer verarbeiten Information durch Manipulation von Bits auf Basis logischer Schaltungen (Gatter). Beispielsweise erzeugt ein NOT-Gatter aus der Bitfolge 01001… die Folge 10110…; es invertiert also die Binärfolge, das ist genau eine Manipulation. Ein Quantencomputer vermag dagegen durch die Nutzung von N verschränkten Qubits bereits 2^N Manipulationen pro Gatteroperation durchzuführen. Mit $N = 2, 3, 4, 5, \ldots$ entspricht das 4, 8, 16, 32, … Manipulationen pro Operation. Auch hier wird abermals der „Exponentialeffekt" evident, der zu einem erheblichen Speed-up des Quantencomputers gegenüber einem traditionellen Rechner führen kann. Es ist nun nicht weiter schwer sich vorzustellen, dass ein skalierbarer (um

beliebige Qubits erweiterbarer) Quantenrechner theoretisch eine unermessliche Rechenpower verspricht.

Entropie, Information und Quantencomputer Die Möglichkeiten der Quanteninformation können also zu einem erheblichen Speed-up eines Computers führen. Information ist in der modernen Physik allerdings ein noch viel tiefer gehender Begriff, was besonders für die Quantentheorie gilt.

In der Natur gibt es häufig Vorgänge, die sich nicht umkehren lassen und nur in einer Richtung ablaufen. Ein Beispiel ist etwa eine heiße Kaffeetasse. Für sich belassen wird sich der Kaffee allmählich abkühlen, so lange, bis sich ein Temperaturgleichgewicht mit seiner Umgebung einstellt. Dabei wird die Tasse erwärmt, der Kaffee jedoch kälter. Ebenso könnte die Tasse dann zu Boden fallen und einen Scherbenhaufen hinterlassen. Beiden Vorgängen ist gemeinsam, dass man niemals den umgekehrten Vorgang beobachten wird. Weder wird der Kaffee von selbst heißer noch springen die Scherben von sich aus wieder zu der ursprünglichen Tasse zusammen. Derartige Vorgänge nennt man in der Physik irreversibel. Beschrieben wird die Irreversibilität durch eine Größe, die man Entropie nennt. Sie wurde von Rudolf Clausius um 1865 in die Physik eingeführt, und zwar deshalb, weil man mit dem Energieerhaltungssatz allein nicht entscheiden kann, ob ein Vorgang umkehrbar oder irreversibel ist. Wie allen Größen in der Physik kann man auch der Entropie einen Zahlenwert und eine Einheit (Joule pro Kelvin) zuordnen. Von praktischer Bedeutung ist aber nicht der genaue Wert der Entropie, sondern nur ihre Änderung. Bei irreversiblen Prozessen ist diese stets positiv, sie nimmt also immer mehr zu, bis ein finaler Gleichgewichtszustand erreicht ist. Im 19. Jahrhundert war diese Idee deshalb so bedeutsam, weil sie zum Beispiel zu der Erkenntnis geführt hat,

dass man beim Bau von Wärmekraftmaschinen Wärme niemals vollständig in mechanische Arbeit verwandeln kann. Es kann demnach keine solche Maschine mit einem Wirkungsgrad von 100 % geben, ein realer Kfz-Dieselmotor kann bestenfalls einen Wirkungsgrad von wenig über 50 % erreichen – selbst unter Aufbietung modernster Sensoren und Elektronik.

Dennoch war nicht so ganz klar, was die Entropie im eigentlichen Sinne genau ist (sie wird unter anderem auch als Maß für die Ordnung oder Unordnung eines Systems bezeichnet, was diesem Begriff nicht wirklich gerecht wird). Während Clausius noch kryptisch vom „Verwandlungswert" sprach, wollte der österreichische Physiker Ludwig Boltzmann den Dingen näher auf den Grund gehen. Dieser untersuchte daraufhin den mikroskopischen Aspekt der Entropie. Obgleich Boltzmann damals Begriffe wie Ensemble, Mikro- oder Makrozustände verwendete, ist die Frucht dieser Untersuchungen heute klar: Die Entropie hat etwas mit Wahrscheinlichkeit und Information zu tun.

Wir wollen dazu ein oft diskutiertes Beispiel betrachten: Man stelle sich einen Behälter vor, der in der Mitte eine Trennwand enthält. Auf der linken Seite befinde sich ein Gas, auf der rechten Seite dagegen Vakuum. Was wird passieren, wenn man die Trennwand entfernt? Das Gas wird sich sofort im gesamten Behälter ausbreiten. Die Atome beziehungsweise Moleküle, aus denen das Gas besteht, werden also nicht weiter auf der linken Seite verbleiben, sondern im Schnitt werden sich 50 % der Teilchen im rechten Bereich aufhalten. Wir wollen nun nach der Information fragen, ob sich ein bestimmtes Teilchen links oder rechts befindet. Wir könnten also fragen: „Teilchen, bist du auf der linken Seite?" Antwort: Ja oder Nein. Wie oben dargelegt, entspricht dies einem Informationswert von 1 Bit. Daraufhin könnte man ein

weiteres Teilchen fragen. Informationswert wieder 1 Bit, usw. Bei N Atomen oder Molekülen müsste man demnach N Fragen stellen (praxisbezogene N-Werte sind im Allgemeinen unvorstellbar groß). Die Entropie ist nun ganz einfach so definiert, dass sie in Beziehung zur Anzahl der Fragestellungen gesetzt wird – sie ist somit qualitativ gleich der Anzahl der Bits. Würden wir also nach dem Anfangszustand fragen, in dem alle Teilchen im Behälter links sind, wäre die Entropie logischerweise 0 (denn man muss ja jetzt keine Fragen stellen). Fragen wir aber nach dem Endzustand, so wäre die Anzahl der Bits sehr groß (da sich jetzt sehr viele Teilchen auch rechts aufhalten können). Die Entropie hat demnach stark zugenommen, sich also zu einem hohen positiven Wert hin verändert. Gleichzeitig beschreibt sie aber ebenso die Tendenz des Gases, sich auszubreiten. Das ist natürlich ein irreversibler Prozess – denn ohne äußere Einwirkung geht das Gas nicht von selbst auf die linke Seite im Behälter. Es ist intuitiv auch klar, dass die Wahrscheinlichkeit, dass das Gas einen Zustand mit hoher Entropie einnimmt, um vieles größer sein muss als der Anfangszustand. Zur Zeit Boltzmanns freilich gab es den Begriff „Bit“ noch nicht. Deshalb untersuchte Boltzmann, welche verschiedenen Zustände einzelne Teilchen selbst einnehmen können und brachte diese Anzahl direkt mit der Entropie in Verbindung. Sind diese „Mikrozustände“ (in Abgrenzung zu einem durch wenige Größen wie Volumen oder Temperatur charakterisierten „Makrozustand“) in großer Zahl vorhanden, so ist dementsprechend auch die Entropie sehr groß, andernfalls sehr niedrig. Die Entropie S ist also sowohl ein Maß für die Information in einem Zustand als auch für dessen Wahrscheinlichkeit W. Die berühmte Formel, welche diesen Zusammenhang beschreibt, ist in den Grabstein von Ludwig Boltzmann auf dem Wiener Zentralfriedhof eingraviert: $S = k \cdot \log W$. k ist dabei die sogenannte

Boltzmann-Konstante und der darin enthaltene Logarithmus (log) rührt von der Tatsache her, dass N Bit an Information ja 2^N Fragestellungen entsprechen. Will man daraus den Exponenten N gewinnen, benötigt man die Umkehrfunktion, also den Logarithmus.

Was hat die Entropie (also die Information) nun mit der Quantenphysik zu tun? Wir erinnern uns, dass der Beginn der Quantentheorie mit der „Quantenhypothese" von Max Planck um 1900 einsetzte. Allerdings sah sich dieser mit großem Widerstreben dazu quasi gezwungen – er sprach von einem „Akt der Verzweiflung". Was aber hatte Planck so sehr zur Verzweiflung getrieben? Ein wesentlicher Grund dafür lag darin, dass dieser anfangs in starker Opposition zur statistischen Physik und somit den grundlegenden Erkenntnissen Boltzmanns stand. Erst als Planck diese Position aufgab und statistische Methoden im Sinne Boltzmanns einsetzte, konnte er schließlich das nach ihm benannte Strahlungsgesetz erfolgreich herleiten. Dazu musste Planck allerdings das „Abzählen" lernen, also die Einteilung der Natur in diskrete Zustände, was letztlich zu der Annahme von diskreten Energiepaketen führte. Genau dies ist das wesentliche Merkmal der Quantentheorie, das in krassem Gegensatz zur klassischen Physik steht (dort geht man von beliebigen, kontinuierlichen Energiewerten aus). Ein anderes berühmtes Beispiel ist Einsteins Photonenhypothese. Interessant ist, dass Einstein zur Annahme der Lichtquanten ganz entscheidend dadurch angeregt wurde, dass er die Entropie eines Gases (modern gesprochen also die Bits) mit derjenigen von Licht verglich. Dabei fiel ihm eine verblüffende Ähnlichkeit auf, was letztlich zum Postulat der teilchenartigen Photonen führte. Allein diese historischen Beispiele legen demnach eine enge Verwandtschaft von Information und Quantenphysik nahe. Für den bekannten amerikanischen Physiker und Informatiker Seth Lloyd vom MIT (Massachusetts

Institute of Technology) folgt daraus jedenfalls die Erkenntnis, dass sich „alle physikalischen Objekte in eine endliche Menge von Bits codieren lassen, welche durch die Gesetze der Natur bestimmt sind“ (https://www.youtube.com/watch?v=XirbbUxOxiU). Falls dies zutreffen sollte, dann resultiert hieraus eine ganz wesentliche Hoffnung für das Potenzial von Quantencomputern. Schon heute gibt es erste Quantensimulationen, mit deren Hilfe das Verhalten komplexer Atom- und Molekülstrukturen simuliert wird. Der Grund für diese Bestrebungen liegt vor allem in der Tatsache, dass derartige Aufgaben für klassische Computer oftmals sehr schwierig bis unlösbar sind. Da Quantencomputer auf der Basis von Quanteninformation arbeiten, ist es angesichts einer endlichen Menge von Qubits denkbar, dass hiermit auch noch viel komplexere Strukturen darstellbar wären. So könnte bereits ein 100 Qubit-Rechner unmittelbar zur Entwicklung von noch unbekannten Stoffen und Materialien führen. Im weitesten Sinne könnte man sogar von „programmierbarer Materie“ sprechen. Diese Einschätzung der eigentlichen technologischen Bedeutung des Quantencomputers entspricht nachgerade der Doktrin von Nobelpreisträger Richard Feynman. Davon zeigen sich viele, vor allem auch amerikanische Entwickler und Forscher nachhaltig inspiriert. Und gerade die USA sind es, wo die bekannten Computer- und Software-Giganten mit großem Einsatz an der Entwicklung des Quantenrechners arbeiten. In jedem Fall impliziert das Zusammenwirken von Information und Quantenphysik noch ungeahnte technologische Möglichkeiten und Konsequenzen für die Menschheit.

2

Das Quanteninternet

„Ich sage das Jahrhundert neuer Quantentechnologien voraus, welche sowohl die Wissenschaft als auch die Wirtschaft verändern werden. Wir beginnen gerade erst zu verstehen, welche Möglichkeiten daraus erwachsen“
(Rainer Blatt).

2.1 Technologische Grundlagen

Der Begriff Quantennetzwerk (salopp auch Quanteninternet) bezeichnet prinzipiell die Vernetzung von Quanteninformationsträgern über Quantenkanäle. Unter Quanten versteht man ganz allgemein physikalische Objekte, welche durch Zustandswechsel in ein System mit diskreten Werten einer physikalischen Größe übergehen. Oft wird die Bezeichnung „Quant“ auch für kleinste Mengeneinheiten verwendet. Etwa die kleinste Menge Licht (Lichtquanten = Photonen) oder die kleinste Menge Energie

G. Fürnkranz, *Vision Quanten-Internet*,
https://doi.org/10.1007/978-3-662-58453-8_2

(Energiequanten). Gewöhnlich wird mit dem Begriff ein Teilchencharakter assoziiert, was jedoch nur ein Teilaspekt der eigentlichen Bedeutung ist. Etwas ungenau stehen „Quanten" salopp auch für Atome, was allerdings kein physikalischer Terminus dafür ist. Informationstheoretisch fasst man Quanten als Qubits (Quantenbits) auf und spricht dann auch von Quanteninformation, sie entsprechen den klassischen Bits auf bisherigen Computern. Qubits definieren gleichermaßen die kleinstmögliche Speichermenge wie auch ein Maß für die „Übertragung" von Quanteninformation. Gegenwärtig nutzt die Informationstechnologie Quanteneffekte erst in sehr geringem Ausmaß. Der zukünftige Schritt vom Bit zum Qubit eröffnet dagegen völlig neue Perspektiven. Eine dieser Möglichkeiten, die Quantenkryptografie, gestattet die Erzeugung völlig sicherer Quantenschlüssel zur anschließenden kryptografischen Übertragung mit gängigen Verfahren über das herkömmliche Internet. Eine ebenso faszinierende wie futuristisch anmutende weitere Möglichkeit besteht in der systematischen Vernetzung technisch einsetzbarer Quantencomputer.

Internet vs. Quanteninternet

Das heutige Internet ist ein komplexes Netzwerk aus Computern, in dem der Datentransfer in Form von klassischen Informationseinheiten (Bits) erfolgt. Diese können grundsätzlich immer einem Lauschangriff unterzogen beziehungsweise gehackt werden. Die Sicherheit hängt von der aktuellen Rechnerleistung sowie der Vertrauenswürdigkeit einzelner Personen ab. Für die Auslegung und somit die Leistungsfähigkeit bisheriger Computerchips zeichnet sich in wenigen Jahren eine physikalisch definierte Grenze ab.

Das Quanteninternet ist im Prinzip ein System von Quantenknoten, das einen durchgehenden Quantenkanal zu den Endknotenpunkten herstellt. Im fortgeschrittenen Stadium handelt es sich um ein Netzwerksystem von Quantencomputern, welche Quantenbits (Qubits) durch Teleportation miteinander austauschen. Da Qubits einerseits

überlichtschnell synchronisiert werden können, andererseits physikalisch inhärent abhör- und Hacker-sicher sind, ferner viel mehr Information speichern und übertragen können als klassische Bits, kommt diese Technik einem Paradigmenwechsel gleich. Quantencomputer haben zudem das Potenzial, Probleme zu bewältigen, welche selbst für Supercomputer unlösbar erscheinen.

Quantendownload via Teleportation

Den neuartigen Eigenschaften entsprechend unterscheidet sich auch die Physik des Quanteninternets von der des herkömmlichen in wesentlichen Dingen: Beim klassischen Internet kommt vorwiegend Glasfasertechnik zum Einsatz, wobei die Information in modulierten elektromagnetischen Wellen (Infrarotstrahlung) codiert ist. Diese Wellenzüge entsprechen periodisch variierenden Intensitäten eines großen Kollektivs von Photonen. Die Information ist hierbei in die schiere Anzahl der Lichtquanten geschrieben, deren relative Änderung pro Zeiteinheit gemessen wird. Die Quantenkommunikation nutzt hingegen die „inneren" Eigenschaften einzelner Photonen selbst. Damit lässt sich das bestehende Glasfasernetz zu erheblich größerer Effizienz steigern. Ganz wichtig ist in diesem Zusammenhang das Phänomen der Verschränkung zu nennen. Ändert man am Ort A den Quantenzustand eines Systems, so verändert sich instantan (und damit überlichtschnell) auch der Zustand des verschränkten Systems am Ort B. Zwar ist das genaue Merkmal des Zustands vor der Messung nicht determiniert, sehr wohl aber seine Beziehung zum bei A gemessenen Wert. Wesentliches Charakteristikum eines Quanteninternets ist, dass die Informationsübertragung nicht über klassische Repeater (Signal messen, verstärken und weiterleiten) erfolgen kann, sondern es muss die Quanteninformation als Ganzes vom

Sender zum Empfänger transferiert werden. Dieser Vorgang heißt Quantenteleportation, wozu die Verschränkung als dafür notwendige Ressource dient. Wer hier allerdings an körperliches „Beamen" à la „Raumschiff Enterprise" denkt, liegt weit daneben. Nicht die Materie oder elektrische Felder werden übertragen, sondern reine Information. Quantenteleportation bezeichnet insbesondere die sofortige Übertragung einer Zustandsänderung von speziell verschränkten Quantensystemen. Zur Übertragung muss außerdem zusätzlich zum Quantenkanal auch ein klassischer Kanal eingerichtet werden.

Da die Quantenteleportation überlichtschnell erfolgt, steht dies scheinbar im Widerspruch zu Einsteins Relativitätstheorie. Diese untersagt ausdrücklich eine instantane Übertragung von nutzbarer Information. Entscheidend ist jedoch das Adjektiv „nutzbar", das heißt, ob die Information für uns wirklich zugänglich ist. Die rein quantische Übertragung erfolgt zwar tatsächlich überlichtschnell – mit allen Vorteilen, die sich daraus ergeben – um diese jedoch auswerten zu können, ist ein klassischer Kanal nötig (zum Beispiel eine herkömmliche Internetverbindung). Da auf einem solchen Kanal die Informationsübertragung bestenfalls mit Vakuum-Lichtgeschwindigkeit erfolgen kann, sind die Verhältnisse in bester Übereinstimmung mit Einsteins Relativitätstheorie wiederhergestellt. Klassische Kanäle sind also auch in der Quanten-IT eine unabdingbare Voraussetzung, woraus sich die Schlussfolgerung ergibt, dass ein Quantennetzwerk das klassische Internet niemals vollständig ersetzen kann. Dieses wird also auch weiterhin seine volle Daseinsberechtigung haben, wobei die Quantentechnik als sehr fruchtbare Ergänzung zu verstehen ist Mithin dürften auch die Arbeitsplätze der vielen kompetenten und verdienten IT-Fachkräfte nicht in Gefahr sein. Ein Quanteninternet erweist sich jedenfalls nicht als Jobkiller, sondern

es bildet ganz im Gegenteil die Basis für die Entstehung völlig neuer Berufszweige.

Inhärente Sicherheit

In engem Zusammenhang damit steht eine weitere Eigenheit der Quantenmechanik, welche das zentrale Element des Quanteninternets bildet: Das No-Cloning-Theorem. Es besagt, dass es unmöglich ist, einen Quantenzustand perfekt zu kopieren – mit Betonung auf „perfekt". Somit können auch keine Qubits original dupliziert und beliebig vervielfältigt werden (siehe hierzu auch Abschn. 3.6). Hier liegt das besondere Geheimnis der physikalisch inhärenten Datensicherheit. Startet ein Spion einen Lauschangriff, muss die Information für ihn unabhängig vom Sender existieren; sie muss also mindestens verdoppelt werden. Qubits können aber nicht dupliziert und demnach auch nicht abgehört werden. Geschieht es, würde das zum Beispiel Einsteins Relativitätstheorie grob verletzten (da Qubits durch Teleportation instantan übertragen werden, käme dies einem überlichtschnellen Informationsgewinn gleich, was die millionenfach bewiesene Relativitätstheorie kategorisch ausschließt). Wie in Abschn. 3.6 noch gezeigt wird, ist das No-Cloning-Theorem konsistent mit der Speziellen Relativitätstheorie. Nicht zuletzt aufgrund seiner Gültigkeit reagieren Quantensysteme auf äußere Einwirkungen extrem empfindlich und können sehr leicht zerstört werden. Aus diesem Grund haben auch Hackerangriffe der üblichen Art keinerlei Chance: Firewalls knacken, Trojaner einschleusen, Viren streuen etc. – das geht so nicht bei einem Quantencomputer!

Quantenrepeater

Das No-Cloning-Theorem stellt dann auch die eigentliche Herausforderung in der Entwicklung eines Quantennetzwerks dar und besitzt weitreichende Folgen für die

Quanteninformatik. So können keine klassischen Fehlerkorrektursysteme angewendet und vor allem keine herkömmlichen Repeater eingesetzt werden. Es müssen vielmehr spezielle Quantenrepeater-Systeme entwickelt werden. Für ein Quantennetzwerk sind grundsätzlich zwei Sorten von Qubits nötig: Einerseits „ruhende", sogenannte stationäre Qubits (etwa für Quantenspeicher) und andererseits mobile Qubits als Überträger der Quanteninformation zu anderen Knotenpunkten. Für eine funktionierende Teleportation müssen alle – ruhende wie mobile – Qubits miteinander verschränkt werden. Sie werden sozusagen zu einem einzigen Quantenobjekt zusammengespannt, das wie durch Zauberei mit sich selbst verbunden ist. Das elementare Problem dabei ist das Herstellen von verschränkten Systemen über größere Distanzen. Dazu ist zwingend ein Quanteninternet notwendig. Zu seiner Realisierung muss das bestehende Glasfasernetz grundlegend modifiziert werden und mit zahllosen Quantenrepeater-Nodes (Knotenpunkten) versehen werden. Der Fachausdruck hierfür ist „Entanglement Swapping". Damit gelingt es, die Verschränkung vieler kleinerer Teilsysteme auf große Distanzen auszudehnen. Wegen der Empfindlichkeit der Quantenzustände (No-Cloning-Theorem) gilt die technische Realisierung jedoch als äußerst schwierig, obwohl die prinzipielle Funktionsweise unter Laborbedingungen bereits bewiesen werden konnte.

Skalierbarer Netzausbau

Im Lastenheft der Entwickler stehen zahlreiche Forderungen zum evolutionären Netzausbau (Skalierung). Dazu einige Inhalte: die Projekte sollen grundsätzlich auf einheitliche Standards und Protokolle abzielen, die international tragfähig sind. Dabei geht es insbesondere um die Entwicklung geeigneter Repeatersysteme.

Die Schlüsselbausteine hierzu müssen auf Basis der jeweiligen Repeaterarchitektur konzipiert werden und für folgende Anforderungen ausgelegt sein: Speicherung von Quantenzuständen mit hoher Fidelity (Übereinstimmung zwischen Eingangs- und Ausgangszustand), Reinigung verschränkter Zustände (Verschränkungsdestillation, Abschn. 2.8), Implementierung quantenlogischer Gatter, Konversion zwischen mobilen und stationären Qubits; ferner geeignete Kommunikationsprotokolle und adressierbare Quantenregister zum Transfer von Quanteninformation. Für die Realisierung dieser Komponenten kommen verschiedene Ansätze zum Tragen, die alle Gegenstand der aktuellen Forschung sind. Zu den bislang aussichtsreichsten physikalischen Ressourcen zählen neben Photonen, Ionen und ultrakalten Atomgasen auch Halbleiterstrukturen, Supraleiter, Quantenpunkte sowie Hybridsysteme. Besonderes Augenmerk gilt auch der Verwendung neuer Materialien wie etwa Graphen, ebenso Farbzentren in diamantartigen Gitterstrukturen mit vielversprechenden Kohärenzeigenschaften. Nähere Details hierzu werden im Folgenden noch weiter ausgeführt. Ganz allgemein ist die Entwicklung eines Quantennetzwerks eng mit der Realisierung von Quantencomputern verbunden, wobei letztere in technologischer Hinsicht die noch viel größere Herausforderung darstellen.

2.2 Netzwerktopologie

Der heute schon so fantastischen Welt des Internets liegen ausgeklügelte Netzwerksysteme zugrunde, über welche digitale Informationen weltweit zwischen verschiedenen Knoten übertragen werden. In einer hierarchischen Anordnung werden hierbei Provider-, Firmen- und Forschungsnetzwerke über Backbones vorwiegend durch

faseroptische Elemente zu einem globalen Web verbunden. Entsprechende Technologien für ein Quanteninternet stellen eine enorme Herausforderung dar. Ein Erfolg versprechendes Konzept ist ein Netzwerksystem aus Quantenspeichern, den stationären Netzwerkknoten (Nodes), zwischen denen Quanteninformation über mobile Qubits (zumeist Photonen) über weite Strecken reversibel ausgetauscht wird.

Die grundlegende Infrastruktur eines Quantennetzwerks verhält sich durchaus analog zum klassischen Gegenstück (Abb. 2.1). Die eigentlichen Operationen werden an den sogenannten Endnodes (Endknotenpunkten) ausgeführt, wobei man ein System anstrebt, in dem diese miteinander durch Verschränkung verbunden werden. Die Endnodes bestehen im einfachsten Fall aus einem einzelnen Qubit, welche mit zunehmender Anzahl

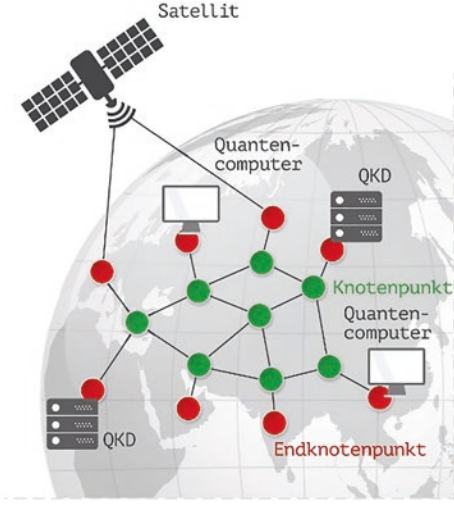

Abb. 2.1 Quanteninternet-Topologie. Es ist charakterisiert durch ein System von Quantenknoten, das einen durchgehenden Quantenkanal End-to-End herstellt

an Qubits immer mehr einem leistungsfähigen Quantenprozessor entsprechen. Für einfachere Anwendungen wie der Quantenschlüsselverteilung (QKD) sind die Endnodes mit vergleichsweise simplen Devices ausgestattet. Allerdings erfordern einige Protokolle viel kompliziertere Nodes. Diese Systeme erlauben dann schon eine größere Prozessorleistung und können auch als Quantenspeicher verwendet werden. Ebenso können auf ihnen quantenlogische Operationen ablaufen. Um Quanteninformation von einem Node zum anderen zu transportieren, sind spezielle Kommunikationslinien, die Quantenkanäle nötig. Hier besteht naturgemäß die Tendenz, möglichst die bereits existierenden Glasfaserverbindungen nutzen zu können, was für die QKD auch ausreichen dürfte. Um eine effiziente Kommunikation zu gewährleisten, benötigt man – analog dem klassischen Internet – Router und Switches, um die Qubits zu den gewünschten Endnodes weiterzuschalten. Die Switches müssen allerdings in der Lage sein, Quantenkohärenz für einen relevanten Zeitraum sicherzustellen (der im Allgemeinen sehr kurz ist), wodurch sich ihre technische Realisierung ungleich schwieriger gestaltet als bei heutigen Standardgeräten.

Freiraumnetzwerke operieren ähnlich wie Fiberglasnetzwerke, benutzen jedoch eine direkte Visierline (Freistrahlstrecke) zwischen Sender und Empfänger, etwa eine direkte Laserverbindung. Wie aktuell durch das QUESS-Experiment bewiesen wurde, können speziell auch Quantensatelliten eingesetzt werden, welche über extraterrestrische Quantenkanäle kommunizieren. Diese bieten vor allem auch die Möglichkeit, eine direkte Verschränkung ohne Quantenrepeater über größere Entfernungen herzustellen. In Zukunft können sie auch eine wichtige Rolle spielen beim Verlinken von kleineren, bodenbasierten Netzwerken über größere Distanzen. Mit einem global verteilten Satellitensystem und entsprechender Logistik ist auch eine

weltweite Vernetzung denkbar. Rein theoretisch können Quantensatelliten kurzzeitig selbst als Quantenrepeater fungieren.

Solch ein Netzwerk könnte entweder als Quantennetzwerk für Computing oder als eines für Kommunikation ausgelegt sein. Im ersten Fall wären verschiedene Quantenprozessoren zu einem Quantencomputer-Cluster verbunden. Man spricht dann von Networked beziehungsweise Distributed Quantencomputing. In diesem Fall werden weniger leistungsstarke Quantenprozessoren verlinkt, wodurch sich jedoch insgesamt ein viel leistungsfähigerer Quantenrechner ergibt. Dies verhält sich analog zu klassischen Computern, die zusammengeschaltet einen Cluster bilden. Networked Quantencomputing wird oft auch als möglicher Weg für die Realisierung eines skalierbaren Quantencomputers betrachtet, denn mehr und mehr Quantenprozessoren zusammen können naturgemäß die Rechenpower theoretisch immer weiter steigern. Bei den bisherigen Ansätzen zum Networked Quantencomputing sind die individuellen Prozessoren oftmals nur durch winzig kleine Distanzen voneinander getrennt.

Ein Quantennetzwerk für Kommunikation bietet dagegen unter anderem die Möglichkeit, Qubits auch über große Entfernungen von einem Quantenprozessor zum anderen zu übertragen (Long Distance Q-Communication). Auf diese Weise können – analog dem klassischen Internet – kleinere lokale Netzwerke zu einem größeren zusammengeschaltet werden, wodurch letztlich ein globales Quanteninternet vorstellbar wird. Ein solches würde verschiedenste Applikationen gestatten, wobei die Leistungsfähigkeit neben der Prozessorfähigkeit der Nodes maßgeblich dadurch bestimmt wird, in welchem Ausmaß Verschränkung erzeugt und aufrechterhalten werden kann.

2.3 Quantenschnittstellen

Bereits das heutige Internet verschickt eine ungeheure Datenmenge vorwiegend über Lichtwellenleiter um den Globus. Die Quantennetzwerke der Zukunft könnten noch um vieles leistungsfähiger sein, da sie Quantenbits austauschen, die viel mehr Information tragen und übertragen können. Dafür notwendig sind allerdings – als ganz wesentliche Forderung – Bauelemente, mit denen die Quanteninformation von einem Quantenspeicher auf mobile Qubits in reversibler Weise übertragen werden kann. Der Begriff Schnittstelle bezeichnet allgemein zentrale Übergabepunkte, die Daten zwischen Rechnern und externen Geräten übertragen. Mit einer Quantenschnittstelle (Quanten-Interface) sei hier speziell ein Device bezeichnet, das stationäre Qubits mit mobilen Qubits verbindet, um auf diese Weise einen Quantenkanal zwischen weit entfernten Knotenpunkten herzustellen. Obwohl die Vorgänge in Wahrheit sehr komplex sind, lässt sich das (in starker Vereinfachung und sehr anschaulich) auch mit bekannten Begriffen beschreiben: An einem Node 1 ist die Quanteninformation in einem stationären Quantenspeicher (Q-Memory) abgelegt. Sodann wird sie „ausgelesen“ und auf ein mobiles Qubit übertragen. Dieses bewegt sich anschließend mit Lichtgeschwindigkeit zu Node 2 und schreibt die Quanteninformation in ein dort vorhandenes Q-Memory. Die beiden Nodes werden auf diese Weise miteinander verschränkt. Dabei wird die Quanteninfo nicht kopiert, sondern die erzeugte Verschränkung ist ein einziger gemeinsamer Zustand, sodass es zu keiner Verletzung des No cloning – Theorems kommt. Dieser Vorgang lässt sich beliebig in beiden Richtungen wiederholen (Reversibilität). Was sich hier jedoch so einfach anhört und in der normalen IT ein

Standardverfahren ist, gestaltet sich für die Belange eines Quantennetzwerks ungleich schwieriger. Daher wird weltweit intensiv daran geforscht, wie man effiziente Quantenschnittstellen implementieren kann. Wesentlich dabei ist auch, wie präzise und kontrolliert man die Operationen durchführen kann, ohne die dabei auftretenden äußerst sensiblen Quantenzustände zu zerstören.

Kardinalproblem Dekohärenz

Wie später noch gezeigt wird (Abschn. 2.5, 3.1 und 3.3), unterliegen Quantenobjekte dem Superpositionsprinzip, das die Grundlage der Verschränkung bildet. Wenn Berge und Täler zweier Wellen eine feste Phasenbeziehung zueinander besitzen, (siehe auch Abschn. 3.2) oder sich gesetzmäßig zeitlich ändern, nennt man sie kohärent, das gilt genauso für die Wellenfunktionen, welche Quantenzustände beschreiben. Da Quantensysteme jedoch unweigerlich mit den Freiheitsgraden ihrer Umgebung in Wechselwirkung treten, geraten die Phasenbeziehungenvabstände der Wellenbend -einan aus dem Gleichtakt und die Kohärenz geht lokal verloren. Durch diese Dekohärenz verliert die Quantenwelt ihre typischen Eigenschaften und geht in den Bereich der klassischen Physik über. Technologisch bedeutet das, dass man extrem Vorsicht gegenüber äußeren Einflüssen walten lassen muss, das heißt, es müssen Systeme entwickelt werden, welche die Kohärenz ausreichend lange gewährleisten, um daran quantenmechanische Operationen durchführen zu können. Darüber hinaus müssen die Quantensysteme andererseits auch manipuliert, gemessen und ausgelesen werden. Hierin liegt die eigentliche technologische Herausforderung in der Entwicklung eines Quantennetzwerks.

2.3.1 Nobelpreisgekrönte Vorarbeiten

Eine wichtige Basis für die Quanteninformationstechnik und speziell für Quantenschnittstellen bildeten die Arbeiten von David Wineland und Serge Haroche, die dafür 2012 mit dem Physik-Nobelpreis ausgezeichnet wurden. Sie liefern bahnbrechende experimentelle Methoden zur Messung und Manipulation von Quantensystemen.

Laserkühlung
Atome sind bekanntlich winzig kleine Objekte. Um sie kontrollieren und manipulieren zu können, muss man sich besonderer „Tricks" bedienen. Dazu kann man etwa ein sehr starkes Vakuum herstellen, wodurch zwar der Druck gegenüber der Umgebung praktisch auf null absinkt, aber immer noch einzelne Atome vorhanden sind, die sich dann gut fangen lassen, wenn man ihnen eine Falle stellt. Dabei wird zum Beispiel eine Spannung zwischen speziell angeordneten Elektroden angelegt. Daraufhin entstehen Potenzialmulden, in denen die Atome dann genauso gefangen bleiben wie ein Golfball im Loch. Darin lassen sich die Teilchen auch für längere Zeiträume einsperren. Um besonders gute Quantenkohärenz zu erlangen, ist es dazu noch notwendig, die Teilchen sehr stark abzukühlen, wodurch sich ihre thermische Bewegung immer weiter reduziert. Hier kommt der Beitrag von Wineland ins Spiel: Auch sehr nahe am absoluten Nullpunkt (−273,15 °C) schwingen die Teilchen immer noch, allerdings nicht in beliebiger Art, sondern nur in bestimmten Auslenkungen, die nach den Gesetzen der Quantenmechanik bestimmt sind. Durch eine spezielle Art der Bestrahlung ist es dann möglich, die Teilchen weiter abzubremsen und in den niedrigstmöglichen Energiezustand zu versetzten. Dazu wird ein Laserstrahl auf das entgegenlaufende Atom gerichtet, wodurch es in einen angeregten

Zustand versetzt wird. Bei der anschließenden Emission erzeugt das emittierte Lichtquant einen Rückstoß, was die Bewegung des Atoms bremst. Das heißt, es verliert Energie in Richtung des Laserstrahls, dem es entgegenläuft. David Wineland perfektionierte diese Technik und zeigte, dass man mit gezielten Laserpulsen Quantenobjekte mit hoher Präzision kontrollieren, manipulieren und auslesen kann.

Hohlraumresonatoren
Von Serge Haroche stammt beispielsweise die Idee eines speziellen optischen Resonators. Darunter kann man sich zwei Spiegel vorstellen, zwischen denen einzelne Photonen hin- und herreflektiert werden. An diesem Pingpongspiel dürfen jedoch nur solche Photonen teilnehmen, bei denen ein Vielfaches ihrer halben Wellenlänge genau in den Abstand der Spiegel passt. Während bei Umgebungstemperatur unzählige Schwingungsarten im Resonator möglich sind, existieren nahe des absoluten Nullpunkts nur noch sehr wenige. Unter diesen exotischen Voraussetzungen kann man speziell präparierte Atome in den Resonator einbringen, wodurch eine spezielle Wechselwirkung zwischen dem Atom und dem elektromagnetischen Feld des Lichts eintritt.

Cavity-QED Die Quantenphysik unterteilt sich grundsätzlich in Quantenmechanik und Quantenfeldtheorien. Davon ist die bekannteste die Quantenelektrodynamik (QED), welche den Elektromagnetismus als von Photonen vermittelte Austauschwechselwirkung erklärt. Die Hohlraum-Quantenelektrodynamik (Cavity-QED) untersucht die Wechselwirkung des Lichts, das in einer reflektierenden Kavität eingeschlossen ist, also zum Beispiel in einem optischen Resonator. Mit solch einer Kavität lässt sich prinzipiell eine Quantenschnittstelle (Quanten-Interface)

oder sogar ein Quantencomputer konstruieren. Wenn sich das Licht im Hohlraum in Resonanz mit einem atomaren Übergang befindet, kommt es zu einem kohärenten Austausch mit dem Feld des Hohlraums. Dabei kann eine Verschränkung zwischen Atomzustand und dem Hohlraumfeld entstehen. An dieser Entwicklung tragen die Physiker Wineland und Haroche ganz maßgeblichen Anteil. Mithilfe der Cavity-QED lässt sich nun das Prinzip einer Quantenschnittstelle sowie deren Kopplung in starker Vereinfachung skizzieren (Abb. 2.2).

Am Knotenpunkt 1 in Abb. 2.2 ist ein einzelnes Atom in einer Kavität gefangen und befindet sich in einem mittleren Energiezustand. Danach erfolgt eine Anregung durch einen Laser, wodurch der Quantenzustand des Atoms kurzfristig den obersten Energiezustand einnimmt.

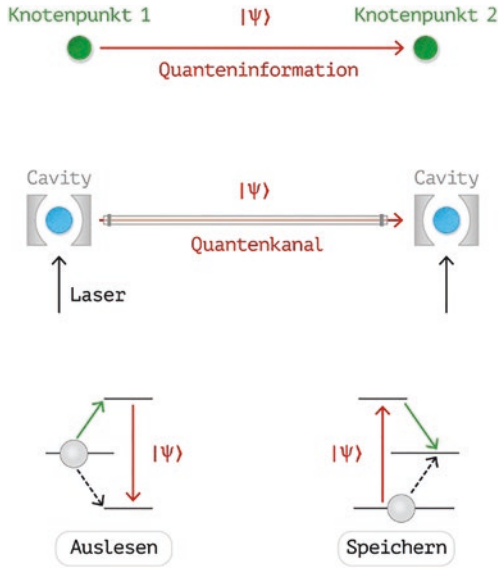

Abb. 2.2 Verschränkung von Knotenpunkten via Quanten-Interface, Prinzip

Unmittelbar danach „fällt“ das Atom auf das niedrigste Niveau, dabei entsteht ein Quantenzustand $|\psi\rangle$, der sich auf ein Photon (mobiles Qubit) überträgt und über eine Faserleitung zum baugleichen Knoten 2 transferiert wird. Dort ist das Atom im niedrigsten Zustand, erfährt eine Anregung durch das einlaufende Photon, geht kurzfristig in den höheren Zustand über und fällt sodann auf das mittlere Niveau zurück. Auf diese Weise wird ein verschränkter Kanal zwischen Knoten 1 und Knoten 2 erzeugt. Anschaulich gesprochen entspricht dies einem reversiblen Speicher- und Ausleseprozess von Quanteninformation über räumlich entfernte Knotenpunkte.

2.3.2 Implementierungen (Beispiele)

Um dem Leser einen Eindruck von der zukünftigen „Quanten-IT“ zu verschaffen, seien hier einige wenige Implementierungsversuche von Quantenbauelementen genannt, welche die Möglichen der exotischen Technologie wie auch ihre Schwierigkeiten zumindest erahnen lassen.

Atome in der Falle
Eine Forschergruppe um Rainer Blatt in Innsbruck konnte bereits vor Jahren den Prototyp einer elementaren und weitgehend gut kontrollierbaren Quantenschnittstelle implementieren. Dazu wird ein geladenes Atom, konkret zum Beispiel ein Calcium-Ion, in einer sogenannten Paul-Falle gefangen und zwischen zwei stark reflektierenden Spiegel platziert, also in einem optischer Resonator. Ein Laser regt das Ion an und verschränkt es mit den Photonen des Lasers. Über die Frequenz und Amplitude des Lasers lässt sich der Verschränkungsgrad gezielt beeinflussen, wodurch sich die Ausbeute an verschränkten

Photonen optimal einstellen lässt. Wie kann man sich diesen Vorgang, der einem Einschreiben der Quanteninformation vom einem stationären Qubit auf ein mobiles Qubit entspricht, konkret vorstellen? Dazu ein anschaulicher Vergleich: nehmen wir an, dass die Elektronen nach dem bohrschen Atommodell um den Atomkern kreisen (freilich ist das nur eine praktikable Hilfsvorstellung, die physikalisch streng genommen ziemlich falsch ist). Ferner entspreche jeweils eine von zwei möglichen Elektronenbahnen den Zuständen 0 beziehungsweise 1. Die Überlegenheit von Quantenprozessoren besteht nun gerade darin, dass eine Superposition der beiden Zustände erzeugt wird, also sozusagen 0 und 1 zugleich. Diese Anregung entspricht gewissermaßen einer Überlagerung beider Elektronenbahnen. Der angeregte Zustand wird daraufhin mit dem Polarisationszustand des Laserphotons verschränkt, das heißt, der Gesamtzustand kann nicht mehr in einzelne Subzustände separiert werden, er ist nur noch gesamtheitlich zu beschreiben. Wenn sich nun das mobile Qubit durch eine Faserleitung zu einer zweiten Schnittstelle bewegt, dann „trägt" es die gemeinsame Quanteninformation, die durch die Verschränkung zwischen Atom und Photon bestimmt ist, zu diesem zweiten Knotenpunkt hinüber.

Erstes Prototyp-Netzwerk

Physiker am Max-Planck-Institut in Garching um Gerhard Rempe konnten bereits 2012 ein elementares Quantennetzwerk aus 2 Nodes demonstrieren, und zwar als Kopplung zweier Hohlraumresonatoren. Das Besondere dabei war die Verschränkung von massiven Objekten, in diesem Fall von Atomen. Anschaulich gesprochen entspricht dies einer Art Nanoschaltsystem aus Atomen, das wie ein Transistor in einem Mikroprozessor agiert. Durch die Verschränkung der Nodes arbeitet das

System allerdings über größere Entfernungen wie ein einziger synchronisierter Schalter, der als Datenträger und Rechenwerk fungiert. Zunächst mussten die Atome im Resonator über längere Zeit festgehalten werden. Via fein abgestimmter Laserstrahlen wurden die Atome zum Aussenden von Lichtquanten gebracht. Auf diese Weise gelang es, die in den Photonen eingeschriebene Quanteninformation über längere Zeit reversibel zu speichern und auszulesen Aufgrund dieses symmetrischen Verhaltens erscheint das System gut geeignet für Netzwerke aus vielen Resonatoren: Ähnlich wie in Abb. 2.2 erzeugt Node 1 eine Verschränkung zwischen dem Atomzustand und dem Polarisationszustand des emittierten Lichtquants Diese Verschränkung überträgt sich bei der Absorption auf das Atom bei Node 2. Auf diese Weise konnte die Verschränkung von Atomen über eine 60 m lange Glasfaserverbindung demonstriert werden. Die Verschränkungszeit lag zwar nur bei ca. 100 μs, war jedoch um vieles länger als für die Erzeugung des Kanals benötigt wurde. Mittlerweile ist den Forschern auch die Übertragung von Quantenzuständen auf ultrakalte Atomgase beziehungsweise Bose-Einstein-Kondensate (BEK) geglückt. Ebenso war es bereits möglich, auf den Resonatoren quantenlogische Gatteroperationen durchzuführen, was einen wichtigen Schritt in Richtung Networked Quantencomputing bedeutet. Unter einem BEK versteht man einen größeren Atomverband, der unterhalb einer sehr tiefen Sprungtemperatur komplett in einen kollektiven Quantenzustand übergeht und einem extremen Aggregatzustand entspricht. Der gesamte Atomverband wird dann durch eine einzige Wellenfunktion beschrieben und verhält sich ideal kohärent. Das Verhalten von BEK ist eng mit dem von Supraleitern verwandt, deswegen könnte man mit solchen kontrollierten ultrakalten

Atomgasen noch ungeklärte Vorgänge in Supraleitern simulieren und so im Detail erforschen.

Quantenchips und Diamanten

Am renommierten amerikanischen MIT arbeitet man in Kooperation mit der Harvard-Universität an einer neuartigen Verbindung von Quantenkommunikation und traditioneller Chiptechnik. Hauptziel ist unter anderem die Entwicklung einer skalierbaren Quantenschnittstelle. Wie dargelegt, dreht sich dabei alles um die Frage, wie man Atome kontrolliert einfangen und manipulieren kann. Dies kann auch auf „natürliche" Weise erfolgen, etwa durch diamantartige Strukturen, das heißt eine Atomfalle in einem modifizierten Kohlenstoffgitter. Ein bereits realisiertes Bauelement besteht aus sogenannten NV-Zentren, die als Quantenspeicher fungieren[1]. Jedes NV-Zentrum speichert die Quanteninformation in einer Kombination aus Elektronenspin und Kernspin. Verschiedene weitere Spinzustände werden zur Fehlerkorrektur benötigt. Ein spezieller integrierter Schaltkreis routet die NV-Photoemission, einerseits für Nachweisverfahren, andererseits für die Verschränkung mit mobilen Qubits für das Netzwerk. NV-Zentren zeigen ganz allgemein gute Eigenschaften für einen Quantenspeicher, etwa lange Spin-Kohärenzzeiten (1 s – das ist in der Quanten-IT schon eine Ewigkeit), ebenso lassen sich 2-Qubit-Gatter und Quantenfehlerkorrektursysteme realisieren. Bereits 2015 konnte die Verschränkung von zwei NV-Zentren über 1 km Entfernung demonstriert werden als wichtiger Schritt in Richtung Quantenschnittstelle sowie für das Networked Quantenprocessing.

[1]In einem NV-Zentrum sind zwei benachbarte Plätze im Diamantgitter nicht mit Kohlenstoffatomen belegt, sondern mit einem Stickstoffatom (N) und einer Leerstelle oder Vakanz (V).

Hybride Quantenknoten

Wie die bisherigen Beispiele zeigen, gibt es unterschiedliche Arten von Implementierungen.

Ähnlich dem heutigen Internet, das ja ebenso eine Unzahl verschiedenartiger Geräte vernetzt, wird auch ein Quantennetzwerk verschiedenste Quanten-Devices verbinden. Deshalb sind auch viele Forscher der Ansicht, dass die Zukunft in hybriden Netzwerkknoten bestehen wird und nicht nur in der Verbindung völlig gleichartiger Schnittstellen. Da einige Node-Implementierungen für bestimmte Aufgaben besser geeignet erscheinen als andere, würde ein Quantennetzwerk davon profitieren, auf verschiedene Arten von Knotenpunkten zugreifen zu können. Ultrakalte Atomgase können zum Beispiel mühelos Qubit-codierte Photonen erzeugen, dotierte Kristalle eignen sich dagegen gut für das langfristige Speichern von Quanteninformation. Verschiedene Knoten emittieren und verarbeiten Photonen jedoch bei unterschiedlichen Wellenlängen und Bandbreiten, was einen Qubit-Transfer zwischen ihnen erheblich erschwert. Eine Gruppe um Hugues de Riedmatten (ICFO Barcelona) konnte bereits eine elementare hybride Knotenverbindung demonstrieren. Konkret fungierte eine lasergekühlten Wolke aus Rubidium-Atomen als stationäres Qubit, das in ein einzelnes mobiles Qubit, und zwar ein Photon der Wellenlänge von 780 nm codiert wurde. Dabei steht nm für Nanometer, was einem Milliardstel Meter entspricht. Der Transfer erfolgte zwischen zwei benachbarten Laborstationen, wobei die Wellenlänge auf 606 nm reduziert wurde, sodass es mit dem aus dotierten Kristallknoten aufgebauten Empfänger interagieren konnte. Dabei wurde das Photon zwischenzeitlich auf „IT-übliche“ 1552 nm konvertiert, um zu zeigen, dass eine prinzipielle Kompatibilität mit der herkömmlichen Telekommunikationsinfrastruktur besteht. Diese elementare Demonstration der Interaktion

verschiedener Quanten-Nodes sowie die Nutzung ihrer jeweiligen Vorteile sehen die Forscher als wichtigen Markstein für die Entwicklung eines Quantennetzwerks auf Basis einer faseroptischen Struktur.

2.4 Anwendungsbeispiele

Die Gesichtspunkte eines Quanteninternets sind so vielfältig wie unvorhersehbar, sodass hier noch kein Überblick möglich ist, welcher einen Anspruch auf Vollständigkeit erheben könnte. Wie immer zu Beginn einer völlig neuen technischen Entwicklung kann niemand seriös vorhersagen, was genau kommen wird. Oft genug mögen dabei auch die Vorstellungen von Physikern und Technikern auseinandergehen. Dennoch lassen sich wichtige Grundfunktionalitäten heute schon erkennen und zeitnahe Entwicklungen antizipieren (siehe hierzu auch Abschn. 2.9).

2.4.1 Datenschutz, Koordination und Processing

Die im Augenblick wichtigste und am weitesten vorangeschrittene Applikation des Quanteninternets ist die Quantenschlüsselverteilung, englisch Quantum Key Distribution (QKD). Gerade in Verbindung mit Protokollen, welche auf dem Effekt der Verschränkung beruhen, ist diese Art der Quantenkommunikation in Verbindung mit klassischen Verfahren eine sehr zukunftsträchtige Sicherheitstechnologie. Diese Einschätzung wird durch die Tatsache gestützt, dass erste QKD-Systeme bereits auf dem Markt sind. Dies betrifft sowohl Geräte, die eine abhörsichere Punkt-zu-Punkt-Verbindung herstellen, als auch Produkte, die auf den Einsatz in echter Netzwerkumgebung abzielen.

Seit Jahren laufen zudem in diese Richtung gehende wissenschaftliche Großprojekte. Weil eine Direktverschränkung im Moment über große Distanzen noch nicht realisierbar ist, haben sich die bisherigen Bemühungen unter anderem auf die Demonstration der Infrastruktur und die Funktionsweise der Geräte konzentriert. Man spricht hier von „Stufe 0“ -QKD-Netzwerken auf Basis von „Trusted Repeaters“, die anfangs in Laborstudien getestet, mittlerweile jedoch auch in realen Netzwerken im städtischen Bereich implementiert wurden. Als Paradebeispiele für derartige metropolische Netzwerke sind die QKD-Netzwerke in Japan und China zu nennen, worauf noch näher eingegangen wird (Abschn. 2.4.2 und 2.4.3).

Größere Quantennetzwerke, die außerhalb der Laborumgebung mehrere Qubits an den Endnodes via Verschränkung verlinken, sind dagegen noch nicht realisiert worden. Natürlich ist diese Möglichkeit die viel schwierigere, aber auch umso spannendere Variante. Zu den bislang bekannten Anwendungsmöglichkeiten zählen beispielsweise: Koordination verteilter Systemprobleme, Taktsynchronisation, Positionsverifikationen sowie Standlinienverlängerungen für Teleskope (zwecks höherer Auflösung). Ein Beispiel ist etwa die Synchronisation von Atomuhren. Schon heute erfolgt die präzise Zeiterfassung international durch ein globales Netzwerk von Atomuhren, die per Satellit synchronisiert werden. Mittlerweile gibt es ultrapräzise optische Atomuhren, die auf das Zeitalter des Universums gerechnet (ca. 13,8 Mrd. Jahre) weniger als 1 s falsch gehen. Um diese unglaubliche Präzision jedoch nutzen beziehungsweise sie miteinander vergleichen zu können, reicht eine Satellitenverbindung nicht aus, weil die dadurch entstehenden „Rauscheffekte“ diese Vorzüge zunichtemachen. Wie Forscher bereits demonstrieren konnten, lassen sich optische Uhren via Glasfaserkabel verschränken Die ultimative Lösung wäre

ein globales Quanteninternet optischer Atomuhren, was – anschaulich gesprochen – dazu führt, dass ultrapräzise Uhren auf der ganzen Welt im völligen Gleichtakt ticken. Dabei profitiert ein Quantennetzwerk von der Tatsache, dass es zwar nicht schneller als das Licht kommunizieren, sich aber sehr wohl überlichtschnell koordinieren und synchronisieren kann. Gerade letzteres (welches in einem klassischen Internet völlig unmöglich wäre) macht die Quantenkommunikation so wertvoll und interessant. Schon heute treten in klassischen Netzwerken unzählige Koordinationsprobleme auf, die künftig viel schnellere und effizientere Lösungen erforderlich machen. Hierzu nutzen Quantenbits aus, dass sie via Verschränkung automatisch und instantan aneinander gekoppelt sind. Ebenso kann der Ausgangszustand eines Quantenprozessors durch Quantenteleportation zu einem anderen Quantencomputer transferiert werden, welcher diesen als Input nutzt. Auf diese Weise entsteht eine viel höhere Datenrate.

Eine damit verbundene wichtige Anwendung ergibt sich im Distributed beziehungsweise Networked Quantencomputing, wo sozusagen das gesamte Netzwerk zu einem einzigen Computer verschmilzt. Bereits in kleinem Maßstab als Miniquantennetz demonstriert, ließe sich das System theoretisch auch auf größere Distanzen ausweiten. Damit verbindet sich der Vorteil, dass komplexere Prozessoren, die an verschiedenen Punkten der Erde mit unterschiedlichster Technologie gefertigt wären, sich zu einem einzigen Quantengroßrechner zusammenspannen ließen. Schon jetzt zeichnet sich ab, dass auch für Quantencomputer ein modularer Aufbau viele Vorteile bietet. Dazu werden viele Quantenprozessoren, die jeweils nur eine begrenzte Zahl von Qubits speichern und verarbeiten können, durch Quantenkanäle miteinander vernetzt. Nach einer ungefähren Schätzung wäre ein solches „Kombisystem“ ab einer Anzahl von etwa 60 Qubits imstande,

bestimmte Probleme hoher Komplexität schneller zu lösen als klassische Computer. Dabei gilt es zu beachten, dass jedes zusätzliche Qubit die Rechenleistung exponentiell (!) ansteigen lässt. Genauso wie beim klassischen Computing lässt sich das System durch Vernetzung weiterer Quantencomputer theoretisch beliebig hochskalieren. Die große Leistungsfähigkeit künftiger Netzwerke von Quantencomputern wäre durch zwei Faktoren bestimmt:

1. Welche Probleme können von Quantencomputern überhaupt bewältigt werden und
2. wie könnte man die (womöglich sehr unterschiedlichen) Fähigkeiten und Konzepte einzelner Rechner so verknüpfen, dass damit noch viel komplexere Probleme lösbar werden?

Wie noch eingehend besprochen wird, liegt das heute bekannte Potenzial von Quantenrechnern außer bei Such-, Optimierungs- und Logistikalgorithmen primär bei Berechnungen mit explosiv anwachsender Zahl von Rechenoperationen sowie in der Simulation von Atom- und Molekülstrukturen. Gerade letzteres könnte, auch abseits der Forschung, eine nachhaltige Auswirkung auf die ökologische und ökonomische Entwicklung der Menschheit haben. Angesichts der obigen Ausführungen kann man die Anwendungsmöglichkeiten des Quanteninternets in vier Grundfunktionalitäten sehen:

1. abhörsichere Kommunikation durch QKD,
2. überlichtschnelle Synchronisation und Koordination von Quantensystemen,
3. Quantenkommunikation zwischen Quantenprozessoren im Sinne von Networked Computing beziehungsweise als modularer Quantencomputer,
4. Multiuserzugriff auf eine Quanten-Cloud.

Unter dem letzten Punkt ist der Zugriff auf leistungsfähige Cloud-Quantencomputer für viele Menschen auf der ganzen Welt zu verstehen. Diese Zentralrechner, die naturgemäß im Besitz einschlägiger Firmen beziehungsweise Institutionen wären, können selbst wieder als lokale Quantennetzwerke implementiert sein. Bezüglich Sicherheitsfragen setzt das Quanteninternet in jedem der genannten Aspekte völlig neue Standards.

2.4.2 Tokyo-QKD-Netzwerk

In Ergänzung zur üblichen Sicherheitstechnik stellt die Quantenkryptografie eine hochsichere Alternative dar. Derartige Systeme wurden vor allem seit den 1990er Jahren verstärkt entwickelt und ab den 2000ern aus der Labor- in eine echte Netzwerkumgebung entlassen.

In sogenannten QKD-Feldversuchen wurde getestet, wie weit diese Technik praxistauglich ist beziehungsweise für verschiedene Applikationen nutzbar gemacht werden kann. Im Jahr 2010 nahmen neun Organisationen aus Japan und Europa am bis dahin größten QKD-Test teil. Dieser sollte vor allem demonstrieren, wie gut diese High-End-Sicherheitstechnik kommerziell genutzt werden kann. Dazu zählen etwa sichere TV-Konferenzen oder Handytelefonie. Während in früheren Versuchen die Bitraten nur bei wenigen kbit/s lagen und die Entfernung auf etwa 10 km beschränkt war, konnten nun wesentlich höhere Bitraten über Entfernungen um die 100 km demonstriert werden. Aufgrund der hohen Erzeugungsrate war auch eine Verschlüsselung in Echtzeit möglich. Das Tokyo-QKD besteht aus Teilen des früheren NICT-Testnetzes und hat vier Hauptzugangspunkte, die durch kommerzielle Glasfaserleitungen verbunden sind. Diese befinden sich in den bis zu 400 km voneinander entfernten Orten

Koganei, Otemachi, Hakusan und Hongo auf der japanischen Hauptinsel Honshu. Die großen Distanzen innerhalb dieses sogenannten metropolischen Netzwerks führen zu der Schwierigkeit, dass die langen Fiberglasleitungen erhebliche Verluste bewirken (etwa 0,3–0,5 dB/km). Die Einheit Dezibel (dB) ist ein logarithmischer Verhältniswert für Pegel und Maße. Bei Licht bezieht sich diese Angabe auf die Helligkeit und damit die Lichtintensität, welche im Quantenmodell der Anzahl der Photonen entspricht. Durch optische Schwächung (Intensitätsverlust), Umgebungseinflüsse beziehungsweise „Crosstalk" durch benachbarte Fiberleitungen im selben Kabel treten deutliche Rauscheffekte (Noise) auf. Es ist demnach einiges an technisch-physikalischem Know-how gefragt, um die Verluste möglichst gut zu kompensieren. Dieses kam auf japanischer Seite von den Firmen NEC, NTT und Mitsubishi, aus Europa nahmen Toshiba Europe UK sowie ID Quantique aus der Schweiz teil. Weitere Unterstützung kam durch das „All Vienna"-Team, bestehend aus dem Austrian Institute of Technology (AIT), dem Institut für Quantenoptik und Quanteninformation (IQOQI) sowie der Universität Wien. Alle Organisationen benutzten ihre selbst entwickelten Quanten-Devices unterschiedlichster Art, sodass insgesamt ein Node-Mischtyp auf Basis von (hauptsächlich) Trusted Repeaters entstand.

Trusted Repeater

Wie angesprochen, erfordert die Einrichtung eines Quanteninternets eine direkte Verschränkung zwischen allen Endnodes, was letztlich die Entwicklung spezieller Quantenrepeater erforderlich macht. Da deren praxistaugliche Realisierung jedoch noch einige Zeit benötigen dürfte, werden im Moment als Zwischenschritt größere Netzwerksysteme auf Basis von sogenannten Trusted Repeaters implementiert. Ein solches System lässt sich mit

einem Staffellauf vergleichen, das heißt einer quantensicheren Übergabe von Punkt zu Punkt. Dabei muss allerdings vorausgesetzt werden, dass jeder Übergabe-Node „trusted“, also vertrauenswürdig ist und keine Informationen unautorisiert weiterleitet. Für eine möglichst hohe Sicherheit innerhalb der vertrauenswürdigen Knotenpunkte werden asymmetrische bzw. hybride Verfahren verwendet (siehe Abschn. 2.6.1)

Nähere Details
Zwischen den Endnodes A und B eines sicheren Datenlinks befindet sich ein Trusted Repeater R. Zunächst werden per QKD quantenmechanisch zwei Private Keys k_{AR} sowie k_{BR} erzeugt. Daraufhin sendet A einen Schlüssel k_{AB}, mit k_{AR} chiffriert, zu R. R dechiffriert, um k_{AB} zu erhalten. Daraufhin verschlüsselt R den k_{AB} erneut mit k_{RB} und sendet ihn zu B. B dechiffriert mit k_{RB}, um k_{AB} zu erzeugen. Auf diese Weise wird ein gemeinsamer Schlüssel k_{AB} generiert, der zum anschließenden Datentransfer über eine herkömmliche IT-Verbindung benutzt werden kann. Das System ist absolut sicher vor Angreifern außerhalb der Verbindung A und B, nicht jedoch innerhalb des Übertragungskanals, da R alle Schlüssel rekonstruieren kann und somit vertrauenswürdig sein muss.

Netzwerkarchitektur
In einer Art hierarchischer Anordnung kommt in QKD-Netzwerken eine Architektur aus drei Ebenen zum Einsatz. Die unterste Ebene bildet der Quanten-Layer basierend auf speziellen Relaisstationen via Trusted Nodes. Jeder Link generiert den Sicherheitsschlüssel auf seine eigene Weise, ebenso unterscheiden sich die verwendeten Protokolle sowie Formate und Größen der Schlüssel. In der Mehrzahl der Fälle kommen hier verschiedene Decoy-State-BB84-Systeme zum Einsatz. Die große Ausnahme bildet

die „All Vienna"-Group, welche ein verschränktes System verwendet. Über QKD-Devices gelangt das Schlüsselmaterial zur mittleren Ebene, dem Key Management (KM) Layer. Hier erhält ein Key Management Agent (KMA) die Schlüssel via ein Application-Interface, das von NEC und NICT so entwickelt wurde, dass es mit dem System kompatibel ist. Der KMA ist ein klassischer Computer, der als Trusted Node arbeitet. Sein Job ist, das Schlüsselmaterial auf die passende Größe sowie in übliche Formate zu bringen und zu identifizieren. Dann speichert er die Schlüssel in numerischer Reihenfolge, um den Schlüsselgebrauch für das Chiffrieren/Dechiffrieren zu synchronisieren. Ebenso speichert er statistisch relevante Daten wie etwa die Quantenbit-Errorrate (QBER) und die Schlüsselerzeugungsrate. Daraufhin leitet er diese Daten an den Key Management Server (KMS) weiter, der für das zentrale Networkmanagement zuständig ist sowie alle Links überblickt und koordiniert. Alle Netzwerkfunktionen laufen komplett auf dem KM-Layer unter Aufsicht des KMS. Ebenso überwacht der Server den Lebenszyklus eines Schlüssels und avisiert sichere Pfade. Die Authentifizierung erfolgt nach dem sogenannten Wegman-Carter-Schema, welches auf vorher erzeugten Schlüsseln beruht.

Die dritte Ebene garantiert schließlich die sichere Kommunikation durch die speziell erzeugten Quantenschlüssel für das Chiffrieren/Dechiffrieren von Text-, Audio- oder Videodaten. Die User befinden sich innerhalb der Trusted Nodes. Ihre Daten werden zum KMA geschickt und durch ein Verfahren namens OPT chiffriert/dechiffriert (Abschn. 2.6.1), und zwar in einem Stored-Key-Modus. Weil das Mischtyp-Netzwerk beschränkte Relaisstationen besitzt, organisiert der KMS einen Routenplan für die Endpoints der Useranfragen und selektiert die jeweils geeignete Route. Dabei kommen autonome Suchalgorithmen zum Einsatz.

Demonstration
Im Oktober 2010 wurde der Öffentlichkeit der erfolgreiche Funktionstest präsentiert, und zwar mit einer Videokonferenz zwischen Koganei und Otemachi. Der Live-Videostream wurde quantenkryptografisch verschlüsselt und dann im Stored-Key-Modus mittels OPT verschickt. Die Schlüsselrate lag bei 128 kbit/s. Ebenso konnten sichere Schlüssel über eine Gesamtentfernung von bis zu 135 km erzeugt werden. Auf einer 90 km langen Strecke wurde dann als besonderer Sicherheitstest ein Hackerangriff simuliert. Dabei wurde der Link durch einen Laserstrahl heftig attackiert. Der KMS detektierte diesen Angriff durch einen sofortigen Anstieg der QBER und gab Alarm. Die KMAs Koganei 1 und Koganei 2 stellten für diesen Fall gespeicherte Schlüssel zur Verfügung, und die Konferenz konnte sicher weitergehen. In der Zwischenzeit schaltete der KMS sofort auf eine Ersatzroute, um die Quantenschlüsselerzeugung fortzuführen, bevor die Schlüssel zu Ende gingen. Die TV-Konferenz konnte also ungestört weitergehen und die Sicherheit blieb garantiert. Außerdem gab es erfolgreiche Switchtests für verschiedene Relaisrouten (https://arxiv.org/abs/1103.3566).

2.4.3 2000-km-High-End-Backbone

Nach der Präsentation des japanischen QKD-Networks konnte das ehrgeizige China hier natürlich nicht nachstehen und setzt noch gewaltig einen obendrauf. Das Beijing-Shanghai-Projekt (China-QKD-Netzwerk) realisiert ein rund 2000 km langes Vertriebsnetz, das in Zukunft das Rückgrat des nationalen Kommunikationsnetzes bilden könnte. Von Beijing im Norden über Jinan und Hefei bis zur Küstenstadt Shanghai verbindet dieser Backbone

vier metropolische Quantennetzwerke. Basierend auf ähnlicher Technik wie in Japan, unterscheidet sich das chinesische Netzwerk neben seiner größeren Länge auch dadurch, dass mit dem QUESS-Experiment erstmals die Quantensatelliten-Technik demonstriert wurde. Damit besteht die wichtige Option, weit entfernte Endnodes mittels Quantensatelliten direkt miteinander zu verschränken und die QKD so auf ein viel größeres Sicherheitslevel zu heben. Medienberichten zufolge wird das Netz bereits von Verwaltung, Regierungsmitgliedern, Akteuren der Finanzwelt und Militärs genutzt. Ebenso gibt das Jinan Institut of Technology an, dass auch die kommerzielle Verwendung einsatzreif sei. Die High-End-Kommunikationslinie sei zudem viel sicherer als herkömmliche Telekom-Verbindungen, welche über keinen physikalischen Sicherheitsmechanismus verfügen. Damit hofft China, dass das Pilotprojekt sich über das Land hinaus ausweiten wird und erfolgreich auf der ganzen Welt Verbreitung findet. Seit 2014 wurde an diesem bis dato weltgrößten QKD-Web gebaut, die erste Projektstufe war im September 2017 fertiggestellt. Während der Eröffnungszeremonie wurde medienwirksam eine Banktransaktion von Shanghai nach Beijing durchgeführt. In Wuhan, der Hauptstadt der Provinz Hubei, erfolgte zusätzlich eine Anbindung, was mit weiteren städtischen Quantennetzen entlang des Jangtse-Flusses wiederholt werden soll. Schlussendlich ist geplant, den Ausbau um zusätzliche 11.000 km voran zu treiben. Freilich wird der Sicherheitsaspekt dadurch eingeschränkt, dass das chinesische Quantennetz genau wie das japanische vorwiegend mithilfe von Trusted Nodes arbeitet. Genauer gesagt handelt es sich um eine Kette von Verbindungslinien, die durch 32 Trusted Nodes miteinander verbunden sind (Stand 2017). Wie angesprochen, ergibt dies noch keine optimale Sicherheit. Trotzdem ist auch diese Projektstufe bereits viel sicherer als klassische

Netze, weil sich die theoretisch unendlich vielen Abhörpunkte auf 32 reduzieren. Die hiesigen Forscher verbinden mit ihrem Konzept jedenfalls Hoffnungen auf ein globales Quantennetzwerk, das laut Wissenschaftler Jian-Wei Pan am Ende der nächsten Dekade zum Einsatz kommen sollte. Mit detaillierteren Äußerungen hierzu halten sich die Forscher allerdings noch bedeckt.

2.4.4 Das Wiener Multiplex-QKD-Web

Ein wesentlicher Grund für die Einrichtung eines Quantennetzwerks liegt auch darin, dass die QKD möglichst vielen Usern zur Verfügung stehen soll. Da viele Implementierungen lediglich für zwei Parteien ausgelegt sind, ist es deshalb ein zentraler Forschungsansatz, möglichst effiziente Multiuserlösungen bereitzustellen. Österreichischen Forschern um Rupert Ursin ist jüngst ein wegweisender Schritt in diese Richtung gelungen. So konnte in einer Proof-of-Concept-Studie eine Ressourcen sparende und skalierbare Netzwerkarchitektur demonstriert werden, die einen erheblichen Geschwindigkeitsvorteil gegenüber bisherigen Auslegungen verspricht. Sensationell ist zudem, dass es sich um ein vollverschränktes QKD-System und somit um ein „echtes“ Quantennetzwerk handelt. Wie später im Detail angesprochen wird, bedeutet dies ein deutlich höheres Sicherheitslevel als bei Varianten mit Trusted Repeaters. Im Testversuch konnte gezeigt werden, dass eine einzige passive Verschränkungsquelle durch Frequenzmultiplexing die hochsichere QKD zwischen vier Kommunikationspartnern ermöglicht. Konkret erzeugt ein spezieller Laser einen verschränkten Polarisationszustand. Das Frequenzspektrum des Lichts wird sodann über Bandpassfilter in zwölf Kanäle gesplittet, wovon jeweils drei Frequenzen

über eine Glasfaser den vier Nutzern an den Endnodes zugeteilt werden. Die Frequenzen werden durch dieses Multiplexing gerade so geschaltet, dass sich ein Partner mit dem anderen stets gemeinsam ein verschränktes Photonenpaar teilt. Auf diese Weise können alle sechs bei vier Teilnehmern denkbaren Kombinationsmöglichkeiten realisiert werden. Die Auslegung ist besonders kostengünstig und benutzerfreundlich, da die Endnodes bei den Verbrauchern mit vergleichsweise einfachen Devices ausgestattet sind. Die Forscher stellen in Aussicht, dass die Wiener Architektur direkt an jede andere Netzwerktopologie adaptiert werden kann und zudem linear skalierbar wäre. Neue Clients können also mit geringen Modifikationen in das System aufgenommen werden. Durch die Verwendung von Wellenlängen im „telekomüblichen" Bereich ist das Netzwerk kompatibel mit der existierenden Infrastruktur des Internets, was es insgesamt zu einem der aussichtsreichsten Implementierungen für ein kommerzielles QKD-Netzwerk macht (https://arxiv.org/abs/1801.06194).

2.4.5 Die Quanten-Cloud

Schon heute ist Cloud-Computing eine wichtige Komponente des Internets und wird von vielen Usern, vor allem auch Firmen genutzt. Hierzu zählt beispielsweise die Bereitstellung von Infrastrukturen wie Anwendungssoftware, Rechenleistung oder Speicherplatz an entfernte Nutzer. Ernsthafte Bedenken erheben sich allerdings bezüglich des Datenschutzes bei der zentralen Erfassung und Auswertung von Nutzeraktivitäten (Stichwort Big Data), was mit Hinblick auf die zukünftige Entwicklung des Internets umso dringlicher werden wird. Auch Lösungsansätze

wie homomorphe Verschlüsselungen bieten immer noch Angriffspunkte. Eine Quanten-Cloud vermag dagegen nicht nur zu einem Speed-up bei bestimmten numerischen Aufgaben beizutragen, sondern kann vor allem auch zu einem noch nie da gewesenen Sicherheitslevel führen. Begriffe wie Privatsphäre oder Integrität würden auf eine neue Stufe gestellt werden: Immerhin wird eine hochsichere Client-Server-Umgebung geschaffen, wo die gesamte Server-Computation völlig unbekannt bleibt – eine Funktionalität, die es in der klassischen IT nicht gibt. Die Idee dahinter führt auf den zentralen Begriff Blind-Quantencomputing (BQC). Ein Beispiel: man möchte die Vorteile nutzen, die ein Quantencomputer in bestimmten Applikationen bietet. Nun wäre es aber so, dass dies eine sehr komplexe und teure Hardware erforderlich macht, wodurch es für die meisten User zu teuer und zu schwierig zu handhaben wäre. Bei einer Quanten-Cloud beantragt nun der Client Rechenzeit, während ein Quanten-Server eine Verbindung zu einem Quantenprozessor herstellt, welcher dann die Aufgaben ausführt. Wesentlich ist dabei, dass der Quantencomputer „blind" rechnet, das heißt, der Client erteilt nur Instruktionen, welche der Server ausführt. Dabei kann dieser (aus physikalischen Gründen) nicht wissen, um welche Informationen es sich konkret handelt. Gut vorstellbar, dass ein zukünftiges Quanteninternet via Cloud den Zugang zu sehr teuren und leistungsfähigen Quantencomputern anbietet, die naturgemäß im Besitz einschlägiger Firmen und Institutionen wären. Dank BQC wäre nicht nur ein besonderes Maß an Sicherheit gewährleistet, sondern man könnte auch überprüfen, ob die Computation wirklich von einem Quantenprozessor stammt und kein Fake ist.

Bezüglich der Umsetzung gibt es mittlerweile zahlreiche Vorschläge und Studien: Eine Möglichkeit besteht

zum Beispiel darin, dass der Client dem Server eigene Qubits aus einem Cluster zur Verfügung stellt. Der Server besitzt die Ressourcen, um damit die erforderlichen Rechenoperationen auszuführen, und zwar nach Instruktionen, die der Kunde dem Server klassisch mitteilt. Als mobile Qubits eignen sich zum Beispiel Photonen, denn sie können ja durch Glasfasern transportiert werden. Der Server verschränkt nun diese Qubits durch spezielle Quantentransformationen, ohne jedoch zu wissen, welche Art der Verschränkung vorliegt. Daraufhin nimmt er Messungen nach dem Prinzip des Einweg-Quantencomputers vor (nach den vom Kunden erhaltenen Instruktionen; Abschn. 2.5.4). Mit den Messresultaten allein kann allerdings der Server nichts anfangen, weil er das Zufallselement der vom Client eingebrachten Qubits nicht kennt. Wenn er die Resultate an den Kunden zurücksendet, kann sie ausschließlich dieser korrekt interpretieren, denn nur er kennt die objektiv zufälligen Messwerte seiner Qubits. Insgesamt beruht das System also auf dem Grundsatz, dass der Server niemals die volle Information über die Quantenzustände seines Clients haben kann.

In den letzten Jahren wurden mehrere verschieden BQC-Protokolle entworfen, die es jedoch allesamt erfordern, dass die Clients über spezielle Quanten-Devices verfügen (entweder zum Präparieren oder zum Messen der Qubits). Wie ein Forscherteam unter der Leitung von Jian-Wei Pan und Chao-Yang Lu an der Universität of Science and Technology in Hefei zeigen konnte, ist es aber auch möglich, dass sogar ein rein klassischer Computer eine Quantencomputation an einen Quanten-Server delegieren kann (Abb. 2.3). Dabei wurde an einem simplen Beispiel – der Zerlegung der Zahl 15 in die Faktoren 3 und 5 – demonstriert, dass ein völlig klassischer Client mit zwei Quantenservern kommunizieren kann,

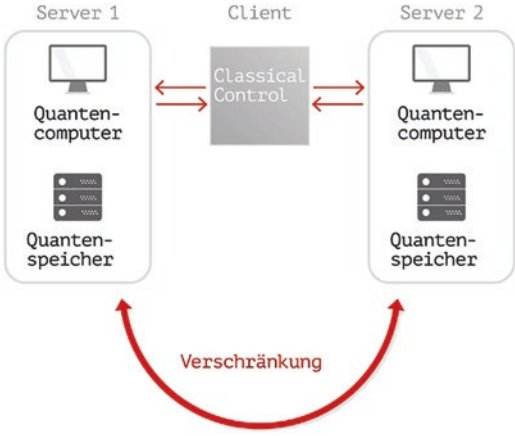

Abb. 2.3 Blind-Quantencomputing

ohne dass diese wissen können, was genau gerechnet wird. Möglich wird das, weil beide Server jeweils nur Teile der Berechnung durchführen und es physikalisch unmöglich ist, dass die Server miteinander auf klassischem Wege Informationen austauschen können. Gleichzeitig kann das Ergebnis der Quantencomputation daraufhin überprüft werden, ob „geschummelt" wurde. Die Forscher stellen mit ihrer Prinzipdemonstration in Aussicht, dass diese Methode auf „echte" Rechnerprobleme hochskaliert und eines Tages in Cloud-Servern implementiert werden könnte. Ein weiterer großer Vorteil wäre Lu zufolge darin zu sehen, dass der User keine speziellen (womöglich teuren) Quanten-Devices bräuchte. Das spart Ressourcen und macht skalierbares Quantencomputing theoretisch weltweit verfügbar. Eine wunderbare und gleichzeitig realisierbare Vision: Quantenpower wird durch „Multi-User-BQC" diskret und ohne Fake an die Nutzer verteilt.

2.5 Quantencomputer

> „Build Quantum-computers to simulate nature, because goddammit the world is quantum!“ (Richard Feynman, Physiknobelpreis 1965).

Die Leistungsfähigkeit und somit die Relevanz des zukünftigen Quanteninternets wird neben dem besonderen Sicherheitsaspekt auch maßgeblich davon abhängen, welche Fähigkeiten Quantencomputer eines Tages entwickeln werden. Wir wollen uns daher eingehender mit diesem äußerst innovativen Konzept beschäftigen und ein Schlaglicht auf die aktuelle Situation in der Forschung werfen.

Bereits in den 1960er Jahren spekulierte der US-Amerikaner Richard Feynman, ob man die Quantenphysik zum Rechnen benutzen könne. Dabei macht es einen Unterschied, ob ein Computer Bauteile verwendet, deren Funktion den Regeln der Quantenmechanik folgt (wie etwa Flash-Speicher, TFET-Transistor etc.) oder ob die Datenverarbeitung selbst auf Basis der Quanteninformatik vonstattengeht. Nur letzteres ist echtes Quantencomputing. Zum besseren Verständnis sei zunächst ein herkömmlicher, klassischer Computer betrachtet. Ganz naiv besehen kann man sich einen traditionellen Rechner als eine Art Blackbox vorstellen, die mit 0/1-Bits gefüttert wird (Input) und schließlich wieder 0/1-Bits ausgibt (Output). Der eigentliche Rechenvorgang (das Computing) entspricht einer definierten Veränderung der Bitfolge, vergleichbar mit einer Reihe von Schaltern, die in vorherbestimmter Weise umgelegt werden. Für hohe Verarbeitungsgeschwindigkeiten müssen naturgemäß sehr viele dieser Schalter in kürzester Zeit bedient werden. In der Praxis wird das durch winzig kleine Halbleitertransistoren realisiert, die zu Milliarden auf winzigen

Mikrochips untergebracht sind. Die Abfolge, nach der diese Schalter bedient werden, entspricht den Programmschritten, also dem Algorithmus. Als besonderes Charakteristikum klassischer Computer bleibt festzuhalten, dass alle Schritte streng seriell ablaufen (das heißt, einzelne Schalter werden stets sequenziell, also in einer bestimmten Reihenfolge umgelegt). Damit wird jedoch automatisch die Verarbeitungsgeschwindigkeit begrenzt.

Das mooresche Gesetz

Um die Leistungsfähigkeit klassischer Rechner zu erhöhen, bedient sich die Computerindustrie seit Jahrzehnten eines (von der Grundidee her) sehr einfachen Prinzips. Man nimmt einfach mehr und mehr Schalter in immer kompakterer Bauweise, wodurch bei immer schnelleren Taktfrequenzen einerseits mehr Bits verarbeitet werden können und andererseits der Stromverbrauch pro Schalter immer geringer wird. Auf diese Weise gelang es über viele Jahre hinweg, die Prozessorleistung pro Chip in etwa alle 18 Monate zu verdoppeln. Dieser exponentielle Zusammenhang ist gemeinhin als mooresches Gesetz bekannt (benannt nach Intel-Mitbegründer Gordon E. Moore). Zu beachten gilt es allerdings, dass es sich dabei um kein Naturgesetz handelt, sondern um eine ambitionierte Vorgabe an die Ingenieure der Computerindustrie. Auf einem Naturgesetz beruht dagegen der Umstand, dass diese beliebige Skalierung überhaupt möglich ist. Die „Silicium-Revolution“ beruht auf der Fähigkeit von UV-Licht, aus einem daumengroßen Silicium-Wafer Milliarden kleine Transistoren heraus zu ätzen. Da UV-Licht eine minimale Wellenlänge von etwa 10 Nanometern aufweist, kann man auf diese Weise Transistoren bis etwa 30 Atomdurchmesser herstellen. Dennoch kann dieses Spiel der fortwährenden Miniaturisierung nicht ewig so weitergehen, wofür es mehrere Gründe gibt: Einer

liegt zum Beispiel in der Tatsache, dass die Wärmeentwicklung leistungsfähiger Chips viel stärker ansteigt als die Möglichkeit, die Chips zu kühlen. Ein anderer liegt darin, dass die für noch kleinere Strukturen benötigten Wellenlängen im Bereich der Röntgenstrahlung liegen, welche nicht ausreichend fokussiert werden kann. Trotz dieser Schwierigkeiten sollen Anfang der 2020er Jahre Strukturen von nur noch 7 nm Größe produziert werden (etwa 20 Atomdurchmesser). Das ultimative Limit setzt jedoch eine unüberwindliche Grenze, die aus den Gesetzen der Quantenmechanik folgt.

Der Quantenparallelismus

Der Grund für das angesprochene Limit liegt in der heisenbergschen Unschärferelation, die sinngemäß besagt, dass Aufenthaltsort und Geschwindigkeit eines Quantenobjekts niemals gleichzeitig genau angegeben werden können. Als Konsequenz davon ist die genaue Lage von Atomen oder Elektronen ungewiss – sie sind in gewissem Sinne verschmiert oder „unscharf". Als weitere Folge entstehen „Leckströme", indem die geladenen Partikel durch die hauchdünne Schicht der Chips „tunneln" und Kurzschlüsse verursachen. Ab dann ist die klassische Informationsverarbeitung auf Basis von elektrisch codierten Bits automatisch nicht mehr möglich. Um diesem grundlegenden Problem beizukommen, reagiert die Computerindustrie zum Beispiel mit dem schon länger bekannten Parallelrechner. Dabei wird der Rechenaufwand auf mehrere Prozesse verteilt, um Aufgaben separat und gleichzeitig zu erledigen – am Ende werden die Ergebnisse wieder zusammengeführt. Dennoch gestaltet sich dieses Delegieren von Teilaufgaben an mehrere Chips in manchen Fällen als überaus diffizil, da es immer einen zusätzlichen Aufwand kostet, die Verteilung zu organisieren und zu koordinieren. Abhängig vom vorliegenden Problem kann

sich die zeitliche Koordination der Teillösungen als ernsthafte Schwierigkeit erweisen. Insbesondere gibt es auch kein Standardverfahren, wie dies erfolgen sollte. Auch aus diesem Grund sucht die Computerindustrie längst nach neuen Mitteln und Wegen, welche einmal eine neue Ära einläuten könnten, das sogenannte Post-Silicium-Zeitalter. Zukünftige Entwicklungen liegen möglicherweise in der Nutzung biologische Systeme, weiterer Verknüpfung zwischen biologischer und technischer Informationsverarbeitung, optischer Signalverarbeitung und neuen physikalischen Modellen. Zu diesen neuartigen Zugängen zählt insbesondere auch das Konzept des Quantencomputers. Sein revolutionärer Grundgedanke beruht darauf, dass er genau am „wunden Punkt" des klassischen Computers ansetzt. Wie angesprochen besteht ein Grundproblem in der sequenziellen Abfolge seiner Programmschritte, welche automatisch die Verarbeitungsgeschwindigkeit begrenzt. Was, wenn man diese „Kausalität" einfach außer Kraft setzen könnte? Genau diese Idee macht sich der Quantenprozessor zunutze, indem er durch ein ganz spezielles Parallelverfahren auch „akausal" rechnen kann. Diese Zeitumkehrinvarianz kann nicht nur die Reihenfolge von Logikgattern betreffen (das heißt, Ein- und Ausgänge können vertauscht werden), sondern es bezeichnet auch den sogenannten Quantenparallelismus. Damit wird es möglich, dass mehrere Lösungen eines Problems im gesamten Quantenzustand bereits zugleich enthalten sind und das gewünschte Ergebnis durch eine spezielle Messreihe ausgelesen wird. Die wesentliche Grundlage dieser merkwürdigen Parallelwelt bilden sowohl das Superpositionsprinzip als auch die damit eng verwandte Verschränkung. Sozusagen 0 und 1 gleichzeitig, und das in multidimensionaler und stark korrelierter Form. Entsprechend diesen völlig neuartigen Eigenschaften wird das

Bit, die kleinste Einheit der Informationsverarbeitung, zum Qubit einer quantenmechanischen Linearkombination von 0 und 1.

2.5.1 Das Qubit – ein Multitasking-Genie

Um die Eigenschaften von Qubits näher kennenzulernen, greifen wir zu einer vereinfachten Darstellung: Stellen wir uns dazu einen Kreisquadranten vor, der von zwei Koordinatenachsen begrenzt wird (Abb. 2.4a[2]). Nun steht jeder Punkt auf diesem Viertelkreis für einen möglichen Zustand, den das Qubit einnehmen kann. Dabei sei jeder Zustand durch einen Pfeil (Vektor) repräsentiert, dessen Schaft im Ursprung des Koordinatensystems liegt und dessen Spitze zum Punkt zeigt. Wenn wir nun gedanklich den Vektor entlang des Viertelkreisbogens bewegen, erhalten wir die Vorstellung, dass ein Qubit all diese Zustände gleichzeitig in sich vereint. Dies sind unendlich viele, da bereits der Viertelkreis eine unendliche Punktmenge ist (der Vollkreis sowieso). Professionell gesprochen ist jeder einzelne Zustand ein zweidimensionaler Vektor, der sich als Linearkombination der Basisvektoren $|0\rangle$ und $|1\rangle$ darstellen

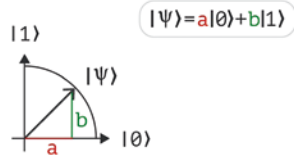

Abb. 2.4a Darstellung der Linearkombination von Basisvektoren

[2] *Anmerkung zu Abb. 2.4a:* Dies ist eine didaktische Vereinfachung. Der Zustand eines Single-Qubits wird in der QM als normierter Vektor in einem komplexen Hilbertraum beschrieben. Die Zustände lassen sich als Punkte auf der Oberfläche einer Kugel darstellen (Bloch-Sphäre).

lässt: $|\psi\rangle = a|0\rangle + b|1\rangle$ Dabei stehen die Faktoren a und b für beliebige Zahlen zwischen 0 und 1. Sie regulieren sozusagen die Länge der Basisvektoren und bilden zusammen mit dem Zustandsvektor stets ein rechtwinkeliges Dreieck, dessen Hypotenusenlänge 1 beträgt. Ein Spezialfall ergibt sich für a oder b gleich 0. Hier ist das Dreieck entartet. Bei dem Symbol $|\psi\rangle$ (sprich „Psi-Vektor“) handelt es sich um die für die Quantenmechanik typische Bra-Ket-Schreibweise von Quantenzuständen.

Nobody is perfect

Angesichts der Tatsache, dass das Qubit unendlich viele Zustände gleichzeitig enthält, könnte man auf die irreführende Idee kommen, dass ein einziges (single) Qubit für Berechnungen in Quantencomputern ausreicht. Doch so einfach ist das nicht. Die Zustandsüberlagerung in einem Qubit existiert nur, solange es nicht „beobachtet“ wird, das heißt physikalisch gesprochen, solange der Quantenzustand nicht gemessen wird. Geschieht dies, so zerfällt es in einen seiner beiden Eigenwerte 0 oder 1. Noch eine Schwierigkeit: bei Quantenzuständen kann nicht genau vorhergesagt werden, ob eine 0 oder eine 1 gemessen wird. Dafür kann lediglich eine Wahrscheinlichkeit angegeben werden, die man übrigens aus unserem Qubit-Quadranten ablesen kann: Sie ergibt sich aus den Quadraten der Faktoren a beziehungsweise b, wobei nach dem Lehrsatz des Pythagoras dann selbstverständlich gelten muss: $a^2 + b^2 = 1$. Dabei steht die 1 für 100 % Wahrscheinlichkeit. Ein Beispiel: angenommen, der Zustandsvektor $|\psi\rangle$ schließt mit den Koordinatenachsen einen Winkel von 45° ein. Dann besitzen die Faktoren a und b denselben Wert. Somit wird jeweils mit 50 % Wahrscheinlichkeit eine 0 oder eine 1 gemessen, da die Summe beider Wahrscheinlichkeiten ja 100 % ergeben muss. Falls der Winkel 0° beziehungsweise 90° beträgt (entartetes Dreieck), so wird

mit 100 % Wahrscheinlichkeit, also mit Sicherheit, eine 0 beziehungsweise eine 1 gemessen (da dann entweder $a = 1$ oder $b = 1$). In allen anderen Fällen ergeben sich je nach Winkel unterschiedliche Wahrscheinlichkeiten für die Messung von 0 beziehungsweise 1. Damit stellt sich unwillkürlich die Frage, welchen Vorteil das Qubit gegenüber dem herkömmlichen Bit haben sollte. Schließlich besitzt es den großen Makel, dass es zwar theoretisch unendlich viel Information tragen kann, jedoch bei seiner Messung immer wieder nur in seine Eigenwerte 0 oder 1zerfällt, und dies außerdem noch mit variablen Wahrscheinlichkeiten. Damit scheint sich das Quantenbit auf den ersten Blick als Bumerang zu entlarven.

Viele Qubits im Register

Die Situation ändert sich schlagartig, wenn mehrere, idealerweise extrem viele Qubits miteinander in eine Superposition gebracht werden. Denken wir uns zunächst ein Register bestehend aus zwei Qubits. Nun gibt es bereits vier Basisvektoren: $|00\rangle$, $|01\rangle$, $|10\rangle$ und $|11\rangle$. Aufgrund des quantenmechanischen Superpositionsprinzips können daraus erneut alle nur erdenklichen Überlagerungszustände gebildet werden. Anschaulich vorstellen kann sich das der Mensch freilich nicht mehr, da er nur dreidimensional denken kann und jetzt ein vierdimensionales Koordinatensystem nötig wäre. Zumindest jedoch können wir den Quantenzustand des 2-Qubit-Systems symbolisch angeben: $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$. Die entsprechenden Wahrscheinlichkeiten ergeben sich in Analogie zu oben aus den Faktoren *a, b, c* und *d,* deren Quadratsumme wiederum 1 ergeben muss. Wir sehen somit, dass die Anzahl der möglichen Linearkombinationen und damit die Zahl der Superpositionszustände deutlich zugenommen hat – einfach deshalb, weil wir jetzt (gedanklich) mit den vier Basiszuständen einen vierdimensionalen Raum aufspannen.

Betrachten wir nun 3, 4, 5 oder allgemein N Qubits im Register, dann erkennen wir, dass die Anzahl der Basisvektoren exponentiell zunimmt, das heißt unser Zustandsraum wird 8-dimensional, 16-dimensional, 32-dimensional und allgemein 2^N-dimensional. Vergleicht man diese Tatsache mit einem normalen Computer, so wird evident, dass mit zunehmender Zahl von Qubits im Register die Möglichkeiten eines Quantencomputers diejenigen des klassischen weit übertreffen. Letzterer benötigt zur Darstellung eines N-wertigen Registers genau N Bit an Information, die lediglich 0 oder 1 bedeuten können. Ein Quantencomputer besitzt jedoch ungleich mehr, nämlich 2^N Superpositionszustände, sozusagen 0 und 1 gleichzeitig in multidimensionaler Form. Wichtig ist dabei festzuhalten, dass zwar beileibe nicht jeder Überlagerungszustand für einen Algorithmus benutzt werden kann – falls dies jedoch gegeben ist, dann können extrem viele Schritte, die zur Lösung eines Problems beitragen, in einem einzigen Zustand enthalten sein. Dies kann eine erhebliche Verkürzung der Rechenzeit bedeuten, vor allem bei Problemen mit exponentiell wachsender Zahl von Rechenschritten.

Funktionsprinzip des Quantencomputers

In der Tat kann man mit einem simplen 2-Qubit-System schon einfache Aufgaben lösen. Dazu ein Prinzipbeispiel das die Idee erläutern soll. Die Aufgabenstellung: stellen wir uns einen Computer als eine Art Blackbox vor, die einen Input (0 oder 1) annimmt und für jeden Input wieder eine Binärzahl (0 oder 1) als Output ausgibt. Die Aufgabe für den Computer besteht darin, festzustellen, ob beiden Outputzahlen identisch sind. Zunächst wird ein passendes Quantensystem präpariert, das den Zustand als Superposition von 0 und 1 abbildet. Im nächsten Schritt wird dieser Überlagerungszustand als

Input für die Blackbox verwendet. In der Blackbox wird der Eingangszustand (der ja beide Zahlen 0 und 1 enthält) so transformiert, dass man ihm beide Ausgabenwerte entlocken kann. Dies geschieht zum Beispiel durch einen Quantenschaltkreis. Da die Gesetze der Quantenmechanik vorschreiben, dass man nur eine einzige Messung machen darf, um eine Information aus dem Zustand herauszulesen, muss das System geschickt transformiert werden. Etwa so, dass die Messung mit Sicherheit den Wert 0 ergibt, wenn die Zahlen gleich sind, andernfalls der Messwert mit Sicherheit 1 beträgt. Wenn man also abschließend, diese *einzige* Messung durchführt, hat der Quantencomputer seine Aufgabe bereits erledigt und man hat die Lösung der gestellten Aufgabe. Ein klassischer Computer hätte zur Lösung desselben Problems *zwei* Anfragen an die Blackbox stellen müssen – und arbeitet auf diese Weise ineffizienter.

Ein Quantencomputer erledigt dieselbe Aufgabe also schneller, wenn ihm, wie in diesem Beispiel demonstriert, die „richtige" Frage gestellt wird. Es ist nämlich nicht der genaue Wert der Rechnung von Interesse, sondern nur, ob gleiche Outputzahlen vorliegen oder nicht (die Zahlen selbst verbleiben unbekannt) Wir sehen uns später eine konkrete Simulation an, die zeigt, wie ein Quantencomputer tatsächlich effizienter arbeitet. Bei einem Quantencomputer kommt es also auf die Fragestellung an – er ist deshalb keineswegs für jedes beliebige Problem geeignet, sondern nur für ganz bestimmte Aufgaben – diese schafft er allerdings in frappant schnellerer Zeit als ein klassischer Computer. Seine Stärken liegen etwa im Bereich der Kryptoanalyse, der Logistik oder der Suche in großen Datenbanken. Eine große Hoffnung liegt vor allem in Problemen mit exponentiell zunehmendem Rechenaufwand, an denen selbst Supercomputer scheitern. Quantencomputer sind also Spezialrechner, die definitiv nicht das Notebook oder Tablet ersetzen werden.

2.5.2 Quantensoftware

Das Kernstück normaler Computer sind Prozessorchips, welche aus Rechenregistern und Logikgattern bestehen. Erstere übernehmen das Rechnen mit Zahlen, letztere das Abarbeiten von logischen Entscheidungen in Programmen. Unter einem Algorithmus versteht man ganz allgemein eine Handlungsabfolge zur Lösung eines Problems. Mehrere Einzelschritte lassen sich zu Befehlen von höheren Programmiersprachen („Software“) zusammenfassen. Grundsätzlich gilt: Jede Programmanweisung muss in Maschinenbefehle übersetzt werden, welche der Computer dann abarbeitet. Im Falle eines klassischen Computers ist der Code der Maschinenbefehle in der Bit-Sprache verfasst, also eine Abfolge von Nullen und Einsen. Das Computing bedeutet dann prinzipiell nichts weiter, als Inputbits in der durch den in Bits codieren Algorithmus bestimmten Weise in Outputbits zu verwandeln. Dabei sind alle Schritte durch logische Grundschaltungen (Gatter) darstellbar, welche auf mathematischen Regeln beruhen.

In ähnlicher Weise kann man auch Anweisungen für Quantencomputer angeben. Es existiert zwar noch keine Quantensoftware im eigentlichen Sinne, es gibt jedoch bereits einige Quantenalgorithmen. Hier entwickelt sich ein neuer Zweig der Informatik: die Quanteninformatik, welche die Wirkung von Algorithmen auf Qubit-Register beschreibt. Da Qubits grundsätzlich Überlagerungszustände und nicht 0/1-Bits darstellen, unterscheidet sich auch die Mathematik, welche diese beschreibt, grundsätzlich von der bei traditionellen Computer eingesetzten. Beispielsweise besteht ein Quantenschaltkreis aus mehreren Quantengattern, die in fester zeitlicher Abfolge auf das Qubitregister angewendet werden, wie etwa die Quanten-Fouriertransformation als Bestandteil des

prominenten Shor-Algorithmus. Sie arbeitet auf einem Quantenregister mit *N* Qubits und bildet jeden der 2^*N* Basiszustände auf eine Superposition aller Basiszustände ab. Dies verhält sich sozusagen wie in der Musik, wo die individuelle Klangfarbe eines Instruments aus Grund- und Obertönen zusammengesetzt wird. Ein weiterer Unterschied ergibt sich aus dem Grundsatz der objektiven Zufälligkeit: Viele Quantenalgorithmen sind deshalb nur probabilistisch zu formulieren, liefern also nur mit einer gewissen Wahrscheinlichkeit Ergebnisse. Dabei kann jedoch der Fehler wegen des Gesetzes der großen Zahlen durch sehr häufiges Wiederholen der Messungen beliebig klein gehalten werden.

Shor-Algorithmus

Aus der „Quantenmusik" der Fourier-Reihen folgt ein Algorithmus, der die Kryptologen einst das Fürchten lehren könnte. Er berechnet einen nichttrivialen Teiler einer zusammengesetzten Zahl in wesentlich schnellerer Zeit als ein klassischer Algorithmus. Wie bereits angesprochen beruhen viele Verschlüsselungsverfahren im Internet auf der Faktorisierung sehr großer Primzahlen. Die Sicherheit der weit verbreiteten „RSA-Codierung" beruht also beispielsweise darauf, dass kein effizienter Algorithmus existiert, der diese Aufgabe in polynomialer Länge erledigen kann. Der Aufwand für Probleme, die nicht in Polynomialzeit gelöst werden können, ist mit klassischen Rechnern nicht in einem überschaubaren Zeitraum lösbar. Einfacher ausgedrückt: Es ist viel schwieriger, die Zahl 323 in ein Produkt zweier Primzahlen zu zerlegen als 17 mal 19 zu rechnen. Falls die zu zerlegenden Zahlen nun 600 und mehr Stellen besitzen, wird dies selbst für Supercomputer zum Problem, da die Mathematik bis heute kein Verfahren kennt, wie man sehr große Primfaktoren effizient berechnen kann. Ein technisch

nutzbarer Quantencomputer, auf dem der Shor-Algorithmus arbeitet, könnte diese goldene Regel jedoch überwinden und die RSA-Codierung wertlos machen. Die Idee hierzu entwickelte Peter Shor im Jahre 1994 bei den Bell Laboratories. Der Algorithmus besteht jeweils aus einem klassischen und einem Quantenteil und arbeitet außerdem probabilistisch, das heißt, er liefert in manchen, jedoch beliebig wenigen Fällen kein Ergebnis. Bereits 2001 wurde von IBM bewiesen, dass ein Baby-Quantencomputer die Zahl 15 in die Faktoren 3 und 5 zerlegen kann. Das mag bescheiden wirken und den Kryptologen ein mildes Lächeln entlocken – was aber, wenn das Baby einmal erwachsen wird? In der Tat werden Quantencomputer in der Öffentlichkeit hauptsächlich mit ihrer theoretischen Fähigkeit zum Code-Knacken in Verbindung gebracht, manchmal sogar als potenzielle „Monster" dargestellt. Hier kann vorerst Entwarnung gegeben werden. Für praktisch relevante Aufgaben ist der Shor also heute noch nicht anwendbar, Präventiv wird aber bereits an asymmetrischen Kryptosystemen gearbeitet, die auch gegen Quantencomputer resistent sein sollen, dies wäre dann die sogenannte Post-Quantenkryptografie. Schließlich weiß niemand zu sagen, wie der State of the Art in Jahren einmal aussehen könnte. Neue wissenschaftliche Erkenntnisse und Durchbrüche in der Forschung können zu völlig unvorhersehbaren Erkenntnissen und Konzepten führen. Die Gefahr, dass bestehende Verschlüsselungscodierungen eines Tages durch Quantenrechner in Sekundenschnelle gebrochen werden, ist niemals auszuschließen. Whistleblower Edward Snowden zufolge soll die NSA schon seit vielen Jahren an so einem Quantencomputer arbeiten.

Grover-Algorithmus

Eine wichtige Aufgabe der Informatik ist die Suche in einer unsortierten Datenbank, sei es für Suchmaschinen

oder bei Optimierungs- und Logistikproblemen. Der schnellstmögliche Suchalgorithmus ist gewöhnlich die lineare Suche, die bei N Einträgen auch dieselbe Größenordnung von Rechenschritten erfordert. Angenommen, Sie suchen eine bestimmte Person im Telefonbuch. Solange die Namen alphabetisch gereiht sind, geht das sicher rasch, nicht aber, wenn die Namen völlig willkürlich gelistet wären. Im schlimmsten Fall müssten Sie dann alle Namen anschauen, bis sie die gewünschte Person gefunden hätten. Bei N Personen sind das also maximal N Schritte. Das dauert natürlich umso länger, je größer N ist. Klassische Suchalgorithmen benötigen für unsortierte Daten im Schnitt einen Aufwand von $N/2$. In diese Kerbe schlägt nun der Grover-Algorithmus, welcher für N Einträge nur etwa $\sqrt{N}$ Schritte benötigt. Für $N=1$ Billion wären das nur 1 Million benötigte Schritte, für $N=1$ Trillion nur 1 Milliarde usw. Außerdem skaliert der Speicherbedarf sogar nur logarithmisch, was sich aufgrund der sehr schwach steigenden Logarithmusfunktion für sehr großes N besonders bezahlt macht. Als Nachteil mag gelten, dass der Grover-Algorithmus probabilistisch arbeitet, das heißt, er liefert zwar mit hoher Wahrscheinlichkeit eine richtige Lösung, aber eben nicht mit Sicherheit. Allerdings lässt sich auch hier die Fehlerchance durch mehrmaliges Wiederholen beliebig reduzieren.

Anschaulich kann man sich die Wirkungsweise des Grover-Algorithmus durch ein Mikadospiel plausibel machen: Aus sehr vielen gleich langen, dünnen Mikadostäbchen werden 4 Stück herausgenommen und als Quadrat auf ein Blatt Papier gelegt. Auf dieses Quadrat werden N Punkte aufgemalt, die der Anzahl der Sucheinträge entsprechen sollen. Wenn N sehr groß ist, wird diese Punktmenge die Fläche des Quadrats fast vollständig ausfüllen. Irgendwo auf dieser Fläche befindet sich ein Punkt, der dem gesuchten Eintrag entspricht.

Ein klassischer Computer müsste jetzt schlimmstenfalls alle N Punkte durchprobieren, bis er den richtigen gefunden hätte – das kann dauern! Ein Quantencomputer geht da ganz anders zu Werke: Der Quantenparallelismus gestattet ihm, die restlichen Mikadostäbe einfach in wahlloser Unordnung auf das Quadrat zu werfen. Da wird dann mit hoher Wahrscheinlichkeit auch ein Stäbchen darunter sein, das den gesuchten Punkt trifft. Da die Länge des Mikadostäbchens genau der Seitenkante des Quadrats mit der Fläche N entspricht, braucht er dann nur maximal $\sqrt{N}$ Punkte anzusehen, bis er den richtigen gefunden hat. Falls kein Stäbchen den gesuchten Punkt trifft, wiederholt er den Vorgang. Je öfter er das macht, desto höher ist die Wahrscheinlichkeit, dass er die gesuchte Lösung findet.

Quantensimulatoren

Die Domäne, auf der Quantencomputer einen großen Vorteil ausspielen, ist die Simulation von anderen, klassisch nicht zu berechnenden Quantensystemen, etwa im Bereich der Materialwissenschaften. Jeder Festkörper ist ein kristallartiges Gebilde, bestehend aus Abertrilliarden von Atomen beziehungsweise Molekülen. Er ist ein unvorstellbar komplexes Quantensystem. Seine Elektronenzustände werden eigentlich durch die Schrödinger-Gleichung beschrieben. Mit ihr lässt sich theoretisch jedes Atom, jedes Molekül und damit auch das Verhalten des gesamten Festkörpers vorherberechnen. Allerdings nur theoretisch. Wie schon jeder Physikstudent weiß, ist bereits die Lösung der Schrödinger-Gleichung für ein Wasserstoff-Atom im Grundzustand ziemlich aufwendig, obwohl dies das einfachste Problem ist. Komplexere Zustände lassen sich nur näherungsweise behandeln, und selbst das wird ab 50 bis 60 Atomen auch für leistungsstarke Rechner beziehungsweise Supercomputer unmöglich. Wünschenswert sind

daher neue Berechnungsmodelle, die so hart an der Realität dran sind wie nur möglich. Von Richard Feynman stammt die Grundidee der Quantensimulation. Er schlug 1982 einen „analogen Quantencomputer“ vor, der nicht auf digitaler Codierung beruht, sondern die Natur selbst imitiert. Man verwendet dazu ein völlig anderes System, dessen Eigenschaften sich jedoch analog auf einen Teilaspekt des zu simulierenden Systems übertragen lassen. Diese Eigenschaften werden dann untersucht, ohne das System selbst (mit dem damit verbundenen Speicherplatz- und Verarbeitungsproblem) simulieren zu müssen. Auf diese Weise speichert und verarbeitet der Quantensimulator die interessierende Information sozusagen ganz von sich selbst aus, wodurch man ihn auch als Quantencomputer bezeichnen kann. Quantensimulatoren könnte zum Beispiel das Verhalten von Supraleitern viel besser vorhersagen und damit eines Tages den immer noch nicht geklärten Mechanismus der Hochtemperatursupraleitung enthüllen. Ebenso könnte die Untersuchung des Quantenmagnetismus dazu führen, dass die Lese- und Schreibgeschwindigkeit auf der Festplatte eines klassischen Computers erhöht wird. Feynmans Ansatz ist immer dann sinnvoll, wenn quantenmechanische Effekte in einem System die tragende Rolle spielen. Wie Feynman und andere zeigen konnten, würde die Simulation solcher Systeme auf einer klassischen Turing-Maschine exponentiell viele Rechenschritte erfordern und diese sozusagen an ihrer eigenen Komplexität ersticken. Klassisches Computing stellt daher keinen Lösungsansatz für derartige Probleme dar. Ein weiterer großer Vorteil der Quantensimulation besteht darin, dass keine Kontrolle für jede Einzelkomponente erforderlich ist und deshalb einen Vorteil im Vergleich zu anderen Konzepten von Quantenrechnern bietet. Zu unterscheiden sind statische Modelle, welche die statischen Eigenschaften von wechselwirkenden Quanten-Vielteilchensystemen

untersuchen – im Unterschied zu dynamischen Quantensimulatoren, welche sich von einem Gleichgewichtszustand wegbewegen und eine komplexe Zeitentwicklung aufweisen. Dabei können Simulationen auf verschiedene Weise durchgeführt werden: Digitale Quantensimulatoren basieren auf Quantenschaltkreisen (siehe unten), die auch auf einem Quantencomputer implementiert werden können. Analoge Simulatoren sind besonders vielversprechend, da sie etwa die Zeitentwicklung eines wechselwirkenden Vielteilchensystems voraussagen können und bereits mit heutigen Technologien Systeme realisiert wurden, die selbst Supercomputer in den Schatten stellen. Man verwendet unterschiedliche physikalische Ressourcen wie ultrakalte Atomgase oder gefangene Ionen, aber auch Cavity-QED-Systeme oder Photonenkondensate. Ein Schlüsselziel in diesem sehr aufstrebenden neuen Gebiet ist die Entwicklung von verschiedenen Plattformen mit hoher Kontrollierbarkeit und Komplexität.

2.5.3 Quantenlogische Gatter

Klassische Computer verwenden für die maschinelle Umsetzung ihrer Algorithmen logische Schaltungen aus einem oder mehreren Transistoren. Heutige Mikroprozessoren besitzen Milliarden von Logikgattern. Sehr oft wird dabei das XOR-Gatter verwendet (exklusives Oder). Es entspricht einer bitweisen Addition beider Eingänge modulo 2. Das heißt, immer wenn die Eingänge am Gatter mit ungleichen Bits belegt sind, erzeugt das Gatter eine logische 1 („wahr“), bei gleichen Eingängen eine logische 0 („falsch“). Symbolisch kann das durch einen Schaltplan oder eine Wahrheitstafel (Abb. 2.4b) dargestellt werden.

Das quantenlogische CNOT-Gatter (Abb. 2.4c) erweitert die Charakteristik des XOR, denn es hat zwei

Bit 1	Bit 2	XOR	Ausgang
0	0	→	0
1	0	→	1
0	1	→	1
1	1	→	0

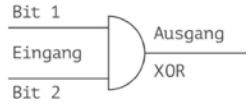

Abb. 2.4b Klassisches XOR – Gatter

Target-Qubit	Kontroll-Qubit	CNOT	Target-Qubit	Kontroll-Qubit
0	0	↔	0	0
1	0	↔	1	0
0	1	↔	1	1
1	1	↔	0	1

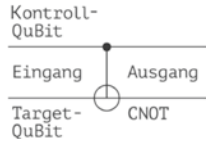

Abb. 2.4c 2 – Qubit CNOT- Gatter

Eingänge und zwei Ausgänge. Anhand der Wahrheitstafel sieht man, dass der Zustand des ersten Qubits (Kontrollbit) nach der Gatteroperation unverändert bleibt, der Wert des zweiten Qubits (Targetbit) dagegen der Logik des klassischen XOR folgt: Es wird genau dann invertiert, wenn das Kontrollbit auf 1 gesetzt wird. Ebenso erkennt man den „akausalen" Charakter: Die Operation läuft vorwärts wie rückwärts völlig gleich ab, diese Zeitumkehrinvarianz ist typisch für Rechenprozesse in einem Quantencomputer. Ein weiterer wichtiger Unterschied ist, dass Superpositionszustände als Kontroll- und Targetbits verwendet werden können – und aus diesen auch spezielle korrelierte Zustände gebildet werden können.

Erzeugung verschränkter Zustände

Quantencomputer profitieren also vom Quantenparallelismus, der zunächst einmal in den schier unerschöpflichen Linearkombinationen des Superpositionsprinzips zum

Ausdruck kommt. Es gibt aber noch ein anderes Phänomen, welches diese Begrifflichkeit umfasst: Einsteins „Quantenspuk“, also die Verschränkung, welche ganz besonders für das Quantenrechnen charakteristisch ist. Betrachten wir wieder Abb. 2.4c: Wenn zum Beispiel am Eingang das Kontrollbit auf den Superpositionszustand $|0> + |1>$ und das Targetbit auf $|0>$ gesetzt wird, erzeugt ein CNOT-Gatter einen verschränkten Bell-Zustand (ohne Normierungsfaktor):

$$\Phi = |0\rangle_{\text{Kontrolle}}|0\rangle_{\text{Target}} + |1\rangle_{\text{Kontrolle}}|1\rangle_{\text{Target}}.$$

Die Qubits sind also durch die Gatterfunktion miteinander verschränkt worden. Ein verschränkter Zustand ist dadurch charakterisiert, dass er sich sich nicht aus einzelnen Teilzuständen der Systemkomponenten zusammensetzen lässt, sondern er ist ein völlig neu erzeugter Zustand, der nicht faktorisierbar ist. Im Fachjargon sagt man, er ist „nicht von Produktform“, da er nicht als Tensorprodukt einzelner Qubit-Zustände geschrieben werden kann. Der Superpositionszustand (Eingang Kontrollbit) wird übrigens durch ein single Hadamard-Gatter erzeugt, das auch Superpositionen aller Qubits in einem Register erzeugen kann. Wenn man zwei oder mehr Qubits als einen einzigen Quantenzustand betrachtet, so entspricht er dem Tensorprodukt der einzelnen Qubits im Register. Hierin liegt der formale Unterschied zwischen superponierten Qubits (als Tensorprodukt beschreibbar) und verschränkten Qubits (nicht als Tensorprodukt darstellbar).

Universelle Quantengatter

Grundsätzlich ist anzumerken, dass Quantencomputer im Unterschied zum klassischen Pendant keine universell programmierbaren Rechner sind. Bei herkömmlichen Computern können beliebige Schaltkreise aus wenigen

Grundgattern aufgebaut werden (beispielsweise aus einer geeigneten Schaltung von NAND-Gattern). Für Quantencomputer sind derartige Zerlegungen in universelle Gatter aber ebenso möglich. Eine Menge (oder „Familie“) von Quantengattern bezeichnet man dann als universell, wenn jede beliebige (unitäre) Transformation als Schaltkreis mit Quantengattern darstellbar ist. Man kann zeigen, dass ein CNOT- Gatter verknüpft mit single Qubit- Gattern universell ist. Ein wichtiges Beispiel für ein Single -Gatter ist das oben angesprochene Hadamard- Gatter (auch Hadamardtransformation H genannt). Es erzeugt einen Superpositionszustand aus den Basisvektoren $|0\rangle$ und $|1\rangle$, d. h. entweder $|0\rangle \rightarrow H \rightarrow |0\rangle + |1\rangle$ oder $|1\rangle \rightarrow H \rightarrow |0\rangle - |1\rangle$ mit jeweils 50 % Wahrscheinlichkeit. In dieser Darstellung wird auf Normierungsfaktoren verzichtet, die wegen der Bedingung auftreten, dass die Wahrscheinlichkeit in der Quadratsumme 1 (100 %) beträgt. Andere Beispiele für Single-Gatter sind etwa Pauli-, Wurzel-NOT- oder die „Familie“ der Phasenschieber-Gatter.

Weitere verschränkte Zustände können durch Kombination von CNOT- mit Single-Qubit-Gattern erzeugt werden, was diese Auslegung universell macht. Damit ist theoretisch ein „universeller“ Quantencomputer realisierbar. Das ist nun auch sehr spannend, denn es bedeutet, dass jede Transformation, welche die Quantenmechanik erlaubt, auf einem Quantencomputer theoretisch implementiert werden kann. Bei entsprechender Skalierung kann auf diese Weise nicht nur jedes Quantenprogramm ablaufen, sondern es erlaubt die Simulation vieler physikalischer Systeme selbst. Manche Experten sind sogar der Meinung, der Quantencomputer könne das ganze Universum abbilden. So wäre bereits ein 300 Qubit-Rechner gleich mächtig wie ein Computer, der jedes Atom im sichtbaren Universum als Speicherzelle verwendet.

Wie rechnet ein Quantencomputer?
Wir wollen uns nun die Simulation eines Quantenschaltkreises ansehen, welcher auf dem Deutsch-Algorithmus basiert (benannt nach dem israelisch-britischen Physiker David Deutsch). Das gewählte Beispiel mag auf den ersten Blick trivial erscheinen, aber vergessen wir nicht, dass bereits aktuelle Computer nur deshalb so irrwitzig viel können, weil ebenso irrwitzig viele Operationen in extrem kurzer Zeit abgearbeitet werden. Wie oben angesprochen, kann ein klassischer Computer bei exponentieller Zunahme von Operationen hingegen auch zur lahmen Krücke verkommen. Es sind deshalb neue Konzepte gefragt. Die Aufgabenstellung: Gegeben sei die Funktion f: $(0,1) \rightarrow (0,1)$ mit der Vorschrift an den Computer: Bilde die Summe $f(0) + f(1)$ modulo 2 (d. h. $0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 0 = 1$ und $1 + 1 = 0$). Die Inputzahlen seien dem Computer allerdings zunächst unbekannt, er muss sie also erst aufrufen. Man beachte dabei die Tatsache, dass ein klassischer Computer zur Berechnung der Ergebnisse die Funktionen jeweils *zweimal* aufrufen muss. Denn aus der Kenntnis des einen Funktionswerts folgt ja nicht die Kenntnis des anderen. Nun sei der Computer ein Quantencomputer. Selbe Aufgabenstellung. Wir werden gleich sehen, dass dieser für die Berechnung nur *einen* einzigen Aufruf benötigt und somit die Aufgabe im Prinzip in der halben Zeit löst. Nehmen wir als einfachste Möglichkeit einen 2-Qubit-Prozessor an. Die Basiszustände an den beiden Eingängen werden auf den für Quantenrechner üblichen Inputzustand $|0\rangle$ gesetzt. Was sich daraufhin in der Blackbox abspielt, lässt sich wie bei klassischen Computern durch einen Quantenschaltkreis (Abb. 2.4d) darstellen. Dabei stehen N für das NOT-Gatter, H für die Hadamard-Transformation und U_f für den Funktionsaufruf.

Input	Funktion	Output	Messung	Addition
$\|o\rangle\|o\rangle$	$f(0)=0 \quad f(1)=0$	$\|o\rangle\|1\rangle$	0	0 + 0 = 0
$\|o\rangle\|o\rangle$	$f(0)=1 \quad f(1)=1$	$-\|o\rangle\|1\rangle$	0	1 + 1 = 0
$\|o\rangle\|o\rangle$	$f(0)=0 \quad f(1)=1$	$\|1\rangle\|1\rangle$	1	0 + 1 = 0
$\|o\rangle\|o\rangle$	$f(0)=1 \quad f(1)=0$	$-\|1\rangle\|1\rangle$	1	1 + 0 = 1

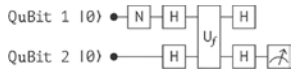

Abb. 2.4d Quantenschaltkreis und Simulation

Wie anhand der Tafel (Abb. 2.4d) zu entnehmen ist, entsprechen die Messwerte genau den Lösungen der gestellten Aufgabe, nämlich der Addition modulo 2. Das Revolutionäre besteht darin, dass durch einen einzigen Funktionsaufruf alle Funktionswerte „gleichzeitig" im Superpositionszustand enthalten sind. Zwar erlauben die Gesetze der Quantenmechanik nicht die genaue Kenntnis der Funktionswerte, sehr wohl aber die Berechnung der Funktionsvorschrift. Ebenso zeigt dieses Prinzipbeispiel, dass ein Quantencomputer die „passende" Aufgabenstellung benötigt, um seine Fähigkeiten voll entfalten zu können. Insgesamt mag dieses Beispiel nicht weiter weltbewegend wirken, kann jedoch bei viel komplexeren Operationen mit exponentiell ansteigendem Rechenaufwand eine zig milliardenfach kürzere Rechenzeit bedeuten. Damit können Quantenrechner in bestimmten Anwendungen einen erheblichen Speed-up bewirken.

2.5.4 Konzepte

Quantencomputer ersetzen die traditionellen Transistoren durch Qubits, die durch physikalische Ressourcen (wie beispielsweise den Elektronenspin oder Suprastöme) implementiert werden. Der exponentiell vergrößerte Rechenraum wird durch eine zentrale Wellenfunktion

beschrieben, welche durch die Superposition aller möglichen klassischen Zustände repräsentiert ist. Erst die Messung erzeugt einen konkreten Zustand, dessen Wahrscheinlichkeit durch das Amplitudenquadrat der Wellenfunktion gegeben ist. Im Unterschied zum klassischen Computing, das auf diverse Prozessorkerne aufgeteilt wird, müssen Wahrscheinlichkeitsamplituden konstruktiv übereinstimmen, um eine Lösung des interessierenden Problems darzustellen. Erfolgreiches Quanten-Computing wird daher manchmal auch mit einem perfekt eingestimmten Orchester verglichen, bei dem ein (klassischer) Dirigent Takt und Phrasierung vorgibt. Entsprechend den Vorgaben gibt es verschiedene Konzepte zur Realisierung. Wir wollen hier kurz drei davon ansprechen.

Schaltkreismodell

Hierbei handelt es sich um ein algorithmisches Modell, das stark an klassische Computer erinnert (siehe Simulation oben).Um Rechenergebnisse zu erzielen, muss ein Quantenprogramm absolviert werden, das aus einem Quantenschaltkreis und einem oder mehreren abschließenden Messungen besteht. Die Ergebnisse der Messungen sind als Wahrscheinlichkeiten interpretierbar, ggf. muss das „Programm“ mehrfach ablaufen, um die Ergebnisse zu verifizieren. Ein Quantenschaltkreis besteht aus mehreren Quantenlogikgattern, welche in fester zeitlicher Abfolge auf das Quantenregister angewendet werden. Zwar können einzelne Operationen reversibel ablaufen (wie beim CNOT), dies gilt jedoch nicht über den gesamten Algorithmus gesehen; dieser folgt einer klassischen Abfolge von Anweisungen. Wie angesprochen bleiben üblicherweise alle Operationen auf Single- und 2-Qubit-Gatter beschränkt. Diese werden auf ein Set von

Qubits angewendet, woraufhin die Resultate ausgelesen und am Ende als Output einer Single-Qubit-Messung dargestellt werden. Konkret wird zunächst jeder Basiszustand zur Computation vorbereitet. In der Blackbox wirkt eine universelle Familie von Quantengattern auf die Qubits in der gewünschten Weise ein. Die Quantenalgorithmen laufen durch Anwenden von Single- und 2-Qubit-Gattern auf der Computational Basis (Blackbox) ab. Wie ebenso dargelegt, kommen in der Regel Gatter der Typen H, CNOT, Pauli- und Phasengatter, usw. zum Einsatz (es gibt aber auch Multi-Qubit-Gatter). Dabei baut sich das nötige Maß an Verschränkung auf, was den Speed-up des Quantencomputers bewirkt. Falls irgendwelche Hilfszustände verwendet werden, muss deren Zustand gelöscht werden, damit sie nicht mit den restlichen Qubits bei der Computation interferieren. Die letzte Messung an der Computational Basis ergibt das Resultat. An dieser Stelle sei noch einmal darauf hingewiesen werden, dass Quantengatter weder technische noch elektronische Bauteile repräsentieren, sondern in einer physikalischen Manipulation an ein oder mehreren Qubits bestehen. Dabei ist die Art der Manipulation von der benutzten Implementierung abhängig. Üblicherweise werden etwa Anregungszustände von Atomen durch Laserpulse, Kern- oder Elektronenspins dagegen durch Magnetfelder beeinflusst.

Einweg-Quantencomputer

Ein genauso leistungsfähiges Konzept, das anders als das Schaltkreismodell in der klassischen Informatik kein Analogon kennt, beruht auf der messbasierten Computation. Zunächst wird in der Regel ein universeller Quantenzustand (meist ein stark verschränkter „Multiparticle State“) hergestellt und die Rechnung durch eine Reihe

gezielter Messungen an diesem Zustand durchgeführt. Dabei bestimmen die Ergebnisse früherer Messungen, welche weiteren Messungen durchgeführt werden. Die gesamte Ressource wird also schon zu Beginn bereitgestellt, und die Information wird dann durch eine Serie adaptiver Single-Qubit-Messungen gewonnen. Das Prinzip verhält sich sozusagen wie der sagenhafte Turm, der alle Bücher enthält, die jemals geschrieben wurden – und man sucht dann aus dieser Unzahl von Büchern nur jene verschwindend kleine Teilmenge heraus, die von persönlichem Interesse ist. Die Bezeichnung rührt von der Tatsache her, dass gleich zu Beginn eine möglichst große Zahl verschränkter Qubits bereitgestellt wird. Das Computing erfolgt daraufhin durch Messung einzelner Qubits, wodurch die Verschränkung des Ausgangzustands nicht mehr rückgängig gemacht werden kann (daher auch „Einweg") – im Unterschied zum Schaltkreismodell, wo sich die Verschränkung erst durch Anwenden entsprechender Gatteroperation sukzessive aufbaut. Um das Ergebnis zu erhalten, ist der parallele Einsatz klassischer Computer essenziell, zumal die Messbasis sequenziell von der früheren Ergebnissen abhängt. Dieses messbasierte System bildet auch die Grundlage für das Blind-Quantencomputing (BQC) und somit für eine inhärent sichere Quanten-Cloud. Auf Basis des Einweg-Computers konnte Stephanie Barz in einem Proof of concept bereits 2012 Blind-Quantencomputing realisieren.

Zum besseren Verständnis noch ein konkretes Beispiel: Nach dem Prinzip der Parametric Down conversion erzeugt ein spezieller Laser zwei verschränkte EPR-Paare (also 4 Photonen, von denen jeweils zwei in der Polarisation miteinander verschränkt sind). Daraufhin werden die EPR-Paare mit polarisierenden Strahlteilern

paarweise verschränkt. Dieses System kann man als Einweg-Quantencomputer betrachten, dem folgende Aufgabe gestellt wird: es sind 4 Bits in einem Register gegeben, von denen drei den Wert 0 besitzen und eines den Wert 1 hat. An welcher Stelle im Register ist 1? Während ein klassischer Computer für diese Aufgabe im Schnitt 2,25 Bits überprüfen muss, benötigt der Quantencomputer dagegen nur einen einzigen Schritt. Die Wahrscheinlichkeit für die korrekte Lösung liegt bei 90 %, d. h. in 9 von 10 Versuchen liefert der Quantencomputer das richtige Ergebnis. Freilich ist das nur ein Proof of principle (das tatsächlich durchgeführt wurde) – eine technisch verwertbare Implementierung dieser Art müsste einen Cluster von mindestens hundert Qubits bereitstellen, was experimentell nahezu unmöglich wäre.

Adiabatischer Prozessor („Quantum Annealing“)

Gerade deshalb, weil ein riesiger Qubit-Cluster technisch sehr schwer zu realisieren ist, sucht man nach einer „natürlichen“ Ressource und folgt damit der Grundidee des Quantensimulators.

Ein dahin gehender Ansatz liegt deshalb dem adiabatischen Quantencomputer zugrunde, welcher den Grundzustand eines quantenmechanischen Systems ausreichend langsam in einen anderen, einfacher auslesbaren Zustand überführt. Das Wort adiabatisch stammt aus der Wärmelehre, wo es ein System bezeichnet, das keine Wärme mit seiner Umgebung austauscht. Bezogen auf Quantencomputer beschreibt es eine physikalisches System, bei dem ein interessierender Quantenzustand nicht verloren geht. Den Gesetzen der Quantenmechanik zufolge verbleibt ein quantenmechanisches System (das sich im Grundzustand befindet) auch bei seiner Veränderung im Grundzustand, solange diese nur hinreichend langsam

(adiabatisch) vor sich geht. Die Idee besteht nun darin, die Lösung eines Problems auf einen zunächst unbekannten quantenmechanischen Grundzustand eines Systems abzubilden. Daraufhin wird ein zweites, viel leichter zu präparierendes System hergestellt und dieses adiabatisch in das erste überführt. Geschieht dies hinreichend langsam, so bleibt der interessierende Grundzustand erhalten und kann anschließend gemessen werden. Dabei verändert sich der Anfangszustand (Initial State) adiabatisch zum Zielzustand (Target State), in dem die Lösung codiert vorliegt. In dieser Auslegung sind zwingend klassische Computer erforderlich, um den Zustand zu „decodieren", der das Problem enthält. Diese Bauart ist vor allem durch ein kanadisches Start-up bekannt geworden, das bereits seit Jahren kommerzielle Anwendungen dieses Prinzips anbietet. Die Bezeichnung „Quantum Annealing" ist sozusagen die Quantenversion vom sicher bekannteren Begriff Simulated Annealing. Dabei handelt es sich um ein heuristisches Approximationsverfahren, das als Näherungslösung herangezogen wird, wenn das vorliegende Problem eine zu hohe Komplexität besitzt. Das Konzept unterliegt allerdings der Einschränkung, dass der adiabatische Rechner im normalen Arbeitszustand kein universeller Quantencomputer ist und hauptsächlich Optimierungsprobleme löst.

2.5.5 Implementierungen (Beispiele)

Nachdem nun das Grundprinzip des Quantencomputers umrissen wurde, stellt sich die sehr viel schwierigere Frage nach konkreten Realisierungen. Hier ist zunächst einmal völliges Umdenken erforderlich. Während bei einem klassischen Computer die kleinste Informationseinheit, das Bit, in der Regel durch einen Spannungswert dargestellt wird,

der einen vorher definierten Pegelwert entweder übersteigt (1) oder darunter liegt (0), muss das Quantenbit dagegen durch eine Linearkombination der Basisvektoren I0> und I1> repräsentiert sein. Wie angesprochen, bedeutet ein single- Qubit für den Quantencomputer rein gar nichts, deshalb dreht sich alles um die Frage: Wie können sehr große Quantenregister realisiert werden, die einerseits speicherbar, andererseits manipulierbar und messbar sein sollen? Immerhin müssen darauf ja sehr komplexe Superpositionen beziehungsweise verschränkte Zustände herstellbar sein. Die technischen Herausforderungen sind gewaltig, da jegliche Interaktion mit der Umgebung einer ungewollten Messung gleichkommt, welche die Quantenkohärenz beeinträchtigt oder zerstört. Dies macht eine nahezu perfekte Abschirmung und Stabilität der äußerst fragilen Qubits erforderlich. Ähnlich dem analogen Computer handelt es sich um Systeme mit kontinuierlichen Amplituden (Wellenfunktion!), die weitaus fehleranfälliger sind als herkömmliche digitale Pendants.

Relaxation und Dekohärenz

Eine grundsätzliche Schwierigkeit bei der Realisierung von Quantencomputern hängt mit den Phänomenen Relaxation, Dekohärenz und Fehlertoleranz zusammen. Eng damit verbunden ist auch die Suche nach einer möglichen Architektur und damit insbesondere nach einem geeigneten Konzept zur Skalierung (Erhöhung der Qubitzahl). Als Generalproblem erweist sich hier das fehlertolerante Rechnen, das heißt, unvermeidliche Fehler dürfen unabhängig von Zahl und Entfernung der Qubits das Ergebnis nicht unzulässig verfälschen. Hinzu kommt, dass die sogenannten Dekohärenzzeiten viel länger sein müssen als die für die Gatteroperationen benötigten Zeiten, sodass eine Korrektur durch Fehlercodierung möglich ist. Mit dem Begriff Relaxationszeit ist jener charakteristische

Zeitraum gemeint, bis ein präpariertes Quantensystem in seinen stationären Zustand übergeht. Im Alltag kennt jeder das Phänomen, dass ein zu Beginn kühles Glas Bier allmählich die wärmere Umgebungstemperatur annimmt (und dann nicht mehr schmeckt), also ein thermisches Gleichgewicht anstrebt. Ebenso führt das bei einem Qubit dazu, dass es aus dem Zustand $|1\rangle$ nach einer gewissen Zeit in den Zustand $|0\rangle$springt. Die Wahrscheinlichkeit für solch ein Ereignis wächst in der Regel exponentiell mit der Zeit an. Ein ähnlich exponentielles Zeitverhalten zeigt zumeist auch die Dekohärenz, welche den Verlust der Superposition von Quantenzuständen bezeichnet. Ein dekohärentes Qubit verhält sich nur noch wie ein klassisches Bit und wäre somit wertlos. Selbstredend müssen Dekohärenz- und Relaxationszeiten ausreichend lang bemessen sein, damit die Quantencomputation überhaupt zuverlässig durchgeführt werden kann. Dabei geht es in der Praxis meist um winzige Bruchteile einer Sekunde, in denen auch noch Quantenfehlerkorrekturen durchzuführen sind, um die Verlässlichkeit zu gewährleisten. Damit tut sich das nächste Problemfeld auf: klassische Verfahren wie Redundanz (Daten perfekt kopieren, mehrfach speichern und vergleichen) sind hier aufgrund des No-Cloning-Theorems gänzlich ausgeschlossen. Es ist aber möglich, Teile der Quanteninformation eines Qubits auf ein verschränktes System mehrerer Qubits zu übertragen. Dazu kann eine Art Code generiert werden mit dem sich die partielle Information eines Qubits in dem verschränkten System zwischenspeichern lässt. Danach wird eine spezielle Messung an den Qubits durchgeführt, welche die relevante Quanteninformation nicht stört, und sogar eine Information über die Art des Fehlers preisgibt (Syndrommessung). Damit kann bestimmt werden, ob und welches Qubit in welcher Weise beschädigt wurde. Ebenso wird das System durch die Messung in einen

Zustand gezwungen, der die anschließende Fehlerkorrektur erleichtert. Die Suche nach skalierbaren, fehlertoleranten Quantensystemen sowie Quantengattern, die auf verschiedenen Qubits parallel ausgeführt werden können, bleibt auf jeden Fall eine wichtige Aufgabe der aktuellen Forschung. Von den unzähligen Implementierungen, mit denen dies bis dato versucht wurde, sei im Folgenden eine Auswahl angesprochen.

Ionencomputer und Netzwerk

Wie dargelegt, können Qubits auf geladenen Atomen (Ionen) implementiert, kontrolliert und manipuliert werden, und das mit sehr hoher Genauigkeit. Gute Resultate erreicht man mit makroskopischen Ionenfallen bei hoher Fidelity in allen Gattern, eingeschränkt allerdings durch einen bescheidenen Skalierfaktor, das heißt, man kann nur wenige Ionen einfangen und individuell adressieren. Problematisch ist auch, dass sich eine Kette gefangener Ionen ab einer Länge von etwa 14 Qubits zunehmend wie normale Bits verhält. Um die Leistungsfähigkeit zu steigern, wäre ein Mini-Quanteninternet wünschenswert, in dem kleine Nodes (mit jeweils wenigen Qubits) zusammengeschaltet werden – was auch bereits demonstriert werden konnte. Mit diesem System ist ebenso Quantencomputing möglich und es ist auch für größere Architekturen vorstellbar. Die Verschränkung der Zellen wird auf Basis der Cavity-QED durch mobile Photonen erreicht, ähnlich der vorhin besprochenen Schnittstellentechnik. Allerdings laufen die Operationen ziemlich langsam ab und benötigen außerdem eine große Anzahl von Switches, welche zu spürbaren Photonenverlusten führen. Demnach gilt es vordringlich, Switches mit sehr geringem „Loss“ zu schaffen. Ein neuer Zugang sind deshalb integrierte Ionenfallen, in denen standardmäßige Halbeiterprozessoren verwendet werden, um Chipfallen im

Mikrometerbereich zu realisieren. Dazu werden Ionen mit lokalen Magnetfeldern auf Silicium-Trägerelementen in Mikrowellenresonatoren gefangen – dies ist deutlich besser, als jedes Ion einzeln zu manipulieren, zumal die Laser dafür ultrapräzise ausgerichtet sein müssen. Ein weiterer Vorteil ist, dass weniger Kühlleistung benötigt wird (auf „nur" circa $70\ \mathrm{K} = -203,15\ ^\circ\mathrm{C}$). Unterstützt wird das Verfahren durch eine Stickstoffkühlung, die in über den Chipmodulen angebrachten Mikrokanälen verlaufen. Darin besteht auch ein großer Vorteil gegenüber Ansätzen mit klassischen Supraleitern, die einen viel größeren Kühlaufwand erfordern. Weitere Ansätze bestehen darin, die Quanteninformation nicht mehr durch Laser auszulesen, sondern dafür eigens angepasste Rechenmodule einzusetzen. Diese sind in kleinen modularen Vakuumzellen untergebracht, wobei dann auch gleich spezifische Fehlerkorrektursysteme implementiert werden. Insgesamt ein vielversprechendes Konzept, das jedoch für eine hohe Leistungsfähigkeit sehr viele Qubits braucht, wozu es dann doch noch sehr viel zu tun gibt. Dennoch ist man optimistisch, wie so manches Start-up beweist.

Supraleiter-Qubits

Ein Supraleiter ist ganz allgemein ein Material, das bei Unterschreiten einer spezifischen Sprungtemperatur (die im Allgemeinen sehr tief liegt) einen Phasenübergang erfährt und danach einen Stromfluss ohne elektrischen Widerstand ermöglicht. Schon heute besitzt dieser merkwürdige Quanteneffekt einen festen Platz in vielen technischen Anwendungen. Dazu zählen etwa die Erzeugung starker Magnetfelder oder deren hochempfindliche Messung. Eine oft angedachte Zukunftsvision spart auf diese Weise enorme Mengen an elektrischer Energie ein. Dabei gilt es allerdings zu bedenken, wie viel Energie zur Kühlung notwendig wäre, was den Vorteil gleich wieder

infrage stellt. Auf der theoretischen Ebene gibt es viele Erklärungsansätze und Modelle, die nach wie vor diskutiert werden. Auf der praktischen Ebene sucht man intensiv nach „heißen“ (bei Raumtemperatur funktionierenden) Supraleitern, etwa für Hochspannungsleitungen der Zukunft oder Magnetschwebebahnen, welche praktisch ohne Reibung unterwegs wären. Für Quantencomputer eröffnen sich ebenso viele Möglichkeiten, wenn es gelingt, supraleitende Qubits zu implementieren. Ein Beispiel ist das sogenannte SQUID, ein supraleitender Ring, der in der Mitte durch einen sehr dünnen Isolator unterbrochen ist. Durch diesen mikroskopischen Spalt können Elektronenpaare hindurch-„tunneln“, wobei die Qubits in Superpositionen von gegenläufig fließenden Suprastrømen bestehen. Was in der klassischen Physik völlig unmöglich wäre, ist in der Welt der Quantentheorie dagegen ganz alltäglich. Versuche an Single-Qubit-Gattern erreichen bereits 99,9 % und auch bei 2-Qubit-Gattern noch 99,4 % Fidelity. Zudem liegt diese „Wiedergabetreue“ (Maß für die Fehlerrate) innerhalb der Toleranzgrenze für den Fehlercode, was die Implementierung spezieller Qubit-Anordnungen erlaubt. Obwohl dieses System von der Miniaturbauweise seiner Devices profitiert, hat es dennoch mehrere Nachteile. Einer davon betrifft den „Crosstalk“ zwischen den eingesetzten Nanokabeln – damit sind dreidimensionale Strukturen kaum möglich (dies wäre vorteilhaft, auch für die Fehlertoleranz). Der größte Nachteil ist aber, dass die infrage kommenden Supraleiter nur in der Nähe des absoluten Nullpunkts (−273,15 °C) funktionieren, was ein Problem für die Skalierung bedeuten kann, allein schon aufgrund beschränkter Kühlkapazitäten. In der Öffentlichkeit bekannt geworden ist diese Implementierung vor allem durch die „Quantenabteilung“ von Google.

Photonencomputer

In früheren Ansätzen scheiterte ein auf mehreren Photonen basierendes Konzept zur Realisierung von Quantencomputern immer an unzureichenden Methoden zur Herstellung und Manipulation von verschränkten Photonenpaaren. Mittlerweile hat sich das Bild geändert: auf Basis der sogenannten kohärenten Photonenkonversion gelingt es, Photonen miteinander in eine spezielle Wechselwirkung zu bringen, ohne die Quanteninformation dabei zu zerstören. Dazu wird das Licht zweier Einzelphoton-Laser von unterschiedlicher Wellenlänge (und damit Energie) gleichzeitig in eine faseroptische Leitung eingebracht. Im Gesamteffekt kann dann ein relevanter Einphotonenzustand in einen Zweiphotonenzustand umgewandelt, also konvertiert werden. In der Regel interagieren Photonen überhaupt nicht mit ihrer eigenen Spezies, was man alleine schon daran erkennt, dass die gekreuzten Lichtkegel zweier Taschenlampen ungehindert übereinander hinweglaufen. Photonen sind also sozusagen isoliert und erweisen sich deshalb als sehr gute Träger von Quanteninformation. Dies bildet auch die Basis der linearen Optik, wo man davon ausgeht, dass sich die optischen Eigenschaften eines Materials unabhängig von der Intensität des eingestrahlten Licht verhalten. Will man Licht aber für Quantencomputer nutzen, benötigt man notwendigerweise eine Wechselwirkung zwischen einzelnen Photonen. Diese wird durch sogenannte hoch-nichtlineare optische Materialien möglich, deren Verhalten durch die Intensität des eingestrahlten Laserlichts beeinflusst wird. Vor Jahren wurde dieses Konzept bereits von Physikern der Universität Wien sowie aus Japan und Australien vorgeschlagen. Nicht genau vorhersagbare 2-Qubit-Operationen sowie Photonenverluste sind allerdings noch eine große Herausforderung für diese Technologien. Eine Reihe von theoretischen Durchbrüchen zusammen mit technischen

Fortschritten machen dieses System aber zu einem kompetitiven Mitstreiter im Wettlauf um den Quantencomputer. Die Architektur verwendet einen ähnlichen Ansatz wie der Einweg-Quantencomputer. Die Fähigkeit zur Miniaturisierung optischer Elemente auf einem einzigen Chip mithilfe der Nanofabrikationstechnik ist zudem ein erfolgsversprechendes Zeichen für die potenzielle Realisierung optischer Quantencomputer mit Millionen von Elementen pro Chip. Ein weiterer Vorteil besteht darin, dass Kühleinrichtungen nur für die Photonendetektoren benötigt werden und schließlich ganz wegfallen sollten. Neueste Untersuchungen weisen darauf hin, dass in ähnlicher Weise auch Dreiphotonzustände erzeugt werden könnten, woraus sich neue Gesichtspunkte für die Realisierung des Photonencomputers ergeben.

2.5.6 Quantum Supremacy

Ein Markstein für den aktuellen Entwicklungsstand von Quantencomputern ist der Begriff der „Quantum Supremacy", zu Deutsch etwa „Quantenüberlegenheit". Dieser von dem amerikanischen Theoretiker John Preskill geprägte (durchaus vage) Begriff bezeichnet jenen Punkt, an dem es Quantenprozessoren erstmals gelingen sollte, die Rechnerleistung selbst von Supercomputern (zumindest in bestimmten Applikationen) zu übertrumpfen. Seit Jahren arbeiten verschiedene Forscherteams, vor allem aber auch Hightechgiganten wie IBM oder Google intensiv daran, dieses Ziel zu erreichen. Als Beispiel für diesen Optimismus sei John Martinis vom Google Research Lab an der Uni Kalifornien in St. Barbara genannt. Dieser holte führende Wissenschaftler zusammen, um einen Prototyp mit 22 Qubits in zwei Reihen von je 11 Qubits zu demonstrieren. Als Nächstes ging ein Quantenchip mit 49 Qubits

in Betrieb – im 7 × 7-Format und auf Basis von Supraleiter-Qubits. Verglichen mit Ionenrechnern, wie sie etwa sein Kollege Chris Monroe an der Uni Maryland betreibt, sind Martinis' Qubits geradezu als riesig zu bezeichnen. Dieses Bauteil esteht aus einem kleinen Metallkreuz von etwa 0,5 mm Länge, das aus einer Folie herausgeschnitten ist. An seinen Enden befindet sich ein Josephson-Kontakt, bestehend aus zwei supraleitenden Schichten mit einem extrem dünnen Isolator dazwischen, ähnlich wie bei einem SQUID (siehe oben). Sodann wird dieser „Sandwich" bis nahe am absoluten Nullpunkt heruntergekühlt, wodurch sein Verhalten nur noch quantenmechanisch erklärbar wird: Infolge des quantenmechanischen Tunneleffekts können Elektronen durch die Isolationsschicht durchtunneln, was das Gebilde zu einem Qubit macht. Möglich wird das, weil der Strom dank Superpositionsprinzip und Supraleitertechnik in beiden Richtungen gleichzeitig fließt. Gesteuert und ausgelesen wird über Mikrowellen im GHz-Bereich. Diese elektromagnetische Strahlung dient auch zur Verschränkung der Qubits. Freilich geht es hier erst einmal um einen Systemtest, der den Quantencomputer von der reinen Grundlagenforschung in eine konkrete Technologie überführen soll. So werden nur zufällig einige Quantengatter geschaltet, was für sich allein noch keinen nutzbaren Algorithmus ergibt. Dennoch zeigt sich Martinis optimistisch und sieht sein Projekt auf einem guten Weg. Wichtig sei vor allem die Qualität der Qubits und die damit verbundene niedrige Fehlerrate. Diese gestatte bereits mehrere hundert Operationen, bevor die Qubits ein Opfer der Dekohärenz werden. Neueren Medienmeldungen zufolge ist ein 72-Qubit-Chip implementiert worden, welcher der „Supremacy" noch näherkommen soll. Im ständigen Wettstreit mit IBM und chinesischen Forschern – auch die Volksrepublik investiert erheblich in diese Zukunftstechnologie – plant Google

einen ersten echten Fähigkeitsnachweis des Quantencomputers zu erbringen.

Der Wettlauf hat begonnen

Der Run auf den Quantencomputer hat längst eingesetzt. Neben vorwiegend amerikanischen Computer- und IT-Riesen sind hier auch Europa, vor allem jedoch China als wichtige Wettbewerber zu nennen. Namhafte Firmen bieten via Internet heute schon einen Zugang zu Quantenprozessoren an. Allerdings hat das noch nichts mit einer „echten" Quanten-Cloud zu tun, sondern entspricht eher einem spielerischen Kennenlernen in sehr rudimentären Aspekten. Der Grundgedanke erscheint jedoch zukunftsweisend: Eines Tages könnte eine weltweite Community an der Entwicklung von Quantensoftware direkt beteiligt sein. Dennoch sollten die Erwartungen im Moment keinesfalls zu hoch angesetzt werden. Verglichen mit der Entwicklung herkömmlicher Computer ist gerade einmal das Kleinkindstadium erreicht. Wie man weiß, lag die Leistungsfähigkeit der allerersten Computer um Lichtjahre von heutigen Standards entfernt. Auf der anderen Seite leben wir heute in einer hochtechnologischen Zeit, wo Entwicklungssprünge in immer kürzerer Zeit erfolgen. Dazu trägt vor allem auch die weltweite Kommunikation über das Internet bei, wodurch auch die Wissenschaft im ständigen interkontinentalen Austausch steht. Die zentralen wissenschaftlichen Herausforderungen auf dem Weg zum Quantenrechner liegen in den folgenden Punkten: So sollte etwa die Fidelity möglichst nahe bei 100 % liegen, um die Voraussetzungen für effiziente Fehlerkorrekturverfahren zu ermöglichen. So muss man sich vor Augen halten, dass eine Fehlerrate von lediglich 0,1–1 % in praxistauglichen Realisierungen um die 10.000 zusätzliche Qubits zur Redundanz erforderlich macht. Es sind

demnach Systeme gefragt, die einen derart absurden Komplexitätszuwachs vermeiden. Ebenso wichtig sind die Kohärenzzeit und die Geschwindigkeit der Gatter. Vor allem gilt es auch, Initialisierung und Auslesequalität und -geschwindigkeit der Qubits zu verbessern, um sinnvolle Fehleralgorithmen realisieren zu können. Vermutlich am wichtigsten ist die Suche nach skalierbaren Architekturen. Hierzu ist die Herstellung entsprechender Chips ebenso nötig wie auch die klassische Kontrolle der Operationen mittels optimierter Kontrollspannungen, auch bei Laser-, Radiowellen- oder Mikrowellenpulsen. Schließlich müssen auch die klassische Hardware und diejenige vom Quantencomputer optimal aufeinander abgestimmt werden. Weitere Entwicklungsziele liegen in der Kompatibilität mit üblichen Halbleiterfertigungsprozessen. Experten lassen sich im Moment noch kaum zu einer Prognose hinreißen, halten jedoch einen Zeitraum von 10–20 Jahren bis zu einem ersten echten Durchbruch für wahrscheinlich. Ist dieser erst einmal geschafft, könnte die weitere Entwicklung dann sehr rasant gehen und heute noch ungeahnte Entwicklungen anstoßen. Bis dahin gilt es allerdings, Wege zu finden, um mit den ungeheuren technischen Schwierigkeiten fertig zu werden, die hier gerade skizziert wurden. Physikalisch gesehen ist vor allem interessant, inwieweit man die Dekohärenz besiegen kann.

Die andere Seite der Medaille betrifft das Geschäft, also den potenziellen Marktwert dieser Technologie, und damit globales Interesse, Investment und Prestige. Letzteres spielt gerade in Ländern wie China gewiss eine wichtige Rolle. Dennoch räumen Kritiker ein: Auch wenn die Supremacy erreicht werden sollte, also ein Quantenrechner in relevanten Algorithmen einen klassischen erstmals outperformen kann, was wäre damit gewonnen? Kosten und Komplexität würden die Sinnhaftigkeit stark limitieren. Zudem werden natürlich auch klassische Rechner weiterentwickelt,

sie sind schon heute universell einsetzbar – und das weit ökonomischer: Wozu einen Jumbo chartern, nur um die Straße zu überqueren? Die Firmen-Labs stehen offenbar unter einigem Druck. Bei der Zukunftsware Quantencomputer wird hoch gepokert, und dabei kann man am Ende viel verlieren. Solche Aussichten könnten Investoren abschrecken, die jetzt schon hunderte Millionen Dollar auf Start-ups gesetzt haben. Bedenkt man allerdings die Summen, die anderswo im Spiel sind, kann man im Sinne eines strategischen Investments den Quantenrechner durchaus riskieren, denn sein Wert könnte eines Tages umso höher liegen. Im Übrigen hinkt der Vergleich mit einem klassischen Computer: Hier geht es um kein Substitut, sondern um spezielle Applikationen, die klassisch noch gar nicht angegangen werden können. Faktum ist: ab etwa 50 Qubits droht ein klassischer Rechner an seiner eigenen Komplexität zu ersticken und kann bestimmte Probleme gar nicht mehr sinnvoll behandeln. Genau hier setzt der Quantencomputer an. Letztlich geht es um das Unnachahmliche, das Innovative, um völlig neue Lösungsansätze und Gesichtspunkte, die der Quantenrechner einst liefern könnte. Vom wissenschaftlichen Wert und Nutzen reden wir da erst gar nicht. John Preskill sagt sinngemäß, dass man Quantum Supremacy weder missverstehen noch überbewerten sollte. Seiner Einschätzung nach befinde man sich im Moment in einer durch die Dekohärenz bedingten Anfangsära („noisy Stage“) Der Quantencomputer werde aber letztlich eine revolutionäre Auswirkung auf die Menschheit haben. In jedem Fall bleibt festzuhalten: Der Quantencomputer ist definitiv die „heißeste Ware“ und spannendste Frage der zukünftigen Informationstechnik.

2.6 Abhörsichere Datenübertragung

Schon seit Jahrtausenden scheint es ein Grundbedürfnis des Menschen zu sein, geheime Botschaften zu versenden, die für keinen Unbefugten lesbar sind. Die ältesten bekannten Belege finden sich im dritten vorchristlichen Jahrtausend in der altägyptischen Kryptografie. Im Mittelalter waren zahlreiche Geheimschriften vor allem für den diplomatischen, aber auch medizinischen Briefverkehr in Gebrauch. Bekannt ist ebenso die Geheimmaschine Enigma, die von den Deutschen im Zweiten Weltkrieg benutzt und von alliierten Wissenschaftlern um Alan Turing geknackt wurde. Mit Claude Shannon entstand nach dem Zweiten Weltkrieg die wissenschaftliche Kryptografie als mathematische Fachdisziplin. Das heutige Zeitalter der umfassenden Digitalisierung und globalen Vernetzung verbindet damit hingegen vor allem das Thema Informationssicherheit, das auch Konzepte zur Widerstandsfähigkeit gegen Manipulationen und unautorisierte Zugriffe umfasst. Dabei werden Ziele wie der Schutz von Datenbeständen verfolgt, aber auch Begriffe wie Vertraulichkeit, Integrität, Authentizität oder Verbindlichkeit. Damit verbinden sich Schutzmaßnahmen gegen unberechtigten Zugriff, Veränderung von Daten, Fälschung sowie geistigen Diebstahl.

2.6.1 Klassische Verschlüsselungen

Das riesige Feld der Kryptografie bietet unzählige Möglichkeiten und Algorithmen. Dennoch lassen sich alle Verfahren grundsätzlich in drei Typen einteilen: symmetrische, asymmetrische und hybride Systeme. Symmetrische Verschlüsselungen sind die einfachsten und verwenden je einen Schlüssel pro Kommunikationsteilnehmer. Dieser darf nur

diesen beiden Parteien bekannt sein und auch nur ein einziges Mal verwendet werden. Das zu versendende Dokument wird mit dem Schlüssel chiffriert und sodann über das Internet versendet. Beim Empfänger wird dieses Chiffrat mithilfe des Schlüssels dechiffriert, wodurch sich der Klartext ergibt. Diese Systeme sind einfach in der Handhabung und eignen sich daher für sehr große Datenmengen, die schnell transportiert werden sollen. Die Sicherheit des Systems hängt unter anderem von der Länge des Schlüssels ab. Dazu ein vereinfachtes Beispiel, welches das Prinzip verdeutlichen soll: Falls der Schlüssel nur 1 Byte lang ist, also einer zufälligen Folge von 8 Binärzahlen entspricht, so gibt es $2^8 = 256$ Schlüsselmöglichkeiten. Das wäre natürlich kein gutes Verfahren, da ein Computer mit einer „Brute-Force-Attacke" alle möglichen Schlüssel ausprobiert und sofort den richtigen gefunden hätte. Ist der Schlüssel dagegen 256 Bits lang, so gäbe es bereits $2^{256} \approx 10^{77}$ Variationen – das sind schon fast so viele, wie das ganze Universum Atome besitzt! Wird etwa eine Videokonferenz in Echtzeit verschlüsselt, so liegt die Bitrate im Mbit/s-Bereich. Die rechnerische Wahrscheinlichkeit, dass eine Hackerattacke dann zum Ziel führt, ist de facto null – selbst wenn ein Supercomputer zur Verfügung steht. Die Sicherheit hängt also vorwiegend von der Schlüssellänge (sowie der Zufälligkeit ihrer Bitfolge) ab. Hier ergibt sich jedoch ein Problem: Der Schlüssel wird in der Praxis immer algorithmisch generiert. Computer können nämlich gar keine wirklichen Zufallszahlen erzeugen, diese sind immer nur „pseudozufällig". Das macht derartige Systeme prinzipiell antastbar, denn es stellt eine wichtige Voraussetzung infrage: die absolute Gleichwahrscheinlichkeit aller möglichen Bitfolgen. Das entscheidende Problem einer symmetrischen Verschlüsselung liegt jedoch in der Schlüsselverteilung vom Sender zum Empfänger. Die Übermittlung erfolgt in der Praxis immer über das Internet, und die Botschaft kann

demnach an jeder Stelle abgegriffen werden. Selbstredend kann der Schlüssel überall unautorisiert gespeichert sein.

Um die Sicherheit zu erhöhen, werden daher in der Regel asymmetrische Verschlüsselungen eingesetzt, wie etwa die weitverbreitete RSA-Codierung, die auf der Faktorisierung sehr großer Primzahlen beruht. Das Verfahren besteht jeweils aus einem Public Key (öffentlicher Schlüssel) und einem Private Key (persönlicher Schlüssel), der geheim zu halten ist. Beide Teile hängen auf mathematische Weise so miteinander zusammen, dass mit dem Public Key chiffrierte Nachrichten ausschließlich mit dem dazugehörigen Private Key dechiffriert werden können. Um ein Dokument von A nach B zu transportieren, werden die Daten also mit dem öffentlichen Schlüssel chiffriert und versendet, wonach sie nur mit dem geheimen Schlüssel des Empfängers geöffnet werden können. Dazu muss allerdings gesichert sein, dass die richtige Zuordnung des Public Key zum Empfänger gewährleistet ist. Wichtig ist, dass die benutzten Funktionen nicht (oder nur extrem schwer) umkehrbar sind, da ansonsten aus dem öffentlichen Schlüssel der private berechnet beziehungsweise rekonstruiert werden kann. In der Praxis wird dies sehr oft durch sogenannte Einwegfunktionen erreicht. Das Public-Key-Verfahren kann allerdings auch in beiden Richtungen ablaufen, wenn man die Möglichkeiten der digitalen Signatur in Betracht zieht. Dabei macht man sich Verschlüsselungssysteme zunutze, die neben der Vertraulichkeit und Integrität auch die Authentizität und Verbindlichkeit einer Nachricht sicherstellen. Die bei symmetrischen Verfahren gewährleistete Sicherheit kann informationstheoretisch mit einem asymmetrischen Modus jedoch nicht äquivalent bewertet werden, weil ein entsprechend mächtiger Angreifer immer das zugrunde liegende mathematische Problem lösen könnte. Wie früher bereits angesprochen,

könnten insbesondere Quantencomputer genau dazu in der Lage sein.

Da rein asymmetrische Verfahren von Haus aus sehr langsam sind, versucht man mit hybriden Methoden symmetrische und asymmetrische Verschlüsselungen miteinander zu kombinieren. In derartigen Verfahren wird das zu versendende Dokument zunächst symmetrisch verschlüsselt, wobei ein zufällig generierter elektronischer Schlüssel (Session Key) genutzt wird. Dieses System bietet gerade bei sehr großen Datenmengen einen beträchtlichen Geschwindigkeitsvorteil. Im nächsten Schritt wird der Session Key asymmetrisch mit dem Public Key des Empfänger verschlüsselt. Die beiden Informationen (verschlüsseltes Dokument und verschlüsselter Session Key) werden sodann in einer gemeinsamen kryptografischen Nachricht zum Empfänger geschickt. Zum Dechiffrieren wird zunächst der Session Key asymmetrisch entschlüsselt, wozu der Private Key des Empfängers genutzt wird. Auf diese Weise erhält der Empfänger schließlich den Session Key, mit dem er das Dokument symmetrisch entschlüsseln kann. Faktisch arbeiten praxisgerechte Varianten so gut wie immer mit hybriden Systemen, was folgendermaßen begründet werden kann: Da einerseits die Userdatenmenge zumeist groß ist, wird der Geschwindigkeitsvorteil der symmetrischen Verschlüsselung genutzt. Andererseits ist der Session Key in der Regel relativ kurz, daher fällt die langsame asymmetrische Chiffrierung nicht wesentlich ins Gewicht und minimiert gleichzeitig die Risiken der Schlüsselverteilung erheblich.

Oft werden auch Hashverfahren verwendet, um aus einer beliebig langen Information einen eindeutigen Fingerprint zu erzeugen. Die Idee dahinter ist vergleichsweise einfach: Der Absender erzeugt von einer abzusichernden Information einen Hashwert (zum Beispiel die Quersumme der als Binärzahl aufgefassten Daten)

und sendet sowohl diesen als auch die Information an den Empfänger. Dieser berechnet den Hashwert der erhaltenen Daten und vergleicht ihn mit dem Hashwert vom Absender. Stimmen beide Werte überein, so impliziert dies, dass die Information beim Transfer unverändert geblieben ist. Genau hier liegt aber auch eine Schwierigkeit des Hashverfahrens – einerseits soll es möglichst schnell mit größeren Dateien arbeiten können, andererseits soll der Hashwert so eindeutig sein, dass es extrem schwierig ist, eine Information zu manipulieren.

Die hier genannten Beispiele umfassen nur eine Teilmenge der digitalen Sicherheitstechniken. Darüber hinaus existieren viele weitere Verfahren und Methoden, die noch viel Entwicklungspotenzial besitzen. Diesem aufstrebenden Gewerbe muss in Zukunft eine immer höhere Bedeutung zukommen und sie wird immer mehr IT-Fachkräfte beschäftigen.

Das One Time Pad (OPT)

Ein besonders einfaches Verfahren, an dem sich die digitale Kryptografie gut demonstrieren lässt, ist das symmetrische One Time Pad (OPT). Eine Person, Partei oder ein Computer (nennen wir sie Alice) möchte einer anderen Person/Partei/Computer (Bob) verschlüsselte Daten über das Internet schicken. Dazu chiffriert Alice die zu versendende Nachricht und schickt sie öffentlich über das Internet. Bob dechiffriert das erhaltene Chiffrat mit dem nur ihm und Alice bekannten geheimen Schlüssel (Private Key) und erhält so den Klartext. Die Verschlüsselung erfolgt zum Beispiel durch die Addition von Binärzahlen mittels der XOR-Verknüpfung $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$ und $1 + 1 = 0$. Das heißt, Alice codiert ihre Nachricht in Binärzahlen und erzeugt durch binäre Addition mit dem Private Key das Chiffrat. Bob addiert

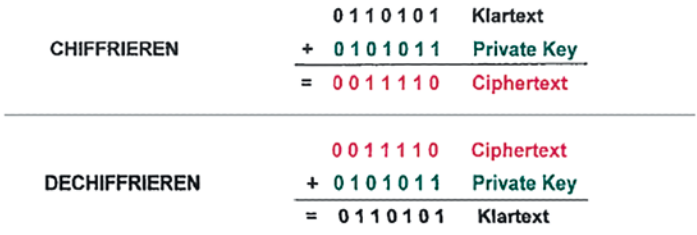

Abb. 2.5 One Time Pad, Beispiel

den Schlüssel zum Chiffrat (Ciphertext) und erhält den Klartext. Abb. 2.5 zeigt ein Beispiel.

Dieses Verfahren ist trotz seiner Einfachheit unter folgenden Voraussetzungen als 100 % sicher, d. h. informationstheoretisch perfekt sicher, zu betrachten:

1. der Schlüssel muss ein absolutes Original sein und darf nur ein einziges Mal verwendet werden, Er darf auch nicht in Teilen wiederverwendet werden.
2. die Schlüssellänge muss mindestens der zu versendenden Datenlänge entsprechen, jedenfalls einer Mindestlänge, sodass ein Brute-Force-Angriff keine realistische Chance hat,
3. der Schlüssel muss geheim bleiben, d. h. er darf nur Alice und Bob bekannt sein,
4. der erzeugte Schlüssel muss 100 % gleich verteilt zufällig sein und
5. menschliche Fehlleistungen wie Irrtum oder Korruption seien ausgeschlossen

Damit erfüllt OPT das wichtige Prinzip, dass die Sicherheit nicht von der Geheimhaltung des Algorithmus abhängt, sondern von der Geheimhaltung des Schlüssels. Wie bereits angesprochen, stellt in der Praxis Anforderung 4, vor allem jedoch Punkt 3 ein ernstes Sicherheitsbedenken

dar, wodurch ein rein symmetrisches Verfahren heute nicht mehr zeitgemäß ist. In Verbindung mit Quantentechnik wird dieses grundsätzliche Problem jedoch ideal gelöst.

2.6.2 Quantenschlüsselaustausch (QKD)

Ein zentrales Problem der heutigen IT besteht in der nicht vorhandenen physikalischen Sicherheit. Damit meint man, dass klassische Information stets beliebig vervielfältigt und abgehört werden kann – somit jederzeit der unautorisierten und kriminellen Verwendung preisgegeben ist. Selbst das ausgeklügeltste Sicherheitssystem besteht dann grundsätzlich nur im Erschweren des Datenzugriffs durch den Hacker beziehungsweise Spion. In den meisten Fällen beruht die Sicherheit somit einzig auf der Schwierigkeit mathematischer Problemstellungen sowie dem Vertrauen auf eine unzureichende Computerleistung des Angreifers. Genau in diese Kerbe schlägt die Quantenphysik. Der Begriff Quantenkryptografie bezeichnet allgemein den Gebrauch quantenmechanischer Effekte als Bestandteil kryptografischer Verfahren. Neben verschiedenen anderen aktuell untersuchten Auslegungen ist vor allem das Verfahren des Quantenschlüsselaustauschs (QKD) zu nennen, das einen vielversprechenden Lösungsweg für das Problem der Schlüsselverteilung bei einer symmetrischen Codierung darstellt. Dabei geht es um folgende Ziele:

1. Alice und Bob einigen sich auf einen gemeinsamen, geheimen Private Key, ohne dass ein Spion Eve (ohne böse Absicht so genannt) davon in irgendeiner Weise Kenntnis bekommt.
2. Aufbau eines physikalisch inhärent sicheren Quantenkanals zur Übermittlung des Quantenschlüssels. Die Sicherheit beruht dabei auf dem Umstand, dass jeglicher

Abhörvorgang durch Eve den Quantenkanal so verändert, dass dies eindeutig bemerkt werden kann. Zwar kann Eve versuchen, den Quantenzustand zu kopieren – dem No cloning Prinzip zufolge ist es jedoch niemals möglich, davon eine perfekte Kopie herzustellen.

3. Es muss die Möglichkeit einer sicheren Authentifizierung von Alice und Bob bestehen, um zu verhindern, dass Eve die Positionen von Alice oder Bob einnehmen kann. Unter den genannten Bedingungen kann die Sicherheit der QKD auch gegen unbeschränkte Angriffe bewiesen werden, was bei klassischen Schlüsseltauschprotokollen nicht möglich ist.

Verschlüsselungsprotokolle

Generell handelt es sich bei QKD-Systemen immer um zweistufige Verfahren, bei denen die erste Stufe eine Folge echter Zufallszahlen erzeugt. In der zweiten Stufe wird der generierte Quantenschlüssel zur Kryptografie klassischer Art verwendet und über das normale Internet versendet. Hierzu reicht bereits ein einfaches symmetrisches Verfahren wie das (durch Quantentechnik beweisbar sichere) OPT aus. Weil die Erzeugung des Schlüssels quantenzufällig erfolgt, der Zufall also von der Natur selbst stammt, kann der Key in diesem Fall niemals algorithmisch „nachgerechnet“ werden. Zudem ist jede erzeugte Bitfolge absolut gleichwahrscheinlich und bietet (abhängig von der Schlüssellänge) eine derart astronomische Anzahl von Kombinationsmöglichkeiten, dass das Verfahren als maximal sicher anzusehen ist. Jedenfalls für einen relevanten Zeitraum, der selbst für Supercomputer viele Jahrtausende und mehr betragen kann. Für die QKD existieren grundsätzlich zwei Verfahren (darauf basieren auch alle Varianten).

BB84-Protokoll Dies ist das bekannteste Verfahren zur Quantenkryptografie. Es wurde von den beiden Physikern Charles H. Benett sowie Gilles Brassard 1984 bei IBM ausformuliert. Die Grundidee geht allerdings auf Stephen J. Wiesner zurück, der sie um 1970 vorschlug. BB84 beruht auf der Übertragung einzelner Qubits, welche in der Regel als Polarisation oder Phase von Photonen implementiert werden. Die Übertragung erfolgt entweder via Glasfaserkabel oder in direkter Visierlinie. Derartige Geräte sind überwiegend kommerziell erhältlich und werden (Herstellerangaben zufolge) von Regierungen und Unternehmen eingesetzt, ebenso gibt es strategische Investmentpartner. Bei den Schweizer Parlamentswahlen wurden auf diese Weise bereits 2007 Ergebnisse von Wahllokalen im Kanton Genf über ca. 100 km nach Bern übertragen.

Ekert-Protokoll Dieses technisch viel aufwendigere, jedoch überaus zukunftsträchtige Verfahren wurde 1991 von Artur Ekert vorgeschlagen. Im krassen Unterschied zu BB84 werden hierbei verschränkte Qubits erzeugt. Die erste quantenoptische Realisierung gelang 1999 einer Gruppe um Anton Zeilinger über eine Distanz von 360 m. Besonders medienwirksam wurde 2004 – ebenfalls von Zeilinger – die erste quantenkryptografische Geldüberweisung demonstriert. In Anwesenheit des Wiener Bürgermeisters Michael Häupl gelang ein Transfer von einer Bank aus über 1,5 km zum Wiener Rathaus. Der sprichwörtliche Quantensprung dieser Entwicklung war dann die erste interkontinentale Übertragung mittels Quantensatelliten, welche am 29.09.2017 gelungen ist (Abschn. 1.4).

Das Ekert-Protokoll Schritt für Schritt

Schritt 1 – Authentifizierung Alice und Bob müssen zunächst sicherstellen, dass Eve nicht eine ihrer Positionen einnimmt. Dazu gibt es eine Reihe von Verfahren, die wieder auf der Quantenphysik beruhen und hier mit „Quantenpasswort" bezeichnet seien. Zusätzlich muss ein authentifizierter klassischer Kanal eingerichtet werden, der möglicherweise abgehört wird.

Schritt 2 – Quantenschlüsselerzeugung (QKD) Aus einer Quelle für verschränkte Teilchen werden speziell korrelierte Single-Qubits zu Alice und Bob gesendet, die bei ihrer Messung quantenzufällig in ihre Eigenwerte 0 oder 1 zerfallen. Aus einer ausreichend langen Messreihe trennen Alice und Bob die eindeutig korrelierten Fälle (relevante Bits) von den unkorrelierten (irrelevante Bits). Dazu benötigen sie zwingend einen klassischen Informationskanal.

Schritt 3 – Fehlerkorrektur Die in der Praxis unvermeidlichen Messfehler werden durch spezielle Verfahren (wie etwa Paritätstest, Privatsphärenverstärkung usw.) korrigiert.

Schritt 4 – Spionagetest Echte Sicherheit kann nur gewährleistet sein, wenn die Verschränkung maximal intakt bleibt. Ist das nicht der Fall, so wird das System entweder teilweise oder völlig dekohärent. Dies kann statistisch erfasst werden, zum Beispiel durch Auswerten der bellschen Ungleichung oder Ähnliches. Wird die Ungleichung nicht verletzt, so liegt eindeutig entweder eine Abhörattacke oder aber ein technisches Gebrechen vor. Damit lässt sich ein erfolgter Spionageangriff direkt aufdecken und gleichzeitig die Funktionstüchtigkeit des Systems überprüfen.

Schritt 5 – OPT-Verschlüsselung Erst wenn die obigen Schritte bis hier eingehalten wurden, erfolgt die Übertragung der eigentlichen Daten. Dazu wird der Quantenschlüssel (der aus den fehlerkorrigierten relevanten Bits besteht) für ein symmetrisches Verfahren wie OPT verwendet und über das normale Internet versendet.

Schritt 6 – Dechiffrieren Bob erhält den Ciphertext und dechiffriert ihn mit dem bei ihm genauso erzeugten Private Key. Das Einzigartige bei der QKD: Der Schlüssel wurde nirgendwo übertragen, sondern entsteht bei Alice und Bob durch den Messprozess „wie von selbst". Die inhärente Sicherheit des Systems beruht auf dem No-Cloning-Theorem, welches das Abhören von Qubits unmöglich macht.

2.6.3 Quantenkryptografie mit verschränkten Photonen

Im Nachfolgenden wird eine konkrete Versuchsanordnung angegeben, welche die Technik der Quantenschlüsselverteilung (QKD) gemäß dem Ekert-Protokoll im Einzelnen vorführt (Abb. 2.6). Diese kann sowohl in satellitenbasierten Systemen (Quantensatellit) als auch in Glasfasernetzwerken implementiert werden. Die Quanteninformation ist in diesem Beispiel in der Polarisation (Schwingungsebene) des Lichts codiert. Sie lässt sich grundsätzlich jedoch auch über die Phase oder die Energie-Zeit-Unschärfe einschreiben. Alice und Bob stehen allgemein für zwei Personen/Parteien/Computer, welche einander inhärent abhörsichere digitale Informationen übersenden wollen. Bei Quantensatelliten (wie etwa QUESS) stehen Alice und Bob stellvertretend für observatorische Messeinrichtungen.

Versuchsbeschreibung
Die Verschränkungsquelle VQ erzeugt nach dem Prinzip der Parametric Down Conversion eine große Menge maximal verschränkter Photonenpaare (anschaulich dargestellt durch punktierte Linien). Davon wird je ein Partnerteilchen bei Alice, das andere bei Bob gemessen.

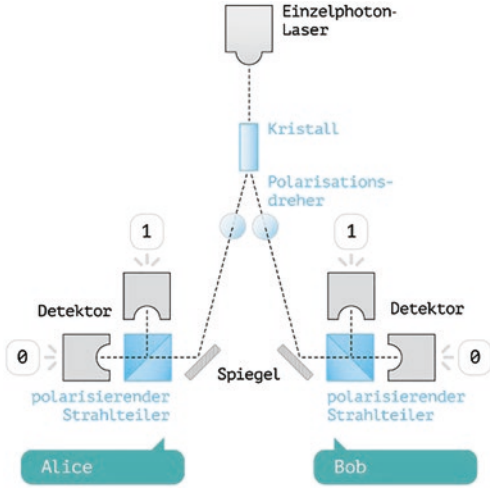

Abb. 2.6 Versuchsaufbau zum Ekert-Protokoll. Die Verschränkungsquelle ist ein nichtlinearer *Kristall,* durch nicht eingezeichnete Zusatzelemente kann der Grad der Verschränkung beeinflusst werden; der ansteuerbare *Polarisationsdreher* verändert entsprechend seiner Einstellung die Schwingungsebene des linear polarisierten Lichts; der *polarisierende Strahlteiler* splittet in horizontal beziehungsweise vertikal polarisiertes Licht und der *Detektor* dient zum Nachweis einzelner Photonen

Bevor die Messung über die Detektoren erfolgt, passieren die Photonen jeweils einen Polarisationsdreher PD sowie einen polarisierenden Strahlteiler PST. Abhängig von den Relativpositionen von PD und PST werden die Photonen beim PST entweder transmittiert oder reflektiert. Diesen Richtungen werden willkürlich den Binärzahlen 0 oder 1 zugeordnet, in diesem Beispiel gilt 0 = transmittiert und 1 = reflektiert.

Sammeln von Messdaten

Nach jeder Teilchenpaarerzeugung in VQ werden beide PD völlig zufällig und unabhängig voneinander gedreht

(in beiden Fällen sollte die gleiche Wahrscheinlichkeitsverteilung gelten). Alice stellt dazu ihren PD genau auf die Werte 0° oder 30°, Bob reguliert seinen PD auf die Werte 30° oder 60°. Es gibt demnach 4 Möglichkeiten, wie die PD relativ zueinander stehen können: (0°, 30°), (0°, 60°), (30°, 60°) und (30°, 30°). Eine perfekte Korrelation beziehungsweise Verschränkung liegt allerdings nur im Fall (30°, 30°) vor, dann misst Alice mit Sicherheit eine 1, wenn auch Bob eine 1 misst; und Alice bekommt eine 0, immer wenn Bob eine 0 vorliegen hat. In diesen Fällen spricht man von *relevanten Bits*. Ob es sich dabei jedoch konkret um eine 0 oder 1 handelt, ist rein durch den objektiven Quantenzufall bestimmt (Abschn. 2.6.3 „Nähere Details"). Bei allen anderen Winkelpaaren liegen dagegen keine perfekten Korrelationen vor, das heißt, es kann nicht mit Sicherheit gesagt werden, ob Alice und Bob dieselben Binärzahlen messen; das sind die *irrelevanten Bits*. Jedes einzelne Messergebnis wird in numerischer Reihenfolge festgehalten, sodass Alice und Bob je eine Liste aus relevanten und irrelevanten Bits erhalten.

Test auf Spionage

Mit einer ausreichend großen Zahl von fehlerkorrigierten Bits auf der Liste wird eine statistische Auswertung vorgenommen. Daraus können Wahrscheinlichkeiten berechnet werden, welche die Bell-Ungleichung entweder verletzen oder nicht. Wird sie verletzt, so beweist dies, dass die Verschränkung bei der Biterzeugung völlig intakt war und der Quantenkanal als sicher zu betrachten ist. Wird die Bell-Ungleichung hingegen erfüllt (nicht verletzt), so wurde der Quantenkanal unterbrochen – entweder durch Spionage oder aufgrund eines technischen Gebrechens – und die Übermittlung muss als unsicher angesehen werden.

Die Bell-Ungleichung kann für praktische Auslegungen in vielen Formulierungen existieren, wie etwa der oft verwendeten CHSH-Ungleichung. In diesem Beispiel wird jedoch eine Ungleichung nach Eugene Wigner angegeben. Bezogen auf die angegebenen Winkel beziehungsweise den Bell-Zustand Φ_+ (= speziell eingestellter Verschränkungszustand) lautet die Wigner-Ungleichung

$$P_{++}(0°,\ 30°) < P_{++}(0°,\ 60°) + P_{+-}(0°,\ 30°)$$

Dabei steht P für die Wahrscheinlichkeit (Probability), dass bestimmte Bitkombinationen für die angegebenen Winkelpaare bei Alice und Bob gemessen werden. Das Symbol „++" bezeichnet Fälle, wo eine perfekte Korrelation gegeben ist. Als Schätzwert für P dient die relative Häufigkeit der Ereignisse. Wegen des Gesetzes der großen Zahlen ist die Schätzung ab einer hinreichenden Anzahl von Messwerten beliebig zuverlässig. Angenommen, die Wigner-Ungleichung ergibt sich zu $0,35 < 0,13 + 0,13$, dann ist sie offensichtlich verletzt, da ja $0,35 < 0,26$ eine falsche Aussage ist. Man folgert in diesem Fall somit, dass es keine Attacke auf den Quantenkanal gab.

Quantenschlüssel Da die Wigner-Ungleichung im obigen Beispiel einen erfolgreichen Spionageangriff ausschließt, trennen Alice und Bob im nächsten Schritt die relevanten von den irrelevanten Bits, wodurch sich der fertige Quantenschlüssel als die Menge der fehlerkorrigierten relevanten Bits ergibt. Im Unterschied zur klassischen IT ist der Schlüssel

1. ohne Internettransfer direkt bei Alice und Bob erzeugt worden,
2. jedes Mal ein absolutes Original aufgrund der Quantenzufälligkeit und

3. eine echte Zufallsfolge im Unterschied zu pseudozufälligen Computerzahlen.
   Da der objektive Zufall ein irreduzibles Ereignis darstellt (wie indirekt auch das Bell-Theorem beweist), sind Quantenzufallszahlen die besten, die es geben kann.

Zu beachten gilt es dabei, dass die echte Zufallsfolge nicht bei der (eventuell nicht ganz zufälligen) Drehung der PD entsteht, sondern am PST (Abschn. 2.6.3, „Nähere Details“).

Verwenden für OPT siehe hierzu Abschn. 2.6.1.

Inhärente Sicherheit Mit Eve sei wieder ein(e) Person/Partei/Computer bezeichnet, welche die zu übertragenden Daten unautorisiert abhören möchte. Eve hat dazu grundsätzlich zwei Möglichkeiten: Sie kann entweder den klassischen Kanal oder aber den Quantenkanal angreifen.

Attacke auf den klassischen Kanal Alice und Bob benötigen für die Erzeugung des Quantenschlüssels zwingend einen klassischen Informationskanal, also eine herkömmliche IT-Verbindung. Auf den ersten Blick erscheint gerade dieser eine lohnende Angriffsfläche für Spionage aller Art zu sein. Allerdings gilt es zu beachten, dass Alice und Bob hierbei nur eine Liste von Gradangaben und keine konkreten Bitfolgen austauschen. Diese Information ist für beide ausreichend, zumal sie wissen, dass bei gleichen Winkelpaaren eine perfekte Korrelation vorliegt. Ob es sich dabei konkret um eine 0 oder 1 handelt, können sie anhand ihrer Detektoren feststellen. Eve hingegen kann die Werte der relevanten Bits niemals kennen, da sie objektiv zufällig bei Alice und Bob entstehen. Selbst wenn Eve wüsste, dass bei (30°, 30°) eine

perfekte Korrelation vorliegt, ist jedes Mal völlig unklar, ob es sich dabei jeweils um Nullen oder Einsen handelt. Schließlich verbleibt Eve noch die Möglichkeit, das mit OPT verschlüsselte Chiffrat abzuhören und zu versuchen, es mit einer „Brute-Force-Attacke" zu knacken. Da die QKD jedoch alle Sicherheitskriterien für die Anwendung von OPT erfüllt (was bei einer normalen IT-Schlüsselzuteilung zu bezweifeln ist), muss auch dieses Unterfangen zwangsläufig scheitern.

Attacke auf den Quantenkanal Hier bestehen für Eve prinzipiell drei Möglichkeiten:

Attacke 1: Eve hört die direkte Visierlinie (oder die faseroptische Verbindung) zwischen der Verschränkungsquelle VQ und den Messeinrichtungen ab. Dazu muss sie jedoch den Polarisationszustand der Photonen messen, was den gesamten Quantenzustand automatisch stört und die Messstatistik so verändert, dass die Wigner-Ungleichung nicht mehr verletzt wird. Dies bemerken Alice und Bob natürlich und ignorieren den so erzeugten Quantenschlüssel.

Attacke 2: Eve hört VQ direkt ab und funkt zum Beispiel den entstehenden Quantenschlüssel an einen geheimen Ort weiter. Das ist aber ebenso unmöglich, da die Bits objektiv zufällig erst durch den Messprozess bei Alice und Bob und nicht schon bei VQ entstehen. Eine versuchte Messung von Eve liefe letztlich wieder auf Attacke 1 hinaus. Derartige Attacken wären nur dann erfolgreich, wenn der gesamte Quantenzustand unabhängig von Alice und Bob auch bei Eve koexistieren könnte. Dies setzt also zumindest eine (perfekte) Verdoppelung der Quanteninformation voraus, was wegen des No-Cloning-Theorems physikalisch unmöglich ist (Abschn. 2.1). Sehr wohl wäre es natürlich denkbar, dass die Messgeräte bei Alice und

Bob den erzeugten, in der Praxis auf einem klassischen Computer gespeicherten Quantenschlüssel im Geheimen weiterleiten. Selbstverständlich müssen sich Alice und Bob dahin gehend absichern, dass die Geräte nicht manipuliert sind beziehungsweise eine korrekte Auswertung der Ungleichung vornehmen.

Attacke 3: Eve startet einen Man-in-the-Middle-Angriff. Dazu gibt sie sich selbst als Quelle aus und täuscht die verschränkten Photonenpaare vor. Alice und Bob könnte das zwar verborgen bleiben, jedoch wird auch in diesem Fall die Wigner-Ungleichung nicht mehr verletzt. Der Grund liegt darin, dass dies nur auf einem klassisch physikalischen Weg für Eve möglich wäre, wodurch per se keine Verschränkung mehr vorliegt. Da die Wigner-Ungleichung jedoch ein direktes Kriterium für die Existenz der Verschränkung darstellt, fällt somit auch dieses Täuschungsmanöver automatisch auf.

Nähere Details:

Parametric Down Conversion Die Einzelphoton-Quelle erzeugt in diesem Beispiel Photonen der Wellenlänge 405 nm (blaues Licht). Die Lichtquanten treffen auf ein nichtlineares Kristallsystem, woraufhin aus jedem blauen Photon ein verschränktes Paar infraroter Photonen der doppelten Wellenlänge 810 nm entsteht. Die so erzeugten Photonenpaare bewegen sich anschließend entlang eines Kegels, das heißt, sie können mit einer bestimmten Wahrscheinlichkeit all jene Richtungen beschreiben, die einem Kegelmantel entsprechen. Um die Verschränkung zu erzeugen, ist es notwendig, zwei nichtlineare Kristalle hintereinander so zu platzieren, dass anschließend zwei derartige Kegelmäntel entstehen, die

einander teilweise überlappen. Entlang dieser Überlappbereiche sind die Teilchen ununterscheidbar (das heißt, eine Art Informationsverlust liegt vor), was eine wichtige Voraussetzung für Verschränkung darstellt. Durch Zusatzelemente wie Polarisationsdreher und Phasenschieber kann der Grad der Verschränkung eingestellt werden. In dem dargelegten Beispiel lassen sich vier verschiedene maximal verschränkte Zustände (sogenannte Bell-Zustände) mit unterschiedlichen Polarisationen erzeugen.

Gesetz von Malus Wenn polarisiertes Licht durch einen Analysator fällt, wird seine Schwingungsrichtung entsprechend der Stellung des Filters gedreht. Dabei zeigt sich, dass die Intensität (Helligkeit) des durchgelassenen Lichts mit steigendem Drehwinkel immer mehr abnimmt, bis schließlich bei 90° gar nichts mehr durchgelassen wird. Dem Gesetz von Malus (siehe auch Abschn. 1.5) zufolge ist diese Abnahme dem quadrierten Kosinus ($\cos^2$) des Winkels proportional. Fällt polarisiertes Licht dagegen durch einen polarisierenden Strahlteiler, so stellt man fest, dass bei einem Winkel von 45° je eine Hälfte des Lichts transmittiert und die andere Hälfte reflektiert wird. Bei anderen Winkeln bilden sich andere Verhältnisse, so tritt bei 30° ein Verhältnis von 75 % zu 25 % auf. Aus Sicht der Quantenphysik treten in diesen Fällen einzelne Lichtquanten durch den Strahlteiler, wobei es objektiv zufällig ist, ob das einzelne Photon transmittiert oder reflektiert wird. Obwohl sich in der Gesamtstatistik eine prozentuale Verteilung wie oben ergibt, unterliegt das quantenmechanische Einzelereignis dem absoluten Zufall. Wichtig ist, dass die Winkel nicht 0° beziehungsweise 90° betragen, da ansonsten die Photonen zu 100 % entweder transmittiert oder reflektiert werden und die Anordnung dann keinen Quantenzufallsgenerator mehr darstellt.

Das Photon als Qubit Erinnern wir uns an die Darstellung der Linearkombination am Viertelkreis in Abschn. 2.5.1 und erweitern wir diese Vorstellung jetzt zum Vollkreis (Abb. 2.7). Das ändert zunächst nichts an den Faktoren a und b vor den Basisvektoren, außer dass sie jetzt auch negative Werte aufweisen können und deshalb für die Wahrscheinlichkeit die Bedingung zu setzen ist, dass die Betragsquadrate in der Summe gleich 1 sein müssen. Nun kann man ein so visualisiertes Qubit direkt mit der Polarisation eines Photons in Verbindung bringen. Analog den unendlich vielen Zuständen eines Qubits gibt es theoretisch ebenso unendlich viele Möglichkeiten, wie man den Polarisationszustand eines Photons messen kann. Die Betragsquadrate der Faktoren a und b geben dann jeweils die Wahrscheinlichkeit an, eine 0 oder 1 zu messen.

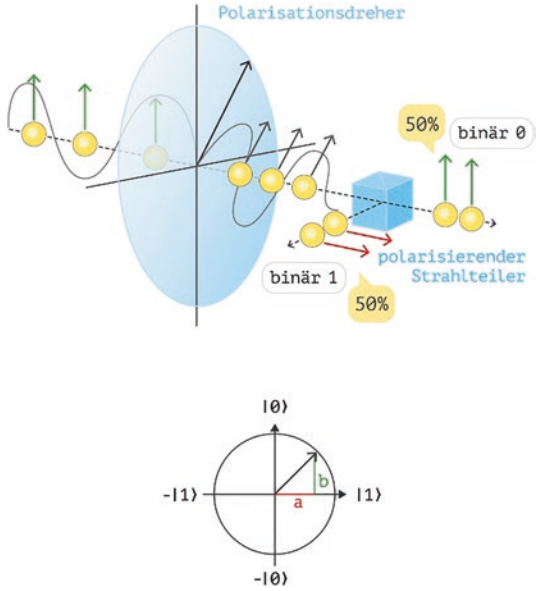

Abb. 2.7 Darstellung und Messung des Qubits (als Photon implementiert)

Sei also das einlaufende Photon bezüglich einer beliebigen Richtung linear polarisiert und schließe zur Horizontalebene des PST die Winkel 0° oder 90° ein, so wird mit der Wahrscheinlichkeit $P = 1$ (100 %), also immer, eine 0 beziehungsweise 1 gemessen. Sei der Winkel dagegen 45°, dann wird mit jeweils $P = 0{,}5$ (50 %) objektiv zufällig eine 0 oder 1 gemessen. In diesen (und allen anderen Fällen) ergeben sich die Wahrscheinlichkeiten gemäß dem Gesetz von Malus (siehe oben). Insgesamt wird ersichtlich, dass ein Single-Qubit an den Endnodes eines Quantennetzwerks die einfachste Form eines Quantenzufallsgenerators darstellt, der zur QKD verwendet werden kann.

2.7 Quantenteleportation

Dass man physische Objekte, vor allem aber auch Menschen, vom Ort A zum Ort B teleportieren oder auch „beamen" kann, ist eine beliebte Vorstellung des Science-Fiction-Genres.

Ein Beispiel ist die bekannte TV-Serie „Raumschiff Enterprise", welche vor vielen Jahrzehnten ein besonderer Renner war. „Scotty, beamen Sie uns zu dem fremden Planeten hinunter", heißt es da etwa. Was dann folgt, ist ein futuristischer Mechanismus, der die Crew scheinbar in ihre Atome zerlegt, diese auf die Planetenoberfläche überträgt und dort wieder zusammensetzt. Daraufhin erledigt die Mannschaft völlig unbeschadet ihre Aufgaben, um schließlich wieder ins Raumschiff zurückgebeamt zu werden. Diese Vorstellung scheint mit realer Wissenschaft sehr wenig zu tun zu haben. Umso erstaunter reagierte die Öffentlichkeit, als der Begriff Teleportation plötzlich in den Wissenschaftsmeldungen auftauchte. Wie sonst ist es zu erklären, dass populärwissenschaftliche Bücher über dieses Thema plötzlich zum Bestseller wurden?

Die Art von Teleportation, welche beweisbar in der Welt der Wissenschaft existiert, gibt sich allerdings wesentlich unspektakulärer. Hier geht es nicht darum, physische Objekte, schon gar keine Menschen zu teleportieren, sondern um Quanteninformation, welche auf diese Weise völlig unbehelligt von A nach B transportiert werden kann. Es ist auch nicht das Ziel, verwertbare Information überlichtschnell zu übertragen, was weiterhin – in bester Übereinstimmung mit Einsteins Relativitätstheorie – unmöglich bleibt. Die besondere Bedeutung der Quantenteleportation liegt darin, dass sie es erlaubt, auch speziell präparierte Quantenzustände unbeschadet zu transferieren, ohne sie dabei durch ihre Messung zu verändern. Ebenso ist es möglich, völlig unbekannte und insbesondere auch verschränkte Zustände zu teleportieren. Daraus resultieren völlig neuartige technische Möglichkeiten für die Übertragung von Qubits sowie für die Realisierung von Quantenrepeatern. Die Quantenteleportation ist damit ein sehr vielversprechendes Werkzeug für das Quanteninternet, ebenso für neue Möglichkeiten zur Verarbeitung von Qubits in Quantencomputern.

2.7.1 Teleportation von Qubits

Das Quanteninternet erlaubt es, Qubits von einem Sender (Alice) zu einem Empfänger (Bob) zu übertragen. Bei der Long-Distance-Quantenkommunikation sind Alice und Bob dabei räumlich weit voneinander getrennt. Beim Quantencomputing sind die Distanzen hingegen meist winzig klein – dennoch kann in beiden Fällen dasselbe physikalische Prinzip zum Einsatz kommen, eben die Quantenteleportation. Im Unterschied zu klassischen Bits können Qubits aufgrund von Dekohärenzeffekten nicht gemessen werden, ohne dabei den Quantenzustand

zu verändern. Der teleportierte Zustand ist daher nach der Übertragung auf der Senderseite nicht mehr rekonstruierbar, weshalb zusätzlich ein klassischer Kommunikationskanal zwischen Sender und Empfänger einzurichten ist (zum Beispiel via normaler IT-Verbindung). Bei diesem wird natürlich die Übertragungsrate durch die Lichtgeschwindigkeit begrenzt. Der Transfer der Qubits selbst erfolgt hingegen instantan (überlichtschnell) durch einen speziellen Quantenkanal. Dazu benötigen Alice und Bob einen maximal verschränkten Quantenzustand als Ressource, welcher beim Vorgang der Teleportation vernichtet wird. Wesentlich ist, dass die Quantenteleportation auch dann funktioniert, wenn der zu übertragende Zustand völlig unbekannt ist, und dieser zudem mit weiteren Systemen verschränkt sein kann. Im Übrigen ist es irrelevant, in welchem physikalischen System Ausgangs- und Zielzustand vorliegen.

Photonische Teleportation

Ein Beispiel: Alice möchte den Polarisationszustand eines Photons zu Bob teleportieren. Dazu erhalten beide zunächst jeweils ein Photon aus einer gemeinsam verschränkten EPR-Quelle (Abb. 2.8). Daraufhin führt Alice eine spezielle Bell-Messung durch, und zwar mit dem zu teleportierenden Zustand und ihrem persönlichen EPR-Photon. Durch diesen Messprozess verändert sich infolge der Verschränkung instantan ebenso auch der Quantenzustand von Bobs persönlichem EPR-Teilchen. Da aufgrund der objektiven Zufälligkeit von Messergebnissen der jeweils gemessene Zustand nicht bekannt ist, teilt Alice ihr Ergebnis über den klassischen Kanal Bob mit. Dieser führt daraufhin eine Manipulation an seinem Zustand aus und kann auf diese Weise den ursprünglichen Quantenzustand wieder herstellen. Da nach dem No-Cloning-Theorem ein Quantenzustand niemals original dupliziert werden

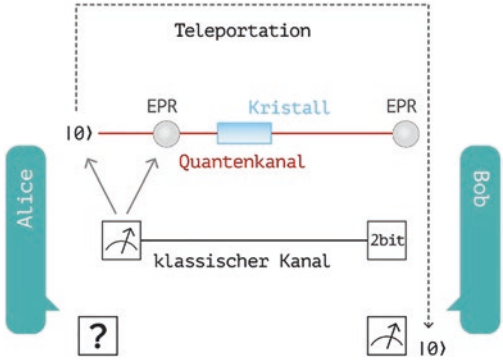

Abb. 2.8 Prinzip der Quantenteleportation

kann, muss dieser demnach bei Alice zerstört worden sein. Insgesamt ist also die Quanteninformation von Alice am Ort A verschwunden und an den räumlich beliebig weit entfernten Ort B von Bob übertragen worden. An dieser Stelle sei nochmals darauf hingewiesen, dass zwar die Übertragung der Quanteneigenschaften überlichtschnell erfolgt, der nutzbare Informationsgewinn jedoch durch den klassischen Kanal und damit maximal mit Lichtgeschwindigkeit kommuniziert wird. Ebenso gilt es zu beachten, dass Vokabeln wie „Übertragung" nur in einem anschaulichen Sinn zu verstehen sind. Hier wird in der Tat nichts transferiert, sondern es kommt zu einer (durch die Art der Messung bestimmten) quantenmechanischen Zustandsänderung, bei welcher die Quanteninformation an einem Ort verschwindet und an einem anderen Ort repliziert wird.

Protokoll zur Quantenteleportation

Ziel: Die Quanteninformation von Alice (Source-Qubit) soll auf eine physikalische Ressource von Bob (Target-Qubit) übertragen werden, wobei der Zustand bei Alice annihiliert wird. So gehen sie vor:

- Quantenkanal herstellen, verschränktes EPR-Paar erzeugen
- via Quantenkanal je ein Qubit des EPR-Paares zum Sender (Alice) und zum Empfänger (Bob) übertragen
- Alice nimmt eine spezielle Bell-Messung vor, das heißt eine gemeinsame Messung des verschränkten EPR-Qubits und des zu teleportierenden Qubits. Diese Messung beeinflusst den Zustand des EPR-Qubits bei Bob instantan.
- Das Messergebnis von Alice ist einer von vier objektiv zufälligen Zuständen, dieses wird in zwei Bits codiert und auf einem klassischen Kanal an Bob übermittelt.
- Mit dieser klassischen Information kann das Target-Qubit von Bob so transformiert werden, dass es zwangsläufig den gleichen Zustand annimmt wie das Source-Qubit, das am Anfang bei Alice vorgelegen hatte.

Die Idee der Quantenteleportation hat mehrere Väter. Sie wurde 1993 von den Theoretikern Asher Peres, William Wootters, Gilles Brassard, Charles H. Bennett, Richard Josza und Claude Crepeau vorgeschlagen. 1997 gelang einer Gruppe um Anton Zeilinger erstmals der experimentelle Nachweis, fast zeitgleich auch der Gruppe von Sandu Popescu et al. In den genannten Fällen ging es jeweils um die Übertragung quantenoptischer Zustände. Im Jahr 2003 konnte ein Schweizer Team um Nicolas Gisin eine photonische Teleportation über deutlich größere Distanzen demonstrieren, später auch in kommerziellen Glasfasernetzwerken der Swisscom. Nachdem 2004 Innsbrucker sowie US-amerikanischen Forschern erstmals die Teleportation von Atomzuständen gelang, konnte eine weitere österreichische Gruppe um Anton Zeilinger und Rupert Ursin einen Zustand über eine Distanz von 600 m unterhalb der Donau „hindurchbeamen“, was 2012 zwischen den Inseln La Palma und Teneriffa über 144 km in freier Visierlinie wiederholt wurde. Die innovative Quantensatellitentechnik setzte auch hier die aktuelle

Weltrekordmarke, als Jian-Wei Pan 2017 eine photonische Teleportation auf einer Entfernung von über 1000 km nachwies.

2.7.2 Implementierung auf Atomen

Abb. 2.9 zeigt (vereinfacht) die Schaltskizze einer Teleportation von Qubits, die in einzelne Atomzustände geschrieben sind und zum Beispiel mit drei Calcium-Ionen implementiert werden kann. Der Zeitablauf ist von links nach rechts zu lesen: Zunächst wird der zu teleportierende Zustand (beispielsweise $|1\rangle$, $|0\rangle$ oder $|1\rangle + |0\rangle$)

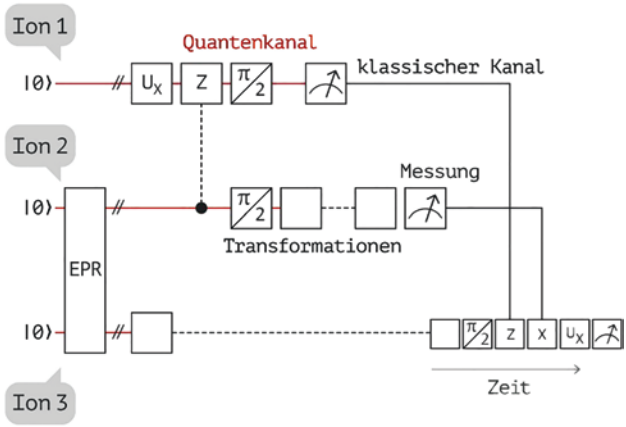

Abb. 2.9 Teleportation, implementiert auf Ionen (in vereinfachter und verkürzter Darstellung): Die Gatteroperationen beziehen sich auf eine Qubit-Darstellung als Bloch-Sphäre. Die Operation U_x codiert den Zustand von Ion 1. Die Bell-Zustandsmessung bei Ion 2 besteht aus kontrolliertem Z-Gatter, $\pi/2$-Rotation und Messung (hier zum Beispiel Fluoreszenz-Photomultiplier). Reihenfolge bei Ion 3: abhängig von der Bell-Basis zunächst Rotation um $\pi/2$, dann Rekonstruktion von Z und X; die Operation U_x dient dann der Fidelitätsanalyse, zum Schluss kommt die Messung durch Fluoreszenz-Multiplying

auf Ion 1 eingeschrieben sowie ein spezieller EPR-Zustand auf Ion 2 und Ion 3 präpariert. Daraufhin ermittelt Alice das Ergebnis der Bell-Messung (Zustände von Ion 1 und Ion 2) und übermittelt es auf einem klassischen Kanal an Bob. Die vier möglichen Ergebnisse können in zwei klassischen Bits codiert werden, das heißt in den Binärzahlen 00, 01, 10, 11. Aufgrund der empfangenen Bitfolge nimmt Bob eine von dieser Information abhängige Manipulation an seinem Teilchen vor und führt die finale Messung durch. Dabei wird der von Alice erzeugte Zustand von Ion 1 auf Ion 3 teleportiert. Das No-Cloning-Prinzip sorgt sowohl für die inhärente Sicherheit der Übertragung als auch für die Tatsache, dass der eingeschriebene Quantenzustand bei Alice verschwinden muss, wenn er bei Bob als Original repliziert wird.

2.8 Quantenrepeater

Ein wesentliches Element eines Kommunikationsnetzwerks über große Distanzen verkörpern zahlreiche Repeaterstationen. Wie dargelegt, werden beim aktuellen Internet die Daten als modulierte elektromagnetische Wellenzüge übertragen. Diese Signale werden an den einzelnen Repeaterstationen gemessen, verstärkt und weitergeleitet. Diese Technik, die sich beim Internet sehr gut bewährt hat, kann jedoch in einem Quantennetzwerk keine Verwendung finden. Die prinzipielle Schwierigkeit liegt darin, dass aufgrund des No-Cloning-Prinzips Quanteninformation nicht perfekt kopiert werden kann. Jede Messung würde somit automatisch die Qubits so weit stören, dass sie nicht reproduzierbar sind. Deshalb sind neue technologische Ansätze zwingend erforderlich. Ein sehr vielversprechender Lösungsansatz liegt im Konzept des

Quantenrepeaters, der bereits 1998 von den Theoretikern Hans Jürgen Briegel, Juan Ignacio Cirac sowie Peter Zoller vorgeschlagen wurde. Sein prinzipieller Ansatz besteht darin, dass eben nicht das zu sendende Signal verstärkt wird, sondern dass der Repeater nur zum Aufbau eines gewissen maximal verschränkten Zustands verwendet wird. Dieser kann dann in einem weiteren Schritt beispielsweise zur Long-Distance-QKD mit verschränkten Photonen genutzt werde. Das Design beziehungsweise die Auslegung muss beinhalten, dass zwischen Alice und Bob eine Reihe von Quantenrepeatern zwischengeschaltet wird, die jeweils klassische und quantenmechanische Signale empfangen, verarbeiten und senden können. Der Aufbau maximal verschränkter Zustände über weite Distanzen erfolgt dabei nach einem speziellen Protokoll, das drei Punkte enthält:

1. die Erzeugung verschränkter Zustände zwischen benachbarten Knotenpunkten,
2. das sogenannte Entanglement Swapping (auch Verschränkungsaustausch genannt), bei dem die Verschränkung gewissermaßen auf weiter entfernte Knotenpunkte „überschwappt“, und
3. eine Art Fehlerkorrektursystem, die sogenannte Verschränkungsdestillation (oder auch Verschränkungsreinigung), bei der aus vielen schwach verschränkten Zuständen wenige stark verschränkte erzeugt werden.

In der Praxis müssen die Schritte 2. und 3. im Wechsel vorgenommen werden, da der Verschränkungsaustausch maximal verschränkte Zustände voraussetzt. Eine wesentliche weitere Vorgabe für das Design von Quantenrepeatern beinhaltet, dass – trotz mit der Entfernung exponentiell wachsender Verluste – die Kommunikation mit nur polynomial zunehmenden Ressourcen (Dauer,

Anzahl der Stationen, Menge der benötigte Qubits, Messungen) möglich sein soll. Aktuell gibt es für das Design zahlreiche theoretische Varianten und Implementierungsvorschläge, aber noch keinen entscheidenden Durchbruch. Quantenrepeater wurden bereits in verschiedenen Proof-of-Concept-Exprimenten erfolgreich demonstriert. Dennoch gestaltet sich eine technologisch verwertbare Realisierung als extrem schwierig.

Quantenrepeater – auf einen Blick

Die wesentliche Zielsetzung des Quanteninternets sieht eine Verschränkung zwischen den Qubits an den Endnodes vor. Das Grundproblem der Long-Distance-Quantenkommunikation besteht aber gerade darin, dass die Verschränkung von Qubits entlang eines „verrauschten Quantenkanals" sehr schwierig ist. Wenn sich mobile Qubits über Faserleitungen zu Knotenpunkten bewegen, treten in der Praxis erhebliche Absorptions- sowie Dekohärenzeffekte auf. Da diese Verluste mit der Länge des Kanals exponentiell skalieren, kann ab einer gewissen Distanz die Verschränkung nicht intakt gehalten werden. Das Konzept des Quantenrepeaters muss so ausgelegt sein, dass es dieses Kardinalproblem überwinden kann. Die zentrale Idee ist dabei das Entanglement Swapping, bei dem es gelingt, verschränkte Teilchenpaare zunächst über nur kurze Distanzen zu erzeugen und diese anschließend durch sukzessives Verschränken weiterer Teilsysteme auf größere Distanzen auszudehnen. Dabei werden verrauschte Zustände mit minimaler Verschränkung zu Zuständen maximaler Verschränkung destilliert. Für den Einsatz in QKD-Systemen können speziell auch Quantensatelliten zur Anwendung kommen, welche einen Quantenkanal über größere Distanzen ermöglichen. Ihr Vorteil besteht darin, dass sie durch das Vakuum im Weltraum über die Gesamtstrecke gesehen mit deutlich weniger Verlusten skalieren (trotz atmosphärischer Beugung). Insgesamt betrachtet erfordert die Entwicklung von Quantenrepeater für ein Quanteninternet sehr komplexe Quantentechnologie.

2.8.1 Funktionsweise

Um die Funktionsweise des Quantenrepeaters prinzipiell nachvollziehen zu können, wollen wir uns ein vereinfachtes Beispiel ansehen: Angenommen, Alice und Bob betreiben Quantenkryptografie mit verschränkten Photonen nach dem Ekert-Protokoll (Abschn. 2.6.2). Nun sind beide aber so weit voneinander entfernt, dass „Pfadverluste" eine Rolle spielen. So könnten die Photonenrate infolge Absorption im benutzten faseroptischen System zu gering sein oder Dekohärenzeffekte eine Rolle spielen. Was sollen sie tun? Sie müssen die Verschränkung möglichst „rauschfrei" über eine größere Distanz ausdehnen. Dazu benutzen sie einen Quantenrepeater. Die Logik, nach der nun vorgegangen wird, kann folgenderweise dargestellt werden:

$$\text{wenn} \quad A = B \quad \wedge \quad C = D, \quad \text{dann} \quad A = D$$

(das Symbol „=" entspricht der Verschränkung und „∧" steht für eine spezielle Bell-Zustandsmessung). Zwischen Alice und Bob befindet sich eine Repeaterstation. Diese stellt zunächst sowohl eine Verschränkung mit Alice her als auch eine mit Bob. Es entstehen somit zwei verschränkte Teilsysteme. Sodann wird die Bell-Messung durchgeführt, woraufhin die Verschränkung von den Teilsystemen auf Alice und Bob gewissermaßen „überschwappt" (Entanglement Swapping). Auf diese Weise wird zwischen Alice und Bob ein reiner verschränkter Zustand erzeugt, der vorher noch nicht vorhanden war. Ab dann kann die Quantenkryptografie prinzipiell nach dem Ekert-Protokoll erfolgen. Zur praktischen Funktionsweise müssen die Qubits allerdings in einem lokalen Quantenspeicher abgelegt werden. Aktuelle Implementierungsversuche arbeiten mit Photonen als

mobilen Qubits, welche via Glasfaser von beiden Seiten in den Repeater einlaufen. Dort wird der Quantenzustand jeweils in einem separaten Quantenspeicher (zum Beispiel einem gefangenen Atom) abgelegt. Durch eine spezielle Kopplung (entspricht der Bell-Zustandsmessung) können auf diese Weise zwei stationäre Netzwerkknoten miteinander verschränkt werden. Ähnlich der fragilen Technik von Quantenschnittstellen erweist sich die Suche nach robusten Quantenspeichern, die effizient mit Photonen interagieren können, als besonders große Herausforderung. Schließlich gilt es noch, die Verschränkung schneller herzustellen, als die gespeicherten Zustände verfallen.

2.8.2 Verschränkungsaustausch

Es sei im Folgenden der Vorgang des „Entanglement Swapping" näher betrachtet. Wie dargelegt, erlaubt die Quantenteleportation die Übertragung von konkret determinierten Quantenzuständen, also speziell präparierten Qubits. Es ist aber genauso möglich, auch völlig unbekannte Zustände zu teleportieren, insbesondere auch verschränkte Zustände selbst. Genau diesen Umstand macht sich der Quantenrepeater zunutze. Zunächst werden ja die beiden verschränkten Paare A = B und C = D erzeugt (Abb. 2.10). Die Bell-Messung bewirkt dann, dass B und C miteinander verschränkt werden, wodurch die Voraussetzung zur Quantenteleportation erfüllt wird. Als Folge wird der Quantenzustand, welcher der ursprünglichen Verschränkung von A = B entspricht, auf das System A = D teleportiert. Dadurch werden instantan die Photonen A und D miteinander verschränkt. Bemerkenswert ist, dass die Photonen A und D daraufhin stark korreliert sind, obwohl sie in der Vergangenheit in keinerlei

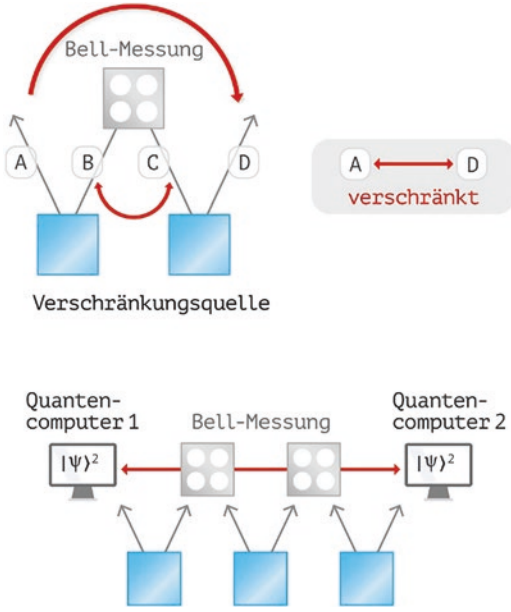

Abb. 2.10 Schema des Quantenrepeaters

Zusammenhang miteinander standen. Dieser Vorgang lässt sich theoretisch mit beliebig vielen Repeatern wiederholen, wodurch die Verschränkung auf große Distanzen ausgedehnt werden kann. Als wesentlich bleibt festzuhalten, dass es sich beim „Entanglement Swapping" um die Teleportation von Verschränkung handelt. Entlang einer Kette von Wiederholstationen können demnach Quantenkanäle durch Mehrfachteleportation erzeugt werden. Für die Realisierung eines Quanteninternets wird es dadurch (theoretisch) möglich, zwei Quantencomputer über tausende Kilometer miteinander zu verlinken. Gleichzeitig erlaubt jede Zwischenstation noch eine Verschränkungsdestillation („Fehlerkorrektur"), womit auch über große Entfernungen ein maximal verschränkter Zustand aufrechterhalten werden kann. Da die Teleportation von Qubits nur mit maximal

verschränkten Zuständen möglich ist, kommt dieser Auslegung eine ganz entscheidende Rolle zu. Willkommen in der Quanten-Telekom von übermorgen!

2.9 Vision und Wirklichkeit

Angesichts der gewaltigen Schwierigkeiten und der überwiegend völlig neuartigen Technologie, die es noch zu entwickeln gilt, ist die Realisierung eines (globalen) Quanteninternets in unmittelbarer Zukunft noch eine Vision. Allerdings gilt es dabei verschiedene Stufen zu unterscheiden: Die erste Phase, die Installation größerer QKD-Topologien an verschiedenen Punkten der Erde sowie der vermehrte Einsatz von Quantensatelliten, erscheint innerhalb der nächsten 10–15 Jahre durchaus wahrscheinlich. Führende Forscher gehen sogar davon aus, dass es bereits in diesem Zeitraum ein Quanteninternet parallel zum bestehenden geben wird. Zunächst geht es vordergründig darum, die kritische Infrastruktur am Boden wie auch im Weltraum abzusichern, zumal staatliche Einrichtungen sowie Unternehmen Interesse bekunden. Dazu gilt es Systeme zu entwickeln, die vor allem auch ökonomisch betrieben werden können. Im Mittelpunkt steht ferner das Forschungsziel, ein Netzwerk skalierbarer Quantenknoten zu implementieren als Prototypen für ein zukünftig vollverschränktes globales Quanteninternet. Dies schafft ein wichtiges Fundament für die praxistaugliche Realisierung von Quantenrepeatern. Ebenso gilt es, die zur skalierbaren Steuerung nötige Software sowie das Netzwerkstack zu entwickeln. Wichtig ist zu verstehen, dass die komplexe Quantentechnologie heute schon ihren Startschuss erfahren muss, damit sie morgen ausgereift zur Verfügung stehen kann. Wie die zahllosen Implementierungsversuche

zeigen, steckt die Quanten-IT freilich überwiegend noch in ihren Kinderschuhen. Dies betrifft vor allem auch den Quantencomputer, dessen Entwicklung eine vermutlich noch viel größere Herausforderung darstellt als die bloße Netzwerktechnik (und von dieser grundsätzlich getrennt zu sehen ist). Nichtsdestotrotz gibt es allerorts zahlreiche Bemühungen, um das „Q-Web" aus dem Stadium der reinen Grundlagenforschung auf die Ebene der technologischen beziehungsweise kommerziellen Nutzbarkeit zu heben.

Wie ernst man das mittlerweile nimmt, zeigt beispielsweise die Europäische Union, welche die Quantentechnologien 2016 zu ihrem dritten milliardenschweren Flaggschiffprojekt erklärt hat. Dabei zielt die Initiative nicht nur darauf ab, die Vorteile für Wissenschaft, Industrie und Gesellschaft nutzbar zu machen, sondern die EU möchte sich hiermit als Global Player in dieser zukunftsträchtigen neuen Domäne etablieren. Im Sinne eines strategischen Investments verspricht man sich davon, Europa zu einer attraktiven, dynamischen Region für innovatives Business zu machen und ein neues Niveau der Kooperation zwischen Wissenschaft und Industrie zu schaffen, um die Entwicklung zügiger vorantreiben zu können. Selbstverständlich dürfen solche Pläne keine Lippenbekenntnisse bleiben und erfordern entsprechende Fördermaßnahmen und Investitionen, die zeitnah und in angemessenem Umfang gewährleistet sein sollten. Während Asien speziell in der Q-Satellitentechnik die führende Position einnimmt, ist Europa in der Grundlagenforschung gut genug aufgestellt, um die bestehende Glasfaserstruktur des Internets „Q-fit" zu machen. Europa sollte diese Chance nutzen, seine Ressourcen bündeln und dieser internationalen Entwicklung eine prägende Kontur verleihen. Nicht zuletzt auch deshalb, weil viele der Ideen, die in Asien aufgrund der viel größeren Ressourcen heute

umgesetzt werden, bereits vor 10–20 Jahren in Europa und den USA entwickelt wurden.

Die EU-Kommission hat führende Vertreter aus Wissenschaft und Industrie um ihre Einschätzung gebeten, wie eine realistische Roadmap mit Zielen und Timeline aussehen könnte. Diese zeigt das Quanteninternet eingebettet in ein 4-Säulen-Modell, das die Kernbereiche umfasst, welche die potenzielle zweite Quantenrevolution charakterisieren: Quantenkommunikation, -simulation, -sensorik und -computing. Für die Prototypenentwicklung eines skalierbaren Quantennetzwerks hat die EU- Kommission aktuell eine erste Förderung genehmigt. Die verantwortliche „Quanteninternet-Allianz" (Leitung Qu Tech Universität Delft), ein europaweites Konsortium führender Forschungseinrichtungen, verfolgt das Ziel, gemeinsam mit Industriepartnern und Hightech-Unternehmen die erforderliche Technologie zu entwickeln, um sich in dieser hochinnovativen Domäne an die vorderste Front zu setzen. Besonders zu erwähnen wäre hier auch das britische „Quantum Communications Hub", ein Forschungs- und Entwicklungskonsortium aus Universitäten, Industriepartnern und staatlichen Interessengruppen, das durch das britische National Quantum Technologies-Program finanziert wird und sich auf die Vermarktungsreife konzentriert. Als noch ferneres, aber umso faszinierenderes Ziel wird die Entwicklung eines leistungsfähigen Quantencomputers avisiert, der Europas zukünftiger Smart-Industry-Vision die ultimative Krone aufsetzen soll. Bezüglich seiner ehrgeizigen Ambitionen befindet sich Europa in bester Gesellschaft mit Ländern wie Japan, China oder den USA, mit denen die EU nicht nur konkurrieren, sondern auch kooperieren will. Gerade das hohe Interesse amerikanischer Tech-Giganten am Quantencomputer wie auch die Tatsache, dass die Quanteninformationstechnologie sowieso zur wichtigsten Zukunftsware zu zählen ist, lässt

die Vision Quanteninternet in einem viel reelleren Licht erscheinen, als manche ihr zugestehen möchten.

Unter der Annahme, dass die physikalisch-technologische Machbarkeit im Wesentlichen gegeben ist (was noch nicht abschließend bewiesen ist), erscheinen drei Entwicklungsfelder für das Quanteninternet maßgeblich (siehe Kasten).

Entwicklungsfelder der Quanteninformationstechnologie

- Etablierung eines lokalen, später auch globalen QKD-Netzwerks als wesentliche Stütze für eine langfristige digitale Sicherheitstechnik. Nutzbarkeit der QKD für zahlreiche kommerzielle Anwendungen und mobile Endgeräte. Neben Sat-Boden-Datalinks ist es ein erklärtes Forschungsziel, die faseroptische Struktur des heutigen Internets so zu verändern, dass eine maximal sichere Datenübertragung über den gesamten Globus erreicht wird. Das technologische Ziel bezeichnet ein Netzwerksystem von Quantenknoten zur vollverschränkten QKD ohne Verwendung von Trusted Repeaters. Der Einsatz von Quantenspeichern ist für die Repeatertechnik zwingend erforderlich, nicht jedoch für die User an den Endnodes.
- Entwicklung leistungsfähiger Quantenprozessoren, idealerweise eines skalierbaren Quantencomputers, der via Quanten-Cloud Nutzern aus Wissenschaft, Medizin und Wirtschaft, aber auch privaten Usern zur Verfügung steht. Die damit verbundene Möglichkeit des Blind-Quantencomputings setzt ein Netzwerk zuverlässiger Quantenspeicher voraus, wo die User (im Idealfall) Zustände präparieren, Qubits speichern und teleportieren können. Die prinzipielle Funktionsweise konnte in Laborversuchen demonstriert werden, eine praxistaugliche Realisierung ist jedoch noch ein entferntes Ziel und setzt eine Reihe technologischer Durchbrüche voraus.
- Globale Vernetzung von skalierbaren Quantencomputern und Quanten-Devices verschiedenster Art und Auslegung. Die Endnodes sind leistungsfähige und eigenständige

Quantencomputer, die zuverlässige Fehlerkorrekturen vornehmen können. Ebenso gestatten sie die Erzeugung und Teleportation komplexer Quantenzustände. Falls dieser Entwicklungsstand eines Tages tatsächlich erreicht werden sollte, ergäbe dies eine Art Universal-Quanteninternet für Multiuser-Anwendungen mit vermutlich noch völlig unbekannten Applikationen und noch nicht absehbar vielfältigen Ausbaumöglichkeiten.

2.9.1 Agenda 2030 – das erste globale Quanteninternet?

Die QKD ist in der Entwicklung am weitesten vorangeschritten. Wie dargelegt, wurde sie bereits in Testnetzwerken in Europa, Amerika und Asien in echter Netzwerkumgebung implementiert. Neben Japan nimmt hier zurzeit vor allem China die Vorreiterrolle ein. Mit dem Beijing-Shanghai-Backbone, besonders auch der demonstrierten QUESS-Technik zielt man dort unübersehbar auf globale Vernetzung ab. Als ein weiterer Schritt soll das bestehende terrestrische Netzwerk erheblich ausgebaut und von einer eigens gegründeten Firma betrieben werden. Als Pilotprojekt will dieses beispielgebend für mögliche lokale Netzwerke in aller Welt wirken, die perspektivisch via Quantensatellit weltumspannend mobil vernetzt werden könnten. Als Zeitmarke wird dabei ein Bereich um 2030 angepeilt, wenn laut dem chinesischen Chefwissenschaftler Jian-Wei Pan, unter Einsatz mehrerer Q-Satelliten, die Abdeckung erstmals global werden würde. Wie könnte das aussehen? Eine Möglichkeit wurde durch die Quantentelefonie zwischen China und Österreich bereits demonstriert, allerdings fungiert der Satellit bei sehr großen Distanzen selbst nur als Trusted Repeater und setzt daher in solchen Fällen ein

Vertrauen zum Satellitenbetreiber voraus. Dennoch verkörpert bereits die „Relaistechnik“ einen großen Fortschritt und beweist die technologische Machbarkeit der Long Distance – Quantenkommunikation. Ebenso gilt es zu beachten, dass die (maximal sichere) vollverschränkte QKD über 1200 km bereits möglich wäre -ein gewaltiger Fortschritt gegenüber bisherigen Implementierungen! Es ist demnach mit hoher Wahrscheinlichkeit davon auszugehen, dass China die „Q-Sat-Technologie“ nach ökonomischen Gesichtspunkten zu einem Q-Satellitennetzwerk weiterentwickeln wird, wobei die Fortschritte der klassischen optischen Sat-Kommunikation dabei wohl maßgebliche Unterstützung leisten dürften. Bei entsprechender Logistik lassen sich rein theoretisch sogar mehrere Quantensatelliten kurzzeitig zu einem Quantenrepeater zusammenschalten, wodurch mittels Entanglement Swapping sehr weit entfernte Endnodes direkt verschränkt werden. Ausreichend hohe Erzeugungsraten vorausgesetzt, kann auf diese Weise quantisches Schlüsselmaterial generiert werden, das spätestens nach mehreren Zyklen eine Größenordnung erreicht, die eine hochsichere Übertragung zulässt. Wie oben gezeigt, gibt es bei einer vollverschränkten QKD keine physikalische Möglichkeit, den erzeugten Schlüssel vom Satelliten aus abzugreifen und an Dritte weiterzufunken. Lässt man die technischen Schwierigkeiten einmal außer Acht, ließe sich damit nicht nur das Repeaterproblem (mit Einschränkung) lösen, sondern ebenso Quantenkanäle zwischen lokalen Netzwerken herstellen, welche es dann vermutlich über die ganze Welt verteilt geben dürfte. Der Einschätzung einiger Forscher nach sollte es in den nächsten 10–15 Jahren zu erheblichen Weiterentwicklungen in der Quantenrepeatertechnik kommen, wodurch die vollverschränkte QKD auch in Glasfasernetzen über große Distanzen möglich sein wird. Ab dann kann auch die bestehende faseroptische

Infrastruktur des „alten“ Internets global für die Quantenkommunikation genutzt werden. Gerade auch der europäischen Forschung ist das ein zentrales Anliegen, wie etwa das Vienna Multiplex Q-Web beweist. Unter der Headline „Vision Web Q.0“ verfolgt die QIA (Quanteninternet-Allianz) das Ziel, ein Prototyp-Quanteninternet aus 3 bis 4 Knoten zu implementieren, das mittels Quantenrepeatern vier Städte in den Niederlanden verbinden soll. Bereits 2020 laufen die Anstrengungen für die Realisierung eines ersten Testlinks, wobei unter anderem mithilfe von Frequenzkonversion die Nutzbarkeit bestehender Glasfasern demonstriert werden soll. Im Erfolgsfall wäre das Projekt ein wichtiger Markstein auf dem Weg zur Entwicklung eines „echten“ Quanteninternets ohne Trusted Repeaters. Im Nachfolgenden seien die zwei wichtigsten Funktionalitäten der QKD zusammengefasst.

1. Resistenz gegen Superrechner
Die QKD besitzt den nicht zu unterschätzenden Vorteil, dass sie die schnelle, aber angreifbare symmetrische Verschlüsselungscodierung sicher macht. Wie angesprochen bliebe die klassische Schlüsselzuteilung mit OPT ein schwerwiegendes Problem (Abschn. 2.6.1). OPT ist aber gerade ein Verfahren, das nicht nur sehr schnell gigantische Datenmengen verschlüsseln kann (was in der zukünftigen IT eine große Rolle spielen wird), sondern bei ausreichend hohen Bitraten auch Angriffen zukünftiger Supercomputer und Quantenrechner standhalten könnte. Aus heutiger Sicht vermag letzterer nur mit einer Art Grover-Algorithmus gegen OPT ins Feld zu ziehen. Der Grover schafft zwar, wie gezeigt, eine „quadratische Beschleunigung“, diese vermag aber angesichts der Myriaden möglicher Schlüsselkombinationen dennoch nichts auszurichten. Dazu müsste der Quantencomputer schon mit einer

surrealen Qubit-Zahl (beachte Redundanz!) aufwarten können, was aus heutiger Sicht völlig unrealistisch ist. Wie ebenso im Detail gezeigt, wird mit der QKD ein physikalisch garantierbarer Sicherheitsaspekt wirksam, welcher das Erkennen eines Lauschangriffs in direkter Form ermöglicht. Da es diese Funktionalität in der klassischen IT überhaupt nicht gibt, stellt sie ein absolutes Novum dar. Dies wird die QKD abseits der Interessen von Regierungen, Geheimdiensten, Militär oder großen Unternehmungen auch für private Nutzer und kommerzielle Anwendungen interessant machen. Insbesondere dürfte der digitale Zahlungsverkehr betroffen sein, wie auch hochsichere Bankomat- oder Kreditkarten. Hierbei mag es auch um den psychologischen Vertrauensfaktor gehen: Es ist eben beruhigender, sich auf eine durch Naturgesetze garantierte Sicherheit zu verlassen als auf die immer wieder bewiesene Fehlbarkeit des Menschen, frei nach dem Motto: „Security built by nature“. Zur praxistauglichen Umsetzung sind allerdings noch viele technologische Hürden zu meistern, einschließlich der Repeaterproblematik, damit Quantenkanäle über große Entfernungen funktionieren können. Derart fortgeschrittene Systeme stellen in weiterer Folge auch die Basis für die Visionen der klassischen IT dar. Ein Verbund zukünftiger Smart-Cities wäre jedenfalls ohne eine besondere Sicherheitstechnik kaum vorstellbar. Hierzu bietet die QKD die ideale technologische Grundlage, welche zusammen mit Methoden der Post-Quantenkryptografie auch zukünftigen Angriffen von dramatisch wachsender Rechnerleistung standhalten sollte. Was die QKD allerdings nicht zu leisten vermag, ist einen 100-%-Schutz vor einem Fake bei der Authentifizierung zu garantieren. Doch auch dieses, aus heutiger Sicht generell unlösbare Problem, kann durch QKD-basierte Verfahren erheblich abgemildert werden.

2. Hackersichere Datenspeicher

Die QKD erlaubt zwar per se nur die völlig abhörsichere Punkt-zu-Punkt-Datenübertragung, kann aber auch in Kombination mit klassischen Verfahren ein unerreicht hohes Sicherheitslevel gewährleisten. Dazu ein Beispiel, das ebenfalls bereits in Testnetzwerken implementiert wurde: Schon heute werden in Rechenzentren ungeheure Datenmengen über einen sehr langen Zeitraum gespeichert, auch digitale Archive werden immer größer – wie gelingt ein möglichst umfassender Schutz gegen Hackerangriffe der auch zukünftiger Rechnerleistung standhält? Ein zukunftssicheres Datenspeichersystem muss also die folgenden vier Anforderungen erfüllen:

1. Vertraulichkeit (Daten sind nur autorisierten Parteien zugänglich),
2. Integrität (Daten sollen unverändert bleiben, das heißt digitale Signaturen und Authentifizierungsschemata verwenden),
3. Verfügbarkeit (Daten sind jederzeit abrufbar durch Redundanz) und
4. Funktionalität (Daten lassen sich ohne Dechiffrieren weiterverarbeiten, was eine sogenannte homomorphe Verschlüsselung voraussetzt).

Ein möglicher Ansatz sei hier vorgestellt: Aus einem zentralen Datensatz werden Teile durch Polynommultiplikation auf verschiedenen verteilten Speichern abgelegt. Bei N Speichern können die Daten rekonstruiert werden, indem mindestens k Pakete eingesammelt werden. Bei $k-1$ Paketen können die Daten selbst bei unbegrenzter Rechenleistung nicht rekonstruiert werden (vorausgesetzt die Zahl korrupter Teilspeicher ist kleiner als k). Dieses System stellt Vertraulichkeit sicher (1) und es können Teile algorithmisch multipliziert werden, sodass (4) erfüllt

wird. Selbst wenn Teile verloren gehen, können die Daten wieder rekonstruiert werden, was (3) erfüllt. Anforderung (2) wird dagegen nicht zwangsläufig gewährleistet, vor allem muss auch die Kommunikation zwischen den Teilspeichern geschützt werden, was durch QKD ideal gelöst wird. Die QKD ermöglicht somit auch einen langfristigen Integritäts- und Vertraulichkeitsschutz bei hackersicheren Datenspeichern.

2.9.2 Futurezone: Das universale Q-Hypernet

Mit steigender Zahl von Qubits an den Endnodes könnte ein Quantennetzwerk immer besser und leistungsfähiger werden. Falls es gelingt, die Repeaterproblematik in den Griff zu bekommen, ferner Kohärenzzustände und Fehlerkorrektursysteme stetig zu optimieren, könnte eines Tages ein weltumspannendes Netzwerk entstehen, das als äußerst leistungsfähiges Hypernet mit zusätzlicher Quantenpower die Visionen der klassischen IT ergänzt. Basierend auf ultraschnell koordinierbarer, äußerst komplexer Netzwerktechnik und erweitert um zahlreiche Quantensatelliten, die theoretisch im Mikroformat gebaut werden können, wäre es dazu angetan, die Menschheit in eine neue technologische Ära zu führen Ein solches Hypernet könnte auch abseits der Wissenschaft (wo es einen unschätzbaren Wert besäße) zu vielen Innovationen beitragen: Zunächst einmal zu absolut sicheren Kommunikationskanälen, die von QKD-Systemen (in ihrer Endform auf vollverschränkter Basis) gewährleistet werden und klassische Computer wie auch verschiedene Formen mobiler Endgeräte vernetzen. Dazu zählen neben Smartphones oder Wearables auch Satelliten, Drohnen oder selbstfahrende Autos. Besonders auch als wirksamer Hackerschutz gegen den Zugriff auf Datenbanken und digitale Archive, die in Zukunft

noch viel inflationärer auftreten werden. Damit hält es auch für den Normaluser eine Vielzahl kommerzieller Anwendungen bereit.

Abgesehen vom hochsicheren Online-Finanzverkehr, der in dieser Ära wohl bereits unabdingbar wäre, sind auch andere Applikationen denkbar: Dank Superpositionsprinzip kann eine Quanten-Blockchain zu völlig neuen Methoden der Validierung von Angeboten, Verträgen oder Kryptowährungen wie Bitcoins führen. In ähnlicher Weise ließen sich Fake News viel effizienter eindämmen. Ein anderer Aspekt unterstützt ein verstärktes Bedürfnis nach Privatsphäre, dem in der Zukunft vermehrt Bedeutung zukommen dürfte. Aktuell übergibt der Mensch (vor allem der junge) dem Internet im Prinzip sein ganzes Leben in Form digitaler Fußstapfen. Damit läuft er Gefahr, nur noch Spielball von Algorithmen und Institutionen zu werden. Viele Internetdienste tragen dazu gewaltig bei. Schon heute ist es schwierig, seine persönlichen Eigenschaften und Vorlieben verborgen zu halten – mit jedem Aufruf der Suchmaschine wird der persönliche Begehr für die Nachwelt oder die Anzeigenkunden aufgezeichnet. Die Quantentechnik bietet (wenn man sie denn lässt) die Chance, einen wichtigen gesellschaftlichen Wert zu bewahren: das Recht auf Privatsphäre und den Schutz davor, vollends „gläsern" und manipulierbar zu werden. In diese Kerbe schlägt auch eine supersichere Quanten-Cloud.

Einen technologischen Höhepunkt markiert die Entwicklung skalierbarer Quantencomputer, deren Vorteile in weiterer Folge Nutzern auf der ganzen Welt zur Verfügung stehen. Der „Quantenvorteil" für die Wirtschaft könnte eines Tages gewaltig sein. Abgesehen vom Cloud-Betreiber selbst, der sich damit eine goldene Nase verdient (dem aber dennoch verborgen bleibt, welche Funktionalitäten seine Clients ausführen), gilt es, die gesamte notwendige Infrastruktur zu beachten. Sie könnte einst zum Eldo-

rado einschlägiger Firmen werden und völlig neue Berufe und Geschäftsideen entstehen lassen. Im Quanteninternet der Zukunft stellt der Nutzer eine Frage an die Quantensuchmaschine und erhält eine Antwort, ohne dass irgendjemand die Frage kennen kann – auch der Server nicht. Da die Suchmaschinenbetreiber ihr Geld mit der Analyse der Nutzerdaten verdienen, müssen sie bei deren Wegfall zwangsläufig andere Einnahmequellen erschließen. Dem Kunden würde dann die Alternative angeboten, ob er den Inhalt seiner Suchanfrage preisgeben will oder für die hochdiskrete Suche extra bezahlen möchte. Davon abgesehen kann sich der Handlungsreisende seinen optimalen Routenplan genauso berechnen lassen wie der Pharmakonzern seinen neuen Wunderwirkstoff. Die Implikationen reichen also auch bis zur Biochemie und Genetik. Unzählige Firmen profitieren von der Lösung ihrer Logistikprobleme wie auch die Verkehrsbehörden von der Berechnung der Fahrzeugströme. Die Wissenschaft findet dank Quantensimulatoren völlig neue Werkstoffe oder Supraleitung bei Zimmertemperatur, was ganzen Industriezweigen goldene Zeiten bescheren würde. Firmen lassen sich effizientere Konzepte für Akkus und deren Recycling berechnen und optimieren damit die E-Mobilität. Wie heutige Studien bereits nahelegen, eröffnen Quantenrechner ungeahnte Möglichkeiten für Machine Learning, Robotik und KI, womit Smart-Industry-Konzepten erst so richtig auf die Sprünge geholfen würde.

Schließlich könnten dereinst leistungsfähige Quantencomputer und -devices jeglicher Art entweder durch reine Verschränkung verlinkt sein oder aber per Quantenteleportation komplexe Quanteninformation miteinander austauschen. Getreu der Feynman-Doktrin, dass Quantencomputer die Natur selbst abbilden, lassen sich daraus weitere Zukunftstechnologien wie etwa

die „programmierbare Materie“ ableiten. So wäre theoretisch eine Art Quanten-3D-Drucker vorstellbar, der aus der Cloud komplexe Quanteninformation via Teleportation auf einen vorhandenen materiellen Objektträger downloadet. Damit kann man die Eigenschaften von Materie auf der mikroskopischen Skala designen und an die Wünsche des Klienten anpassen. Möglich auch, dass hierin einst das ultimative Konzept für intelligente XD-Materialien liegen wird, welche sich adaptiv an ihre Umgebung anpassen. Bereits zu Beginn wurde die Vernetzung von Quantencomputern via Teleportation als das eigentliche Prinzip angesprochen. Diese Vision ist unter anderem von der Vorstellung geleitet, dass das gesamte Quantennetz im Sinne von Networked Computing zu einem extrem leistungsfähigen modularen Großrechner werden könnte. Da sich das Repeaterproblem wie gezeigt auf Basis der Mehrfachteleportation grundsätzlich lösen lässt, mag diesem dezentralen Konzept die tragende Rolle in der zukünftigen Quanten-IT zukommen. Die Realisierung leistungsfähiger Quantencomputer wird vermutlich eine der größten technologischen Leistung darstellen, die der Mensch in den nächsten Jahrzehnten (und weit darüber hinaus) erbringen könnte. In jedem Fall ist aber seine Entwicklung eng mit dem Quanteninternet korreliert. Abgesehen vom Blind-Quantencomputing benötigt man ein solches – egal in welchem Maßstab – um ihn überhaupt skalierbar entwickeln zu können. Oder aber es trägt dazu bei, seine Fähigkeiten wie die von vernetzten Supercomputern in noch höhere Sphären vordringen zu lassen. Physikalisch sind derlei Zukunftsvisionen und Futurismen prinzipiell alle denkbar – die Frage wird sein, wie weit sich Quantenkohärenz im großen Stil aufrechterhalten lässt, wie weit man technologisch in der Lage sein wird, an jene Möglichkeiten heranzukommen, welche die Natur

grundsätzlich bereithält. In der Quanteninformationstechnik steckt unerhörtes Potenzial – falls sich die „zweite Quantenrevolution“ tatsächlich manifestieren sollte, dann muss das universale Quantenhypernet als ihr krönendes Ornat erscheinen.

3

Didaktische Vertiefung

3.1 Workshop: Quantenoptische Systeme

Quanteninterferenz

Für die Technik der Quantenkommunikation spielen quantenoptische Geräte eine tragende Rolle, insbesondere auch für QKD-Netzwerke. Um deren Bedeutung besser verstehen zu können, sei der Leser an ein fiktives Institut für Experimentalphysik geladen, wo „Professor Quant" Rede und Antwort stehen wird. Dabei geht es auch um Begrifflichkeiten wie Welle-Teilchen-Dualität, Wellenfunktion oder Nichtlokalität. Diese sind sicherlich dazu angetan, der Quantenwelt einen Mystizismus aufzuprägen, der wohl dem Umstand geschuldet ist, dass der Mensch in seiner Vorstellungskraft der alltäglichen Erfahrungswelt in so hartnäckiger Weise verhaftet ist.

G. Fürnkranz, *Vision Quanten-Internet,*
https://doi.org/10.1007/978-3-662-58453-8_3

Zunächst demonstriert uns der Professor ein Mach-Zehnder-Interferometer (Abb. 3.1). So ein Gerät wird in der Technik etwa dazu benutzt, um kleinste Dichteunterschiede in Medien festzustellen, findet aber

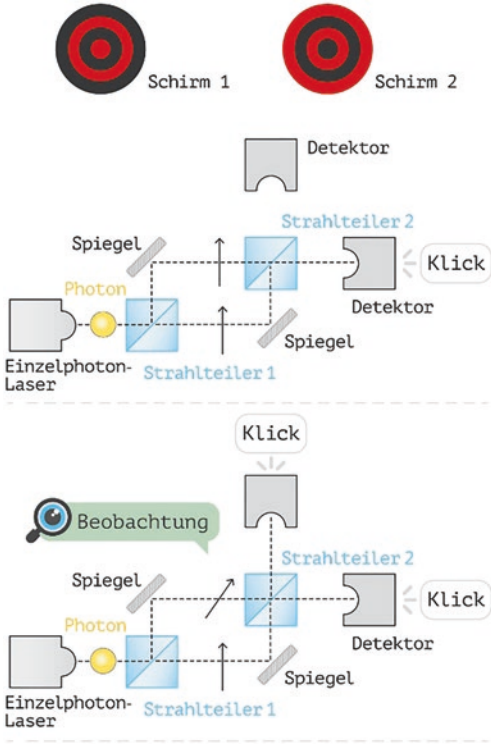

Abb. 3.1 Wohljustiertes Mach Zehnder-Interferometer: Der Einzelphoton-Laser erzeugt einzelne Lichtquanten, die über die Strahlteileranordnung von Detektoren gemessen werden. Abhängig von der Stellung der Polfilter (schwarze Pfeile) kann die Komplementarität zwischen Weginformation und Interferenz demonstriert werden. Beachte: in Abb. 3.1 ist eine zweite Versuchsanordnung angedeutet, die entsteht, wenn unter Einsatz eines herkömmlichen Lasers die Detektoren durch die Schirme 1 und 2 ersetzt werden. Diese wird textlich zuvor erwähnt, um dem Leser zu einem besseren Gesamtverständnis zu verhelfen

auch in abgewandelter Form als Trägheitssensor in Flugzeugen Verwendung. Darüber hinaus besitzt es hohe Bedeutung für quantenoptische Prinzipdemonstrationen. Beachte: in Abb. 3.1 werden zwei Versuchsanordnungen beschrieben, einmal mit Schirmen und gewöhnlichem Laser, einmal mit Detektoren und Einzelphoton-Laser

Zunächst zur Anordnung mit herkömmlichem Laser und Schirmen: Im Aufbau erkennen wir, wie ein Laserstrahl auf einen Strahlteiler 1 trifft und dort in zwei Strahlen getrennt wird, die jeweils über 90°-Spiegel abgelenkt werden, bevor sie in einem Strahlteiler 2 wieder zusammentreffen. Wenn Professor Quant den Laser einschaltet, sehen wir merkwürdige Streifenmuster, sogenannte Interferenzbilder (Abb. 3.1 oben). Diese entstehen jeweils an Schirm 1 und Schirm 2, welche genau dort positioniert sind, wo die Strahlen austreten. Um die Muster mit eigenen Augen deutlich sehen zu können, ist allerdings eine Aufweitungslinse nötig (nicht eingezeichnet). Daraufhin hält Professor Quant seine Hand in einen der Teilstrahlen und ruft aufgeregt: „Sehen Sie?" Wir sehen nichts, außer dass die seltsamen Streifenmuster in dem Augenblick verschwinden, wo er die Hand hinhält. „Verstehen Sie nun?" fragt er eindringlich. Wir verstehen nur Bahnhof. Was soll das bitteschön beweisen?
Daraufhin erklärt uns der Professor geduldig, was es damit auf sich hat. „Sehen Sie, aus sehr moderner Sichtweise der Quantenphysik haben Sie soeben ein 1-Bit-System beobachtet. Wie Sie ja bereits wissen, besteht Licht aus Photonen (Lichtquanten). Wenn nun ein bestimmtes Photon aus dem Laser kommt, hat es am Strahlteiler 1 quantenzufällig eine 50-%-Chance, transmittiert oder reflektiert zu werden. Solange ich meine Hand nicht hinhalte, kann nicht festgestellt werden, welchen Weg das Photon genommen hat. Wir sagen, das System befindet sich dann in einer Superposition, das heißt in

einer Überlagerung von beiden möglichen Teilstrahlen beziehungsweise Wegen, die das Photon nehmen kann. In diesem Fall sieht man das Interferenzbild. Halte ich dagegen meine Hand in einen der beiden Teilstrahlen, so ist ab diesem Moment sofort klar, welchen Weg das Photon genommen hat, da es ja sozusagen mit meiner Hand kollidiert, wenn es diesen Teilstrahl gewählt hat, und sonst eben nicht. Wichtig ist dabei festzuhalten, dass die Kollision aus Sicht eines einzelnen Photons gar nicht passieren muss, es reicht der bloße Konjunktiv. Wir sprechen dann von einer sogenannten Ortsmessung. In diesem Moment bricht die Superposition instantan zusammen und das Streifenbild verschwindet. Niels Bohr, einer der Gründerväter der Quantenmechanik, würde von einem Kollaps der Wellenfunktion sprechen. Verblüffenderweise hängt das Verhalten des Systems also davon ab, ob die Photonen beobachtet werden *können* oder nicht."

„Sie wollen also ernsthaft sagen, und das ist Wissenschaft, Quantensysteme hängen von der Beobachtung ab?"

„Gewissermaßen könnte man das so sagen. Wobei ‚beobachten' nicht automatisch heißt, dass Sie das Teilchen wirklich beobachten müssen, es reicht die pure Möglichkeit dazu. Beobachten bedeutet, physikalisch eine Situation zu schaffen, wo eine oder mehrere physikalische Größen gemessen werden könnten. Dafür muss ich nicht notwendigerweise meine Hand hinhalten; es können genauso gut auch zwei Polarisationsfilter zum Einsatz kommen, welche jeweils in einen der beiden Teilstrahlen eingebracht werden. Polarisationsfilter besitzen die Eigenschaft, dass sie die Schwingungsebene des Lichts verändern. Ich demonstriere Ihnen das einmal. Sehen Sie? Solange beide Polfilter (schwarze Pfeile in Abb. 3.1 oben) parallel stehen, verbleibt das Interferenzbild in seiner bekannten Form. Verdrehe ich

allerdings die Filter gegeneinander (Abb. 3.1 unten), so verschwindet die Interferenz. Der Grund dafür liegt darin, dass in diesem Moment eine Ortsmessung vorliegt, da man aufgrund der verdrehten Schwingungsebenen des Lichts feststellen könnte, mit welchem Teilstrahl ein bestimmtes Photon ankommt. Da liegt dann also eine gewisse Weginformation vor. Und wenn ich jetzt die Filter wieder parallel stelle, habe ich diese Info-Möglichkeit nicht mehr und das System zeigt erneut das Interenzbild."

„Und was hat das mit einem 1-Bit-System zu tun?"

„Ganz einfach – es gibt hier nur zwei Möglichkeiten, die einander gegenseitig ausschließen: Entweder Interferenz *oder* Ortsmessung. Beides ist gleichzeitig nicht möglich. 1 Bit an Information kann beispielsweise ja oder nein, weiß oder schwarz, aus oder ein, kalt oder warm usw. bedeuten. Hier gilt immer das Entweder-oder-Prinzip. In der Sprechweise der Quantenphysik sagt man: Interferenz und Weginformation verhalten sich zueinander komplementär. Wenn wir die Filter aus ihrer parallelen Stellung kontinuierlich verdrehen, sehen wir, dass die Interferenz sukzessive schwächer ausgeprägt ist, bis sie bei 90°-Stellung völlig verschwindet. Ich erhalte also auf Kosten der Interferenz zunehmend mehr Weginformation. Umgekehrt kann man die Filter wieder langsam parallel stellen, wodurch die Weginformation zugunsten der Interferenz kontinuierlich verschwindet. Genau das ist Komplementarität: Je mehr Wissen (also Information) ich von der einen Größe oder Eigenschaft besitze, desto weniger Information habe ich von der anderen. Insgesamt enthält das System aber nur 1 Bit an Information. Niels Bohr hat erkannt, dass Komplementarität eine fundamentales quantenmechanisches Prinzip ist und für alle derartigen Größen oder Eigenschaften gilt, die man messen kann. Sie ist nicht

nur eine Grenze dafür, was wir wissen können, sondern auch dafür, welche Eigenschaften ein System überhaupt besitzen kann."

„Nun aber mal ganz ehrlich: das Ganze wirkt doch künstlich aufgeprägt. Die obigen Phänomene lassen sich ganz leicht aus der klassischen Physik erklären: Wenn die Hand drinnen ist, fehlt natürlich der zweite Teilstrahl, wodurch die Interferenz per se ausgeschlossen ist. Auch das mit den Polfiltern lässt sich leicht erklären. Die auftretenden Interferenzbilder setzen kohärente Teilstrahlen voraus. Wenn aber beide Teilstrahlen bezüglich ihrer Schwingungsebene nicht paralll stehen, ist diese Bedingung automatisch nicht erfüllt. Wozu dann überhaupt Quantenphysik?"

„Ausgezeichnet!" lobt Professor Quant. „Wie ich sehe, verstehen Sie etwas von Physik – jedenfalls von klassischer. In der Tat gebe ich Ihnen recht! Solange es sich um einen für das menschliche Auge sichtbaren Laserstrahl handelt (der aus Abertrillionen von Photonen besteht), braucht man tatsächlich keine Quantentheorie. Sehr wohl aber, wenn der Strahl so weit abgeschwächt wird, dass er nur noch aus einzelnen Photonen besteht. Üben Sie sich ein wenig in Geduld, es wird noch sehr, sehr interessant werden!".

„Was bedeutet übrigens der Begriff Wellenfunktion?"

„Genau das …", lacht Professor Quant laut auf, „… ist das eigentlich Kuriose daran. Überlegen Sie mal logisch: Wenn die Photonen auf den ersten Strahlteiler treffen, haben sie quantenzufällig eine 50 %ige Wahrscheinlichkeit, transmittiert oder reflektiert zu werden. Ein einzelnes Photon im „unteren" Teilstrahl hat beim zweiten Strahlteiler dann wieder eine 50-%-Chance, transmittiert oder reflektiert zu

werden. Statistisch gesehen bedeutet das dann, dass 25 % aller Photonen bei Strahlteiler 2 transmittiert und 25 % an Strahlteiler 2 reflektiert werden. Falls das Photon aber den „oberen" Teilstrahl gewählt hat, kommt es ebenfalls zu einer solchen Aufspaltung bei Strahlteiler 2, also 25 % werden dort transmittiert und 25 % dort reflektiert. In Summe sollte also die Hälfte aller Photonen auf Schirm 1, die zweite Hälfte auf Schirm 2 auftreffen. Das bedeutet dann, dass wir auf jedem der beiden Messschirme einen strukturlosen Lichtfleck sehen sollten. Doch genau das sehen wir *nicht.* Wir sehen stattdessen an beiden Schirmen das Streifenmuster, eben das Interferenzbild. Zwar ist auch hier der Photonenanteil je 50 %, aber wir haben überhaupt keine Erklärung für das Zustandekommen der Hell-Dunkel-Abfolge.

„Was ist daran so besonders tragisch?"

„Der tragische Punkt ist folgender: Wir sind in einem veritablen Dilemma, denn das Experiment zeigt ein anderes Ergebnis, als es die so eben aufgestellte Theorie vorhersagt. Da das Experiment jedoch der höchste Richter in der Physik ist, muss die Theorie so geändert werden, dass sie mit dem experimentellen Befund übereinstimmt. Dies geschieht dadurch, dass man das Licht durch eine Welle beschreibt. Doch Vorsicht! Das Experiment schafft noch ein weiteres Problem: Durch Versuche in Beschleunigeranlagen (wie dem CERN) ist gesichert, dass Licht definitiv aus teilchenartigen Photonen besteht, Ein möglicher Ausweg besteht darin, dass man sagen könnte: Licht besteht zwar ausnahmslos aus Photonen, wie sich diese Partikel jedoch auf den Messschirmen anordnen, kann konsistent nur durch das Modell einer Welle korrekt beschrieben werden. Dieses Wellenbild ist aber im Prinzip eine Fiktion, ein

mathematisches Hilfsmittel, das dem Menschen das Denken erleichtert. Da man aus prinzipiellen Gründen in der Quantenmechanik niemals exakt vorhersagen kann, wo ein bestimmtes Photon genau auf dem Schirm auftreffen wird, kann man dafür lediglich eine Wahrscheinlichkeit angeben. Deshalb hat auch die Wellenfunktion, oder exakter deren Amplitudenquadrat, den Charakter einer Wahrscheinlichkeitswelle. Stellen Sie es sich am besten so vor: Licht besteht aus Teilchen, und die Wahrscheinlichkeit, sie an einer bestimmten Stelle zu messen, ist durch das Amplitudenquadrat der Wellenfunktion bestimmt..

„Und wie erklärt dann dieses Wahrscheinlichkeitswellenmodell das Phänomen?“

„Sehen wir uns nun an, wie es auf Basis der Wellenvorstellung mühelos gelingt, das Auftreten des Interferenzbilds zu erklären. Diese Erklärung ist hier zur klassischen Physik natürlich äquivalent. Wir nehmen jetzt den Fall an, dass die beiden Polfilter parallel stehen: Das Laserlicht wird am ersten Strahlteiler in zwei Teilwellen mit je halber Ursprungsintensität aufgespalten. Verfolgt man den in Abb. 3.1 oberen Teilstrahl, so wird er zweimal reflektiert, bevor er auf Schirm 1 trifft. Soll der untere Teilstrahl ebenso auf Schirm 1 treffen, so wird er dabei ebenso zweimal reflektiert. Beide Strahlen erfahren dabei jeweils eine Reflexion an einem Strahlteiler und an einem Spiegel. Da die beiden Strahlen also in derselben Weise reflektiert werden, besitzen sie eine sogenannte Phasendifferenz 0, was einer konstruktiven Interferenz entspricht. Das bedeutet, dass sich dort die Amplituden beider Teilwellen addieren, somit entsteht in Summe eine Welle mit doppelter Amplitude. Da im Wellenbild die Amplitude der Helligkeit des Lichts entspricht, ist nun alle Helligkeit und somit

das gesamte Laserlicht auf Schirm 1 zu sehen. Damit bleibt kein Licht mehr für Schirm 2 übrig. In einem sogenannten wohljustierten Interferometer (siehe unten) wären also Schirm 1 sehr hell und Schirm 2 völlig dunkel.

Nun ist das wohljustierte Interferometer aber eine Idealisierung. Idealisierungen sind typisch für die Physik; sie sind Hilfsmittel, um die Denkarbeit zu erleichtern. Insbesondere nimmt man dabei an, dass alle optischen Weglängen völlig identisch seien. In der Praxis ist dies jedoch schwierig zu erreichen, da der Laserstrahl trotz seiner schlanken Figur immer eine gewisse Divergenz aufweist. In unserem einfachen praktischen Versuch hier sind daher die optischen Weglängen zumeist nicht exakt gleich bemessen, wodurch es von innen nach außen zu einer Abfolge von konstruktiver und destruktiver Interferenz kommt. Daher beobachtet man an beiden Schirmen ein Interferenzmuster aus hellen und dunklen Ringen. Die beiden Interferenzbilder sind allerdings komplementär, das heißt, befindet sich an einem bestimmten Punkt auf Schirm 1 ein heller Fleck, herrscht an derselben Stelle auf Schirm 2 Dunkelheit vor und umgekehrt. Aber gerade dieser Umstand wird durch das Wellenbild völlig zutreffend beschrieben. Insbesondere wird erst durch das Wellenmodell verständlich, warum sich Licht – und sei es auch nur ein einzelnes Photon! – auslöschen beziehungsweise verstärken kann. Ohne die Wellenvorstellung des Lichts fände die Physik für das obige Experiment keine Erklärung. Es ist daher notwendig, dem Licht im mathematischen Sinne auch einen Wellencharakter zuzuschreiben."

„Was passiert eigentlich, wenn Sie anstelle der Schirme zwei Photonendetektoren anbringen, wie wir sie von der Quantenkryptografie her kennen?"

„Sehr gute Frage. Das wollte ich Ihnen ohnehin gerade demonstrieren. Jetzt wechseln wir zur High Tech-Experimentalphysik: Nehmen wir dazu ein wohljustiertes Interferometer her und verwenden wir anstelle der Schirme zwei Photonendetektoren. Diese können durch eine ausgeklügelte Multipliertechnik auf Basis von speziellen Fotodioden einzelne Photonen registrieren. Als ganz wesentliche Modifikation ersetzen wir jetzt den Laser durch einen Einzelphoton-Laser und wollen uns ansehen, was dann passiert. Statistisch gesehen befindet sich jetzt nur noch ein einzelnes Photon im Interferometer – das können Sie natürlich nicht mit eigenen Augen sehen, weil das Laserlicht jetzt viel zu schwach ist – aber unsere supergenauen Detektoren können die Einzelphotonen registrieren. Sehen Sie? Wenn die Polfilter 90° zueinander verdreht stehen, sprechen beide Detektoren an, das heißt mal der eine, dann der andere usw. Wenn die Polfilter aber parallel stehen, „klickt" immer nur einer der beiden Detektoren. Letzteres ist auf das besagte komplementäre Interferenzbild zurückzuführen. Beachten Sie dabei, dass beim wohljustierten Interferometer kein Muster mehr entsteht, sondern die gesamte Lichtintensität (= Anzahl der Photonen) auf einen einzigen Schirm beziehungsweise Detektor auftrifft. Und jetzt frage ich Sie: Wie können einzelne Teilchen ein solches Verhalten zeigen? Wenn beide Detektoren ansprechen, ist das aus der reinen Teilchenvorstellung heraus noch erklärbar, wie wir uns oben überlegt haben – nicht jedoch der zweite Fall, bei dem die Polfilter parallel stehen. Da brauchen wir zwingend das Wellenmodell. Sehen Sie, je nach Versuchspräparation zeigt das Licht entweder teilchen- oder wellenartiges Verhalten. Diese merkwürdige Eigenschaft von Quantenobjekten wird oft als Welle-Teilchen-Dualität bezeichnet. Zur Beschreibung dieser Ambivalenz benötigen wir die Wellenfunktion."

„Bezieht sich die Wellenfunktion nur auf Lichtquanten oder ist das eine universelle Beschreibung der Quantenphysik?“

„Definitiv eine universelle Beschreibung, die zwar mathematisch deutlich komplizierter als in diesem einfachen Fall sein kann, jedoch überall in der Quantenphysik auftritt. Ja, ja, die Wellen- oder ψ-Funktion ist ein absolutes Muss. Es sind ja nicht nur die Photonen, welche sich so merkwürdig verhalten, sondern alle Teilchen, das heißt Quantenobjekte. Dazu zählen auch Elektronen, Protonen, Neutronen, ganze Atome oder sogar ziemlich große Moleküle. Dazu kommen wir später noch. Vorher möchte ich Ihnen aber noch ein anderes, sehr berühmtes Experiment zeigen. Stellen Sie sich eine Wand vor mit zwei winzig kleinen Spalten, gerade so groß, dass ein Quantenteilchen noch durchpasst. Stellen Sie sich weiter vor, diese Wand werde wie durch ein Maschinengewehr mit sehr, sehr vielen Projektilen beschossen. Dabei muss es sich nicht notwendigerweise um masselose Teilchen wie Photonen handeln; die Munition kann auch aus Partikeln mit Ruhemasse bestehen, beispielsweise aus negativ geladenen Elektronen.“

„Meinen Sie das berühmte Doppelspalt-Experiment mit Elektronen?“

„Ja, ganz genau. Aus einer Quelle trifft statistisch zufällig ein sehr großes Kollektiv einzelner Elektronen auf eine Wand mit zwei kleinen Öffnungen, also einem ‚Doppelspalt‘. Dabei werden viele Elektronen von der Wand absorbiert, aber einige schaffen es durch die Spalte. Dabei hat ein Elektron eine 50-%-Chance, entweder durch den einen oder aber durch den anderen Spalt zu treten. Im Mittel werden also gleich viele Elektronen durch beide Spalt treten. Registriert man all diese Teilchen hinter

der Wand auf einem Messschirm, so erwartet man eine Häufigkeitsverteilung, die so aussieht, wie wenn man sehr viele schmutzige Fußbälle durch zwei Öffnungen auf eine weiße Wand schießt. Jeder Ball hinterlässt einen Fleck auf der dahinter befindlichen Mauer. So weit die Theorie. Macht man das Experiment aber in der Realität, so sieht die Häufigkeitsverteilung dagegen ganz anders aus. Wir haben hier jetzt nicht die Ressourcen, um Ihnen diesen (in der Praxis schwierigen) Versuch zeigen zu können. Dieser wurde bereits 1961 durch Claus Jönsson erstmals durchgeführt, 1990 von Jürgen Mlynek und Olivier Carnal sogar mit ganzen Atomen demonstriert. Und jedes Mal dasselbe Ergebnis: Die Bilder, die dabei auftreten, haben immer eine gewisse Ähnlichkeit mit dem Streifenmuster vom vorherigen Versuch, und in der Tat, es handelt sich auch hier stets um ein Interferenzbild. Ich spreche jetzt stellvertretend wieder für den Versuch mit Elektronen. Überaus seltsam: Die Quanteninterferenz, welche hier auftritt, entspricht einer Art Überlagerung, einer Superposition der beiden Optionen, die ein Elektron hat – eben durch den einen oder den anderen Spalt zu gehen. Kurioserweise verhalten sich die punktartigen Elektronen so, wie wenn sie durch beide Spalte gleichzeitig getreten wären – was natürlich nicht sein kann – deswegen muss ihnen im mathematischen Sinne ein Wellenaspekt zugeordnet werden. Auf dessen Basis kann man die Auftreffwahrscheinlichkeit der Elektronen auf dem Schirm berechnen. Dies ist in dem Sinne zu verstehen, dass sich zwar jedes einzelne Elektron bei seiner Messung am Schirm wie ein punktförmiges Teilchen verhält, die von den Wahrscheinlichkeiten bestimmte Gesamtverteilung der Elektronen am Schirm jedoch wellenartig verteilt ist. Im Übrigen wissen Sie ja schon aus dem vorigen Versuch, dass Interferenzbilder generell nur auf Basis der Wellenvorstellung erklärbar sind. Wie Sie sehen, ist das

Konzept der ψ-Wellenfunktion also nicht nur auf Photonen beschränkt, sondern betrifft genauso materielle Teilchen. Man spricht in diesem Fall von Materiewellen. Insgesamt zeigen alle Quantenteilchen diese bemerkenswerte Welle-Teilchen-Dualität.

Übrigens, mal sehen, ob Sie schon quantenmechanisch denken können: Was wird im Doppelspalt-Experiment passieren, wenn wir einen der beiden Spalte verschließen? Richtig! Dies entspricht einer Ortsmessung, da das Elektron in diesem Moment verrät, durch welchen Spalt es getreten ist. Damit erhält der Beobachter also eine räumliche Information über das Elektron. Als Folge muss das Interferenzbild sofort verschwinden, was es auch tut. Das gemessene Bild sieht dann aus, wie wenn Sie viele schmutzige Fußbälle durch einen einzigen Spalt schießen. Et voilà! Wir haben auch hier wieder das komplementäre Prinzip: Interferenz *oder* Ortsmessung. Beides gleichzeitig ist nicht zu realisieren. Mithin verhält sich das Doppelspalt-Experiment völlig analog zu unserem Mach-Zehnder-Interferometer und zeigt dasselbe ‚informationsbezogene' Verhalten."

„Die Quantenwelt scheint wirklich ziemlich verrückt zu sein! Teilchen, die zwar als Partikel gemessen werden, sich aber ansonsten wie Wellen verhalten, damit sie irgendwie gleichzeitig durch Spalte treten können? Das kann doch unmöglich seriöse Wissenschaft sein! Ist es nicht doch möglich, dass irgendein Wechselwirkungsprozess hinter der Sache steckt? Immerhin besteht sichtbares Licht aus Abertrillionen Photonen. Vielleicht behindern sie sich einfach nur gegenseitig oder prallen irgendwie voneinander ab? Dann könnte man auf den widersprüchlichen Welle-Teilchen-Aspekt doch einfach verzichten?"

„Natürlich könnte man das glauben. Aber sehen Sie, man kann den Doppelspalt-Versuch auch mit *einzelnen* Elektronen durchführen und es zeigen sich *exakt dieselben* Ergebnisse. Sie können also viele einzelne Elektronen hintereinander durch beide Spalte schießen und anschließend jeden einzelnen Auftreffpunkt registrieren. Sie werden verblüfft feststellen, dass wieder so ein wellenartiges Interferenzbild entsteht. Außerdem haben Sie doch gerade das Mach-Zehnder mit dem Einzelphoton-Laser gesehen. Da befindet sich ja ebenso immer nur ein einzelnes Photon im Interferometer und *trotzdem* kommt es zur Interferenz! Somit ist jede Art von versteckter Wechselwirkung automatisch ausgeschlossen. Mehr noch: das Ganze grenzt an Zauberei. Bedenken Sie, dass es ja von der Stellung der Polfilter zueinander abhängt, ob Interferenz entsteht oder nicht. Wie kann aber ein einzelnes Photon wissen, welche Einstellung die beiden Polfilter gerade haben? Wie kann es das wissen, wenn es quantenzufällig immer nur einen der beiden Teilstrahlen nehmen kann? Dazu müsste es – der menschlichen Anschauung nach – sich irgendwie am ersten Strahlteiler aufteilen, um dann in beiden Strahlgängen gleichzeitig zu sein. Aber das ist unmöglich, wie Sie wissen: Photonen sind unteilbar. Das können wir ganz leicht demonstrieren, indem wir einen Strahlteiler aus dem Mach-Zehnder herausnehmen und die Einzelphoton-Quelle auf den verbliebenen richten. Wenn wir jetzt daneben die Photonendetektoren an dessen Ausgängen platzieren, sehen wir, dass abwechselnd immer nur einer der beiden Detektoren „klickt“. Niemals jedoch beide gleichzeitig. Dass Photon teilt sich also nicht, sondern wird mit 50 % Wahrscheinlichkeit quantenzufällig entweder transmittiert oder reflektiert. Eben ein Quantenzufallsgenerator, wie er bei der QKD verwendet wird. Übrigens kann man auch den Quantenzufall nicht mehr weiter „teilen“. Er ist der elementarste Baustein eines

quantenmechanischen Ereignisses. Und deshalb sind auch die bei der QKD erzeugten Zufallszahlen die besten, die es überhaupt geben kann.

Sie sehen also, dass die Quantenphysik die menschliche Vorstellungskraft auf eine harte Probe stellt. Diese Eigenschaft von Quantenteilchen, nämlich dass sie ihre Umgebung gleichsam „ausschnüffeln", wie es Richard Feynman ausdrückte, wird gemeinhin als Nichtlokalität bezeichnet. Um so etwas zu beschreiben, braucht man eben die Wellenfunktion. Deren eigentliche Bedeutung wird bis heute in der Physik heiß diskutiert. Wir können aber auch einfach Bedeutung Bedeutung sein lassen und sie als abstrakte Hilfskonstruktion auffassen, die dem Menschen dazu verhilft, die Spielregeln der Quantenphysik zu begreifen. Außerdem sehen Sie übrigens noch, dass der Begriff Information bei der Sache eine ganz wichtige Rolle spielt: Je nachdem, wie der Versuch präpariert wird, liegt eine Ortsinformation vor oder nicht. Dies hängt eben davon ab, welche Stellung die Polfilter zueinander einnehmen (wie beim Mach-Zehnder) beziehungsweise ob beide Spalte offen sind oder aber einer geschlossen ist (wie beim Doppelspalt). Die Information hat also sozusagen einen direkten Einfluss auf das Verhalten der Teilchen. Wenn wir das, was in einem physikalischen Experiment passiert, als „Wirklichkeit" bezeichnen wollten, dann steht diese jedenfalls in direktem Zusammenhang mit dem Begriff Information. Nach Anton Zeilinger ist Information sogar der fundamentalste Baustein des Universums."

„*Sie sprachen vorhin davon, dass es dem statistischen Zufall unterliege, wo ein einzelnes Teilchen am Schirm auftrifft. Warum kann man das nicht genau vorhersagen?*"

„Tja, auch darüber streiten sich die Philosophen bis heute. Ich bin jetzt einmal sehr mutig, indem ich von sonst üblichen Erklärungen abweiche und liefere Ihnen folgende Begründung: Weil das Quantenteilchen aus irgendeinem Grund die volle Information dafür nicht enthält. Ausgedrückt wird das beispielsweise durch das heisenbergsche Unbestimmtheitsprinzip, welche die Komplementarität zwischen Ort und Impuls ausdrückt. Kommen Sie, ich zeige Ihnen, was das bedeutet!".

Professor Quant kramt einen kleinen Laserpointer hervor und leuchtet auf die Tafel. Wir sehen den typisch runden kleinen Lichtfleck. Daraufhin hält er ein kleines, dünnes Plättchen vor den Laser und fragt: „Was sehen Sie jetzt?" Wir sehen ein lang gezogenes Streifenmuster mit einer symmetrischen Hell-Dunkel-Abfolge. „Das ist", klärt uns der Professor auf, „natürlich wieder ein Interferenzbild. Das Interessante daran ist aber nicht die Interferenz selbst, sondern wie sie hier zustande kommt. Die unmittelbare Ursache dafür ist ein Phänomen, das man Beugung nennt. Vergleichbar ist das mit Wasserwellen, die seitlich auseinanderlaufen, wenn sie durch eine Verengung gehen oder auf Hindernisse treffen. So etwas gibt es auch bei Licht. Normalerweise wird die Beugung von Licht durch Entstehung neuer Wellen entlang einer Wellenfront erklärt. Das nennt man das Huygens-Fresnel -Prinzip. Passen Sie jetzt gut auf, wenn ich ihnen eine modernere, alternative Erklärung liefere: Die Beugung beim Licht lässt sich nämlich auch als Quanteneffekt deuten – vor allem dann, wenn es sich wieder um ein Experiment mit einzelnen Photonen handelt.

Das Plättchen enthält einen mikroskopisch kleinen Spalt, durch den das Licht hindurch muss. Dieser Spalt ist so klein, dass ein Lichtquant, anschaulich gesprochen, gerade noch durchpasst. Informationstheoretisch gesehen ist das eine Ortsmessung, denn wenn die Spaltgröße im

Bereich der Photonenabmessung liegt, weiß ich ja, wie groß das Photon ist. Nun haben wir schon in den vorigen Versuchen gesehen, dass bei einer Ortsmessung die dazu komplementäre Eigenschaft automatisch verschwindet. Bis dato war das immer die Interferenz. Hier jedoch verhält es sich genau umgekehrt. Das Interferenzbild entsteht – im Gegenteil – als Folge der Ortsmessung. Aus diesem Grund muss es sich bei diesem Quantensystem logischerweise um eine andere Komplementäreigenschaft handeln. Damit verbindet sich eine für uns neue Größe – der Impuls des Photons. Er ist grundsätzlich als das Produkt von Masse und Geschwindigkeit definiert, hängt aber andererseits mit dem Wirkungsquantum und mit der Wellenlänge der Licht- beziehungsweise Materiewellen zusammen (darauf komme ich gleich noch einmal zurück). Photonen besitzen zwar keine Ruhemasse, man kann ihnen aber ein Massenäquivalent zuordnen, zumal sie Energie transportieren und nach Einsteins weltberühmter Gleichung $E = mc^2$ Energie und Masse äquivalent sind.

Wie kommt nun Heisenbergs Unschärfebeziehung ins Spiel? Diese besagt sinngemäß, dass das Produkt aus Ortsunschärfe und Impulsunschärfe mindestens so groß ist wie eine sehr, sehr kleine Zahl, das plancksche Wirkungsquantum. Umgemünzt auf die Beugung heißt das nun, dass durch die Ortsmessung an dem Spalt die Ortsunschärfe reduziert wird und im Gegenzug die Impulsunschärfe zunehmen muss. Man kann es auch so sagen: je mehr Ortsinformation vorliegt, desto weniger Information hat man über den Impuls des Teilchens. Berücksichtigt man den vektoriellen Charakter des Impulses (also seinen Richtungssinn), äußert sich das in der Praxis dadurch, dass der Laserstrahl dann nicht gerade durch das Plättchen geht, sondern aufgeweitet wird – was eben der besagten Beugung entspricht. Die dabei auftretenden Beugungswinkel sind dann logischerweise umso größer, je kleiner

der Spalt und desto kleiner demnach die Ortsunschärfe ist. Das kann man auch mathematisch zeigen."

„Kurzer Einwand: Sie haben nun zwar die Beugung erklärt, nicht jedoch die Interferenz. Wie kommt diese zustande?"

„Aber das wissen Sie doch bereits! Diese kommt nach dem Wellenbild immer als Überlagerung diverser konstruktiver und destruktiver Anteile zustande. Das ist hier einfach eine Folge der Beugung – und der wellenartigen Eigenschaften von Quantenobjekten, von deren Notwendigkeit wir uns oben überzeugt haben. Aber gerade die Beugung ist so interessant, weil hier ein sehr wichtiges quantenphysikalisches Grundprinzip zum Tragen kommt: eben die heisenbergsche Unschärferelation, welche zeigt, dass in Quantensystemen offenbar eine limitierte Menge an Information steckt, die unterschiedlich verteilt sein kann. Entweder steckt sie in der Ortsinformation oder aber in der Impulsinformation eines Teilchens. Dazwischen sind auch unendlich viele Zwischenstufen möglich. Je mehr ich von der einen Größe weiß, desto weniger weiß ich von der anderen – und vice versa. Niemals ist es jedoch möglich, die volle Information über beide komplementäre Größen gleichzeitig zu erhalten. Daraus lässt sich eine ganz wesentliche Schlussfolgerung ziehen, die weitreichende Folgen hat: Einem Quantenteilchen kann niemals eine klar definierte Bahnkurve zugeordnet werden, bei der seine exakte Lage in Abhängigkeit der Zeit durch eine mathematische Funktion festgelegt ist."

„Das klingt alles sehr theoretisch. Abgesehen von Ihrem Beispiel, besitzt die heisenbergsche Unschärferelation auch sonst eine Bedeutung? Etwa auch für normale Menschen beziehungsweise Nicht-Physiker?"

„Hust! Prust!“, Professor Quant verschluckt sich fast. „Da habe ich mich wohl unklar ausgedrückt. Das Unschärfeprinzip besitzt allergrößte Auswirkung auf den Menschen. Mehr noch: es würde den Menschen ohne sie gar nicht geben. Sehen Sie, die Unschärferelation steckt ja nicht nur in unserem kleinen Versuch hier, sondern in jedem einzelnen Atom des gesamten Universums! Ich wollte ja gerade ausführen, dass ein Quantenteilchen von Natur aus keine definierte Bahnkurve besitzt. Was glauben Sie eigentlich, warum Sie im Chemieunterricht etwas von Orbitalen, Elektronenwolken oder delokalisierten Elektronen lernen? Das ist alles eine Konsequenz davon. Nur auf dieser Basis lässt sich wissenschaftlich das Zustandekommen von Atombindungen und somit auch der organischen Moleküle erklären, aus denen bekanntlich alles Leben aufgebaut ist. In der Tat hätte sich ohne das Unschärfeprinzip niemals eine menschliche DNA bilden können! Auch wenn sie sich bezüglich der Vererbung nach den Regeln der klassischen Physik verhält.

Abgesehen davon: Was wäre eine Welt ohne Smartphones? Für die allermeisten Menschen heute unvorstellbar! Wissen Sie eigentlich, dass Sie dieses Ding der Quantenphysik zu verdanken haben? Moderne Mikrochips basieren nämlich auf der Halbleitertechnik und diese wiederum auf der Festkörperphysik, welche die Gitterstruktur von Atomen und Molekülen untersucht – und da sind wir schon wieder bei Heisenberg. Übrigens geht die Entdeckung des Halbleitertransistors – der Grundbaustein aller Elektronenrechner – auf drei amerikanische Quantenphysiker zurück. Aber lassen wir das! Ich könnte Ihnen noch unzählige weitere Beispiele nennen, wo am Ende die Erkenntnis steht, dass das gesamte Universum in der uns bekannten Form ohne das Unschärfeprinzip gar nicht existieren würde.“

„Wenn unsere Welt so stark von der Quantenphysik geprägt ist, wieso merken wir dann im Alltag nichts von ihren merkwürdigen Gesetzmäßigkeiten?“

„Das liegt zunächst einmal daran, dass die Planck-Konstante, also das Wirkungsquantum, so außerordentlich klein ist. Diese hat mit etwa 6,5 Zehntausendstel Billionstel Trillionstel Joulesekunden einen so winzigen Wert, dass er viele Zehnerpotenzen unter jeglicher für makroskopische Systeme relevanten Messgenauigkeit liegt. Dies führt bei Objekten des Alltags zu so winzigen Abweichungen, dass sie völlig vernachlässigt werden können.“

„Wo ist dann eigentlich die genaue Grenze zu ziehen? Wo endet die Quantenphysik und wo beginnt die normal bekannte, klassische Physik?“

„Eine gute Frage. Ehrliche Antwort: Wir wissen es nicht. Wir wissen bloß, dass sich Quanteneffekte mit zunehmender Größe, sagen wir besser, mit zunehmender Masse des Objekts immer mehr „herauswaschen“. Der Quantenformalismus geht dann automatisch in den klassischen über. Trotzdem gibt es auch makroskopische Quanteneffekte, wie etwa Supraleiter, die man mit eigenen Augen sehen kann. Da können Sie zum Beispiel das Schweben eines keramischen Supraleiters über einem Dauermagneten eindrucksvoll beobachten. Aber wo genau eine Grenze zu ziehen wäre, wissen wir nicht. Hier muss das Experiment das letzte Wort haben – die Untersuchungen sind nach wie vor im Gange! Es entspricht deshalb der modernen Auffassung in der Wissenschaft, dass es eine wirkliche Grenze, einen sogenannten heisenbergschen Schnitt, gar nicht gibt. Der theoretische Formalismus belegt das eindeutig. Eine Grenze kann daher allenfalls nur auf der experimentellen Seite gegeben sein, das heißt

also, wie weit man imstande ist, Quanteneffekte eindeutig nachzuweisen."

„Sie haben viel über Interferenz gesprochen. Wo liegt denn sozusagen der momentane Weltrekord in Sachen experimentelle Quanteninterferenz?"

„Oh, … einer dieser Rekorde wurde 1999 von Professor Anton Zeilinger und seinen verdienten Assistenten und Doktoranden aufgestellt, mit deren Hilfe und frischer Brainpower komplizierte Experimentalphysik erst möglich wird. Denken Sie an die Elektronen im Doppelspalt-Experiment, die ich Ihnen gerade erklärt habe. Sie befinden sich ja in einer Quanteninterferenz, solange sie nicht beobachtet werden. Kaum dass dies geschieht, etwa indem einer der beiden Spalte geschlossen wird, liegt eine Ortsinformation vor und die Interferenz verschwindet automatisch. Die Zeilinger-Gruppe konnte so etwas Ähnliches mit den „kleinsten Fußbällen" der Welt zeigen, das heißt mit sogenannten Fulleren-Molekülen. Diese bestehen aus 60 oder 70 Kohlenstoff-Atomen in fünf- beziehungsweise sechseckiger Anordnung und sind etwa 720 atomare Masseneinheiten schwer. Zu ihrer Extrahierung wurde ein circa 600 °C heißer Ofen benutzt, aus dem diese Quantenfußbälle dann recht flott herausfliegen, ehe sie auf ein spezielles Beugungsgitter treffen, wo sie durch viele kleine Spalte hindurchmüssen. Danach wird ihre statistische Verteilung durch eine spezielle Messanordnung registriert. Und was glauben Sie, war das Ergebnis? Es zeigte sich wieder so ein wellenartiges Streifenbild, eben Quanteninterferenz. Allerdings war die Messung aufgrund der extrem kleinen Beugungswinkel enorm kompliziert – eine Doktorarbeit für sich."

„Da gratulieren wir herzlich im Nachhinein. Aber wie wurde nachgewiesen, dass diese Quantenfußbälle ein informationsbezogenes Verhalten zeigen, sozusagen auf Beobachtung reagieren?“

„Oh, das hätte ich fast vergessen! Natürlich wurde auch das indirekt überprüft. Allerdings wurden hierzu keine Spalte geschlossen, sondern man hat einfach den Ofen auf über 1000 °C erhitzt, also deutlich heißer als vorhin. Daraufhin war die Quanteninterferenz zwar nicht gänzlich verschwunden, jedoch deutlich schwächer ausgeprägt. Einer der Gründe: Durch die höhere Temperatur entsteht mehr Wärmestrahlung, das heißt mehr Photonenaustausch zwischen den Fullerenen und ihrer Umgebung. Auf diese Weise geben die Moleküle sozusagen mehr Wissen über sich preis, ein Beobachter erhält dadurch ein Mehr an Information. Dies verhält sich wie bei Hänsel und Gretel, wo die Kinder Steine legen und dadurch verraten, wo sie gegangen sind. Hier ist das aber kein Märchen, sondern Wissenschaft, die etwas überaus Interessantes zeigt: Der Quantenzustand des Systems hängt offenbar vom Informationsaustausch mit seiner Umgebung ab. Dabei spielen sogar die gegenseitigen Wechselwirkungen (‚Beobachtungen‘) der Atome im Molekül selbst eine ganz wesentliche Rolle. Je intensiver dieser Infoaustausch ausgeprägt ist, umso schwächer wird der Quantencharakter. Wir sagen im Fachjargon: Das System wird zunehmend dekohärent. Sie können den Effekt aber genauso gut auch als Manifestation der Unschärferelation sehen: Durch die höhere Temperatur haben die Fullerene im Mittel eine höhere Geschwindigkeit als vorhin. Dadurch sinkt die De-Broglie-Wellenlänge, die man den Molekülen zuordnen kann, und damit steigt die Ortsunschärfe, wodurch also die Unschärfe in der Geschwindigkeit

abnehmen muss. Daraus resultieren kleinere Beugungswinkel, wodurch die Interferenz schwächer ausfällt."

„Was ist die De-Broglie-Wellenlänge?"

„Nun, dieser Begriff geht auf einen französischen Prinzen zurück, der das Konzept der Materiewelle einführte. Dazu fällt mir eine Geschichte ein: Sie wissen ja bereits, wofür Albert Einstein seinen – leider – einzigen Nobelpreis bekam. Für die Entdeckung der Photonen. Das war zu damaliger Zeit deshalb eine Revolution, weil man dachte, Licht sei ausschließlich eine elektromagnetische Welle.

Einstein zeigte jedoch, dass ein Effekt, den Sie heute quasi in jeder Solaranlage und in jedem Belichtungsmesser einer Digicam haben, nur auf Basis einer quantisierten Teilchenvorstellung des Lichts erklärbar ist. Einstein hatte damit das physikalische Weltbild aus den Angeln gehoben. Einige Jahre später drehte Prinz Victor Louis de Broglie den Spieß in gewisser Weise um, indem er den Elektronen im Atom, die damals ausschließlich punktförmig betrachtet wurden, auch einen Wellenaspekt zuordnete, eben die Materiewellen. Dazu leitete er eine Formel ab, die sinngemäß besagt, dass materielle Quantensysteme wie das Elektron mit zunehmender Masse immer kleinere Wellenlänge haben und daher immer dekohärenter werden. Tatsächlich wurde diese Annahme, die zunächst reine Hypothese war, Einstein zur Begutachtung vorgelegt. Dieser äußerte: „Er hat einen Zipfel vom großen Schleier gelüftet". Einstein sprach deshalb von einem Schleier, weil die Quantentheorie damals, selbst für Physiker, noch weitgehend undurchschaubar war. Was beide zunächst nicht wussten: Der experimentelle Nachweis der Materiewellen war schon kurz vorher von zwei Amerikanern durch die Elektronenbeugung erbracht worden. Diese hatten jedoch keinen blassen Schimmer von dem, was sie da entdeckt hatten.

De Broglies Geniestreich war jedenfalls ein sehr wichtiger Schritt in der Entwicklung der Quantenmechanik und wurde später von dem österreichischen Nobelpreisträger Erwin Schrödinger im Konzept der Wellenmechanik aufgegriffen."

„Der Mensch besteht ja auch aus Materie, aus Atomen und Molekülen. Kann man das Konzept der Materiewelle dann nicht auch auf den Menschen übertragen? Anders gefragt: Lässt sich auch dem Menschen eine De Broglie-Wellenlänge zuordnen?"

„Ja, das ist im Prinzip möglich. Allerdings ist das Ergebnis eine so winzige Zahl, dass sie viele Zehnerpotenzen unterhalb der kleinsten Objekte liegt, welche die Physik kennt – den Quarks, welche zusammen mit Leptonen und Eichbosonen die fundamentalen Bausteine der Welt bilden. Gott sei Dank ist das so, denn sonst könnten auch beim Menschen Quanteninterferenzen auftreten. Das wäre ja schrecklich! Sehen Sie, die De-Broglie-Wellenlänge wird umso kleiner, je größer die Masse der Objekte ist. Gegenüber einem winzigen Elektron besitzt der Mensch quasi eine unendlich viel größere Masse, daher ist seine Wellenlänge auch unendlich viel kleiner – mithin sind Beugung und Interferenz so verschwindend gering ausgeprägt, dass sie messtechnisch unmöglich erfasst werden könnten.

Damit kommt eine wichtige Eigenschaft zum Ausdruck, die wir bereits mehrfach angesprochen haben: Die Dekohärenz. Es gibt mittlerweile zahllose wissenschaftliche Hinweise dafür, dass die eigentliche Ursache der Dekohärenz im Informationsaustausch mit der Umgebung liegt. Denken Sie an die Fullerene und die ausgelegten Steine bei Hänsel und Gretel. So etwas tritt erst recht beim Menschen auf, denn er befindet sich ständig in

Wechselwirkung mit seiner Umgebung, etwa durch optische Wahrnehmung, Temperaturaustausch oder Gravitation. Vor allem aber stehen die Myriaden von Atomen, aus denen der Mensch besteht, auch in ständigem Kontakt untereinander. Gewissermaßen entspricht auch dies einer Art gegenseitiger ‚Beobachtung'. Dies alles führt dazu, dass der Mensch im Vergleich zu einem Quantenteilchen völlig dekohärent erscheint und dankenswerterweise keine Quanteninterferenzen zeigt."

„Da sind wir aber sehr beruhigt! Vielen Dank für die Ausführungen! Können Sie uns noch etwas mitgeben?"

„Ja, in diesen Grundaspekten, die hier umrissen wurden, steckt ein unerhört großes technologisches Potenzial. Beispielsweise kann man auf dieser Basis Qubits für die abhörsichere Quantenkommunikation erzeugen. Mit Interferometern lassen sich Systeme entwickeln, welche Qubits inhärent sicher von Alice zu Bob transportieren, wobei dieser Sicherheitsaspekt primär auf die Quanteneigenschaften des Systems zurückzuführen sind, die wiederum in einem tieferen Sinn mit dem Begriff Information in Zusammenhang stehen.. Im Übrigen haben Sie gesehen, dass dieses Verhalten eine universelle Eigenschaft ist, die nicht nur auf Licht allein, sondern alle Quantenteilchen, also auch materielle, betrifft. Deshalb können Qubits auch in den Eigenschaften materieller Teilchen implementiert werden, wie etwa im Elektronen- oder Kernspin. Schließlich sehen Sie durch das Phänomen der Dekohärenz auch, wo vor allem die technische Herausforderung bei Quantencomputern und deren Vernetzung durch ein Quanteninternet liegt: Will man keinen technischen Super-GAU riskieren, gilt es, die Dekohärenz tunlichst zu vermeiden – jedenfalls zumindest so weit, dass eine sichere Berechnung beziehungsweise Übertragung gewährleistet ist."

3.2 Phasenkryptografie

Wie in Abschn. 2.6.2 angesprochen, gibt es diverse Protokolle für den Quantenschlüsselaustausch (QKD). Mit dem dort vorgestellten Ekert-Protokoll auf Basis von verschränkten Qubits lässt sich eine zukunftsträchtige Art der Q-Kryptografie durchführen, vor allem auch über größere Distanzen via Quantensatelliten. Die meisten aktuellen Verfahren sowie viele kommerziell erhältlichen Systeme beruhen allerdings auf einer Verbindung über Glasfaserkabel ohne Verschränkung. Zumeist basieren sie auf dem einfacheren BB84-Protokoll. Werden die Qubits in der Polarisation codiert, so entsteht gerade in fiberoptischen Leitungen das Problem, dass die Polarisationsrichtung durch die Fasern sukzessive verdreht wird. Eine Alternative bietet deshalb die Phasencodierung, bei der dieser Effekt keine Rolle spielt und für den Einsatz in Standard-Glasfaserkabeln geeignet ist – wenngleich auch um den Preis einer viel höheren interferometrischen Präzision. Vergleichbare Systeme werden überwiegend auch in aktuellen metropolischen QKD-Netzwerken verwendet.

Was ist die Phase einer Welle?
In der klassischen Physik wird das Licht als elektromagnetische Welle beschrieben. Trennt man die magnetische Schwingung von der elektrischen (die im rechten Winkel zueinander orientiert sind), verbleibt nur noch ein einfacher Wellenzug. Man kann sich solch einen Wellenzug auch folgendermaßen konstruieren: Wir stellen uns einen Pfeil vor, dessen Spitze um einen fixen Mittelpunkt rotiert und dadurch fortwährend einen Kreis beschreibt. Projiziert man gedanklich jeden Punkt des Kreises auf eine gedachte Zeitachse, so ist in Abb. 3.2 zu erkennen, dass sich die Modellbeschreibung einer Welle ergibt Nun

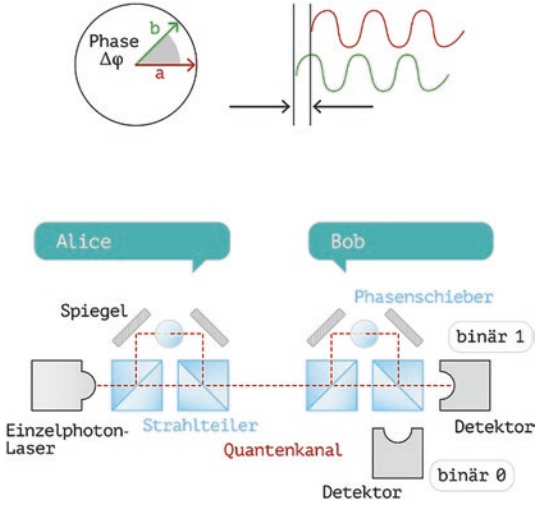

Abb. 3.2 Großes Mach-Zehnder-Interferometer (bestehend aus zwei AMZI) zur Phasenkryptografie, Zeigerdiagramm zur Darstellung der Phasenbeziehung

können wir einen zweiten Pfeil in dieses Modell setzen und erhalten das Bild von zwei einander überlagernden Wellenzügen. Dabei schließen die beiden Pfeile einen bestimmten Relativwinkel $\Delta\varphi$ (sprich: „Delta phi“) miteinander ein, den man Phasenwinkel oder einfach nur die Phase einer Welle nennt. Bei der Überlagerung zweier Wellen gibt es zwei Spezialfälle, die von besonderem Interesse sind: ist $\Delta\varphi = 0$, so sind die Wellen „in Phase“, Berg trifft auf Berg und Tal auf Tal. Summiert man dann die jeweiligen Auslenkungen, so addieren sich ihre Beträge jeweils zum doppelten Wert; man spricht in diesem Fall von einer konstruktiven Interferenz. Beträgt hingegen $\Delta\varphi = 180°$, so erkennt man, dass sich beide Wellenzüge gegenseitig auslöschen, und es liegt eine sogenannte destruktive Interferenz vor.

Das asymmetrische Mach-Zehnder-Interferometer

Als erfolgreiche Absolventen von Professor Quants Quantenoptik-Workshop können wir nun ganz leicht das Funktionsprinzip eines asymmetrischen Mach-Zehnder-Interferometers (AMZI) nachvollziehen (Abb. 3.2). Die Bezeichnung „asymmetrisch" sei durch die unterschiedlich langen u-förmigen Teilstrahlen gerechtfertigt. Dazu nehmen wir idealisierend wiederum ein wohljustiertes AMZI an. Angenommen, das eingestrahlte Licht erfahre bei jeder Reflexion an den Strahlteilern und Spiegeln jeweils einen 90°-Phasensprung, das heißt, die Relativlage einzelner Wellenzüge verändere sich um jeweils $\Delta\varphi = 90°$. Es ist dann leicht zu überlegen, dass in diesem Fall nur der Photonendetektor „binär 1" klicken kann, der Detektor „binär 0" jedoch niemals, da dort kein Photon austreten kann – dies deshalb, weil der Phasenunterschied zwischen dem oberen „u-förmigen" Teilstrahl und dem gerade verlaufenden unteren Strahl 360° und damit sozusagen 0 beträgt. Somit ergibt sich eine konstruktive Interferenz, da weiterhin Wellenberg auf Wellenberg und Wellental auf Wellental trifft. Ganz anders dagegen Wellenzüge, die bei Detektor „binär 0" austreten sollten: hier beträgt die Phasendifferenz von 270°–90° = 180°, was einer Auslöschung entspricht. Das ist unmittelbar einleuchtend, weil ohnehin schon die gesamte Lichtintensität an den Detektor „1" vergeben wurde.

Die Quantenschlüsselerzeugung

Das beschriebene AMZI lässt sich nun gut zur QKD verwenden. Alice und Bob seien wiederum zwei Personen/Parteien/Computer, die einander völlig abhörsichere digitale Botschaften übersenden wollen. Dazu verwenden sie ein QKD-System, das aus je einem AMZI als Sende- und Empfangseinheit besteht, die zum Beispiel über eine Fiberglasleitung miteinander verbunden sind. Die gesamte

Anordnung (bestehend aus zwei AMZI) wird auch als „großes“ MZI bezeichnet. Als Photonenspender verwenden sie einen speziellen Einzelphoton-Laser sowie jeweils einen quantenzufällig angesteuerten Phasenschieber, welcher die Phase der Wellen entsprechend seiner Einstellung verändern kann. Eine Messanordnung für Alice ist nicht eingezeichnet, da sie ihre Werte dem Quantenzufallsgenerator entnehmen kann. Für maximale Sicherheit muss die erzeugte Quantenzufallsfolge allerdings direkt (ohne Zwischenspeichern) auf den automatischen Phasenschieber übertragen werden.

Die Quantenkryptografie erfolge nun nach dem BB84-Protokoll, das in seinem Ablauf dem Ekert-Protokoll nicht unähnlich ist. Die Schritte 1, 3, 5 und 6 können grundsätzlich beibehalten werden, ein prinzipieller Unterschied ergibt sich für die Schritte 2 und 4 (siehe hierzu Abschn. 2.6.2):

- SCHRITT 2: *Erzeugung des Quantenschlüssels:* Alice und Bob variieren mittels Phasenschieber (PhS) quantenzufällig die Phase. Immer dann, wenn die Phasendifferenz von PhS $\Delta\varphi = 0$ ist, muss zwangsläufig Detektor „binär 1“ klicken, bei $\Delta\varphi = 180°$ klickt notwendigerweise Detektor „binär 0“. Wenn nun einzelne Photonen aus der Quelle bei Alice emittiert werden, entsteht eine quantenzufällige Abfolge von Binärzahlen, aus der eine Teilmenge als Schlüssel für das anschließende OPT (siehe hierzu Abschn. 2.6.1) entnommen wird. Allgemein kann man sagen, dass Alice und Bob quantenzufällig Messbasen erzeugen, die daraufhin öffentlich kommuniziert werden, um Messwerte mit unterschiedlicher Basis zu löschen. In den Fällen gleicher Basis spricht man von den relevanten Bits, im Unterschied zu den irrelevanten Bits, bei denen die obigen Phasenbeziehungen nicht bestehen. In den

letztgenannten Fällen kann man nicht mit Sicherheit vorhersagen, welcher Detektor ansprechen wird, da die Emission aus dem Strahlteiler quantenzufällig erfolgt. Um diese Unterscheidung vorzunehmen, benutzen Alice und Bob einen klassischen Kanal, über den sie ausschließlich die Nummer des jeweiligen Photons sowie die zugehörigen Basen kommunizieren (niemals die relevanten Bits)

- SCHRITT 4: *Spionagetest:* Das Aufdecken einer Abhörattacke erfolgt durch statistisches Auswerten der erzeugten Liste, welche von der jeweiligen Art der Implementierung abhängt.
  Dazu entnehmen Alice und Bob eine ausreichende Zahl von Testbits und prüfen diese auf Übereinstimmung. Sie werden danach aus dem eigentlichen Schlüssel selbstverständlich gelöscht.. Zu beachten ist dabei noch einmal der Sinn der QKD: Ziel ist es nicht, mit den Single-Qubits direkt Information zu übertragen (was physikalisch gar nicht möglich wäre), sondern nur die Erzeugung und Zuteilung eines originalen, absolut zufälligen Quantenschlüssels von Alice zu Bob, der zur anschließenden Datenübertragung per OPT über das normale Internet gedacht ist. Die inhärente Sicherheit ist dadurch gewährleistet, dass ein Hackerangriff von Eve bei der Schlüsselübertragung automatisch detektiert werden kann. Falls dies passiert, können Alice und Bob den Schlüssel verwerfen, bevor noch irgendwelche Daten übertragen worden sind. In QKD-Netzwerken würde die Key-Management-Ebene automatisch Alarm schlagen und eine neue Route anbieten beziehungsweise schon erzeugte sichere Quantenschlüssel kurzfristig bereitstellen.

Erkennen eines Lauschangriffs

Die inhärente Sicherheit beruht auf der Gültigkeit des No-Cloning-Theorems. Wenn ein Spion (Eve) die Kenntnis

des Quantenschlüssels erlangen möchte, müsste der gesamte Quantenzustand unabhängig von Alice auch bei Eve koexistieren. Dies ist dem No-Cloning-Theorem zufolge jedoch unmöglich, weil der Quantenzustand nicht perfekt kopiert werden kann. In der Praxis führt das dazu, dass jede versuchte Messung von Eve den gesamten Quantenzustand so beeinflusst, dass dies durch Auswerten der Messstatistik auffällt. Ein Beispiel: Alice und Bob variieren ihre Phasenschieber auf zwei unterschiedlichen Messbasen. Eine Basis sei die Achse „0–180°“ im Zeigerdiagramm, eine zweite Basis bilde die Achse „90–270°“. Bei völlig zufälliger Drehung der Phasenschieber würde Bob im Schnitt zu 50 % in der richtigen Basis messen (relevante Bits), zu 50 % jedoch in der falschen Basis (irrelevante Bits), denn hier wäre $\Delta\varphi$ ja ungleich 0 beziehungsweise 180°. Angenommen, Eve geht dazwischen und möchte die Übertragung unbemerkt abhören. Ferner sei Eve mit Insiderwissen ausgestattet und kenne sogar beide Basen. Weiters benütze sie auch noch dasselbe AMZI zur Messung der Phase und sie soll auch die erhaltenen Bits extrem schnell an Bob weiterleiten können. Auch dann hätte Eve keine Chance: aufgrund der quantenzufälligen Modulation, die niemand im Voraus wissen kann, würde Eve in 50 % aller Fälle in der richtigen, in 50 % der Fälle jedoch in der falschen Basis messen. Letzteres hätte unweigerlich Einfluss auf die Messung von Bob. Dieser würde dann nur noch 50 % der von Eve gesendeten Bits als mit Alice übereinstimmend messen, sodass die Fehlerrate insgesamt bei 25 % liegt. Beim Abgleich ihrer Werte würde ein so hoher Fehler bei Alice und Bob also sofort auffallen. Theoretisch gesehen könnte Eve auch nur jedes 2., 3. usw. Photon abhören, dann verringerte sich die Fehlerrate auf 12,5 %, 6,25 % usw. Irgendwann bliebe der Fehler unentdeckt. Aber auch das nützt Eve nichts, denn sie verliert ja im selben Maße auch sukzessive an Information über den Schlüssel.

Decoy-State-QKD

Im Unterschied zur obigen Prinzipdarstellung gibt es in der Realität keine perfekte Einzelphoton-Quelle. In der Praxis werden daher sehr intensitätsschwache oder sehr schwach kohärente Laser verwendet. Dabei treten jedoch auch Multi-Photonen-Zustände auf, welche die sichere Transmissionsrate signifikant beschränken. So könnte etwa ein Spion mithilfe eines Strahlteilers einzelne Photonen bei der Erzeugung unbemerkt messen. Damit die Übertragungsrate nicht zur lahmen Krücke verkommt und die Sicherheit gewährleistet bleibt, wird das Problem oft über Decoy States gelöst. Dabei verwendet Alice anstelle eines kohärenten Laserstrahls Laserpulse mit verschiedenen Intensitäten (ein Signalzustand und mehrere Decoy-Zustände), resultierend in einer variierenden Photonenzahlstatistik durch den Kanal. Alice meldet Bob öffentlich das Intensitätslevel, das bei jedem Qubit verwendet wurde. Indem die Fehlerrate (QBER) von jedem Level gemessen wird, können Lauschangriffe effizient detektiert werden. Derartige Systeme werden vorwiegend in aktuellen Test-QKD-Netzwerken verwendet. Der Sicherheitszugewinn aufgrund der Decoy-State-Methode gilt als wissenschaftlich bewiesen.

3.3 Schrödingers Katze

Mit Katzen ist das so eine Sache. Einerseits schmiegen sie sich zärtlich schmusend, wohlig schnurrend an uns. Andererseits können sie wild fauchen und schmerzhafte Kratz- und Bisswunden verursachen, kurz zu kleinen pelzigen Teufelchen mutieren. In Katzen scheinen also zwei gegensätzliche Prinzipien zu wohnen, wie zwei konträre Quantenzustände. Vielleicht musste deshalb eine Katze herhalten für eine der berühmtesten Wissenschafts-Analogien der Welt.

Als es die Währung Euro noch nicht gab und in Österreich mit Schillingen bezahlt wurde, war auf der Tausend-Schilling-Banknote der letzten Ära das bläulich gestochene Bild eines Mannes mit hoher Denkerstirn aufgeprägt: Der Quantenphysiker und Wissenschaftstheoretiker Erwin Schrödinger. Um es dorthin zu schaffen, muss man naturgemäß eine sehr verdiente Persönlichkeit gewesen sein, wenn ein Land auf diese Weise seinen Stolz auf einen zum Ausdruck bringt. In der Tat lieferte Erwin Schrödinger als Vater der Wellenfunktion und Schöpfer der Wellenmechanik einen sehr wichtigen Beitrag zur Quantenphysik. Erinnern wir uns an Newtons Aktionsprinzip zurück. Aus der daraus abgeleiteten Bewegungsgleichung lassen sich ja alle erdenklichen Bahnkurven klassischer Objekte berechnen. Allerdings versagt diese Formel völlig, wenn es um nichtklassische Fragen geht, welche beispielsweise Atome betreffen, etwa die „Bahnkurve" eines Elektrons um den Atomkern herum. Dies liegt zum einen daran, dass es wegen der Unschärferelation gar keine definierte Bahnkurve gibt und diese Vorstellung demnach weitgehend sinnlos ist, zum anderen aber auch an der klassischen Elektrodynamik: Eine rotierende und somit beschleunigte Ladung wie das Elektron erzeugt eine elektromagnetische Welle, die zu ihrer Existenz permanent Energie beziehen muss. Dieser Umstand würde dazu führen, dass das Elektron spiralförmig in den Atomkern stürzt und somit die Stabilität von Atomen völlig unerklärlich bliebe. Zur damaligen Zeit war dies nur eines von zahlreichen Problemen, welche die theoretischen Physiker beschäftigten. Schrödinger jedenfalls führte die Atomproblematik einer überraschenden Lösung zu, indem er zwei geniale Einfälle hatte: Einerseits führte er das abstrakte Konzept der Wellenfunktion ein, andererseits zwängte er diese ψ-Funktion in die Struktur einer sogenannten Eigenwertgleichung. Das Ergebnis war die weltberühmte Schrödinger-Gleichung,

die heute zu den meistzitierten Formeln der Physik zählt. Um sie rudimentär begreiflich zu machen denken wir an die Qubits beim Quantencomputer. Dort hatten wir das Quantenbit als eine Linearkombination von Basiszuständen dargestellt, welche bei ihrer Messung stets in die Eigenwerte 0 oder 1 zerfallen. Derartige mathematische Strukturen, die originär aus der linearen Algebra stammen, wurden von Schrödinger aufgegriffen und mithilfe der Funktionalanalysis erfolgreich auf das Atom angewendet. Ähnlich dem Qubit lassen sich auch bei Atomen und Molekülen Eigenzustände und Eigenwerte berechnen, allerdings in wesentlich komplexerer Form. Die Eigenzustände (Eigenfunktionen), deren Amplitudenquadrate von Max Born als Wahrscheinlichkeiten physikalischer Messwerte interpretiert wurden, bilden heute die Grundlage der modernen Chemie und sind gemeinhin als Orbitale bekannt. Die zugehörigen Eigenwerte entsprechen beispielsweise den gequantelten Energiestufen in Atomen. Ganz allgemein werden in der Quantenmechanik beobachtbaren Messgrößen (Observablen) hermitesche Operatoren zugeordnet, wobei die Eigenwerte der zugehörigen Eigenfunktionen reellen Messwerten entsprechen. Wohlgemerkt, die Wellenmechanik war nicht die erste mathematische Formulierung der Quantenmechanik, die gleichwertige heisenbergsche Matrizenmechanik wurde etwas früher entwickelt. Die Schrödinger-Gleichung gilt aber gemeinhin als weniger umständlich, da sie Operatoren und Wellenfunktionen in einer einzigen Bewegungsgleichung für die Zustände betrachtet, wohingegen in der Matrizenmechanik Bewegungsgleichungen für die Operatoren selbst stehen. Später wurde die Schrödinger-Gleichung modifiziert und weiterentwickelt. So kombinierte sie der englische Theoretiker Paul Dirac mit der Speziellen Relativitätstheorie, was zu einer sensationellen Entdeckung führte: Es existieren Antiteilchen, wie etwa das positiv geladene Elektron

(Positron). Damit wurde eine Entwicklung eingeläutet, die später als „Teilchenzoo" verunglimpft wurde, heute jedoch die Grundlage der gesamten modernen Physik bildet. 1933 erhielten Schrödinger und Dirac zusammen den Physik-Nobelpreis.

Das Katzenparadoxon

In der Öffentlichkeit ist Erwin Schrödinger allerdings eher für seine weltberühmte Metapher bekannt – Schrödingers Katze kennt sozusagen jedes Kind. Aber was hat es damit eigentlich auf sich? Mit dem Begriff Wellenfunktion hat uns Professor Quant ja schon eingehend bekannt gemacht. Was sagt die Wellenfunktion zu Überlagerungszuständen, also zum Phänomen der Superposition? Wie dargelegt, beschreibt sie in der Quantenphysik die verschiedensten Zustände: den Quantenparallelismus in Quantencomputern, Überlagerungen in Interferometern, Interferenzen bei Atomen und Fullerenen und so weiter und so fort. Existiert diese Funktion überall, auch in größeren, sogenannten makroskopischen Systemen? Etwa auch beim Menschen? Zu dieser Frage hat uns Professor Quant ebenso bereits einen Standpunkt der Physik dargelegt. Tatsächlich ist die Frage bereits viele Jahrzehnte früher von Erwin Schrödinger in einem 1935 erschienenen Zeitschriftenartikel aufgeworfen worden. Wohl aus Taktgründen benutzte Schrödinger in seinem Essay kein Exemplar der Spezies Mensch, sondern setzte stattdessen eine Katze in Szene. Ohnehin nahm der lebende Organismus an sich eine wichtige Rolle im Interessengebiet dieses Ausnahmephysikers ein. So schrieb er unter anderem ein viel beachtetes Buch, das sich mit Fragen zur Entstehung des Lebens befasst. Darin wurde die menschliche DNA antizipiert, ehe sie kurz darauf von Watson und Crick tatsächlich entdeckt wurde. Da sich mit dem Namen Erwin Schrödinger auch ein stilistisch herausragender

Schriftteller verbindet, sei der besagte „Katzen-Artikel“ auszugsweise im Originaltext wiedergegeben:

> „(…) Man kann auch ganz burleske Fälle konstruieren. Eine Katze wird in eine Stahlkammer gesperrt, zusammen mit folgender Höllenmaschine (die man gegen den direkten Zugriff der Katze sichern muss). In einem Geigerschen Zählrohr befindet sich eine winzige Menge radioaktiver Substanz, so wenig, dass im Laufe einer Stunde vielleicht eines von den Atomen zerfällt, ebenso wahrscheinlich aber auch keines. Geschieht es, so spricht das Zählrohr an und betätigt über ein Relais ein Hämmerchen, das ein Kölbchen mit Blausäure zertrümmert. Hat man dieses ganze System eine Stunde lang sich selbst überlassen, so wird man sich sagen, dass die Katze noch lebt, wenn inzwischen noch kein Atom zerfallen ist. Der erste Atomzerfall würde sie vergiftet haben. Die Psi-Funktion des ganzen Systems würde das so zum Ausdruck bringen, dass in ihr die lebende und die tote Katze (sit venia verbo) zu gleichen Teilen gemischt oder verschmiert sind. Das Typische an solchen Fällen ist, dass eine ursprünglich auf den Atombereich beschränkte Unbestimmtheit sich in grobsinnliche Unbestimmtheit umsetzt, die sich dann durch direkte Beobachtung entscheiden lässt. Das hindert uns, in so naiver Weise ein ‚verwaschenes Modell‘ als Abbild der Wirklichkeit gelten zu lassen (…)“.

Erinnern wir uns an Professor Quants Mach-Zehnder-Versuch zurück (Abb. 3.1) und übertragen wir die Situation auf das Katzenparadoxon: Ein Photon, das aus der Quelle tritt, hat am ersten Strahlteiler quantenzufällig eine 50-%-Wahrscheinlichkeit, transmittiert oder reflektiert zu werden. Analoge Verhältnisse bestehen nun im Katzenparadoxon, denn auch hier besteht eine 50-%-Chance, dass die Katze tot oder lebendig ist. Dies hängt davon ab, ob das Atom zerfällt oder nicht, was statistisch zufällig

mit je 50 % Wahrscheinlichkeit eintritt. Im Mach-Zehnder-Interferometer liegt eine Superposition aus beiden Möglichkeiten vor, welche am Auftreten des Interferenzbilds zu erkennen ist. Die Wellenfunktion würde das zum Beispiel folgenderweise ausdrücken:

$$\psi = \psi_{\text{transmittiert}} + \psi_{\text{reflektiert}}.$$

In Analogie zu oben stellt Schrödinger nun ernsthaft die Frage, ob nicht auch der Zustand der Katze in der Stahlkammer durch einen Superpositionszustand bestimmt sein müsste, also

$$\psi = \psi_{\text{tote Katze}} + \psi_{\text{lebende Katze}}.$$

Dabei tut er dies humorvoll, was ein wenig an Einsteins „Spuk" erinnert, und genau wie Einstein will er zeigen, dass die ganze Situation der Alltagserfahrung widerspricht beziehungsweise paradox ist. Noch niemals hat jemand das Interferenzbild einer Katze gesehen, erst recht nicht von einem Menschen. Weil der Quantenformalismus diese Groteske aber theoretisch zulässt, wirft Schrödinger in seinem Essay indirekt auch eine Reihe weiterer Fragen auf:

1. Ist der Formalismus der Quantenmechanik auch für makroskopische Objekte gültig?
2. Gibt es eine definierte Grenze, ab der dieser nicht mehr gültig wäre?
3. Welche Rolle spielt der Messprozess in der Kopenhagener Interpretation der Quantenmechanik?

Die Erklärung nach Ansicht der meisten Physiker

Tatsächlich ist Schrödingers Katze bis heute nicht eindeutig wissenschaftlich entscheidbar. Damit bietet das Gedankenexperiment Spielraum für zahlreiche Interpretationen, teilweise recht bizarrer Art, aber auch für konkrete Experimente, welche die Situation in

abgewandelter Form nachstellen. Es gibt jedoch eine plausible und elegante Erklärung, die von weitaus den meisten Physikern vertreten wird: Die Superposition von toter und lebendiger Katze kann nur dann gegeben sein, wenn sowohl Katze als auch Höllenmaschine und dergleichen Quantenobjekte sind. Dies kann jedoch ausgeschlossen werden, da es zu einem „inneren" Messprozess kommt, wodurch diese gleich zu Beginn des Experiments völlig dekohärent werden. Damit werden sie zu klassischen Objekten und unterliegen automatisch nicht mehr der Quantentheorie. Diesen inneren Messprozess kann man als Informationsaustausch mit der Umgebung interpretieren, wozu insbesondere auch die Myriaden von Atomen und Molekülen beitragen, aus denen die Katze, das sonstige Gerät und die Luft in der Kiste bestehen. Andererseits nimmt die Kopenhagener Interpretation der Quantenmechanik als wesentliche Forderung an, dass die Realität vor der Messung nicht existiert und diese sich erst durch die Art des Messprozesses determiniert. Wären Atomzerfall und Katze wirklich miteinander verschränkte Quantenobjekte, dann wären Leben und Tod demnach tatsächlich unbestimmt und erst durch das Öffnen der Kammer (was dem Messprozess entspricht) würde einer der beiden Zustände eintreten. Infolge der Dekohärenz reduziert sich der Messprozess jedoch lediglich auf den Atomzerfall, welcher dann also von der Katze völlig zu trennen ist. Dabei wird der Messprozess selbst allerdings willkürlich als klassischer Mechanismus angenommen.

Warum erscheint uns die Welt klassisch?

Das Paradoxe an Schrödingers Katze ist also, dass der Quantenformalismus überall Superposition und Verschränkung zulässt, in unserer alltäglichen Welt davon allerdings nichts zu bemerken ist. Da sind eben keine

Katzen oder andere Objekte, die in seltsamen Überlagerungszuständen existieren und sich verschwommen an mehreren Orten zugleich aufhalten. Im Gegenteil: alles hat seinen festen Ort, klare Konturen, fix definierte Geschwindigkeiten und Bewegungsrichtungen. Diese klassische Wahrnehmung scheint zunächst nichts mit der so bizarren Quantenwelt zu tun zu haben. Nun wäre man geneigt zu sagen, dass die Quanten eben ein Sonderfall der klassischen Physik seien, der nur im Allerkleinsten auftritt. Doch verhält es sich in Wahrheit genau umgekehrt: die alltägliche Welt erweist sich als Spezialfall der Quantenphysik. Dieser tritt immer dann auf, wenn Dekohärenzeffekte eine tragende Rolle spielen. Wie effizient die Dekohärenz ist, wird allein schon daran ersichtlich, dass bereits jedes Bakterium ein klassisches Objekt ist, obwohl auch dies so klein ist, dass wir es mit unseren Augen gar nicht sehen können. Wie entsteht nun die Dekohärenz genau? Tatsächlich macht der Formalismus die Vorhersage, dass aus mikroskopischen Überlagerungen auch makroskopische Superpositionen entstehen sollten. Dabei tritt allerdings eine Verschränkung des Systemzustands mit dem Umgebungszustand auf, wodurch ein nichtlokaler Quantenzustand entsteht, der durch Informationsaustausch mit den Freiheitsgraden der Umgebung die makroskopische Überlagerung delokalisiert. Dieser Vorgang kann mathematisch durch einen vieldimensionalen Konfigurationsraum beschrieben werden, während aus unserem niedrigdimensionalen Blickwinkel heraus gesehen die Welt lokalisiert, isoliert und somit klassisch erscheint. Wesentlich ist dabei festzuhalten, dass hiermit die Quanteninterferenzen zwar lokal verschwinden, nicht jedoch im Ganzen gesehen. Unsere Welt erscheint also nur aus dem Blickwinkel eines lokalen Beobachters heraus betrachtet klassisch. Wie man ebenfalls mathematisch zeigen kann, setzt der Dekohärenzprozess bereits bei

jeder geringsten Wechselwirkung ein (zum Beispiel mit Licht, der Streuung an Luftmolekülen usw.). Die Folge ist, dass uns die wahrgenommene Welt zwangsläufig klassisch erscheinen muss. Der Umstand, dass sie das im Eigentlichen gar nicht ist (wie viele Theoretiker meinen) und stattdessen einen nichtlokalen Charakter besitzt (der sich womöglich durch das gesamte Universum zieht) taugt durchaus als neues naturphilosophisches Paradigma.

Katzenzustände in der Quanten-IT

Die Dekohärenz thematisiert ebenso auch das technologische Grundproblem der Entwicklung eines Quanteninternets. Makroskopische Objekte koppeln unvermeidlich an die Freiheitsgrade der Umgebung. Wie stark dies ausgeprägt ist, hängt von der Art der Umgebung und der Wechselwirkung mit ihr ab. Bei mikroskopischen Objekten wie Atomen ist die Dekohärenz meist so schwach, dass sie ein stark quantisches Verhalten zeigen. Bei größeren Molekülen ist die Kopplung dagegen schon weitaus stärker ausgeprägt. (Deshalb war es bei Zeilingers Fullerenen auch so schwierig, die Quanteninterferenz nachzuweisen.) Das komplexeste bekannte Molekül des Universums, die menschliche DNA, ist hingegen schon so dekohärent, dass es sich weitgehend klassisch verhält. Welch ein Glück auch, sonst wäre die Vererbung gar nicht erst möglich! Aus den genannten Gründen muss man in Quanten-Devices demnach so exotische Bedingungen schaffen, dass der Informationsaustausch mit der Umgebung konsequent unterbunden wird. Das gilt vor allem auch für Quantencomputer. Wie schon die „schräg" anmutenden bisherigen Implementierungsversuche zeigen, geht es hier immer um Systeme, welche die Dekohärenz so gut es geht verhindern sollen. Wer sich je gefragt hat, wozu Ultrahochvakuum oder ultrakalte Temperaturen nahe des absoluten Nullpunkts gut sein sollen, findet

jetzt die Antwort. Genau solche Umgebungen bewahren die Kohärenz möglichst gut und lange. Eine andere Kategorie von Quantenprozessen repräsentieren sogenannte makroskopische Quantenzustände, die zum Beispiel ab einer bestimmten Temperatur sprungartig einsetzen. Dazu zählen etwa das Einsetzen von Supraleitung oder die Bose-Einstein-Kondensation. Gesucht sind also möglichst gut isolierte, gleichzeitig manipulierbare Systeme mit vielversprechenden Kohärenzeigenschaften, was sich für das Quanteninternet, vor allem aber für den Quantencomputer als wichtigste Frage darstellt. Im Moment ist es noch nicht gelungen, derartige Systeme so zu implementieren, dass ausreichend viele Qubits im Verband ihre Kohärenz beibehalten, damit man mit ihnen interessante Operationen durchführen kann. Darin besteht auch die große Herausforderung bei der Entwicklung. Diese ist aktuell noch nicht so weit vorangeschritten, dass eine verbindliche Abschätzung bezüglich Leistungsfähigkeit und Skalierung gegeben werden kann. Wie angesprochen, besteht jedoch das Paradigma genau darin, dass die Welt von Natur aus „kohärent" ist. Die überaus spannende Frage ist daher, wie viel sich davon für technologische Anwendungen tatsächlich nutzen lässt. Die Natur per se scheint jedenfalls genau in diese Richtung geeicht zu sein.

3.4 Workshop: Kann man Menschen beamen?

Kaum ein anderes Gebiet der Physik hat die unbedarfte Menschheit in jüngerer Zeit derart fasziniert wie das Beamen, genauer die Quantenteleportation. Dabei entzündet sich diese Begeisterung vor allem an der Frage: könnte es jemals möglich sein, Menschen à la „Raumschiff Enterprise"

von A nach B zu teleportieren? Zwar steht diese Frage keinesfalls im Fokus der Entwickler des Quanteninternets, aber dennoch: Was wäre, wenn …? Wir begeben uns daher abermals in einer fiktiven Visite an das Institut für Quantenoptik, wo uns Professor Quant dieses Mysterium in Theorie und Praxis näherbringen wird.

„Ich darf Sie zu einem weiteren Workshop herzlich willkommen heißen! Diesmal geht es um eines der spannendsten Dinge der Physik überhaupt: Das Beamen von Quanteninformation. Wie Ihnen bereits bekannt ist, hat das mit Vorgängen, die Sie vielleicht aus der Science-Fiction kennen, eigentlich gar nichts zu tun. Stattdessen geht es darum, dass eine bestimmte Quanteninformation eines Objekts auf einen anderen, räumlich getrennten und bereits vorhandenen quantischen Objektträger übertragen wird. Das bedeutet, nicht die Materie wird übertragen, sondern nur bestimmte physikalische Eigenschaften. Eine Spezialität ist dabei, dass der zu übertragende Zustand nicht einmal dem Experimentator bekannt sein muss, sozusagen eine Teleportation im Blindflug. Sie sehen also, dass sich die physikalische Teleportation grundlegend von derjenigen des Science-Fiction-Genres unterscheidet. Wahrscheinlich wurde letztere nur erfunden, um die Produktionskosten derartiger Filme zu senken … Ich schlage vor, Sie sehen sich einfach mal ein vergleichsweise simples Teleportationsexperiment an, und wir erörtern mögliche Fragestellungen beziehungsweise FAQs hinterher."

Wir werden in einen mysteriös wirkenden, dunklen Raum geführt, der in seltsames Laserlicht getaucht ist. Auf einem großen Tisch sind allerlei Spiegel und sonstiges Gerät zu sehen. Plötzlich nähern sich aus dem Halbdunkel zwei amikal wirkende Gestalten. „Darf ich vorstellen", sagt Professor Quant, „das sind meine beiden Assistenten: Alice und Bob. Sie werden jetzt eine photonische Teleportation durchführen."

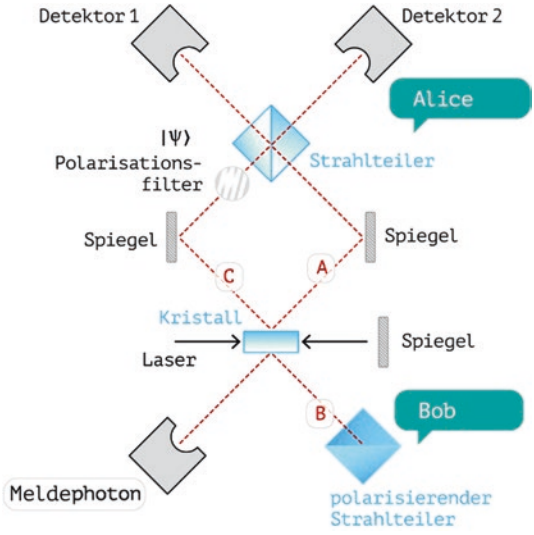

Abb. 3.3 Photonische Teleportation

Daraufhin führt uns der Professor zu einem Whiteboard (Abb. 3.3), auf dem Grafiken den theoretischen Hintergrund des Experiments erläutern sollen. Wir sehen darauf etwas, das irgendwie an das Mach-Zehnder-Interferometer vom letzten Workshop erinnert. „Sie denken richtig …“, lobt der Professor, „… allerdings in stark modifizierter Form. Neben einem nichtlinearen Kristallsystem kommt hier unter anderem auch ein polarisierender Strahlteiler zum Einsatz, mit dem man im Unterschied zum normalen Strahlteiler auch die Polarisation messen kann (in Verbindung mit zwei Detektoren, die nicht eingezeichnet sind). Meine Assistentin Alice startet die Teleportation, indem sie zunächst mittels Parametric Down Conversion zwei EPR-Paare erzeugt. Daraufhin präpariert sie eines der vier Teilchen mit dem zu teleportierenden Zustand und führt mit einem der Teilchen des zweiten EPR-Paares die Bell-Messung durch. Bob misst seinerseits

das ihm zugeteilte Photon des EPR-Paares und erhält damit den Quantenzustand von Alices Photon. Auf diese Weise wird die Quanteninformation von Alice zu Bob gebeamt. Allerdings erfordert die hier gezeigte Auslegung extreme interferometrische Genauigkeit, die wir außerhalb der sterilen Laborumgebung nicht haben. Deshalb verwenden wir in Feldversuchen für die Bell-Messung eine Kombination aus Faserkoppler und Strahlteiler auf Basis des quantenmechanischen Tunneleffekts und …".

„Verzeihen Sie bitte, Herr Professor, können Sie das bitte verständlicher ausführen!"

„Äh … natürlich – ich werde Ihnen die einzelnen Schritte noch einmal ganz langsam erklären.

Zunächst zur Parametric Down Conversion, die Sie ja von der Quantenkryptografie her schon kennen: Ein blauer Laserpuls passiert den Kristall und erzeugt daraufhin ein Paar roter Photonen, die in der Polarisation miteinander verschränkt sind. Eines davon erhält Alice (A) und das andere Bob (B). Der Puls wird vom Spiegel zurückgeworfen und passiert erneut den Kristall, wodurch er ein zweites verschränktes Photonenpaar erzeugt. Davon dient das eine als Meldephoton (es zeigt an, dass ein Photon für die Teleportation bereitsteht), das andere geht zu Alice (C). Dabei tritt dieses durch ein justierbares Polarisationsfilter, wodurch der zu teleportierende Zustand $|\psi\rangle$ erzeugt wird. Die verschränkten Photonen sind aus historischen Gründen nach den Physikern Einstein, Podolsky und Rosen (EPR) benannt."

„Wie kann ein einzelnes blaues Laserphoton ein verschränktes rotes Photonenpaar erzeugen?"

„Das ist zunächst einmal deshalb möglich, weil ein blaues Photon doppelt so viel Energie besitzt wie ein rotes. Das liegt wiederum daran, dass die Frequenz des roten Lichts nur halb so groß ist wie die des blauen Laserstrahls. Aus Gründen, die leider furchtbar kompliziert sind und die ich Ihnen deshalb ersparen will, fliegen die Photonen aus dem Kristall entlang von zwei Kegelmänteln auseinander. An denjenigen Stellen, wo diese Kegel überlappen, sind die Teilchen nicht mehr voneinander zu unterscheiden. Es liegt hier also eine Art Informationsverlust vor, was eine wichtige Voraussetzung für verschränkte Zustände ist."

„In welcher Eigenschaft sind die Teilchen miteinander verschränkt?"

„Sie sind orthogonal zueinander polarisiert. Das bedeutet, wenn zum Beispiel eines der Photonenpaare bezüglich seiner Schwingungsebene gemessen wird, so steht die Ebene des verschränkten Partnerteilchens automatisch im rechten Winkel darauf."

„Wie geht die Bell-Messung genau vor sich?"

„Dazu führt Alice die Photonen A und C im Strahlteiler zusammen und misst sie danach mit Detektor 1 und Detektor 2. Bezüglich der Messung erinnern Sie sich bitte an das Mach-Zehnder vom ersten Workshop. Wir hatten dort Polfilter in die Strahlengänge eingebracht und dabei gesehen, dass die Interferenz sofort verschwindet, wenn die Polfilter orthogonal aufeinander stehen. Das bedeutet aber zwangsläufig ebenso, dass dann auch die Photonen A und C orthogonal polarisiert sein müssen. Nun gilt es zu beachten, dass in einem wohljustierten Interferometer (das hier angenommen wird) in einem solchen Fall

beide Detektoren klicken würden. Im Unterschied zur Interferenz, wo immer nur einer der beiden Detektoren ansprechen wird. Das ist ein eindeutiges Messkriterium".

„Und was hat das mit der eigentlichen Teleportation zu tun?"

„Das ergibt sich aus der Logik: Wenn Alice je ein Photon bei Detektor 1 und eines bei Detektor 2 misst, dann weiß sie mit Sicherheit, dass jetzt A orthogonal auf C stehen muss. Da aber andererseits wegen der Verschränkung wiederum A im rechten Winkel auf B steht, folgt daraus, dass die Zustände B und C identisch sind. Bob misst seinerseits diesen Polarisationszustand mit dem polarisierenden Strahlteiler und zwei Detektoren dahinter (nicht eingezeichnet), wodurch die Verschränkung verschwindet und die Teleportation abgeschlossen ist. Insgesamt wurde also der von Alice erzeugte Zustand $|\psi\rangle$ auf das Photon B von Bob übertragen."

„Alles schön und gut. Dann hat Bob eben nun ein Photon, das im selben Zustand ist wie das von Alice. Was hat das mit Teleportation zu tun? Das ist doch, wie wenn man ein Blatt Papier nimmt, den Zustand von Alice draufmalt und das Papier dann Bob faxt. Warum nennt man das dann nicht Quantenfaxen?"

„In der Tat könnte man auf diese Idee kommen", klärt uns Dr. Quant auf, „Faxen hieße jedoch, Information zu vervielfältigen – aber das ist in der Quantenphysik streng verboten und passiert auch nicht in unserem Experiment. Beachten Sie, dass der Quantenzustand bei Alice in demselben Moment verschwindet, wo er bei Bob auftaucht. Die Quanteninformation wird also nicht kopiert, sondern vielmehr auf einen anderen, lokal getrennten quantischen Objektträger (hier ein Photon) übertragen. Das ist Inhalt

eines fundamentalen quantenmechanischen Prinzips, das man das No-Cloning-Theorem nennt".

„Was ist aber, wenn beide Teilchen bei Alice und Bob gleichzeitig gemessen werden? Dann hätte man am Ende doch zweimal denselben Zustand, und die Info wäre verdoppelt worden. Einstein hätte zwar seine EPR-Einwände, aber das No Cloning-Prinzip wäre widerlegt …".

„Nein – denn glücklicherweise entdeckte derselbe Einstein die Relativitätstheorie, und die besagt, dass es keine absolute Gleichzeitigkeit gibt. Man könnte also immer ein Bezugssystem finden, in dem die Ereignisse eben nicht gleichzeitig sind, wodurch alles wieder in Ordnung wäre- glauben Sie mir, nach heutigem Kenntnisstand ist das No cloning-Prinzip sehr gut mit der Teleportation verträglich. Bis heute gibt es keinen einzigen wissenschaftlich anerkannten Beweis, der das No Cloning – Theorem widerlegt."

„Aber wie kann das Teilchen bei der Teleportation ein Original bleiben, wie kann es seine Identität wahren, wenn doch das Objekt selbst gar nicht übertragen wird?"

„Das bringt uns auf die Frage, was die Identität beziehungsweise Individualität von Dingen überhaupt ist.

Nehmen wir uns Menschen als Beispiel. Jeder Mensch besteht aus vielleicht 10^{28} Atomen, das ist eine unermesslich große Zahl mit 28 Nullen. Sie, ich, Alice, Bob, wir alle bestehen aus denselben Sorten von Atomen, in der Hauptsache Kohlenstoff und Wasserstoff. Die materielle Zusammensetzung ist also die gleiche. Was macht dann aber unsere Individualität aus? Ganz einfach: das *Wie.* Beispielsweise die Art und Weise, wie die Atome angeordnet sind. Das heißt also: Was wir im Eigentlichen sind und

was uns zum Original macht, ist die Information über die Eigenschaften unserer Atome, primär also nicht die Materie selbst. Und genau diese Art von Information wird auch bei der Teleportation übertragen. Da es, wie gesagt, zwischen Information und Individualität keinen Unterschied gibt, kann man sagen, dass tatsächlich das Original teleportiert wurde."

„Gibt es nicht doch einen Widerspruch zu Einsteins Relativitätstheorie? Immerhin läuft die Quantenteleportation überlichtschnell ab. Die Relativitätstheorie untersagt so etwas doch ausdrücklich?"

„Hier muss man beachten, was die Relativitätstheorie wirklich sagt. Sie behauptet ja nicht, dass es nichts geben kann, das sich überlichtschnell bewegt, sondern dass die für uns nutzbare Information nicht schneller als mit Lichtgeschwindigkeit übertragen werden darf. Tatsächlich wird dieses Prinzip auch bei der Quantenteleportation eingehalten, da Bob niemals genau wissen kann, ob die Teleportation erfolgreich war. Dazu muss er beispielsweise Alice fragen, und die könnte ihm die Antwort bestenfalls mit Lichtgeschwindigkeit liefern. Wir sagen im Fachjargon: Bob muss für diese Information den Quantenkanal verlassen und auf einen klassischen Kanal umsteigen."

„Und wieso muss Bob die Alice erst fragen, ob die Teleportation erfolgreich war? Außerdem, wozu fragen? Sie könnte ihm doch, so wie hier, einfach gegenüberstehen. Dann könnte sie ihm ein entsprechendes Zeichen geben."

„Ja sicher könnte er sie auch visuell wahrnehmen – oder auch die Detektoren. Aber dazu braucht es mindestens

ein Photon, das von Alice oder den Detektoren reflektiert wird und in Bobs Auge gelangt. Und wenn irgendetwas nicht schneller als das Licht sein kann, dann das Licht selbst! Aber nun zu Ihrer ersten Frage: Erinnern Sie sich an Doktor Bertlmanns Socken? Falls es sich dabei um Quantensocken handelte, so wäre deren Farbe völlig undefiniert, und zwar so lange, bis John Bell (oder wer auch immer) hinsieht. Dann erst nehmen die Socken eine der möglichen Farben an. Das kann man vorher prinzipiell nicht wissen. In unserem Experiment hier gilt dasselbe: Hier gibt es sogar vier verschiedene Möglichkeiten, sogenannte Bell-Zustände. Und allesamt sind objektiv zufällig. Nur ein einziger dieser vier Zustände ermöglicht die Teleportation. Da alle Zustände mit gleicher Wahrscheinlichkeit auftreten, kann die Teleportation demnach im Schnitt nur in 25 % aller Fälle erfolgen. Also kann Bob niemals mit Sicherheit wissen, ob die jeweilige Messung nun tatsächlich eine Teleportation war oder nicht. Erst wenn er eine diesbezügliche Information von Alice erhält, weiß er mit Sicherheit, welcher Zustand vorliegt. Dazu benötigt er aber eben auch einen klassischen Kanal."

„Gut, gut. Es war also wirklich eine Teleportation, die nicht der Übertragung von konkreten Quantenobjekten, sondern dem Transfer von reiner Information entspricht, wobei Letztere das Original charakterisiert. Unter der Annahme, dass der Mensch nur eine bestimmte Menge an Information wäre und diese auch irgendwie zu übertragen sein muss, ist es dann irgendwann möglich, auch Menschen zu teleportieren?"

„Ich fürchte da muss ich Sie enttäuschen! Menschen zu teleportieren ist der heutigen Einschätzung nach unmöglich!"

„Aber warum denn? Sie sagten ja gerade, dass der Mensch gewissermaßen nur pure Information sei, und die kann doch prinzipiell übertragen werden."

„Na genau hier liegt zum Beispiel eines der unlösbaren Probleme. Sie können die volle Information eines Menschen in unserer Welt niemals herauslesen, da dies wegen der heisenbergschen Unschärfebeziehung unmöglich ist. Denken Sie an die 10^{28} Atome, aus denen der Mensch besteht. Sie müssten deren haargenaue Anordnung feststellen, dazu müssen Sie aber zum Beispiel wissen, wo die Atome genau sind und welche Geschwindigkeit sie besitzen. Das ist aber Werner Heisenberg zufolge unmöglich, weil Ort und Geschwindigkeit eines Teilchens niemals gleichzeitig bekannt sind."

„Aber mit den Photonen in Ihrem Versuch geht es doch auch. Unterliegen diese Teilchen denn nicht der Unschärfebeziehung?"

„Sehr wohl tun sie das. Aber selbst in unserem Experiment hier wird nicht die volle Information über sie übertragen. Bedenken Sie, dass die Teilchen ja nur in der Polarisation miteinander verschränkt sind – somit wird auch nur diese übertragen. Theoretisch kann die volle Information nur dann übertragen werden, wenn sie für uns absolut unbekannt ist. Aber das nützt uns dann natürlich nichts, denn in dem Moment, wo wir an diese Information heran wollen, müssen wir eine Messung machen, was das System automatisch stört."

„Wenn dem so ist, dann bleibt dennoch unklar, warum die Teleportation überhaupt funktioniert. Einerseits basiert sie ja auf der Verschränkung, diese müsste aber sofort zerstört werden, sobald Bob den Teilchenzustand misst. Keine Verschränkung – keine Teleportation, wollte man meinen."

„Das ist scharfsinnig kombiniert. Aber sehen wir uns das genauer an: Anders als beim Mach-Zehnder-Interferometer im ersten Workshop, wo nur ein einziges Photon im Interferometer war, befinden sich hier deren *zwei.* Das ändert die Sachlage erheblich. Detektor 1 und Detektor 2 stellen nur fest, ob die beiden Photonen zueinander orthogonal polarisiert sind, nicht jedoch, welches der beiden Photonen genau welche Polarisation besitzt. Insofern decken die Detektoren nicht die volle Information auf, wodurch eine gewisse Restverschränkung übrig bleibt, mit der die Teleportation erfolgen kann. Diese wird erst in dem Moment zerstört, wenn Bob hinter seinem polarisierenden Strahlteiler die Messung mit den Detektoren (nicht eingezeichnet) durchführt. Denn dadurch wird erst klar, welches Teilchen welche Polarisation konkret trägt."

„Wäre es denn dann nicht zumindest möglich, ähnlich wie bei ihren Photonen wenigstens Teile der Information eines Menschen zu übertragen, also eine Art partielle Teleportation durchzuführen?"

„Sie sind wirklich hartnäckig! Also gut: Selbst wenn wir die Probleme mit der Unschärfebeziehung einmal außer Acht lassen. Wir würden an der praktischen Umsetzung scheitern: Wie sollen wir denn 10^{28} Atome verschränken, wenn wir es gegenwärtig gerade mal mit einigen wenigen schaffen? Selbst wenn wir dazu imstande wären, wie sollte diese Verschränkung ablaufen? Verschränken heißt ja prinzipiell ununterscheidbar machen, also eine Situation mit Informationsverlust herzustellen. Das können Sie auch Quantenkohärenz nennen. Wie sollte das bei einem makroskopischen Objekt wie dem Menschen ablaufen? Denken Sie an Schrödingers Katze! Wenn wir statt der Katze einen Menschen in eine extrem gut geschützte

Stahlkammer sperren, würde auch der sofort dekohärent werden. Allein durch die innere thermische Wechselwirkung, also durch den unvermeidlichen Informationsaustausch zwischen den Myriaden von Atomen, aus denen er besteht, und denen in ihrer Umgebung. Von anderen Dingen, wie etwa der Gravitation, die man nicht einfach wegschalten kann, reden wir da gar nicht. Falls die Teleportation außerdem wie in der hier gezeigten Weise ablaufen sollte, dann stehen wir vor einem weiteren unlösbaren Problem: Unsere Person müsste mit einem EPR-Zwillingspaar verschränkt werden. Völlig unvorstellbar, wie das bei einem Menschen ablaufen sollte beziehungsweise was das eigentlich bedeutet. Nein – die Vorstellung, dass man Menschen beamen könnte, bleibt weiterhin fest in der Hand der Science-Fiction."

„Welche Bedeutung liegt dann in der Quantenteleportation?"

„Die Bedeutung liegt vor allem in der technologischen Zukunft. Sehen Sie, Quantenteleportation ist eine vielversprechende Methode, wie man Quantencomputer durch ein Quanteninternet eines Tages miteinander vernetzen kann. Dass man einzelne Qubits teleportieren kann, ist längst bewiesen worden. Ebenso, dass Teleportation über große Distanzen (aktuell 1200 km) möglich ist, wie ein chinesisches Team eindrucksvoll zeigen konnte. Die oben beschriebene Anordnung lässt sich in viel komplizierterer Form nämlich auch mit einem Quantensatelliten implementieren – da sind Alice und Bob dann eben sehr weit voneinander entfernt. Wie Sie außerdem bereits wissen, lassen sich durch Verschränkungsaustausch beziehungsweise Entanglement Swapping (was einer Teleportation von Verschränkung entspricht) Quantenrepeater realisieren. Damit wird bereits die wesentlichste Anforderung

eines Quanteninternets erfüllt. Sehen Sie, in unserem vergleichsweise einfachen Versuch hier werden nur die Polarisationszustände einzelner Lichtquanten übertragen. Dasselbe Prinzip lässt sich theoretisch aber auch mit viel komplizierter verschränkten Zuständen durchführen. Vielleicht gelingt es den Forschern eines Tages, solche extrem komplexen Zustände herzustellen und zu präparieren. Die können dann als Output von einem Quantencomputer zu einem anderen teleportiert werden, welcher diesen als Input nutzt. Wer weiß, was die Zukunft noch bereithält und welche technologischen Anwendungen daraus noch resultieren werden: Schon heute gibt es beispielsweise 3D-Drucker. Da kann ich mir über das Internet komplexe Daten herunterladen, und der Drucker fertigt mir dann daraus ein dreidimensionales Gebilde. Stellen Sie sich vor, es gäbe einmal ein Quanten-Device, das aus einer Quantencloud komplexe Quanteninformation via Teleportation auf einen vorhandenen Objektträger downloadet. Da Quantencomputer prinzipiell große Atom- und Molekülstrukturen simulieren könnten, ließe sich damit vielleicht in weiterer Folge ein exotischer Werkstoff herstellen, der sich an die Wünsche des Nutzers anpasst. Das wäre dann unheimlich praktisch, denn neben der äußeren Form kann ich dann quasi auch das zugehörige Material, genauer seine Quanteneigenschaften, nach Wunsch synthetisieren. Sozusagen Designermaterie für verschiedenste Anwendungsgebiete. Natürlich ist das im Moment die blanke Spekulation und Fiktion, physikalisch jedoch prinzipiell denkbar. Die Quantenteleportation ist in jedem Fall ein äußerst spannendes Phänomen, bei dem längst noch nicht klar ist, was man alles daraus machen kann."

3.5 Eine Reise in die Zukunft

Für das Quanteninternet spielt nicht nur die Quantenphysik selbst eine Rolle, sondern auch Einsteins Relativitätstheorie. Indirekt ist die Relativitätstheorie ebenso Garant für seine inhärente Sicherheit, vor allem weil sie die Existenz des No-Cloning-Theorems unterstützt. Die folgenden beiden Abschnitte sollen diesen Zusammenhang begreiflich machen. Dazu zunächst ein kleiner Crashkurs in Sachen Spezielle Relativitätstheorie.

Angenommen, Superingenieur Daniel Düsentrieb erfindet die ultimative Rakete, welche alle Dimensionen sprengt und extrem schnell fliegen könnte. Nun setzen Tick und Trick ihren Drillingsbruder Track in das Raumschiff, der mit ihm die Erde verlässt. Er beschleunigt und erreicht nach einigen Monaten fast die Lichtgeschwindigkeit (im Vakuum circa eine Milliarde km/h), ehe er daraufhin wieder zur Erde zurückkehrt. Als er aus der Rakete steigt, ist er jedoch sehr verdutzt: Seine beiden Brüder Tick und Trick, die beim Start noch Kinder waren, sind plötzlich so alt, wie er Onkel Dagobert in Erinnerung hat. Wie konnte das geschehen? Handelt es sich bei der Rakete um eine Zeitmaschine? Offensichtlich ist Track in die Zukunft seiner Brüder gereist – er selbst ist jedoch (fast) genauso jung wie beim Start.

Hand auf's Herz! Sie haben von diesem Zwillings-, Drillings- oder Uhrenparadoxon sicher schon einmal gehört, aber zu glauben, dass so etwas tatsächlich möglich wäre, fällt doch wohl sehr schwer. In der Tat ist das Uhrenparadoxon die blanke Science-Fiction, allerdings nur was die marktkompatible Personenbeförderung anbelangt – mit Elementarteilchen sieht es anders aus. Und es wurde ja bereits dargelegt, dass die Physik Naturgesetze erst dann gelten lässt, wenn diese ausreichend

experimentell verifiziert sind. Sehen wir uns also die entsprechenden Experimente an.

In der Tat ist das Drillingsparadoxon nur die Karikatur eines Phänomens, das zum „Kerngeschäft" der Relativitätstheorie zählt, der sogenannten Zeitdilatation. Freilich kann man ein Experiment in der geschilderten Weise nicht durchführen. Wenn der Astronaut Track aber sehr viel kleiner wird, zum Beispiel auf die Größe eines Elementarteilchens schrumpft, dann ist es viel einfacher, ihn auf ernst zu nehmende, also „relativistische" Geschwindigkeiten zu beschleunigen, und derlei „Zeitreisen" lassen sich entsprechend einfach in der Natur beobachten. Ein solches Beispiel sind die Myonen, die als Folge des Zusammenpralls energiereicher Teilchen der kosmischen Strahlung mit Luftpartikeln etwa 10 km über der Erde entstehen. Diese Myonen rasen fast mit Lichtgeschwindigkeit zur Erde, wo sie messtechnisch erfasst werden können. Der Witz an der Sache ist aber: Das Myon besitzt nur die äußerst kurze mittlere Lebenspanne (= Zerfallsdauer) von 1,5 Millionstel Sekunden. In dieser Zeit kommt es selbst mit Lichtgeschwindigkeit keinen halben Kilometer weit. Des Rätsels Lösung ist in gewisser Weise ganz einfach: Das Myon fliegt – so wie Track im Drillingsparadoxon – in die Zukunft. Oder anders ausgedrückt: Die sogenannte Eigenzeit des Myons verlangsamt sich relativ zur Erdzeit dramatisch. Auf diese Weise vergeht für das Myon auf seinem Flug viel weniger Zeit als für uns Erdenbürger.

Dieser Effekt, den man Zeitdilatation („Zeitdehnung") nennt, besitzt aber noch eine andere Deutung: Verlässt man den Standpunkt des Erdbewohners, für den die Zeit beim Myon langsamer vergeht als bei ihm selbst, kann man die Sache auch aus Sicht des Myons betrachten: Von dessen Standpunkt aus kommt ihm die Erde fast mit Lichtgeschwindigkeit entgegen. Die Gleichungen der Relativitätstheorie zeigen dann, dass die Erde in

solch einem Fall nicht mehr kugelförmig, sondern stark abgeplattet wäre, weil alle Abstände in Bewegungsrichtung (der Erde!) verkürzt werden. Für das Myon beträgt der Abstand zur Erdoberfläche weniger als einen halben Kilometer und es kann ihn problemlos innerhalb seiner Lebenszeit zurücklegen und anschließend von den Physikern auf der Erde nachgewiesen werden. Diese Verkürzung von Distanzen bewegter Objekte nennt man Längenkontraktion.

Erzeugung und Eintreffen des Myons auf der Erde sind zwei physikalische Ereignisse, die vom Standpunkt der Erde aus als Zeitdilatation, vom Standpunkt des Myons jedoch als Längenkontraktion gemessen werden. Und genau hier liegt auch die Kernaussage der Relativitätstheorie: Das Erscheinungsbild der Natur hängt vom Standpunkt des Beobachters ab, genauer gesagt, vom Bewegungszustand seines Bezugssystems, wobei die Spezielle Relativitätstheorie ausschließlich Inertialsysteme betrachtet. Dabei ist die Frage, wer „wirklich" recht hat, sinnlos. Denn im Universum gibt es weder absolute Zeit noch absoluten Raum. Mehr noch, Raum und Zeit sind eng miteinander verbunden und erweisen sich als ähnlich flexibel wie ein Gummiband.

Was ist ein Inertialsystem? Wenn in der Küche ein Teller Suppe auf den Verzehr wartet, dann ist die Oberfläche der Suppe völlig glatt – bis wir mit dem Auslöffeln beginnen. Das würde aber auch dann für die Suppe gelten, wenn sie auf dem Tischchen eines bequemen Verkehrsjets steht, der sich völlig ruhig und gleichförmig dahinbewegt. Wo ist der Unterschied? Wenn man nicht wüsste, dass sich die Suppe in einem Flugzeug befindet, wäre ihr Verhalten nicht von demjenigen auf dem Küchentisch zu unterscheiden. In einem Fall ist die Geschwindigkeit der Suppe relativ zur Erde null, im anderen Fall beträgt sie vielleicht 850 km/h. Genau hier stoßen wir auf eine der beiden Grundannahmen der Speziellen Relativitätstheorie.

In zueinander gleichförmig bewegten Bezugssystemen ohne Fenster besteht für deren Insassen keine Unterscheidungsmöglichkeit zwischen „Ruhe“ und „Bewegung“, weshalb man jedes Inertialsystem als gleichberechtigt ansehen muss. Diese Annahme führt zu höchst interessanten Konsequenzen, nämlich der Relativität der Gleichzeitigkeit: Angenommen, in dem Flugzeug befinden sich eine Stewardess ganz hinten und ein Flugbegleiter im vorderen Bereich der Maschine. Genau in der Mitte der beiden Personen erzeugt jemand einen Lichtblitz mit seiner Digicam. Dabei werden Photonen emittiert, die genau im selben Moment auf die Augen von Stewardess und Flugbegleiter treffen. Beide nehmen dieses Ereignis also *gleichzeitig* wahr. Vom Standpunkt eines Beobachters auf der Erde aus betrachtet ergibt sich dagegen eine ganz andere Schlussfolgerung. Aus seiner Sicht erreichen die Photonen die Stewardess früher als den Flugbegleiter, da das Heck der Maschine dem Lichtstrahl entgegenfliegt, der Bug dagegen den Photonen zu enteilen versucht. Also besteht hier *keine* Gleichzeitigkeit. Wer hat nun recht? Beide! Angesichts der Gleichberechtigung von Inertialsystemen gibt es keine absolute Gleichzeitigkeit von Ereignissen. Geschehen in einem Inertialsystem zwei Ereignisse an zwei verschiedenen Orten gleichzeitig, so finden diese Ereignisse in einem dazu relativ bewegten Inertialsystem zu verschiedenen Zeiten statt. Das ist das Relativitätsprinzip.

Freilich ist die Zeitdilatation nicht nur ein Phänomen von Inertialsystemen. Sie tritt gleichermaßen auch in beschleunigten Systemen sowie im Alltag auf. Wir bemerken sie nur nicht. Wenn Lewis Hamilton nach einem Grand Prix aus dem Rennwagen steigt, ist er tatsächlich etwas jünger als die relativ zu ihm ruhenden Zuschauer auf der Tribüne. Er registriert das nur deshalb nicht, weil der Zeitunterschied so gering ist. Hätte er allerdings eine extrem genaue Atomuhr an der Hand (wenn es

so etwas als Armbanduhr gäbe), dann könnte er den winzigen Zeitunterschied exakt feststellen. Tatsächlich wurden derartige Experimente mit hochgenauen Atomuhren in Flugzeugen und Satelliten durchgeführt und somit der Effekt der Zeitdilatation direkt wissenschaftlich bewiesen. Im Alltag begegnen uns also ständig solche minimalen relativistischen Effekte. Sie können jedoch getrost vernachlässigt werden, weil alltägliche Geschwindigkeiten so viel kleiner als die Lichtgeschwindigkeit sind. Das gilt jedoch nicht uneingeschränkt für technische Anwendungen. Wussten Sie, dass das Navi in ihrem Auto nur deshalb korrekt funktioniert, weil es die Zeitdilatation berücksichtigt? Diese Technik beruht unter anderem auf dem Vergleich von Laufzeitsignalen elektromagnetischer Strahlung. Da Satelliten – denken wir an den Quantensatelliten, für den dasselbe gilt – mit erheblichen Geschwindigkeiten um die Erde rotieren vergeht die Zeit in Ihrem Auto ein wenig anders als auf dem Trabanten. Bei der hohen Genauigkeit, die für das System erforderlich ist, muss diese Abweichung zwingend berücksichtigt werden – andernfalls würde das Navi hunderte Meter danebenliegen!

Ein Wort noch zum Drillingsparadoxon: Ein oft gebrachter Einwand besteht darin, dass man doch gar nicht wissen kann, wer hier der ruhende oder bewegte Beobachter sei (und man deshalb die Zeidilatation naiverweise infrage stellen könnte). Der im Raumschiff sitzende Track ist natürlich der Auffassung, dass er nicht der bewegte, sondern der ruhende Beobachter sei. Aus seiner Sicht rast ja die Erde erst von ihm fort und später wieder auf ihn zu. Tatsächlich kann man dies dadurch entkräften, wenn man sich die Praxis ansieht: Drillingsbruder Track muss ja von der Erde erst einmal starten und somit beschleunigen, um in die Nähe der Lichtgeschwindigkeit zu gelangen. Ab diesem Moment ist sein Raumschiff aber

kein Inertialsystem mehr, das ja unbeschleunigt sein muss. Deshalb wäre dieses System gegenüber dem anderen als ausgezeichnet zu betrachten und daher nicht mehr gleichberechtigt. Außerdem gilt es in der Praxis die Wegumkehr zu beachten, die ja wiederum eine Beschleunigung (auch negativ, im Sinne von Bremsen) voraussetzt. Obwohl eine genaue Analyse in der Tat ganz schön knifflig ist, kann man am Ende definitiv sagen: Für Track im Raumschiff ist die Zeit viel langsamer vergangen als für seine Brüder auf der Erde.

Dennoch erklärt das Relativitätsprinzip allein noch nicht, *warum* es genau zur Zeitdilatation kommt – es schafft zwar eine Voraussetzung, erklärt es aber quantitativ nicht. Deshalb muss diese Grundannahme durch ein ganz wesentliches weiteres Axiom ergänzt werden. Einstein formulierte dieses zunächst als Prinzip der Konstanz der Lichtgeschwindigkeit, erweiterte es später jedoch zugunsten einer viel fundamentaleren Annahme: Die Signalwirkung, also nutzbare Information (das heißt konkret zugängliche) kann niemals schneller als mit Vakuum-Lichtgeschwindigkeit übertragen werden. Wir wollen uns nun ansehen, welche Auswirkung das auf unseren Astronauten Track hat.

Das Ticken der biologischen Uhr

Man stelle sich vor, wie Track in seiner Superrakete dahinbraust; jetzt senkt er den Kopf und beobachtet seine Zehenspitze (Z). Um diese wahrnehmen zu können – um also eine optische Information zu erhalten –, muss jetzt mindestens ein Photon von Z zu seinem Auge (A) gelangen, wozu es klarerweise die Strecke ZA zurücklegen muss. Aus Sicht des ruhenden Inertialsystems auf der Erde muss das Lichtquant dagegen die viel längere Strecke $(ZA)'$ durchmessen, da sich das Raumschiff währenddessen sehr schnell weiterbewegt. Entscheidend

ist nun, dass sich das Photon, das ja nutzbare Information überträgt, Einstein zufolge niemals überlichtschnell bewegen darf. Deshalb benötigt es zwangsläufig für die Strecke (ZA)′ mehr Zeit als für die Strecke ZA. Das heißt, die Information über die Zehenspitze erhält Track im dahinrasenden Raumschiff zu einem späteren Zeitpunkt, als wenn er auf der Erde stehen würde und seine Zehe dort betrachtet. Aus diesem Grund muss sich der Zeitablauf eines bewegten Objekts relativ zu einem ruhenden Beobachter zwangsläufig verlangsamen, damit die Lichtgeschwindigkeit in beiden Sichtweisen den gleichen Wert hat (Photonen besitzen per se immer Lichtgeschwindigkeit) Dies erklärt die Zeitdilatation auch quantitativ, da man sie jetzt aus der Relativ- bzw. Lichtgeschwindigkeit direkt berechnen kann. Dieser Effekt setzt mit jeder Relativgeschwindigkeit ungleich null ein, führt jedoch erst in der Nähe der Lichtgeschwindigkeit zu deutlichen Abweichungen, wodurch er in der alltäglichen Welt verborgen bleibt. Was aber bedeutet das für Tracks biologisches Alter? Immerhin ist er in die Zukunft seiner Brüder gereist – ist die Zeitdilatation gar ein Jungbrunnen? Das bleibt Ansichtssache. Schon 1905 wies Einstein auf die Zeitdilatation von Uhren hin. 1911 dehnte er die Betrachtung auch auf den lebenden Organismus aus, indem er – ganz im Sinne des Zwillingsparadoxons – die Lebenszeit zweier Organismen verglich. Während der ruhende Organismus längst Generationen Platz gemacht hätte, wäre dieselbe Zeitspanne für einen sehr schnell reisenden Organismus (der anschließend wieder zu seinem Anfangspunkt zurückkehrt) bloß ein Augenblick. Einstein zufolge bleibt demnach Drillingsbruder Track nur aus einem einzigen Grund jünger: weil sich seine Eigenzeit relativ zu einem ruhenden Beobachter verlangsamen muss. Anders gesagt; seine „biologische Uhr“ (Eigenzeit) tickt über den gesamten Raketenflug gesehen langsamer als die

biologische Uhr seiner Brüder (Erdzeit). Somit ist er nur deshalb in die Zukunft gereist, weil er sozusagen nicht so schnell gelebt hat. Bei Erreichen der Lichtgeschwindigkeit, wäre Tracks Eigenzeit logischerweise genau Null – die Zeit bliebe also stehen. Glücklicherweise wird das niemals passieren, da Objekte mit Ruhemasse (wie Atome, demnach auch Menschen und Enten) niemals die Lichtgeschwindigkeit exakt erreichen können. Dazu bräuchte man die ganze Energie des Universums, doch nicht einmal das wäre genug. Letzteres lässt sich übrigens wiederum erheblich auf die Zeitdilatation zurückführen: Angenommen, Track wollte auf Lichtgeschwindigkeit beschleunigen, dann würde aber seine Trägheit (= Widerstand der Masse gegen die Beschleunigung) größer und größer, schließlich aber unendlich werden. Die eigentliche Ursache dafür liegt in der relativistischen Massenzunahme, die man beispielsweise aus einer Impulsbetrachtung mithilfe der Zeitdilatation mathematisch herleiten kann. Egal, wie viel Energie der Antrieb der Rakete auch immer aufbieten würde – es hätte am Ende doch keinen Sinn, weil im selben Verhältnis ja auch die Masse und somit die Trägheit wächst. Intuitiv können wir deshalb auch verstehen, dass zwischen Energie und Masse eine Proportionalität bestehen muss, was in Einsteins weltberühmter Gleichung $E = mc^2$ zum Ausdruck kommt.

Die Bedeutung für das Quanteninternet

Der Leser mag sich nun zurecht fragen, was die bisherigen Ausführungen mit einem Quanteninternet zu tun haben. Zunächst wollen wir etwas Wichtiges festhalten: Wie oben gezeigt, basiert Einsteins Spezielle Relativitätstheorie (SRT) ganz entscheidend auf dem Grundsatz, dass klassische (also nutzbare) Information niemals schneller als mit Lichtgeschwindigkeit übertragen werden kann.

Da andererseits die SRT keine bloße Theorie darstellt (wie manche Menschen immer noch glauben) sondern millionenfach bewiesenes Faktum ist, muss dieses sehr wichtige Axiom demnach unmittelbar auch dem Laien einleuchten. Worin besteht nun seine Bedeutung für das Quanteninternet?

1. Das klassische Internet überträgt ausschließlich nutzbare Information, weshalb die Transfergeschwindigkeit klassischer Bits maximal auf die Lichtgeschwindigkeit begrenzt ist. Das ist eine Binsenweisheit, die jeder Nachrichtentechniker kennt – nicht jeder weiß aber, dass das aus der SRT stammt. Das Quanteninternet erlaubt hingegen die instantane Übertragung von Quanteninformation, woraus im Umkehrschluss folgt, dass diese automatisch keine nutzbare Information sein darf – und daher notwendigerweise von der klassischen scharf zu trennen ist.
2. Gerade weil Qubits aber instantan übertragen werden (siehe Quantenteleportation) und das wegen 1.) keine nutzbare Information sein darf, müssen ihre späteren Messwerte zunächst zwangsläufig unbekannt bleiben, weil das sonst wieder klassische Info wäre. Deshalb sind Messungen an verschränkten Qubits automatisch immer objektiv zufällig. Dabei darf dieser Quantenzufall natürlich selbst keine Ursache haben, da man diese Ursache ja wieder kennen könnte. Deshalb sind auch die quantenzufällig generierten Bits bei der QKD die allerbesten Zufallszahlen, die es überhaupt geben kann – sie dürfen nicht einmal im Prinzip eine Ursache haben und können deshalb auch niemals algorithmisch erzeugt werden.
3. Indem Qubits also aus physikalischen Gründen immer „Phantome“ sind, muss demnach auch jeglicher Ablauschvorgang unmöglich sein. Weil die klassische

Information das hingegen erlaubt und eine solche Attacke mindestens eine Verdoppelung der Information voraussetzt, muss für die nichtklassische Quanteninformation automatisch das Gegenteil der Fall sein. Deshalb bewahren Qubits notwendigerweise eine inhärente Sicherheit – und können daher auch nicht dupliziert werden (No cloning – Prinzip). Das ist ein notwendiges, jedoch noch kein hinreichendes Kriterium, weshalb seine Gültigkeit durch einen exakten quantenmechanischen Beweis zu erbringen ist (siehe unten).

4. Die aus 1.)-3.) gefolgerte inhärente Sicherheit wäre nur dann unmittelbar gefährdet, wenn – im glatten Widerspruch zur SRT – eine überlichtschnelle Übertragung von klassischer Information DOCH möglich wäre. Insbesondere müsste dann auch die Gültigkeit des No cloning – Prinzips stark in Zweifel gezogen werden.

3.6 Das No-Cloning-Theorem

Der Dreh- und Angelpunkt der Sicherheit im Quanteninternet ist das No-Cloning-Theorem. Dies betrifft vor allem auch die Technologie, die zur Herstellung von Quantenrepeatern oder auch bei der Entwicklung von quantengeeigneten Fehlerkorrekturverfahren völlig neue Entwicklungswege gehen muss. Nun wird die uneingeschränkte Gültigkeit des No-Cloning-Prinzips gerade in seiner Eigenschaft als physikalisch inhärenter Sicherheitsgarant von verschiedenen Kritikern infrage gestellt. Diesen Positionen sei entgegengehalten, dass man das Theorem aus grundlegenden Annahmen der theoretischen Physik logisch folgern kann. Ein derartiger Beweis wurde erstmals 1982 von William Wootters et al. erbracht. Dieser besteht in einem Widerspruchsbeweis, wo zunächst angenommen

wird, dass ein quantenmechanisches Verfahren existiere, das beliebige Qubits perfekt kopieren könne. Diese Behauptung wird anschließend mit üblicher Operatorenmathematik zu einem Widerspruch geführt. Dabei erweist sich die Existenz des No Cloning-Theorems als Folge der Unitarität von Zeitentwicklungsoperatoren, die sich ihrerseits direkt aus den Axiomen der Quantenmechanik ergibt. Wer nun nicht an die mathematische Beweiskraft sowie die logischen Fähigkeiten dieser namhaften Theoretiker glaubt, dem sei noch ein ganz anderer Grund genannt, nämlich Einsteins Relativitätstheorie. Wie eben dargelegt, beruht die Spezielle Relativitätstheorie auf zwei Grundannahmen: einerseits auf der Gleichberechtigung von Inertialsystemen, andererseits darauf, dass eine überlichtschnelle Signalwirkung völlig unmöglich ist. Tatsächlich liegt auch hier der Anlassfall für den Beweis des No-Cloning-Theorems. Und zwar in einem Gedankenexperiment des US-Physikers Nick Herbert, demzufolge via Quantenverschränkung ein Mechanismus denkbar wird, über den nutzbare Information schneller als das Licht transferiert werden könnte. Herbert fordert hiermit die Wissenschaft auf, einen Beweis zu erbringen, der sein Gedankenexperiment widerlegt.

Überlichtschneller Datentransfer?

Das wäre für ein Quanteninternet natürlich eine feine Sache – wenn man mit der Verschränkung überlichtschnell nutzbare Information übertragen könnte. Man denke etwa an einen Quantensatelliten, der einen verschränkten Kanal zwischen Alice und Bob herstellt. Wenn Alice zum Beispiel (willentlich, also durch sich selbst bestimmt) eine binäre „1“ misst, dann hat Bob im selben Moment und räumlich beliebig weit entfernt, ebenso eine „1“. Misst sie absichtlich eine „0“, dann instantan auch Bob eine „0“, usw. Auf diese Weise könnte Alice digitale

Information zu Bob überlichtschnell übertragen. Das würde jede Dimension der Nachrichtentechnik sprengen. Doch leider ist das nicht möglich. Wie bereits anhand der QKD eingehend gezeigt wurde, zerfallen die Qubits bei jeder Messung in quantenzufällige Bitwerte – wie ja auch jede Messung an verschränkten Systemen der objektiven Zufälligkeit unterliegt. Damit lässt sich also niemals Information direkt übertragen. Außerdem würde ansonsten Einsteins Relativitätstheorie wie ein Kartenhaus in sich zusammenfallen. Immerhin ergibt sich ja die experimentell vielfach bestätigte Zeitdilatation als direkte Konsequenz dieser Unmöglichkeit.

Nick Herberts „Superluminal Device"

In Nick Herberts Gedankenexperiment geht es nun genau um diese Frage. Könnte man auf Basis der Verschränkung nicht doch einen Mechanismus finden, der einen überlichtschnellen Datentransfer zu leisten vermag? Dazu muss man wissen, dass 1982 die Physik des Lasers noch nicht so gut erforscht war. Das Laserprinzip beruht auf der Lichtverstärkung durch stimulierte Emission, wo damals nicht eindeutig war, ob dabei ein bestimmter Quantenzustand x-mal perfekt kopiert wird oder nicht. Wenn dem so wäre, dann könnte man einen Inputzustand in einen Laser schicken, und es würde derselbe Zustand in x-facher Kopie herauskommen. Man könnte dann also ein einziges Photon mit einem ganz bestimmten Zustand in den Laser einbringen, und es kämen als Output Trillionen Photonen exakt derselben Eigenschaften wieder heraus.

Herbert schlug deshalb hypothetisch ein FLASH-System vor – eine Abkürzung für „erste laservertärkte Superluminal-Verbindung". Die Grundidee ist einfach: Wenn Alice und Bob in einem verschränkten Zweiphoton-System eine Messung machen, dann ist (sobald der Messwert bei Alice feststeht) überlichtschnell

auch der Messwert von Bob vorherbestimmt. Aufgrund des Quantenzufalls kann damit aber keine verwertbare Info übertragen werden (siehe oben). Wenn aber das Photon, bevor es zu Bob gelangt, als inputzustand den Laser passiert, dann verlässt es ihn in trillionenfacher Kopie als Outputzustand. Das hat den Vorteil, dass Bob daraufhin diesen Laserstrahl durch einen Strahlteiler splitten kann und mithilfe der „Photonenstatistik" eindeutig feststellen kann, welchen Zustand Alice gerade präpariert hat. Wenn Alice diesen Zustand beispielsweise mit „1" belegt, und einen anderen, unbekannten Zustand mit „0", dann kann Alice durch eine bestimmte Abfolge ihrer Einstellungen klassische Information zu Bob übertragen. Infolge der Quantenverschränkung erfolgt der informationsgewinn demnach überlichtschnell.

Das System funktioniert also insgesamt wie ein Telegraf, bei dem Alice die Auswahl ihrer Messung wie die Punkte und Striche eines Morsecodes verwendet. Bob könnte dabei jedes Bit des Codes überlichtschnell entschlüsseln. Wesentlich ist, dass man dazu zwingend annehmen müsste, dass Quantenzustände perfekt vervielfältigt werden können.

Nähere Details

Man stelle sich dazu eine Quelle vor, die wie bei den EPR-Experimenten verschränkte Photonen in gegensätzlicher Richtung emittiert. Diese können entweder linear oder zirkular polarisiert sein. Zirkular polarisiertes Licht (= Spin des Photons) bedeutet, dass der elektrische Feldstärkevektor entlang der Ausbreitungsrichtung der Lichtwelle eine Kreisbewegung beschreibt. Diese kann rechts- oder linksdrehend erfolgen. Um die Verhältnisse möglichst einfach darzustellen, wollen wir folgende Abkürzungen einführen: linear polarisiertes Licht (Lp) ist H = horizontal oder V = vertikal polarisiert und zirkular

polarisiertes Licht (Zi) ist R = rechtszirkular oder L = linkszirkular polarisiert. Die Korrelationen seien nun so gegeben: Misst Alice H, dann misst Bob gemäß dem Bell-Theorem V; Misst Alice R, dann Bob L. Das heißt, die Messung von Alice beeinflusst wegen der Verschränkung instantan (und damit überlichtschnell) die Messung von Bobs Photon nach obiger Vorschrift. Alice kann natürlich frei bestimmen, ob sie linear oder zirkular messen will. Angenommen, Alice wählt zirkular polarisiert und misst zufällig L. Dann ist wegen der Verschränkung Bobs Zustand automatisch als R determiniert. Jetzt nimmt Herbert an, dass dieses Photon, bevor es zu Bob kommt, als Inputzustand den besagten Laser passiert. Unter der Hypothese, dass bei einem Laser Input- gleich Outputzustand wäre, müsste dann ein Strahl R-polarisierter Photonen zu Bob gelangen. Er könnte dann mit einem Strahlteiler die Strahlen splitten und die eine Hälfte auf linear, die andere auf zirkular polarisiertes Licht messen. In diesem Fall schloss Herbert, dass 50 % Photonen rein im Zustand R und je 25 % in H beziehungsweise 25 % in V wären. Aufgrund dieses Messergebnisses würde Bob demnach mit Sicherheit wissen, dass Alice zirkular gemessen hat. Das heißt also, die Verschränkung, die per se instantan vor sich geht, könnte auf diese Weise direkt das einzelne Bit überlichtschnell transferieren. Ein Beispiel: Alice will etwa die Bitfolge 1 0 0 1 … übertragen und nimmt daher die Messung in der Reihenfolge Zi, Lp, Lp, Zi, … vor, wodurch Bob die Bits eindeutig rekonstruieren kann, wenn er deren Zuordnung kennt.

Theoretiker widerlegen das Gedankenexperiment

Leider würde das Superluminal- Device in der Praxis nicht funktionieren. Wie William Wootters, Wojciech Zurek, Tullio Weber, Giancarlo Ghirardi und Dennis Dieks klarstellen, kann so ein Device keine überlichtschnellen Signale senden. Der Grund: ein Photon im Zustand R

existiert nur als Linearkombination der Zustände H und V. Jeder dieser Subzustände würde im Laser verstärkt werden, deshalb ist der Output kein reiner R-Zustand, sondern eine Superposition aus zwei Zuständen: Einer, wo sich alle im Zustand H befinden und einer, bei dem alle im Zustand V wären – mit je 50 % Wahrscheinlichkeit. Deshalb würde Bob bezüglich der Information von Alice nur „Rauschen" empfangen, das heißt er könnte niemals einen Zustand erhalten, bei dem R mit 25 % H und 25 % V gegeben wäre (da ja 50 % in H oder 50 % in V). Fazit also: Herberts FLASH-System würde nicht funktionieren – und sowohl SRT als auch No Cloning- Theorem bleiben damit bestätigt.

Eine fundamentale Entdeckung

Interessant ist, dass sich die Theoretiker erst auf Herberts Gedankenexperiment hin mit der Thematik beschäftigten und auf diese Weise erst das wichtige No Cloning-Prinzip entdeckten. Herbert nimmt bei seinem Device ja an, dass die Quanteninformation im Laser kopiert wird. Wie der quantenmechanische Beweis ergibt, ist dies aber eben nicht möglich. Ein beliebiger Quantenzustand kann niemals perfekt kopiert werden, ohne den ursprünglichen dabei zu zerstören. Die zweite wichtige Schlussfolgerung besteht in der Feststellung, dass Quantenmechanik und Spezielle Relativitätstheorie (nicht nur in diesem Punkt) miteinander konsistent sind. Das ist nun auch ein sehr glücklicher Umstand, denn sonst könnte das zu heillosen Paradoxien führen: Angenommen, Quanteninformation könnte doch kopiert werden. Dann wäre es im Umkehrschluss also möglich, Information überlichtschnell zu transferieren. Wie man aus der Relativitätstheorie zeigen kann, wäre dann aber dessen Kausalitätsprinzip auf den Kopf gestellt. Indem (professionell gesprochen) die Reihenfolge raumartiger Ereignisse vom Beobachter

abhängt, kann das zu Problemen mit der Kausalität führen. Denn wenn in einem Bezugssystem Ereignis A vor B eintritt, im anderen jedoch B vor A kommt, dann folgt daraus, dass sowohl A Ursache von B als auch B Ursache von A sein kann. Dies führt zu Paradoxien, bei denen ein Ereignis sich selbst in der Vergangenheit rückwirkend verhindert. Gleichzeitig lassen sich dann ebenso Szenarien konstruieren, die Zeitreisen mit Überlichtgeschwindigkeit in die Vergangenheit denkbar machen. Die logische Konsequenz ist die Forderung der SRT, dass sich nur „zeitartig" oder „lichtartig" zueinander gelegene Ereignisse ohne Kausalitätsproblem gegenseitig beeinflussen können. Deshalb wird in der SRT axiomatisch angenommen, dass generell Überlichtgeschwindigkeit nicht möglich ist. Da Licht auch eine Signalwirkung hat und damit Information überträgt, gilt diese Annahme synonym auch für nutzbare Information. Schon Einstein plagte sich mit derlei Problemen, denn daraus entstünde eine Reihe bizarrer Skurrilitäten wie etwa das berühmte „Großvaterparadoxon": Wenn ich in die Vergangenheit reisen könnte, um meinen Großvater zu erschießen, wäre meine Mutter nicht geboren worden, und mich gäbe es dann gar nicht. Aus irgendeinem Grund sorgt die Natur immer wieder dafür, dass so etwas Paradoxes in unserer Welt niemals passiert. Dazu hat sie offenbar auch die Quantentheorie passend eingestellt, indem sie Gesetzmäßigkeiten wie No Cloning oder objektive Zufälligkeit geschaffen hat.

3.7 Schlusswort

Der Leser hat nunmehr die Skizze jener physikalischen Spielwiese kennengelernt, auf der die Technologie des Quanteninternets entstehen kann. Damit wird der wichtigste Teil der Anforderung erfüllt, welche die

Vision zur Verwirklichung bringt. Es ist ja bekanntlich eine Binsenweisheit, dass technologisch nur das umsetzbar ist, was die Naturgesetze auch hergeben. In diesem Fall zeigt sich die Natur von ihrer großzügigen Seite, indem sie die Gesichtspunkte der Informationstheorie maßgeblich erweitert. Das zukünftige Quanteninternet tauscht nicht nur algorithmische gegen physikalische Sicherheit, sondern erlaubt – auch abseits seiner hyperschnellen Koordinationsfähigkeit – die Vernetzung von Quantencomputern für dezentrale und modulare Berechnungen. Dabei kommen Methoden zum Einsatz, die weithin auf der Quantenteleportation beruhen. Die damit verbundene Repeatertechnik gestattet es, Quanteninformation über große Distanzen zu übertragen und in einem lokalen Quantenspeicher abzulegen. Damit öffnet sich eine neue Dimension in Sachen Datenrate, die alles in den Schatten stellt, was bislang möglich ist. Überraschend mag dabei wirken, dass die bizarr anmutende Quantentheorie die eigentliche Struktur dieser Welt widerspiegelt. Unsere alltägliche Welt ist demnach nichts weiter als das Ergebnis einer omnipräsenten Dekohärenz. Es entspricht der heutigen wissenschaftlichen Auffassung, dass die Quantenphysik die fundamentalste Beschreibung der Natur sein muss – oder aber sie ist Bestandteil einer übergeordneten Theorie, aus der sie als Spezialfall, wenn nicht gar als Axiom hervorgeht. Dies festzustellen ist vor allem deshalb wichtig, weil die Geschichte immer wieder gezeigt hat, dass fundamentale physikalische Entdeckungen in aller Regel eine revolutionäre Auswirkung auf die Menschheit haben.

Es mag für so manchen Leser enttäuschend wirken, dass ein Quanteninternet nicht zum ultimativen Streamen, Bloggen oder Spieledownload taugt. Auch wird der übliche Email- und Online-Geschäftsverkehr weiterhin auf Basis des klassischen Internets stattfinden. Doch erreicht der Datenschutz – gerade auch letztgenannter

Transaktionen – dank Quantentechnologie ein bislang unerreichtes Qualitätsniveau. Hier geht es vor allem um eine langfristige Sicherheit der IT-Systeme, wie sie bei Finanztransaktionen, in modernen Industriekonzepten, kritischen Infrastrukturen, zentralen Verwaltungssystemen sowie in zukünftigen Anforderungen der Mobilkommunikation notwendig sein wird. Davon profitiert schlussendlich die gesamte Gesellschaft. Dazu gilt es noch einmal festzuhalten, dass die aktuelle Sicherheit aufgrund bloßer algorithmischer Komplexität kein dauerhaftes Konzept sein kann. Verbesserungen in der Computerleistung können unvorhersehbar einsetzen und abrupte Veränderungen bewirken. Dies erfordert zeitnahe Forschung im Bereich von Algorithmen und Implementierungen. Dies schließt klassische wie auch quantenmechanische Verfahren ein. Die QKD erweist sich in Kombination mit derartigen Methoden als besonders verheißungsvoll. Quantenkommunikation kann zudem für eine Reihe weiterer Verfahren wie sichere Siegel Terminplanungen, oder Quantenauthentifizierung verwendet werden. Hier wird die Forschung nicht abreißen.

Ein noch in Ferne gerücktes Ziel verkörpert die zweite Essenz des Quanteninternets: Die Vernetzung leistungsfähiger Quantencomputer. Heute schon zeigen Quantensimulatoren sehr vielversprechendes Potenzial. Diese erlauben nicht nur tiefe Einsichten in die Welt komplexer Vielteilchensysteme, sondern es lässt sich grundsätzlich damit jedes Quantenproblem lösen, das mithilfe eines klassischen Rechners nicht effizient berechnet werden kann. Mit der Entdeckung topologischer Materialien entstehen zunehmend neue Chancen für festkörperbasiertes Computing. Die daraus gewonnenen Erkenntnisse können zu innovativen Technologien führen, von denen die Menschheit profitiert. Die Zusammenarbeit von Experimentalphysikern, Theoretikern und technologisch-industriellen

Arbeitsgruppen vermag die Realisierung eines technisch verwertbaren Quantencomputers gelingen lassen. Das ist wohl nur eine Frage der Zeit und der zur Verfügung stehenden Ressourcen. Der heutigen Einschätzung nach dürfte es innerhalb der nächsten 10–20 Jahre zu einem ersten echten Breakthrough kommen. Wirklich interessant sollte die Entwicklung aber erst um 2050 werden, wo sie rasant Fahrt aufnehmen könnte. Gut vorstellbar, dass ab dann sehr viele Menschen die Möglichkeit einer originären Quanten-Cloud nutzen. Programmierer auf der ganzen Welt helfen an der sukzessiven Optimierung, woraus noch völlig unbekannte Gesichtspunkte und Applikationen resultieren mögen. In jedem Fall erfordern Quantencomputer einen differenzierten Zugang und eine neue Denkweise, die nichts mehr mit der klassischen Art des Programmierens zu tun hat: Hier kündigt sich ein neues Zeitalter an. „Think quantum!" heißt schon heute das Motto im Research Lab von Google. Das könnte das Leitmotiv der nächsten Generation werden. Viele junge und kreative Menschen werden an diesem Prozess teilhaben und die Entwicklung vorantreiben. Jedes heute neugeborene Kind könnte bereits unmittelbar von dieser neuen Ära des Computer- und Internetzeitalters betroffen sein.

Als der CERN-Physiker Tim Berners-Lee Ende der 1980er Jahre das World Wide Web erfand, konnte er nicht ahnen, welche globale Revolution er damit auslösen würde. Physiker werden auch weiterhin die Geschicke der Menschheit nachhaltig beeinflussen, indem sie die maßgeblichen Inputs für hochinnovative Technologien liefern. Nach Hoimar von Ditfurth besteht die Aufgabe der Physik darin, die Welt ohne Wunder zu erklären. In diesem Bestreben musste sie notwendigerweise die Quantentheorie schaffen. Doch was sie impliziert, ist wundersam genug. So auch das technologische Wunderwerk, das keine Fiktion bleiben muss: Das universale Quantenhypernet.

Literatur

Einstein A, Podolsky B, Rosen N (1935) Can quantum-mechanical description of physical reality be considered complete. Phys Rev 47:777–780

Einstein A (1948) Quantenmechanik und Wirklichkeit. Dialectica 2:320–324

Herbert N (1982) FLASH – a superluminal communicator based upon a new type of quantum measurement. Found Phys 12:1171

Zeilinger A (2003) *Einsteins Schleier.* Beck, München, S 171

Zeilinger A (2005a) *Einsteins Spuk.* Bertelsmann, München, S 201 ff.

Zeilinger A (2005b) *Einsteins Spuk.* Bertelsmann, München, S 86

Zeilinger A (2005c) *Einsteins Spuk.* Bertelsmann, München, S 73

Wootters W, Zurek W (1982) A single quantum cannot be cloned. Nature 299:802

https://de.wikipedia.org/wiki/Ubiquitous_computing

https://www.oeaw.ac.at/detail/event/pan-jianwei-unter-top-ten-forschern/

https://www.nature.com/articles/nphoton.2017.107

G. Fürnkranz, *Vision Quanten-Internet*,
https://doi.org/10.1007/978-3-662-58453-8

https://www.youtube.com/watch?v=Pf92k-sfKdk&t=1349s
https://www.youtube.com/watch?v=XirbbUxOxiU
https://arxiv.org/abs/1103.3566
https://arxiv.org/abs/1801.06194
https://de.wikipedia.org/wiki/Schrödingers_Katze

Stichwortverzeichnis

G. Fürnkranz, *Vision Quanten-Internet*,
https://doi.org/10.1007/978-3-662-58453-8