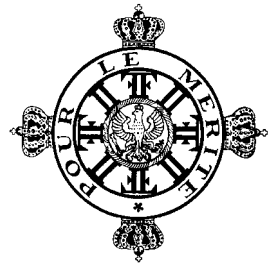
POUR LE MERITE

ANTON ZEILINGER

VOM BOHR-EINSTEIN-DIALOG ZUR QUANTENINFORMATION

Im Jahre 1899 hat Max Planck, später Kanzler des Ordens Pour le mérite, vorgeschlagen, daß es mit Hilfe einer von ihm entdeckten Naturkonstante, die heute Planckscheses Wirkungsquantum genannt wird, möglich ist, universelle Einheiten für Länge, Zeit, Masse und Temperatur zu definieren. Im Jahr 1900 konnte er dann mit der Hypothese, daß Energie zwischen einem Strahlungsfeld und einem Strahler nur in Vielfachen von $E = h\nu$, wobei ν die Frequenz des Strahlungsfeldes ist, ausgetauscht werden kann, das Spektrum der Hohlraumstrahlung – ein lange existierendes Problem – erklären. Einer der wenigen, die dies ernst nahmen, ernster als Planck selbst, war Einstein, bis 1933 Mitglied des Ordens, der 1905 vorschlug, daß Licht aus Teilchen, die später Photonen genannt wurden, besteht. Sowohl Planck als auch Einstein hatten jedoch von Anfang an realisiert, daß die Quantenphysik uns zwingt, von gewohnten Auffassungen über die Welt in einer grundsätzlichen Weise Abschied zu nehmen.

Mit der Entwicklung der modernen Quantentheorie als Matrizenmechanik durch Heisenberg im Jahr 1925 und als Wellenmechanik durch Schrödinger 1926, beide ebenfalls Träger des Ordens Pour le

mérite, setzte eine enorme Blütezeit der Physik ein. Es war plötzlich möglich, viele Dinge zu verstehen, wie zum Beispiel die Emission von Licht durch Atome, Magnetismus, eine unglaubliche Zahl von Phänomenen der Festkörperphysik und vieles mehr.
Gleichzeitig begannen damals Auseinandersetzungen um die konzeptive oder philosophische Deutung der neuen Theorie, die bis heute andauern. Viele dieser Debatten kreisten um Gedankenexperimente, da es damals noch nicht möglich war, detaillierte Experimente mit individuellen Quantenzuständen durchzuführen. Dies änderte sich in den 1970er Jahren aufgrund der technischen Entwicklung, insbesondere der Entwicklung des Lasers sowie des Entstehens von Hochleistungs-Forschungsreaktoren. Zahlreiche Experimente mit einzelnen Quantenteilchen konnten durchgeführt werden, die nicht nur die Vorhersagen der Quantenphysik bestätigt haben, sondern zu vielen neuen Fragestellungen führten. Diese frühen Experimente waren durchwegs aus dem Interesse an Grundlagen der Quantenphysik motiviert. Zur Überraschung aller an diesen frühen Experimenten Beteiligten legten diese Arbeiten, beginnend mit den 1990er Jahren, auch die Grundlagen zur Entwicklung des neuen Gebiets der Quanteninformatik. Die wichtigsten Konzepte hier sind der Quantencomputer, die Quantenkommunikation und Quantenteleportation.

Doppelspaltexperimente

Ein zentrales Instrument im Bohr-Einstein-Dialog[1] ist das Doppelspaltexperiment (*Abb. 1*). Das Phänomen ist im Prinzip sehr einfach. Von links tritt Strahlung ein, nehmen wir der Einfachheit halber Licht an. Es tritt durch den Spalt im ersten Schirm, dann kann es durch die beiden Spalte im zweiten Schirm treten und erzeugt ein Muster auf dem Beobachtungsschirm. Sind beide Spalte offen, so ergeben sich helle und dunkle Streifen entsprechend den Wellen, die durch beide Spalte durchtreten. Ist nur einer der beiden Spalte offen, treten keine Streifen auf, sondern nur eine gleichmäßige Vertei-

lung des Lichts. Nach Einstein überlegen wir uns nun, daß das Licht ja in Wirklichkeit aus Photonen besteht, und wir überlegen uns, das Experiment mit so schwachen Lichtintensitäten durchzuführen, daß immer nur ein Photon durch die Apparatur fliegt, nie mehrere gleichzeitig. Wir sammeln dann viele Photonen am Beobachtungsschirm auf. Einstein folgend muß nun jedes einzelne Photon einen der beiden Wege nehmen. Es kann daher nicht wissen, ob der andere Spalt offen ist, durch den es nicht durchgeht. Es sollten keine Interferenzstreifen auftreten. Einstein meinte, daß die Interferenzstreifen bei starkem Licht, die damals natürlich wohlbekannt waren, leicht zu erklären sind. Nach seiner Ansicht treten sie deshalb auf, weil viele Photonen gleichzeitig durch den einen oder den anderen Spalt treten und es auf diese Weise zu einer Wechselwirkung der Teilchen am Beobachtungsschirm kommt.

Dies ist ein Punkt, in dem Einstein schlicht unrecht hatte. Heute wissen wir, daß solche Interferenzphänomene auch auftreten, wenn die Intensitäten beliebig klein sind, wenn also wirklich nur ein Photon oder ein Teilchen anderer Art durch den Doppelspalt tritt. In *Abb. 2* sehen wir ein Doppelspaltinterferenzexperiment, das von uns vor vielen Jahren in Grenoble mit sehr kalten, also langsamen Neutronen aufgenommen wurde. Die Intensität des Neutronenstrahls war so gering, daß zu jedem Zeitpunkt praktisch nie mehr als ein Neutron auf dem Weg durch den Apparat war. Die insgesamt in der Beobachtungsebene aufgesammelten Neutronen zeigen jedoch die Maxima und Minima entsprechend den Interferenzstreifen[2]. Diese treten also entgegen der Erwartung Einsteins auch dann auf, wenn sich immer nur einzelne Teilchen im Apparat befinden.

Eine interessante Herausforderung heute ist, solche Phänomene für möglichst große Objekte zu realisieren. In *Abb. 3* sehen wir ein Doppelspaltinterferenzbild für Fullerene, in diesem Fall C70-Moleküle.[3] Auch hier genau das gleiche Phänomen, auch hier wieder Interferenz, obwohl nur ein einzelnes Molekül zu jeder gegebenen Zeit durch den Apparat tritt. Ist übrigens in jedem dieser Experimente nur ein Spalt offen, so treten die Interferenzstreifen nicht auf.

In der modernen Sprache ist es so, daß wir den einzelnen Teilchen

keinen Weg zuordnen dürfen ohne Messung. Das heißt, die Teilchen besitzen nur dann einen wohldefinierten Weg, wenn wir das Experiment so durchführen, daß der Weg tatsächlich bestimmt wird. Ist das nicht der Fall, so sprechen wir von Superposition der Wahrscheinlichkeitsamplituden der beiden Wege. Diese Superposition gibt einfach an, mit welcher Wahrscheinlichkeit das Teilchen wo gefunden werden kann. Es ist keine Aussage darüber, daß es sich vor der Messung bereits definitiv an diesem Ort befindet. Genauer ausgedrückt, tritt Interferenz dann auf, wenn keinerlei Information irgendwo im Universum vorhanden ist über den Weg, den das Teilchen nimmt. Es kommt nicht darauf an, ob diese Information von einem Beobachter zur Kenntnis genommen wird. Es reicht die Möglichkeit, diese Information zu bestimmen.
Von einer philosophischen Warte aus betrachtet, hat Einstein die Position vertreten, daß die Physik eine Wirklichkeit beschreiben muß, die unabhängig von der Beobachtung in allen ihren Eigenschaften vor der Beobachtung existiert. Die Messung kann höchstens die Beobachtung stören. Die Auffassung Niels Bohrs war es dagegen, daß das Thema der Physik primär ist, was über die Welt gesagt werden kann. Aussagen über die Wirklichkeit können, wenn überhaupt, nur im Kontext eines spezifischen Experimentes getroffen werden.

Kontextualität in der Quantenphysik

Überlegen wir uns folgendes Spiel: Ein Zauberer hat fünf Becher. Diese ordnet er in einem Fünfeck an (*Abb. 4*). Es ist nun die Aufgabe des Zauberers, die Kugeln so unter den fünf Bechern anzuordnen, daß möglichst oft verschiedene Farben, einmal Schwarz und einmal Weiß, auftreten, wenn er zwei benachbarte Becher hochhebt. Offenkundig kann, wie man sich bei Überlegung der *Abb. 4* leicht überzeugen kann, dies höchstens viermal der Fall sein. Wenn der Zauberer immer abwechselnd Schwarz und Weiß auf die Ecken legt, bleiben am Ende notwendigerweise zwei Becher übrig, die nebeneinanderliegend die gleiche Farbe zeigen. Um die Sache kurz zu machen,

wenn dies Quantenkugeln wären, so wäre es möglich, etwa 4,5mal Schwarz-Weiß zu haben! Dies ist natürlich nicht möglich, wenn die Kugeln ihre Farben besitzen, ehe wir sie beobachten.
Das Konzept geht auf einen Vorschlag von Klyachko et al.[4] zurück. Diese Autoren hatten vorgeschlagen, Messungen an Spin-1-Teilchen entlang fünf verschiedenen Richtungen durchzuführen. Ohne auf die Details eingehen zu können, ist es so, daß wir jeder dieser Messungen zwei Werte + 1 oder − 1, zuordnen können, entsprechend Schwarz und Weiß. Die Frage ist, ob die beobachteten Meßergebnisse dadurch erklärt werden können, daß das Quantensystem $\Psi 0$, in dem wir die Messungen durchführen, bereits vor der Messung definitive Information darüber trägt, was das Meßresultat über die einzelne Messung ist. Es stellt sich heraus, daß dies nicht möglich ist.
Das Experiment selbst wurde mit einzelnen Photonen durchgeführt. Im Experiment waren sie in einer Superposition von drei verschiedenen Wegen und nicht nur zwei wie beim Doppelspalt. Für jeden der drei Wege gibt es eine bestimmte Wahrscheinlichkeit, daß das Photon dort gefunden wird, wenn wir eine Messung durchführen. Das Ergebnis des Experiments[5] ist, daß die Wahrscheinlichkeit, das Photon auf dem dritten Weg zu finden, nicht unabhängig davon ist, welche Art von Messung am Photon auf den ersten beiden Wegen durchgeführt wird. Es hängt also die Wahrscheinlichkeit, das Photon in einem Weg zu finden, vom Kontext des gesamten Meßaufbaus ab und ist für sich nicht unabhängig davon gegeben. Unabhängig von diesem Kontext kann der Wahrscheinlichkeit, das Photon zu finden, keine unabhängige Realität zugeschrieben werden. Dies ist die Kontextualität der Quantenmechanik, die von Kochen und Specker entdeckt worden war.

Superposition, Zufall und Qubit

Das erste Mal kritisierte Albert Einstein die Quantenphysik bereits 1909 auf der Tagung der Gesellschaft Deutscher Naturforscher und Ärzte in Salzburg. Er drückte dort sein Unbehagen über die neue

Natur des Zufalls in der Quantenphysik aus. Er hatte bereits damals festgestellt, daß der Zufall in der Quantenphysik von einer qualitativ neuen Natur ist, nämlich daß es für das Einzelereignis keine kausale Erklärung gibt. Es ist so, daß es nicht unser Unwissen über die Details der Situation ist, wie in der klassischen Physik, sondern es ist ein objektives Fehlen einer Kausalität. Einstein drückte dies in einem berühmten Schreiben an Max Born, auch ein Ordensmitglied, vom 4. 12. 1926 so aus: »Jedenfalls bin ich davon überzeugt, daß der Alte nicht würfelt.«

In *Abb. 5* sehen wir, wie der quantenmechanische Zufall sehr schön in einem einfachen Experiment demonstriert werden kann. Der Aufbau besteht aus einer Lichtquelle und einem Strahlteiler und zwei Detektoren. Der Strahlteiler ist so beschaffen, daß er die Hälfte des Lichts reflektiert und die Hälfte des Lichts durchläßt. Sozusagen ein schlechter Spiegel. Mit dem Wellenbild ist das sehr leicht verständlich. Aber was geschieht, wenn wir uns klarmachen, daß aus der Lichtquelle einzelne Photonen emittiert werden? Führen wir das Experiment durch, stellen wir fest, daß die Hälfte der Photonen reflektiert und die andere Hälfte transmittiert wird. Es werden also mit der gleichen Wahrscheinlichkeit von 50 % die beiden Detektoren ein Photon registrieren. Stellen wir uns nun ein einzelnes Photon vor. Wird es reflektiert werden oder transmittiert werden? Die Quantenmechanik trifft dazu keine Aussage, sondern sie sagt, daß das Photon nach dem Strahlteiler in einer Superposition von beiden Möglichkeiten existiert, genau wie es in einer Superposition von den beiden Möglichkeiten im Doppelspalt existiert. Bei der Messung kann es jedoch nur einer der beiden Detektoren auslösen. Der quantenmechanische Zustand kollabiert. Welcher der beiden Detektoren auslösen wird, ist rein zufällig und hat keinerlei verborgene Ursache. Dies kann man sogar so weit treiben, daß man aus solchen Anordnungen Zufallszahlengeneratoren baut. Zufallszahlen sind ja sehr wichtig in vielen technischen Anwendungen, zum Beispiel für Optimierungsprobleme. Bezeichnen wir es als »0«, wenn der obere Detektor feuert, als »1«, wenn der untere feuert, so bekommen wir nach vielen Photonen eine wunderbare Zufallsfolge. Wie der irische Phy-

siker John Bell so schön formuliert hat, hat die heutige Physik keine Möglichkeit, zu erklären, warum spezifische Ereignisse geschehen, warum also spezifisch der eine und nicht der andere Detektor feuert. Dies nennt man das Meßproblem der Quantenmechanik. Es geht um den Übergang von Möglichkeit zu einer konkreten Wirklichkeit. Interessant ist nun, daß dieser Zustand für ein einzelnes Photon, der eine Überlagerung von beiden Möglichkeiten, »0« und »1«, enthält, eine Erweiterung des klassischen Konzepts des Bit als elementaren Trägers der Information bedeutet. Ein Quantenbit ist nicht entweder »0« oder »1«, sondern es kann in einer noch dazu beliebigen Überlagerung von »0« oder »1« existieren. Diese Möglichkeit ist zentral für die gesamte Quanteninformatik.

Verschränkung – Entanglement

Im Jahr 1935 veröffentlichte Albert Einstein gemeinsam mit Boris Podolsky und Nathan Rosen (EPR) den Artikel »Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?«, der sich als bahnbrechend erwies – dies jedoch erst nach ungefähr 30! bzw. 60!! Jahren!!! Einstein, Podolsky und Rosen überlegten sich den Quantenzustand von zwei Teilchen, die miteinander in Wechselwirkung stehen und dann auseinanderfliegen. Sie stellten fest, daß nach der Quantenmechanik diese beiden Teilchen durch einen einzigen gemeinsamen Quantenzustand repräsentiert werden. Dies bedeutet, daß die einzelnen Teilchen, jedes für sich, keinen eigenen Quantenzustand besitzen, also keine wohldefinierten Eigenschaften. Wegen des gemeinsamen Quantenzustandes verändert die Messung an einem der beiden Teilchen augenblicklich den Quantenzustand des anderen, unabhängig davon, wie weit dieses vom ersten entfernt ist. Einstein selbst nannte dieses Phänomen »spukhafte Fernwirkung«. Er sah ganz klar eine Spannung mit seiner Relativitätstheorie, nach der jede Wirkung sich höchstens mit Lichtgeschwindigkeit ausbreiten kann. Es muß daher eine Messung an einem Teilchen unabhängig davon sein, was zur gleichen Zeit woanders geschieht, insbeson-

dere, welche Messung am zweiten Teilchen durchgeführt wird. Dies ist die sogenannte Lokalitätsannahme, die von den Zuständen, die in der EPR-Arbeit untersucht werden, offenbar verletzt wird.
Weiters forderten EPR, daß das Meßergebnis die physikalische Realität widerspiegeln soll. Natürlich ist es sehr schwer, zu definieren, was man unter physikalischer Realität versteht. Nach EPR müssen solche Elemente der Realität zumindest dann existieren, wenn es möglich ist, ein Meßergebnis mit Sicherheit vorherzusagen. Im Falle unseres Teilchenpaares ist es tatsächlich möglich, aufgrund der Messung am ersten Teilchen bestimmte Meßresultate am zweiten mit Sicherheit vorherzusagen. Nachdem aber nun die Messung am ersten zum Beispiel entweder die Messung des Ortes oder des Impulses des Teilchens betrifft, ist es möglich, Ort und Impuls des zweiten Teilchens mit Sicherheit vorherzusagen, ohne mit diesem direkt in Wechselwirkung zu treten. Ort und Impuls können aber nach der Heisenbergschen Unschärferelation nicht gleichzeitig Realität besitzen. Daher, so das Argument von EPR, sei die Quantenmechanik unvollständig.
Einstein beklagte, daß in der EPR-Arbeit der wesentliche Punkt durch zuviel Gelehrsamkeit verborgen war. Er stellte diesen Punkt im wesentlichen später in seinen Autobiographischen Notizen klarer dar. Er bemerkt dort, daß je nach der Art der Messung am ersten Teilchen dem zweiten ein verschiedener quantenmechanischer Zustand zugeordnet werden muß. Die, wie Einstein sagt, »wirkliche faktische« Situation auf Teilchen 2 muß jedoch unabhängig davon sein, welche Art von Messung am ersten gemacht wird. Es kann daher, so Einstein, der quantenmechanische Zustand keine Beschreibung der Wirklichkeit sein.
Wie man in *Abb. 6* sieht, wurde die EPR-Arbeit lange Zeit weitgehend ignoriert und die Arbeit am Anfang nur äußerst selten zitiert. In den 1960er Jahren begann dann ein Anstieg, und in den 1990er Jahren kam es de facto zu einer Explosion der Zahl der Zitationen. Der erste Anstieg folgte der Entdeckung des Iren John Bell, daß die philosophische Position der EPR-Arbeit in Konflikt mit der Quantenmechanik steht und daher experimentell getestet werden kann.

Der zweite Anstieg kam, als sich herausstellte, daß solche quantenmechanischen Zustände zentral für Quantencomputer sind.
Einer der wenigen, die von der Einstein-Podolsky-Rosen-Arbeit Notiz nahmen, war Erwin Schrödinger. Er zitierte sie gleich zweimal im Jahr 1935, dem Jahr ihres Erscheinens. Zur Beschreibung der Quantenmechanik dieser Situation erfand er für das von Einstein »spukhaft« genannte Phänomen auf deutsch den Namen »Verschränkung«, auf englisch »entanglement«. Schrödinger arbeitete klar heraus, daß wir es hier mit einem neuen Phänomen zu tun haben. Die Quantenphysik gestattet klare Vorhersagen über gemeinsame Resultate an den beiden Teilchen, jedoch macht sie keinerlei Vorhersagen über die Meßresultate an jedem Teilchen getrennt. Jedes einzelne Meßresultat an jedem der Teilchen ist vollkommen zufällig, jedoch wenn an beiden Teilchen die gleiche Messung durchgeführt wird, erhalten wir ein perfekt korreliertes Resultat. Schrödinger nannte dies das »wesentliche Charakteristikum der Quantenphysik«.
Wie schon erwähnt, wurde die EPR-Arbeit über lange Zeit de facto ignoriert. Die darin dargelegten Probleme galten als »nur philosophisch«. Dies änderte sich mit dem Jahr 1964, als der irische Physiker John Bell zeigte, daß die Vorhersage der Quantenmechanik für verschränkte Systeme unter gewissen Voraussetzungen verschieden sind von den Vorhersagen, die man auf der Basis eines Modells à la EPR machen würde.
Der Gedankengang John Bells läßt sich leicht an einem im Prinzip einfachen Experiment erläutern. Eine Quelle sendet Photonenpaare aus, je ein Photon nach rechts oder nach links. Diese Photonen werden einer Polarisationsmessung unterworfen. Sie können entweder horizontal oder vertikal polarisiert sein, wie in *Abb. 7* angedeutet. Das Experiment zeigt nun, daß die Photonen entweder beide horizontal oder beide vertikal polarisiert sind. Man wäre nun geneigt, in einem klassischen Weltbild anzunehmen, daß ebendie Hälfte der Photonen mit horizontaler Polarisation, die andere Hälfte mit vertikaler Polarisation emittiert wird. Nach der Quantenmechanik ist es jedoch so, daß die Photonenpaare in einer Superposition emittiert

werden von zwei Zuständen. In dem eine Zustand sind beide Photonen horizontal, im anderen sind beide vertikal polarisiert. Sie tragen also für sich vor der Messung keine Polarisation. Messen wir eines der beiden, kollabiert der Gesamtzustand entweder darauf, daß beide Photonen vertikale oder beide horizontale Polarisation tragen.
John Bell hat nun die Frage gestellt, ob dieses Phänomen durch verborgene Eigenschaften der Systeme im Sinne des lokalen Realismus erklärt werden könne. Lokaler Realismus ist ebendie oben erläuterte philosophische Position der EPR-Arbeit. Er kommt zu dem Schluß, daß die perfekten Korrelationen sehr wohl innerhalb dieses Weltbildes erklärt werden können. John Bell geht nun einen Schritt weiter und überlegt sich, was auftritt, wenn die beiden Polarisatoren etwas zueinander gedreht sind. Dann ist horizontal/vertikal für das eine Photon nicht mehr das gleiche wie horizontal/vertikal für das andere Photon. Wenn wir daher zum Beispiel bei Messung an einem Photon die Antwort *horizontal* erhalten, ist das andere Photon nicht mehr mit Sicherheit ebenso horizontal polarisiert. Sondern es trägt diese Polarisation nur mit einer gewissen Wahrscheinlichkeit und ebenso mit einer gewissen anderen Wahrscheinlichkeit vertikale Polarisation.
Wir haben es also hier mit der seltenen Situation zu tun, daß eine philosophische Frage, nämlich, ob die Welt lokal und realistisch verstehbar ist oder nicht, im Prinzip durch Experimente entscheidbar ist. Solche Experimente wurden in den 1970er Jahren in verschiedenen Laboratorien begonnen und durchgeführt. Das erste Experiment war von Friedman und Clauser. Besonders hervorzuheben ist eine wunderschöne Serie von Experimenten von Aspect und Mitarbeitern in Paris.
Ein kürzlich von uns durchgeführtes Experiment zur Verschränkung über große Entfernungen[6] zeigt *Abb. 8*. In dem Experiment wurden Photonenpaare auf der Kanarischen Insel La Palma erzeugt. Eines dieser beiden Photonen schickte man über ein Teleskop nach Teneriffa. Das zweite Photon wurde lokal auf La Palma in einer Glasfaser gespeichert und etwas später gemessen. Die Messungen an den beiden Photonen wurden so durchgeführt, daß sie völlig unabhängig

voneinander waren, also so schnell, daß keine Information zwischen den beiden Messungen ausgetauscht werden konnte.
Weiters war es in diesem Experiment so, daß für jedes Photon die Entscheidung, welche Messung an ihm gemacht wird, getrennt durch einen eigenen Zufallszahlengenerator genau der Art, wie er oben beschrieben wurde, ausgewählt wurde. Auf La Palma befand sich dieser Zufallszahlengenerator etwa 1,2 km vom Ort, an dem die Messung dann durchgeführt wurde, entfernt. Die Zufallszahl wurde genau zu dem Zeitpunkt ausgewürfelt, als das Photonenpaar erzeugt wurde. So wurde zusätzlich jede Möglichkeit, selbst eine uns unbekannte, ausgeschlossen, daß die Quelle die Zufallszahl und damit die Art der Messung beeinflußt und umgekehrt. Auf Teneriffa wurde die Zufallszahl einfach ausgewürfelt, kurz bevor das Photon eintraf.
Auf diese Weise ist jede Informationsübertragung als Möglichkeit der Erklärung der quantenmechanischen Korrelationen ausgeschlossen. Das Experiment zeigte genau die Vorhersagen der Quantenmechanik und verletzte die Bellsche Ungleichung, das heißt, eine lokal realistische Erklärung ist auch hier ausgeschlossen. Bei den bisherigen Experimenten hätte es ja sein könnte, daß die Welt zwar lokal realistisch ist, das quantenmechanische Resultat jedoch durch eine unbekannte Kommunikation zwischen den verschiedenen Teilen des Apparats hervorgebracht wird. Diese Art von Experimenten wurde, wie gesagt, in den 1970er Jahren begonnen, um fundamentale Aussagen über die Wirklichkeit zu testen. Zur großen Überraschung begannen diese Resultate jedoch in den 1990er Jahren plötzlich bedeutsam zu werden für neue Formen der Kommunikation und der Informationsübertragung. Es entstand das neue Gebiet der Quanteninformatik.

Quanteninformation

In der gegenwärtigen Informationstechnologie und auch in der klassischen Informationstheorie ist der Repräsentant der Information im allgemeinen ein Bit, dessen beide Werte üblicherweise mit »0« und »1« bezeichnet werden. In der physikalischen Realisierung eines Computers entsprechen die beiden Zustände des Bits verschiedenen physikalischen Eigenschaften, zum Beispiel verschiedenen Magnetisierungen, verschiedenen Polarisationen von Licht, verschiedenen elektrischen Spannungszuständen und vielem mehr. Ein klassisches Bit muß immer eindeutig sein, das heißt, es muß gegenüber äußeren Störungen stabil sein.
Im Gegensatz dazu befindet sich das schon erwähnte Qubit (Quantenbit) in einer Superposition der Zustände »0« und »1«. Es gibt nun unendlich viele verschiedene Superpositionen von »0« und »1«, und damit kann ein Quantenbit sehr viel mehr Informationen tragen als ein klassisches Bit. Bei der physikalischen Realisierung eines Qubits in einem Quantencomputer nimmt man also bestimmte Quantenzustände. Den beiden Bitwerten können zum Beispiel verschiedene Energiezustände eines Atoms, verschiedene Spinzustände eines Elektrons, verschiedene Polarisationen eines Photons und vieles mehr entsprechen. Die quantenmechanische Darstellung der Information ermöglicht nun die Anwendung genau derjenigen fundamentalen Konzepte, die in den philosophischen Diskussionen im Vordergrund standen. Dies sind Superposition, Zufall, Komplementarität und Verschränkung.

Quantenkryptographie

In der Quantenkryptographie geht es darum, auf quantenmechanische Weise einen Schlüssel zu erzeugen, mit dem zwei Mitspieler, üblicherweise mit Alice und Bob bezeichnet, Information verschlüsseln und daher sicher austauschen können. In der auf Verschränkung basierten Quantenkryptographie (siehe *Abb. 9*) erzeugen Alice

und Bob viele Paare von verschränkten Photonen. Diese Photonen werden durch einen nichtlinearen optischen Kristall so erzeugt, daß sie dieselbe Polarisation zeigen, wenn sie gemessen werden, jedoch vor der Messung keine wohldefinierte Polarisation besitzen. Jedes dieser Photonen wird einer Polarisationsmessung unterworfen. Das einzelne Resultat wird daher rein zufällig entweder »0« oder »1« sein. Wichtig ist nun, daß aufgrund der Verschränkung für das zweite Photon ebenfalls genau das gleiche Resultat, eben »0« oder »1«, auftreten wird.

Wenn also Alice und Bob sehr viele Photonenpaare erzeugen, bekommen sie beide eine Zufallsfolge, die wegen der Objektivität des quantenmechanischen Zufalls maximal zufällig ist. Diese Zufallsfolge wird dann verwendet, um eine geheime Nachricht zu verschlüsseln und zu entschlüsseln. Das Wesentliche ist also an der Quantenkryptographie, daß der für die Verschlüsselung notwendige Schlüssel nicht von Alice zu Bob transportiert werden muß, sondern wegen der Verschränkung an beiden Orten gleichzeitig entsteht. Ein Abhörer könnte nun versuchen, sich in die Verbindungen zwischen Quelle und Alice bzw. zwischen Quelle und Bob einzuschalten, dort das Photon zu messen und ein entsprechendes Photon wieder auf den Weg zu schicken (siehe *Abb. 10*). Dabei bricht er aber die Verschränkung zwischen den beiden Photonen. Dies können Alice und Bob sehr leicht nachweisen, indem sie zum Beispiel überprüfen, ob ihre Daten nach wie vor die Bellsche Ungleichung verletzen.

Die so erhaltenen identischen Zufallsfolgen dienen für Alice und für Bob als Schlüssel. Zur Demonstration der Methode wurde ein Bild, in dem Fall die Venus von Willendorf, digitalisiert. Dieses Bild wurde von Alice zu Bob übertragen. Der Schlüssel, den Alice und Bob erhalten haben (Alice' Key und Bobs Key), ist identisch, wie schon die visuelle Inspektion zeigt. Die gezeigten Bilder sind einfach eine optische Darstellung von etwa 50.000 Bit an Information. Dieser Schlüssel wird nun Bit für Bit mit der Darstellung des Originals vermischt. Genauer ausgedrückt ist dies eine Addition modulo 2. Das verschlüsselte Bild (b) enthält keinerlei Struktur, da Alice' Schlüssel rein zufällig ist. Es kann leicht gezeigt werden, daß ein Schlüssel, der

rein zufällig ist und nur einmal verwendet wird, absolut sicher ist gegen Abhören. Bob kann die Nachricht leicht entschlüsseln und das Original leicht erhalten, indem er wieder seinen Schlüssel bitweise zu dem übermittelten Bild dazuzählt. Das erhaltene Abbild enthält noch einige wenige Fehler, die jedoch durch klassische Methoden beseitigt werden können.
Der technische Stand der Quantenkryptographie ist so, daß Entfernungen bis zu etwa 150 km überbrückt werden können. Viel größere Entfernungen sind derzeit nicht möglich, da Quantensignale nicht verstärkt werden können. *Verstärken* würde nämlich *Messen* bedeuten, und dies bedeutet in der Quantenmechanik eine Änderung des Zustandes. Eine langfristig hochinteressante Möglichkeit ist es, Satelliten zur Erzeugung des quantenkryptographischen Schlüssels einzusetzen. Ein solches Satellitenprojekt ist derzeit in Zusammenarbeit mit der Chinesischen Akademie der Wissenschaften in Planung.

Quantencomputer

In einem Quantencomputer würde die Information als Superpositionen bestehen. Ein Quantencomputer kann daher sehr viele verschiedene Inputs in Überlagerung bearbeiten. Man spricht hier von einem massiven Parallelismus. Der Ablauf des Rechenprogramms bedeutet nun eine physikalische Evolution dieses Quantenzustandes. Dabei kann die Art der Wechselwirkung der Quantenbits untereinander gesteuert werden. Die richtige Wahl der Wechselwirkung ist dafür verantwortlich, daß das gewünschte Programm abläuft.
Quantencomputer wären wegen des Parallelismus allein schon sehr viel schneller als existierende Computer. Zusätzlich gibt es Probleme, die in bestehenden Computern von exponentieller Komplexität sind. Das sind Probleme, bei denen der Aufwand an Ressourcen, also etwa an Rechenkapazität oder Speicherkapazität oder Rechenzeit, exponentiell ansteigt mit der Größe des Inputs. Der

exponentielle Anstieg bedeutet wiederum, daß kein klassischer Computer denkbar ist, der das Problem lösen kann, und sei er so groß wie das Universum.
Einige Probleme, die für den klassischen Computer exponentiell komplex sind, sind für den Quantencomputer nur polynomisch komplex, werden also als lösbar angesehen. Dazu gehört etwa die Primzahlfaktorisierung, also die Zerlegung großer Zahlen in ihre Primfaktoren, oder auch die Suche in einer ungeordneten Datenbasis.
Die Entwicklung von Quantencomputern ist ein weltweit sehr aktives Forschungsgebiet. Es gibt viele verschiedene Grundbausteine, auf denen Quantencomputer aufgebaut sein könnten. Untersucht werden etwa Ionen als Träger als Qubits, Atome, Festkörperquantenpunkte, supraleitende Quantenzustände, photonische Zustände und vieles mehr. Der Stand heute ist, daß man Quantencomputersysteme von der Größenordnung von 10 bis 20 Qubits realisieren kann und es keinen fundamentalen Grund gibt, warum die Entwicklung nicht zu sehr viel größeren Zahlen von Qubits weitergehen sollte.
Ein hochinteressantes Konzept, das vor kurzem experimentell Verwirklichung fand, ist das eines blinden Quantencomputers. Das Szenario ist folgendes. Nehmen wir an, wir haben ein künftiges Quanteninternet, in dem einige zentrale große Computer als Server existieren, die die volle quantenmechanische Rechenkapazität besitzen. An diesem Quantencomputer möchten verschiedene Kunden ihre Rechenoperationen durchführen und ihre Aufgaben erledigen. In den heutigen Realisierungen von Cloud Computing muß der Kunde davon ausgehen, daß der Betreiber des zentralen Rechners fair und korrekt vorgeht und sich nicht ansieht, was der Kunde tatsächlich macht. Dies ist natürlich ein großer Unsicherheitsfaktor. Bei einem künftigen Quantencomputer wäre dies anders. Es ist möglich, einen Quantencomputer so zu betreiben, daß nur der Kunde weiß, was gerechnet wird, und der Betreiber des Quantencomputers keinerlei Möglichkeit hat, nicht einmal im Prinzip, herauszufinden, welche Art von Problem der Kunde behandelt. Zusätzlich weiß er natürlich auch nicht, welche Daten der Kunde verwendet.

Das Prinzip von Blind Quantum Computing ist relativ einfach. Der Kunde muß lediglich über die Möglichkeit verfügen, beliebige Quantenbits herzustellen und dem zentralen Server zu schicken. Der zentrale Server erzeugt nun sein Quantenrechenregister dadurch, daß er diese Quantenbits, die ihm der Kunde geschickt hat, miteinander verschränkt. Ein bestimmter Algorithmus wird nun dadurch verwirklicht, daß an diesem hochverschränkten Quantensystem eine spezifische Abfolge von Messungen durchgeführt wird. Das Endprodukt dieser Messungen ist das Rechenergebnis. Da nun der Kunde die Quantenzustände beliebig präparieren kann und dies dem Server nicht mitteilt, weiß der Server nicht, aus welchen Quantenbits sein Rechenregister aufgebaut wird, und kann dies auch durch Messung nicht herausfinden. Jede Messung würde ja den Zustand der Quantenbits stören und die Rechnung unmöglich machen. Diese Idee von Broadbent, Fitzsimons and Kashefi[7] ist wahrscheinlich eine der interessantesten im Quantum Computing. Kürzlich haben wir in meiner Gruppe gezeigt, daß dies im Prinzip möglich ist.[8]

Ausblick

Die großen Herausforderungen für Quanteninformatik sind derzeit primär technologischer Natur. Zum einen gilt es, Quantenkommunikation über größere Entfernungen zu ermöglichen, um die Datenraten zu erhöhen. Es gibt keinerlei Grund, warum dies nicht im Prinzip möglich sein sollte. Es erfordert natürlich einen entsprechend hohen technischen Entwicklungsaufwand.
Ähnliches gilt für den Quantencomputer. Dort ist zentral die Frage der Dekohärenz, das heißt der möglichen Zerstörung des Quantenzustandes eines solchen Computers durch Wechselwirkung mit der Umgebung. Es gibt jedoch Quantensysteme, die gegen Dekohärenz sehr robust sind, zum Beispiel die photonischen Systeme, wie sie in Blind Quantum Computing verwendet werden. Wenn man aus der Entwicklung neuer Technologien etwas lernen kann, dann ist es, daß es am Beginn vollkommen unvorhersehbar ist, zu welchen An-

wendungen es tatsächlich führen wird. So galt etwa der Laser lange Zeit als die ideale Lösung für Probleme, die man noch nicht kannte. Auch bei der Entdeckung von Radiowellen durch Heinrich Hertz kam es niemandem in den Sinn, daß dies zu Informationsübertragung verwendet werden könnte.

Wie schwer man nicht nur die Zukunft vorhersagen kann, sondern sogar die wissenschaftliche Bedeutung von etwas, das man selbst gefunden hat, kann man dem berühmten Brief entnehmen, den Planck, Nernst, Rubens und Warburg am 12. Juni 1913 an die Preußische Akademie der Wissenschaften richteten. In diesem Brief schlugen sie die »Erwählung des Ordentlichen Professors der Theoretischen Physik an der Eidgenössischen Technischen Hochschule in Zürich, Dr. Albert Einstein, zum Ordentlichen Mitglied der Akademie« vor. Nach einer Würdigung seiner Leistungen kommt folgender bemerkenswerte Satz: »Daß er in seinen Spekulationen gelegentlich auch einmal über das Ziel hinausgeschossen haben mag, wie zum Beispiel in seiner Hypothese der Lichtquanten, wird man ihm nicht allzu schwer anrechnen dürfen; denn ohne einmal ein Risiko zu wagen, läßt sich auch in der exaktesten Naturwissenschaft keine wirkliche Neuerung einführen.« Bemerkenswert ist, daß dies 8 Jahre nach dem Vorschlag Einsteins zu Lichtquanten geschah und daß die Unterzeichner Planck einschlossen, von dem die Quantenhypothese stammt, und Rubens, der die Experimente zur Schwarzkörperstrahlung, die Planck zur Entdeckung geführt hatte, gemacht hatte. Wir sollten uns also genauso fragen, wo wir heute unsere Fantasie nicht offen genug spielen lassen.

Anmerkungen

1 N. Bohr, *Discussion with Einstein on Epistemological Problems in Atomic Physics*, in: »Albert Einstein: Philosopher-Scientist«, von P.A. Schilpp, Evanston: Library of Living Philosophers, Inc. (1949).

2 A. Zeilinger, R. Gähler, C.G. Shull, W. Treimer & W. Mampe, *Single and Double Slit Diffraction of Neutrons,* Rev. Mod. Phys. 60 (1988) S. 1067-1073.

3 M. Arndt, O. Nairz, J. Voss-Andreae, C. Keller, G. van der Zouw & A. Zeilinger, *Wave-particle duality of C60 molecules*. Nature 401 (1999) S. 680-682.
4 A. A. Klyachko, M. A. Can, S. Binicioğlu, S. & A. S. Shumovsky, *Simple Test for Hidden Variables in Spin-1 Systems*. Phys. Rev. Lett. 101 (2008) S. 20403.
5 R. Lapkiewicz, P. Li, C. Schaeff, N. K. Langford, S. Ramelow, M. Wieśniak & A. Zeilinger, *Experimental non-classicality of an indivisible quantum system*. Nature 474 (2011) S. 490-493.
6 T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein & A. Zeilinger, *Violation of local realism with freedom of choice*. Proc. Natl. Acad. Sci. USA 110 (4) (2013) S. 1221-1226.
7 A. Broadbent, J. Fitzsimons & E. Kashefi, *Universal blind quantum computation*. In: »Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)« S. 517-526 (2009).
8 S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, P. Walther, *Experimental Demonstration of Blind Quantum Computing*, Science 335, 303 (2012).

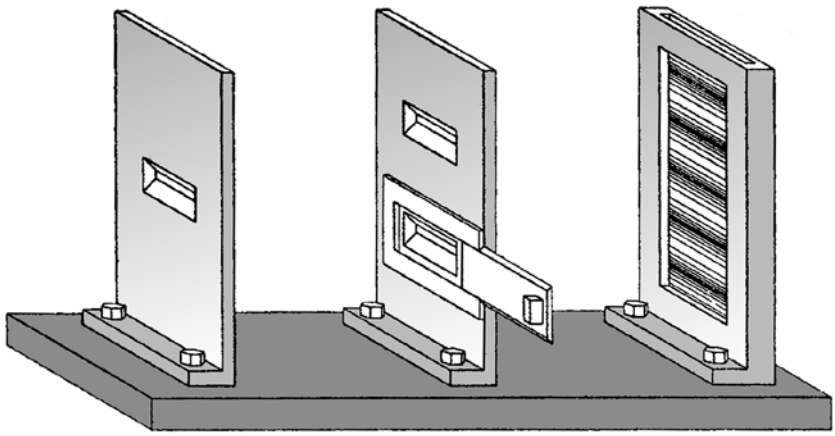

Abb. 1: Das Doppelspaltexperiment in einer Zeichnung von Niels Bohr, nachgedruckt aus Referenz 1. Von links kommendes Licht (oder auch eine andere Art von Teilchen) kann durch beide Spalte im zweiten Schirm treten. Sind beide Spalte offen, treten im dritten Schirm Interferenzstreifen auf. Ist nur einer offen, beobachtet man eine gleichmäßige Verteilung des Lichts.

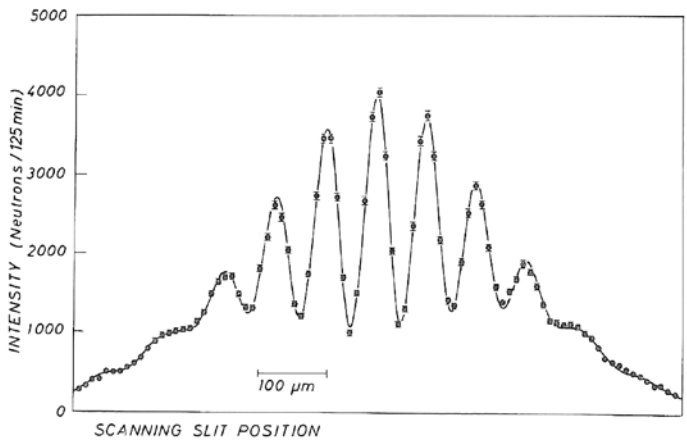

Abb. 2: Doppelspaltinterferenz mit kalten Neutronen (Referenz 2). Die Minima und Maxima sind die Interferenzstreifen. Das Experiment wurde mit vielen einzelnen Neutronen durchgeführt.

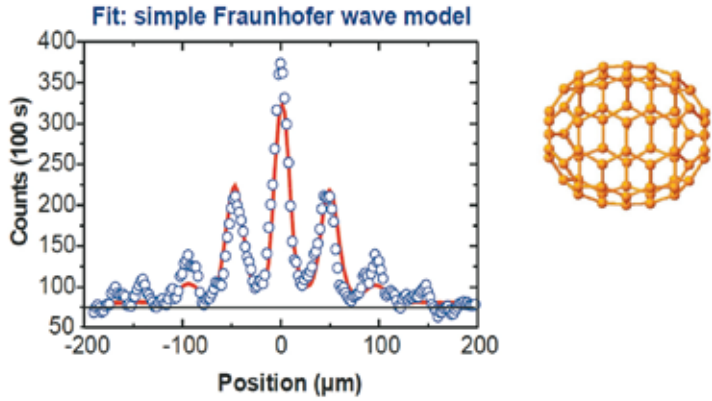

Abb. 3: Doppelspaltinterferenz mit Fullerenen (Referenz 3). C70-Moleküle aus Kohlenstoff (rechts) zeigen genau dieselben Interferenzstreifen, wie sie etwa auch Licht zeigt.

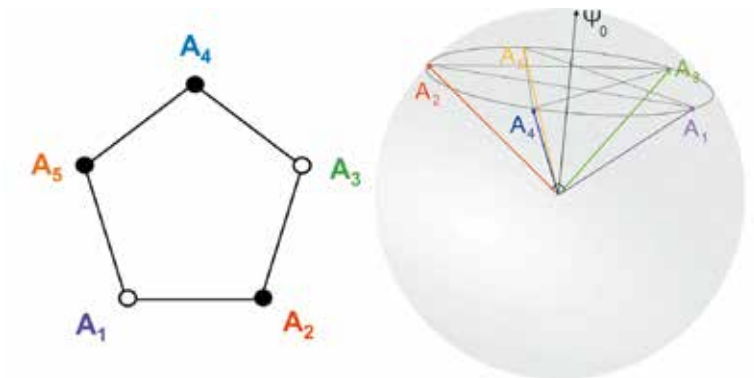

Abb. 4: Ein Gedankenexperiment mit schwarzen und weißen Kugeln (links) und seine quantenmechanische Realisierung (rechts) (Referenz 4, 5). In dem Experiment nach der klassischen Physik (links) ist es unmöglich, auf die Ecken eines Fünfeckes schwarze und weiße Kugeln so hinzulegen, daß öfter als viermal auf benachbarten Ecken eine weiße und eine schwarze Kugel liegt. In der quantenphysikalischen Realisierung (rechts) mißt man den Spin von Spin-1-Teilchen entlang vier verschiedenen Richtungen, wie gezeigt. Die Teilchen befinden sich im quantenmechanischen Zustand Ψ_0. Die Meßwerte – analog zu den Farben der Kugeln – existieren nicht vor der Beobachtung. In diesem Fall ist es möglich, öfter als viermal »verschiedene Farben« zu haben.

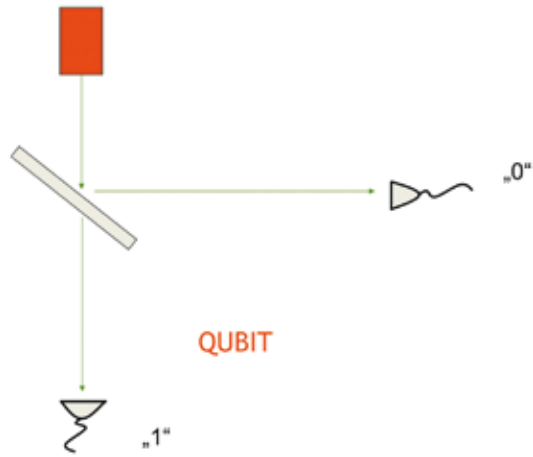

Abb. 5: Illustration des quantenmechanischen Zufalls mit einem Strahlteiler.

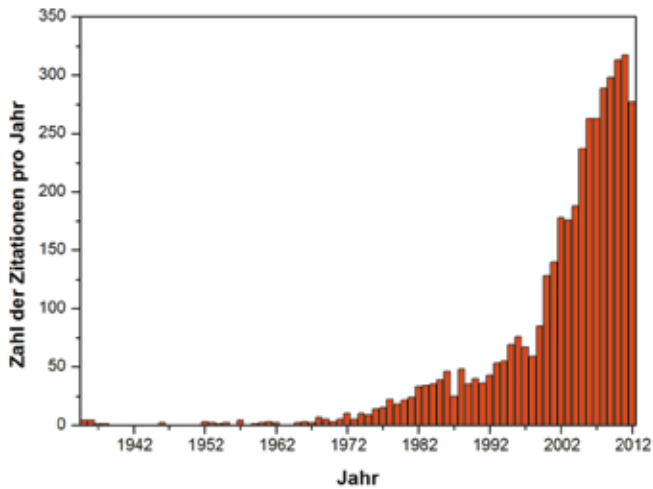

Abb. 6: Zitationen der EPR-Arbeit.

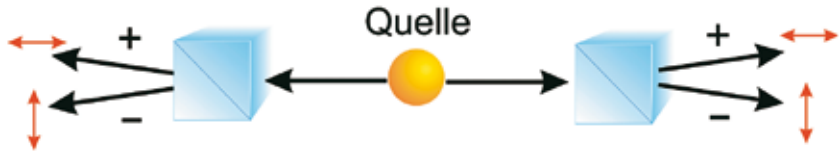

Abb. 7: Polarisationsmessungen an verschränkten Photonenpaaren.

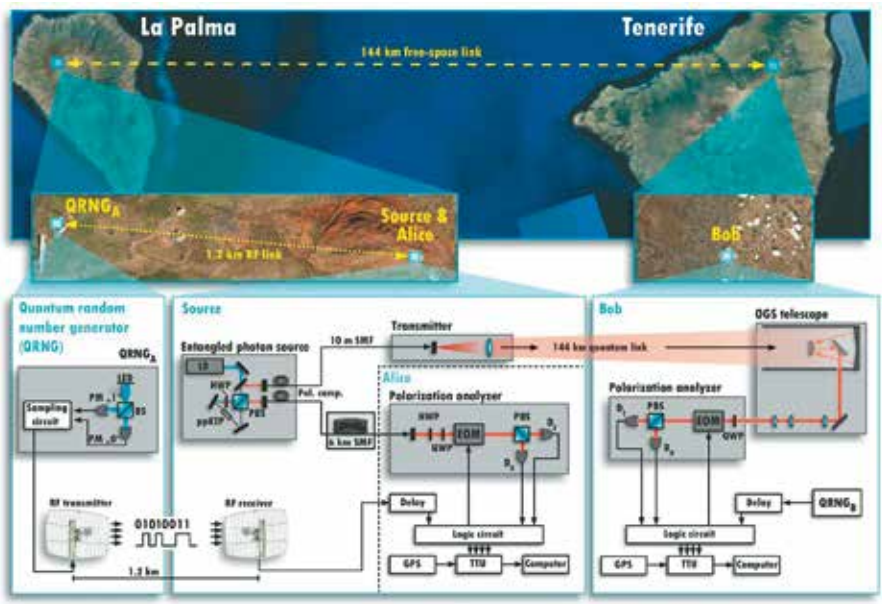

Abb. 8: Experiment zum Test der Bellschen Ungleichung über große Entfernungen zwischen den Kanarischen Inseln La Palma und Teneriffa (Referenz 6).

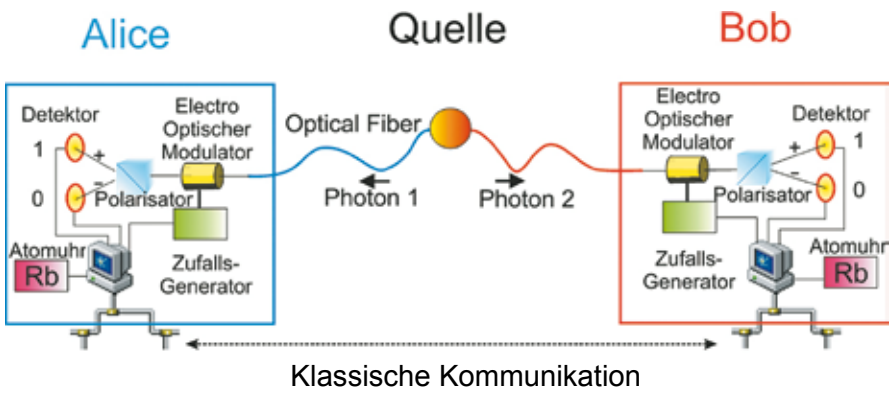

Abb. 9: Quantenkryptographie durch Verschränkung.

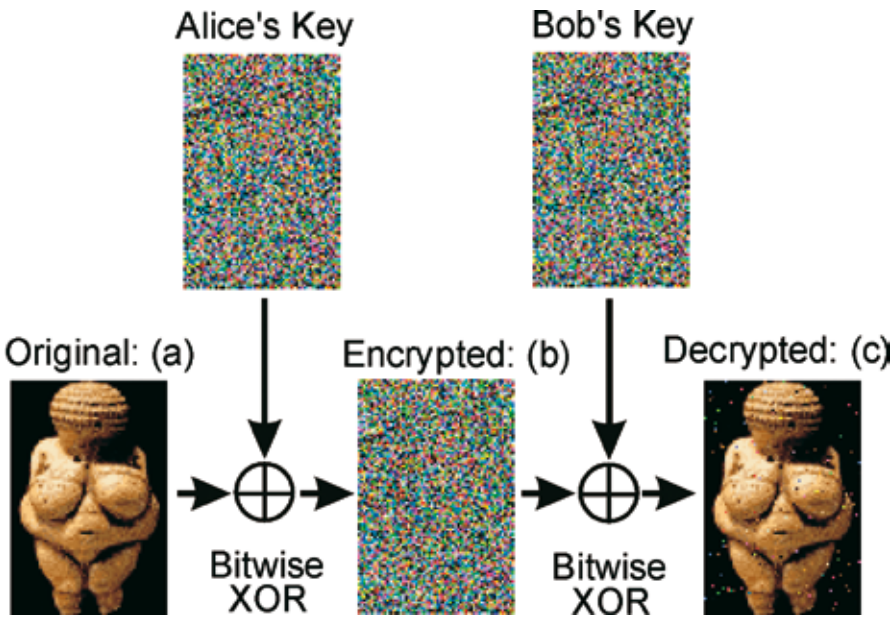

Abb. 10: Erste auf Verschränkung basierende Quantenkryptographie.