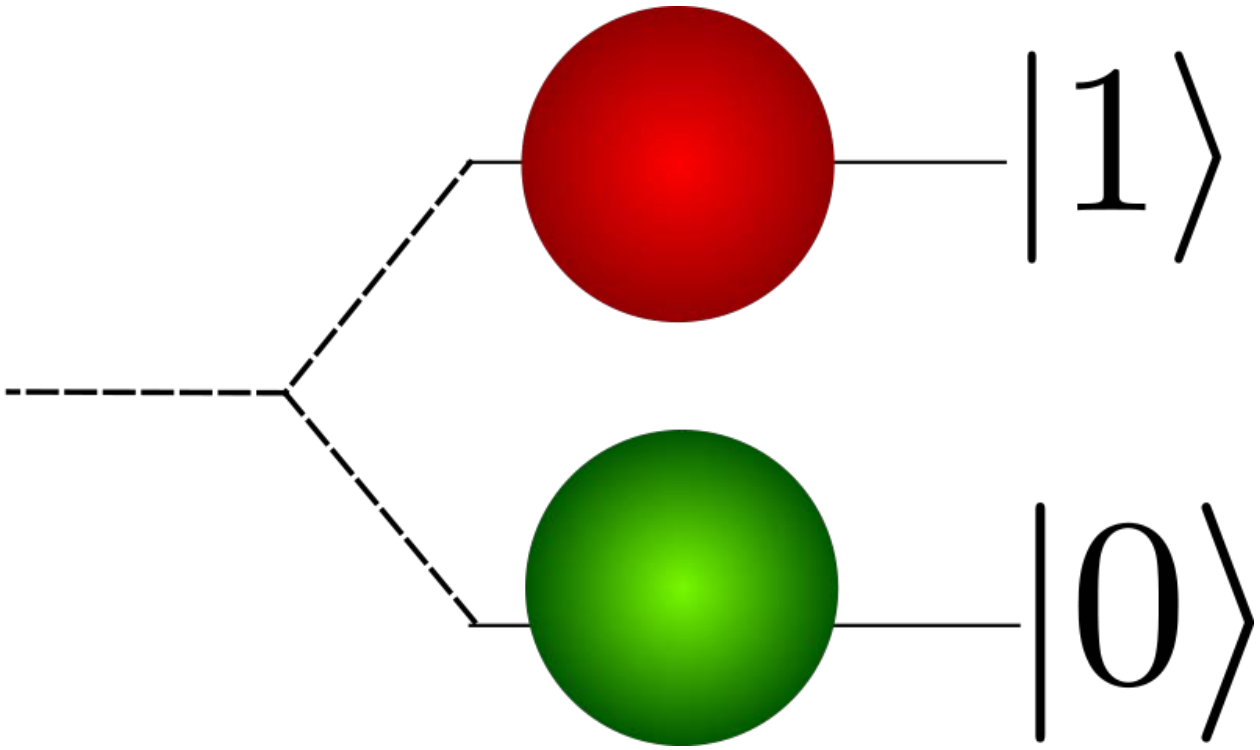
QUANTUM COMPUTING

Zusammenfassung für den Physikunterricht

Franz Kopica



23.01.2009 17:19

Inhaltsverzeichnis

1 Einleitung

Zwei bedeutende wissenschaftliche Revolutionen des 20 Jahrhunderts die theoretische Informatik, vertreten durch Wissenschaftler wie Alan Turing, und die Quantenmechanik, vertreten durch den österreichischen Nobelpreisträger Erwin Schrödinger, wurden in den letzten Jahrzehnten zu einem interdisziplinären Zweig mit dem Namen Quantum Computing zusammengeführt.

Wichtige Auslöser warum Quantencomputer entwickelt und gebaut werden sollen lauten:

- Computer, die den Gesetzen der Quantenmechanik[1] unterworfen sind, können Rechenaufgaben erledigen welche ein klassischer Rechner nicht zu lösen vermag.
- Schätzungen zur Folge werden die Bauteile unserer Rechner vor 2020 die Größe eines einzelnen Atoms erreichen, wodurch die Gesetze der klassischen Physik nicht mehr gelten.

Die sich gegenwärtig im einsatzbefindlichen Computer funktionieren nach den gleichen Grundprinzipien wie die mechanischen Rechenmaschinen, welche noch bis Ende der 1970er Jahre im Einsatz waren[1].

Die Quantenmechanik eröffnet uns neue, faszinierende Perspektiven für den gesamten IKT-Bereich. Experimente, welche als grundlegende Tests der Quantentheorie vorgesehen waren, liefern nun die Bausteine für die Quantentechnologie. Die Entwicklung neuer Ansätze ermöglichen uns die seltsamen Eigenheiten der Quantenwelt wie Nichtlokalität, Überlagerungsprinzip und Unschärferelation nutzbar zu machen und neuartige Anwendungen zu entwickeln. [5].

1.1 Geschichte des Quantencomputer

Die Überlegung, dass Quantencomputer Fähigkeiten haben könnten welche dem klassischen Rechner fehlt ist vom amerikanischen Physiker und Nobelpreisträger Richard P. Feynman. Im Jahr 1982 publizierte er seine Arbeit wie sich ein Quantencomputer simulieren lasse.

David Deutsch gelang der theoretische Durchbruch 1985, als er eine Turingmaschine modelliere, welche die Gesetzte der Quantenmechanik umsetzt. Zur Erinnerung eine Turingmaschine erlaube auf einem Band nur die eintrage 0 und 1. Seine jedoch lässt Superpositionen (s.Pkt. 1.2) zu.

1.1.1 Historische Entwicklung des Quantencomputer

Dazu ein paar wichtige Daten:

- 1982 **Feynman** referiert über Bau von Quantencomputer.
- 1985 **Deutsch** stellt ein theoretisches Modell des Quantencomputers auf.

[1] Die Quantenmechanik ist eine der Hauptsäulen der modernen Physik und bildet die Grundlage für viele ihrer Teilgebiete, so z. B. für die Atomphysik, die Festkörperphysik und die Kern- und Elementarteilchenphysik, aber auch für verwandte Wissenschaften wie die Quantenchemie. Während sich die klassische Physik als ungeeignet zur Beschreibung der Eigenschaften sehr kleiner Systeme erwiesen hat, erlaubt die Quantenmechanik die sehr präzise Berechnung der physikalischen Eigenschaften von Atomen, Molekülen, Festkörpern und einfachen biologischen Systemen. Ihre praktische Anwendbarkeit ist dabei nur durch die zu den erforderlichen Rechnungen verfügbare Rechnerleistung begrenzt [Quelle: http://de.wikipedia.org/wiki/Quantenmechanik].

- 1994 **Shor** findet den effizienten Quantenalgorithmus zur Faktorisierung.
- 1996 **Grover** konstruiert einen Quantensuchalgorithmus.
- 1997 **Zeilinger** gelingt die erste Quantenteleportation.
- 1998 Quantencomputer führt einfachste Rechnung durch.

1.2 Grundlagen

Quantencomputer arbeiten mit der Verarbeitungseinheit Qubit. Diese Einheit - der Quantenzustand - kann nicht kopiert werden. Ein Verfahren, bei dem es dennoch möglich ist, ein Qubit von einem Quantencomputer auf einen anderen über eine Distanz von einigen hundert Metern zu übertragen, wird als Quantenteleportation bezeichnet. Dazu muss Gebrauch von der Quantenverschränkung gemacht werden

Ein klassischer Computer kennt für ein Bit nur die beiden Zustände 0 oder 1. Ein Quantencomputer rechnet mit dem Grundbaustein des Quantencomputer, dem Quantenbit (Qubit). Die Schreibweise dieser Basiszustände erfolgt für

$$|0\rangle \text{ und } |1\rangle$$

So ein Quantenbit kann dabei diese beiden Werte gleichzeitig annehmen. Das Quantenbit kann genau genommen, sich in diesen beiden Zuständen gleichzeitig befinden. Dabei handelt es sich und die sogenannte *Superposition.* Diese besagt, dass sich zwei beliebige Zustände, zu einem bestimmten Zeitpunkt, mit diversen Masszahlen einen neuen möglichen Zustand definieren,

Ein klassischer Rechner kann mit *n* Bits 2^n verschiedenste Zahlen darstellen, aber zu jedem Zeitpunkt nur eine davon speichern. Der Quantencomputer ist in der Lage mit ebenso vielen Quantenbits 2^n Zahlen gleichzeitig darzustellen. Auch die Unterscheidung, dass Quantencomputer etwas ganz anderes als Parallelrechner sind ist wichtig.

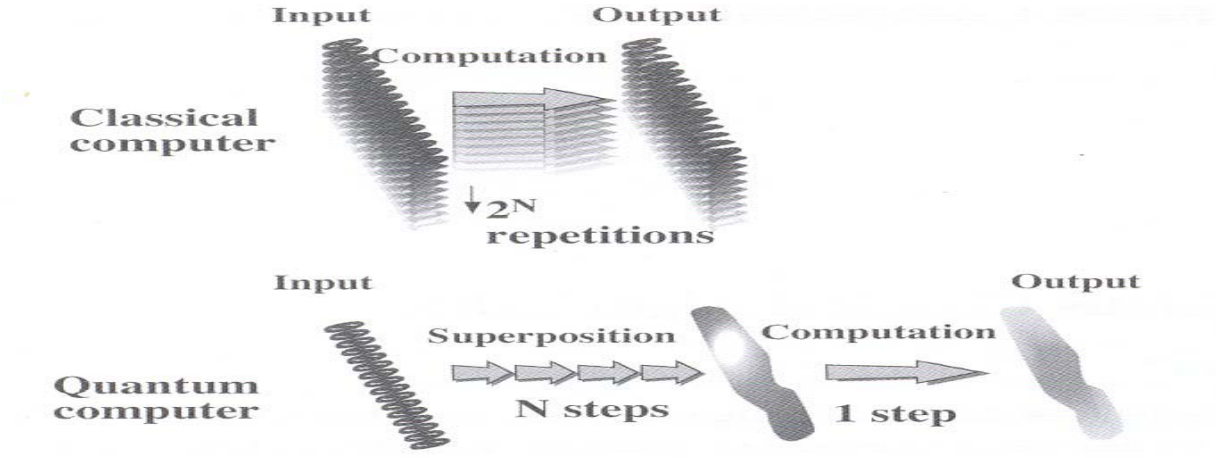


Figure 8.1: Differences in classical and quantum algorithms.

Quelle: [1]

Die Welt der Quantenmechanik ist so zerbrechlich und extrem empfindlich. Alleine der Versuch ein Quantenbit zu lesen bewirkt, dass es seinen Zustand beeinflusst. Eine Messung zerstört auch die Superposition, und das Rechenergebnis wird eher zufällig zurück gemeldet. Wir erhalten auch keine Information darüber zu welcher der gleichzeitig ausgeführten Berechnungen es gehört. Um aus einer solchen Superposition die gewünschte Information zu erhalten bedient man sich der sogenannten Interferenz[2].

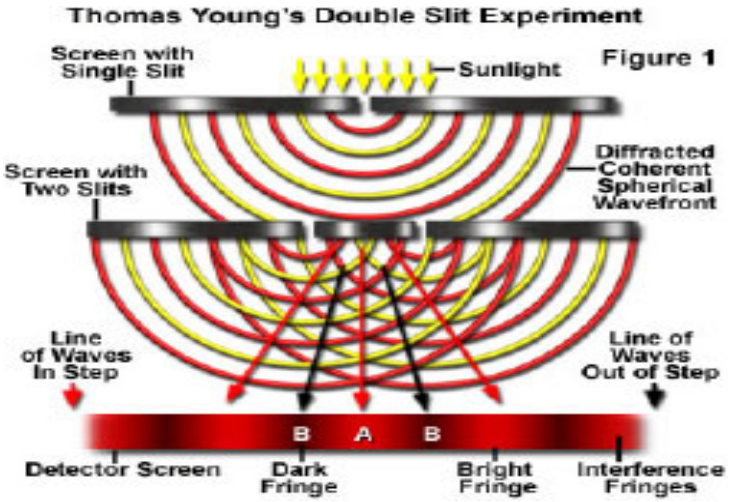


Abb.Interferenz (Quelle:GNU Free Documentation License.)

1.2.1 Superposition und Dekohärenz

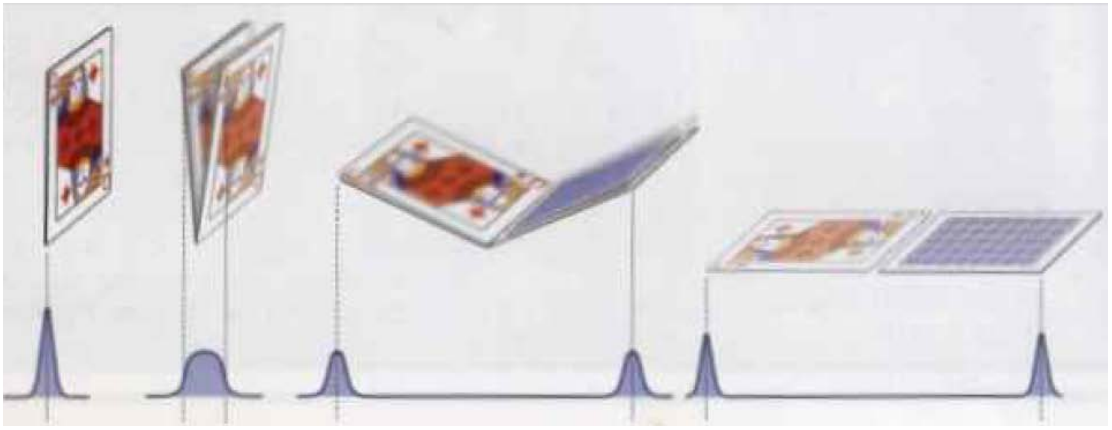
Ein klassisches Teilchen kann sich nur in einem bestimmten Zustand befinden. Ein Photon kann z.B. verschiedene Polarisationen[3] haben, aber immer nur eine in einem bestimmten Augenblick Ein klassisches Teilchen befindet sich immer im definierten Zustand. Da Quantenobjekte sowohl Teilchen- als auch Welleneigenschaften besitzen, ermöglichen diese Welleneigenschaften eine Überlagerung anderer möglichen Zustände, d.h. alle Zustände können gleichzeitig angenommen werden. Diesen Zustand der Überlagerung nennt man Superposition.

Der berühmte Physiker Schrödinger hat sich dazu ein hervorragendes und gleichzeitig makaberes Gedankenexperiment ausgedacht: "Schrödingers Katze". Ein Detektor, ein Atom ein Hammer, sowie ein Gefäß mit einer giftigen Substanz und eine Katze befinden sich in einer Kiste. Sobald das Atom zerfällt, registriert der Detektor dies bewegt den Hammer. Und dieser zerstört das Gefäß, wodurch das Gift freigesetzt wird, welches die Katze tötet. Solange die Kiste aber geschlossen ist und der Betrachter daher nicht sehen kann, ob die Katze noch lebt, befindet sie sich also in einem "Zwischenzustand" zwischen lebendig und tot, also in einer Superposition der beiden Zustände.

[2] Beschreibt die Überlagerung von Wellen

[3] Polarisation nennt man den Zustand, bei dem in einem insgesamt elektrisch neutralen Körper (das kann auch ein Molekül sein) positive und negative Ladungsträger so gegeneinander verschoben sind, dass der Körper wie ein Dipol wirk. (Dipol = Anordnung zweier dem Betrag nach gleich großer, jedoch vorzeichenmäßig entgegengesetzte Ladungen) [Quelle: http://www.chemieonline.de/forum/].

Wird die Kiste aber geöffnet sieht man, ob die Katze noch lebt. Es wird also aus der Superposition ein "reiner Zustand", also ein klassischer. Dies nennt man "Dekohärenz". Jede "Messung" an einer Superposition führt dazu, dass dieses Teilchen wieder einen eindeutigen Zustand annimmt, und zwar zufällig einen der Zustände, die in der Superposition möglich sind. Eine Messung ist jede Interaktion mit der Umwelt, z.B. bereits das Auftreffen von Photonen. Die Dekohärenz macht auch ein "Klonen", also die Verdoppelung eines beliebigen Quantenzustandes unmöglich, da eine Messung die Superposition zerstören würde.



Superposition am Beispiel einer Spielkarte [6]

Durch Messung (= Wechselwirkung mit einem Photon) wird die Spielkarte dekohärent. Sie liegt auf einer Seite

1.2.2 Mathematische Begriffe und Aussagen

Um ein besseres Verständnis für Quantencomputer zu entwickeln bedient man sich mathematischer Grundlagen, mit welchen jeder Schüler in Laufe seiner schulischen Ausbildung zu tun hat bzw. haben wird.

1. Komplexe Zahlen
2. Vektorräume
   a. Basen und Unterräume
   b. Abstände und Winkel im Vektorraum
   c. Projektionen
3. Matrizen
4. Kombinatorik und Wahrscheinlichkeit
5. Zahlen
   a. Teiler und Vielfaches
   b. Modulares Rechnen
   c. Division

1.3 Quantencomputer

Die Verschränkung von einzelnen elementaren Trägern von Information - Quantenbits (Qubit) - ist die Basis für einen zukünftigen Quantencomputer (lateinisch quantum, Menge), der dazu fähig ist, mehrere Berechnungen nicht wie ein klassischer Siliziumchip seriell, sondern parallel durchzuführen. Ein Quantencomputer kann prinzipiell genau dieselben Probleme berechnen wie ein klassischer Computer. Allerdings ist ein

Quantencomputer bei einer bestimmten Klasse von Problemen schneller als ein klassischer Computer.

Der Quantencomputer ist ein überwiegend theoretisches Konzept. Es existiert eine Vielzahl von Vorschlägen, wie ein Quantencomputer realisiert werden könnte. Im kleinen Maßstab wurden einige dieser Konzepte im Labor erprobt und auch Quantencomputer mit wenigen Qubits realisiert; von einer tatsächlichen Anwendung und praktischem Nutzen ist man noch weit entfernt.

1.3.1 Anforderung

David Deutsch hat 1985 die Anforderungen, welcher ein Quantencomputer erfüllen muss wie folgt formuliert:

Der Quantencomputer besteht aus einer Reihe von Qubits(Quantenbit,

1. die in einen Anfangszustand versetzt werden können z.B. |0› ,
2. die Information robust speichern,
3. auf die (universelle) Quantengatter anwendbar sind und
4. die gemessen werden können [1].

Die Unsetzung der Punkte 2 und 3 ist nicht trivial, da Quantenzustände äußerst sensibel gegenüber Einwirkungen von außen reagieren -> Dekohärenz.

1.3.2 Vier Wege zum Quantencomputer

Um eine Quantencomputer zu realisieren gibt es einige Ansätze, welche hier nicht näher beschrieben werden.

- Kernspinresonanz (**N**uclear **M**agnetic **R**esonanz)
- Optische Gitter
- Ionenfallen
- Quantenpunkte
- High Q – optical cavity

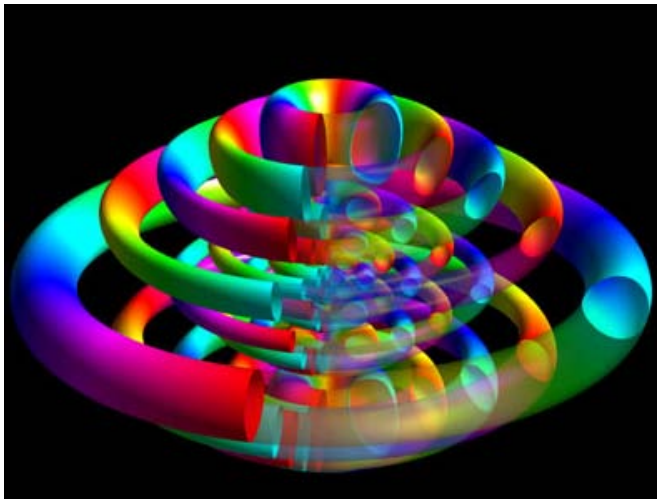


Abb. Elektron im Quantenzustand $n_1 = 6$, $n_2 = 7$, m = 2.(Quelle: B.Thaller, Universität Graz)

In der Welt der Quanten geht es sonderbar zu: Da verhalten sich Objekte mal wie Teilchen und mal wie Wellen; da kann Energie nur Paketweise ausgetauscht werden; da existieren Objekte in mehreren Zuständen zugleich; da lassen sich Eigenschaften wie Ort und

Geschwindigkeit nicht mehr gleichzeitig exakt messen und da sind Zustände weit entfernter Objekte auf geisterhafte Weise miteinander verknüpft[5].

2 Details

2.1 Quanteninformation

Die Informationsmenge wird klassischer Weise in Bit und zwar 0 und 1 angegeben. Dieser Status wird in elektronischen Geräten mittels Spannung V enkodiert[4] (z.B. TTL: 0 wird repräsentiert bei < 0,8 Volt).

In vielerlei Hinsicht äquivalent dazu ist in der Quanteninformation das Qubit. Jedoch ist die Frage, wie viel Information ein Qubit enthält, nicht letztgültig geklärt.

Während ein klassisches Bit sozusagen eindimensional ist, also nur eine 0 oder 1 Alternative, ist das Qubit dreidimensional. Wir sprechen dabei von der willkürlichen(=arbitrary) Superposition [3].

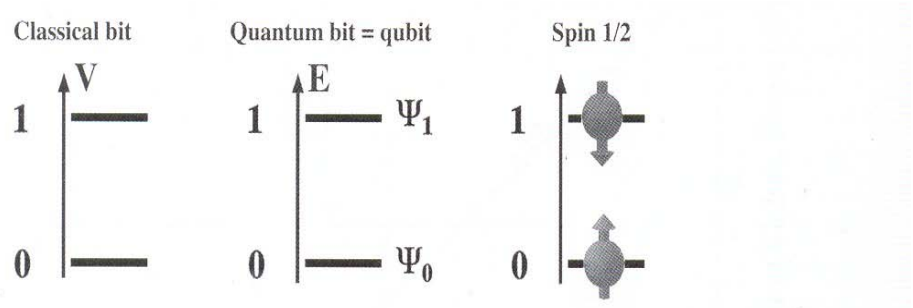


Figure 1.4: Representation of information in a classical computer (left) vs. quantum computer (center). The spin 1/2 (right) is the prototypical example of a qubit.

Quelle:[1]

Am einfachsten ist das bei Spin-1/2-Systemen zu sehen, bei denen die Superpositionen direkt den Raumrichtungen entsprechen, in denen das Ergebnis einer Spinmessung festliegt, es gilt aber für jedes Qubit.

So kann z. B. ein Photon

- linkszirkular oder rechtszirkular,
- horizontal oder vertikal und
- 45° oder -45° polarisiert sein.

2.2 Das Quantenbit, Qubit

Qubits bilden in der Quanteninformatik die Grundlage für Quantencomputer und die Quantenkryptografie. Das Qubit spielt dabei die analoge Rolle zum klassischen Bit bei herkömmlichen Computern: Es dient als kleinstmögliche Speichereinheit, und definiert gleichzeitig ein Maß für die Quanteninformation.

[4] Man versteht in der Nachrichtentechnik unter einem Kodierer (engl. Encoder) in der Regel den ersten Umsetzer, Konverter oder Wandler für digitale oder analoge Signale [Quelle: Wikipedia].

In der Quantenmechanik werden Zustände in der **Dirac-Notation** dargestellt. Wir stellen daher die klassischen Bits wie folgt dar:

$$|0\rangle \text{ oder } |1\rangle .$$

Ein Quantenbit kann sich in zwei Zuständen gleichzeitig befinden, wir sprechen daher von der Superposition. Die Wahrscheinlichkeit, mit der eine Superposition durch eine Messung zu einem bestimmten Zustand wird, lässt sich beeinflussen. In der Regel wählt man 50% für jeden Zustand.

Ein klassisches Bit wird gelesen um seinen Zustand zu ermitteln. Da ist bei einem Quantenbit nicht möglich, da diese gemessen werden muss. Unser Messergebnis hängt von Amplituden ab.

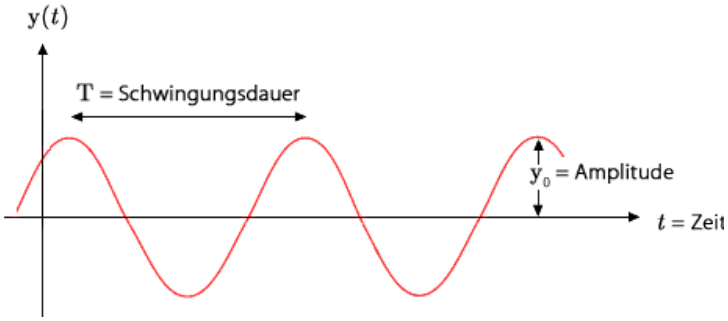


Abb.: Amplitude (Quelle:GNU Free Documentation License.)

Diese Amplituden, wir nennen sie α und β, sind komplexe Zahlen mit

$$|\alpha|^2 + |\beta|^2 = 1.$$

Somit erhalten wir die Form unserer Zustände

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle .$$

Die Zustände der Qubit können mit einem Laserlicht manipuliert werden.
Bei 32 Qubits könnten wir bereits 2^{32} = ~4Mrd Zustände darstellen.

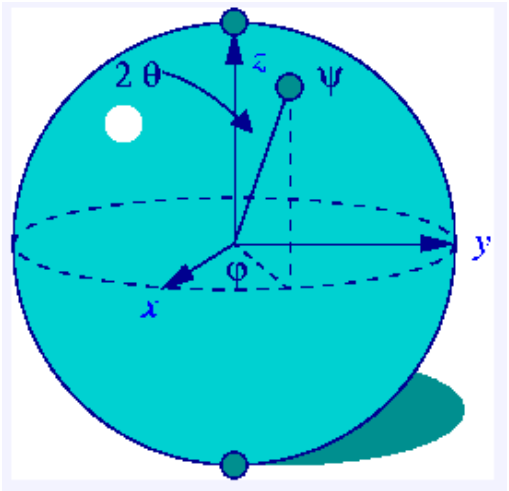


Abb.: Block-Kugel (Quelle:GNU Free Documentation License.)

Die Bloch-Kugel wird in der Quantenmechanik verwendet, um Zustände von Qubits grafisch darzustellen.

2.3 Das Quantenregister

Wie beim klassischen Computer auch, fasst man mehrere Qubits zu Quanten-Registern zusammen. Der nächste Absatz ist für einen Schüler extrem schwer zu verstehen und kann übersprungen werden.

Der Zustand eines Qubit-Registers ist dann gemäß den Gesetzen der Vielteilchen-Quantenmechanik ein Zustand aus einem 2N-dimensionalen Hilbert-Raum. Eine mögliche Basis dieses Vektorraums ist die Produktbasis über der Basis. Für ein Register aus drei Qubit erhält man die Basis |000›,| 001›, |010›, … |111›. Auch der Zustand des Registers kann eine Superposition dieser Basiszustände sein.

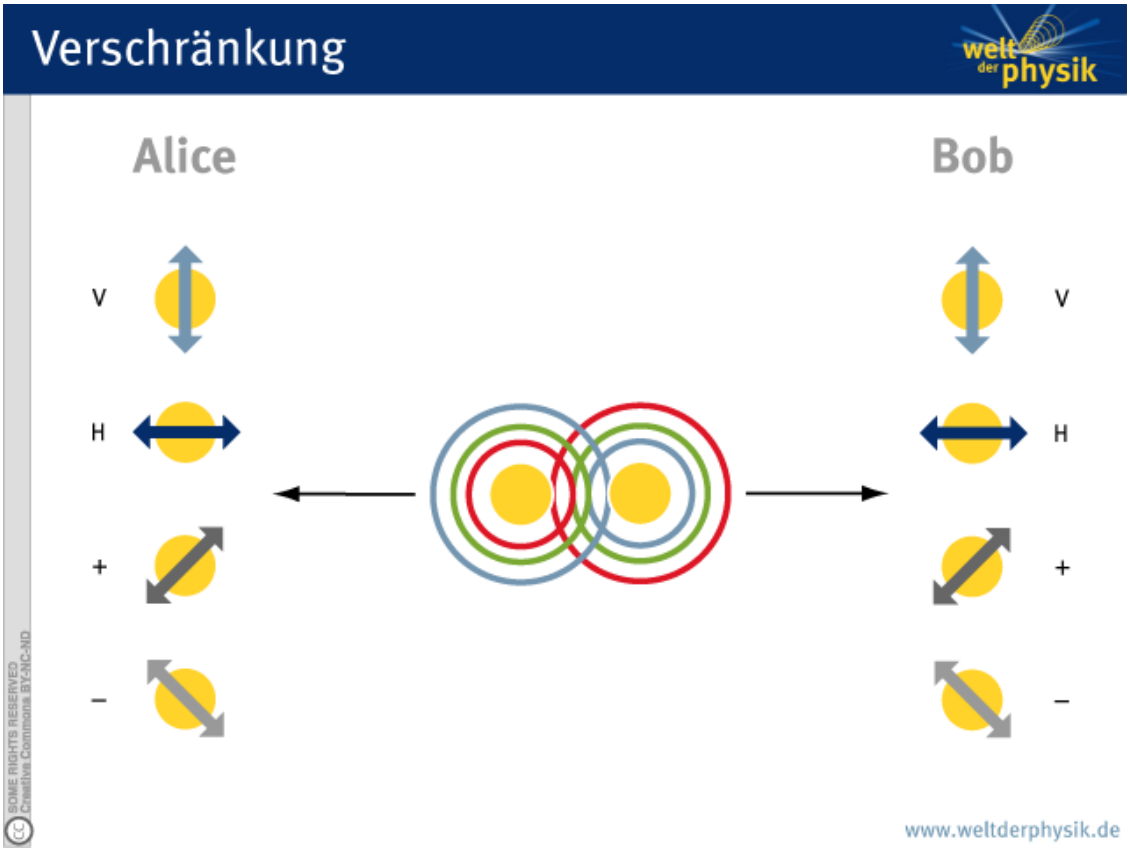
2.3.1 Verschränkung

Zwei durch Verschränkung verknüpfte Teilchen bleiben über beliebige Distanzen wie durch Zauberhand miteinander verbunden

Die sehr merkwürdige Eigenschaft von Quantenregistern ist die Tatsache, dass einzelne Bits verschränkt sein können.

Albert Einstein hat aus Sicht der klassischen Physik, diese seiner Ansicht nach paradoxe Beeinflussung als "spukhafte Fernwirkung" bezeichnet. Erwin Schrödinger hat im Jahr 1930 den Begriff "Verschränkung" eingeführt. Dabei können zwei oder mehr verschränkte Teilchen nicht mehr als einzelne Teilchen mit definierten Zuständen beschrieben werden, sondern nur noch das Gesamtsystem als solches.

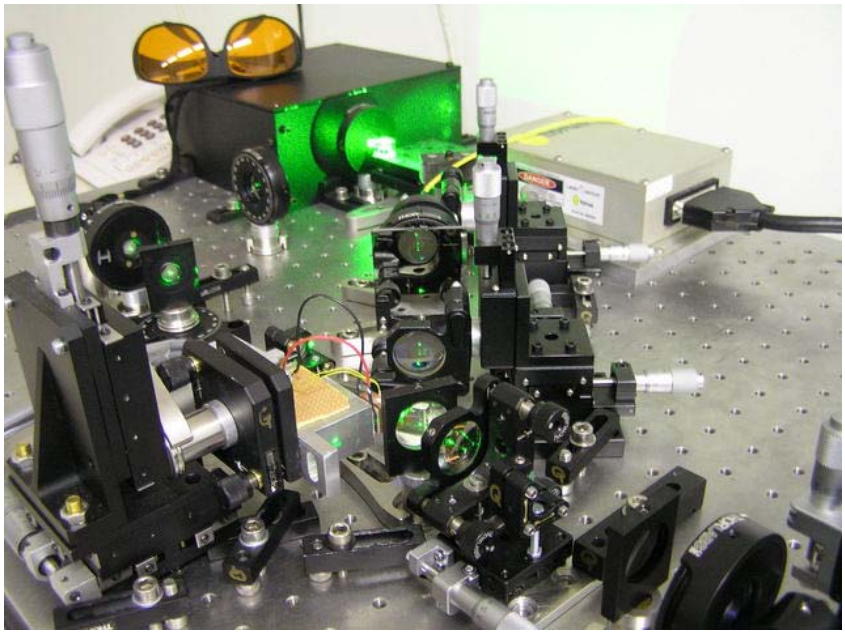
Bei Atomen bezieht sich die Verschränkung auf deren Spin(Eigenrotation). Regt man ein zweiatomiges Molekül mit einem Spin von 0 mit einem Laser derart hoch an, sodass es zerfällt, sind die beiden freiwerdenden Atome bezüglich ihres Spins verschränkt. Bei einer entsprechenden Messung wird eines von ihnen den Spin +1/2 zeigen, das andere -1/2. Es ist aber nicht vorhersagbar, welches der beiden Atome den positiven und welches den negativen haben wird. Misst man aber den Spin eines der beiden Atome, wird dadurch der Spin des anderen festgelegt.



Verschränkte Photonen lassen sich beispielsweise durch den Einsatz optischer Kristalle erzeugen. Bei Photonen bezieht sich die Verschränkung meist auf die Polarisation, die dann entweder wie in unserem Beispiel parallel oder auch um 90 Grad gegeneinander gedreht sein kann[5].

Es gibt zwei verschiedene Klassen der Verschränkung:

- Greenberger-Horne-Zeilinger-Zustände (kurz: GHZ-Zustände)
- W-Zustände.



Die Verbindung zwischen den verschränkten Teilchen ist so groß, dass jedes Teilchen immer den Zustand des anderen Teilchens kennt und auf eine Zustandsänderung auch sofort reagiert.

2.3.2 Umkehrbare Berechnungen

Bei einem Quantencomputer entsprechen die Rechenschritte unitären Transformationen[5].
Diese sind aber umkehrbar und aus dem Ergebnis der Berechnung lässt sich die Eingabe eindeutig berechnen.

Mit einem klassischen Computer ist dies nicht möglich. Eine logische Konjunktion AND zweier Bit ist eine nicht umkehrbare Operation, da die drei Werte **10, 01, 00** der Wahrheitstabelle auf **0** abgebildet wird und wir können nicht erkennen welche der drei Ausgangssituationen vorlag.

a	b	$a \wedge b$
1	1	1
1	0	0
0	1	0
0	0	0

Abb.: Wahrheitstabelle

2.4 Die Quantenteleportation

Im Jahr 1997 führte Anton Zeilinger erstmals mit Photonen ein Experiment durch welcher Quantenzustand mittels einer Zustandsänderung miteinander verschränkter Quante übertrug. Diese war die Geburtsstunde der **Quantenteleportation.**

Zur vollständigen *Übertragung* eines Quantenzustandes muss Information zwischen Sender und Empfänger auf einem klassischen Weg (also mit maximal Lichtgeschwindigkeit) ausgetauscht werden.

Im Jahr 2004 gelang es dem Wiener Forscher Rupert Ursin zusammen mit einigen Kollegen erstmals außerhalb des Labors einen Quantenzustand eines Photons zu teleportieren. Sie überbrückten eine Strecke von 600 m unter der Donau. Dafür wurde ein Lichtwellenleiter in einen Abwasserkanal unter der Donau verlegt, um den Quantenzustand (die Polarisation) des zu teleportierenden Photons von der Donauinsel (Alice von Alice und Bob) auf die südliche Donauseite (Bob von Alice und Bob) auf ein anderes Photon zu übertragen. Das Quantengatter.

2.5 Das Quantengatter

Beim klassischen Computer werden durch Logikgatter (engl. Gates) elementare Operationen auf den Bits durchgeführt. Mehrere Gatter werden zu einem Schaltnetz verbunden, das dann komplexe Operationen wie das Addieren zweier Binärzahlen durchführen kann. Die Gatter

[5] Eine bijektive lineare Abbildung, die längen- und winkelerhaltend ist

werden dabei durch physikalische Bauelemente wie Transistoren realisiert und die Information als elektrisches Signal durch diese Bauelemente geleitet.

Berechnungen auf einem Quantencomputer laufen grundsätzlich anders ab: Ein Quantengatter (engl. Quantum Gate) ist kein technischer Baustein, sondern stellt eine elementare physikalische Manipulation eines oder mehrerer Qubits dar. Ein Quantengatter ist vielmehr eine zeitlich steuerbare Wechselwirkung der Qubit untereinander oder mit der Umgebung.

Wie genau so eine Manipulation aussieht, hängt von der tatsächlichen physikalischen Natur des Qubits ab. So lässt sich der Spin eines Elektrons durch eingestrahlte Magnetfelder beeinflussen, der Anregungszustand eines Atoms durch Laserpulse. Obwohl also ein Quantengatter kein elektronischer Baustein, sondern eine im Verlauf der Zeit auf das Quanten-Register angewendete Aktion ist, beschreibt man Quanten-Algorithmen mit Hilfe von Schaltplänen.

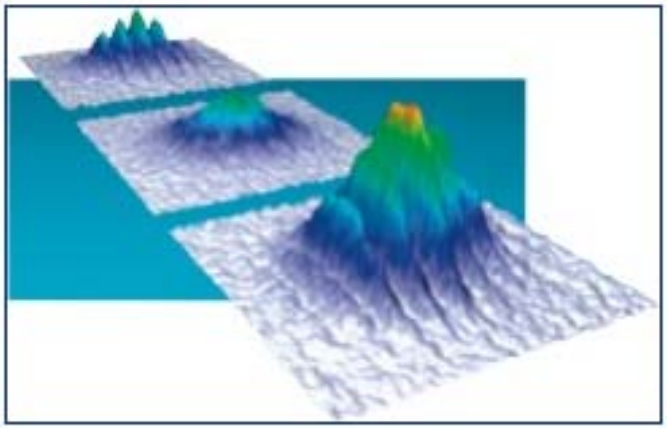


Abb. Interferenzmuster [5]

An solchen Interferenzmustern können die Forscher die Entstehung ihres Quantengatters verfolgen. Das hintere Bild zeigt die Atomwolke im ursprünglichen Mott-Isolator- Zustand. Nach der Rechenoperation entsteht ein neuer, hochgradig verschränkter Quantenzustand, der durch einen flachen Hügel ohne ausgeprägte Interferenzstruktur erkennbar ist (Mitte). Diese Operation lässt sich wieder vollständig rückgängig machen (vorne).

2.6 Algorithmen für Quantencomputer

Die bisher gefundenen Algorithmen für Quantencomputer lassen sich grob in drei Kategorien einteilen.

1.) Die Quanten-Fouriertransformation

Der **Shor-Algorithmus** dient zur Faktorisierung großer Zahlen. Der Zeitaufwand ist dabei polynomiell*) in der Anzahl der Ziffern. Im Gegensatz dazu benötigt der beste zurzeit bekannte klassische Algorithmus exponentiell*) viel Zeit. Die Bedeutung von Shors Algorithmus beruht auf der Tatsache, dass die Sicherheit der weitverbreiteten asymmetrischen Verschlüsselungsverfahren wie RSA darauf basieren, dass keine effizienten Algorithmen zur Faktorisierung großer Zahlen bekannt sind.

*) s. Mathematik

2.) Die Quanten-Suchalgorithmen

Sehr bekannt sind der **Grover-Algorithmus** und dessen Abwandlungen davon. Mit ihm sucht man sehr effizient in einem unsortierten Array. Ein klassischer Computer muss n-Einträgen im schlimmsten Fall alle Einträge vergleichen („ansehen“). Dies bedeutet, dass ein Problem erst in einer gewissen Zeit, und das kann sehr lange dauern, lösbar ist

3.)Quanten-Simulation

Um quantenmechanische Systeme zu simulieren, bietet es sich an, wieder quantenmechanische Systeme zu benutzen. Mit einem geeigneten Satz von Quantengattern lässt sich jeder **Hamiltonian** [6]darstellen, und in vielen Fällen reicht dazu eine geringe Zahl von Gattern aus. Algorithmen dieser Art könnten in der Quantenchemie eine immense Rolle spielen, da man gegenwärtig selbst einfachste Moleküle ohne grobe Näherungen nicht simuliert werden können.

Wenn Algorithmen nur mit einer gewissen Wahrscheinlichkeit ein korrektes Ergebnis liefern so spricht man von **probabilistischen Algorithmen**. Die Fehlerwahrscheinlichkeit, kann natürlich durch n Durchläufe beliebig verkleinert werden. Es kann aber auch sehr vieler Durchläufe bedürfen (s.Pkt. 3).

2.7 Quantenkryptographie

Quantencomputer dienen nicht dazu, Quantenkryptographie durchzuführen. Hierbei handelt es sich um ein eigenes Teilgebiet der Quanteninformatik, auf welchem es bereits realisierte und kommerzialisierte Systeme gibt. Für Quantenkryptographie wird kein funktionierender Quantencomputer gebraucht!

Gegenwärtig gibt es zwei existierende Klassen von Verfahren zur Quantenkryptografie:

- **BB84-Protokoll**
  Es nutzt einzelne Photonen zur Übertragung. Aufgrund des No-Cloning-Theorems können es Angreifer nicht kopieren.

- **Ekert-Protokoll**
  Hier verwenden verschränkte Zustände angewandt.

2.8 Interessante Möglichkeiten

2.8.1 „Knacken“ von Public-Key Kryptographie-Verfahren

Verschlüsselungsverfahren in der modernen Kryptographie bedienen sich der Primfaktorzerlegung. Dieses Verschlüsselungsverfahren könnte aber von Quantencomputern "geknackt" werden.

[6] Der **Hamiltonoperator** bestimmt in der Quantenmechanik die Zeitentwicklung und die möglichen Energien des zugehörigen physikalischen Systems

Beispiel:

Es ist zwar einfach(trivial) die Zahl 15 in ihre Primfaktoren, also in ein Produkt, welches nur aus Primzahlen besteht zu zerlegen, also 3*5. Bei der Zahl 875747 ist das schon etwas schwieriger. Mit einem CAS wird auch dieses Problem zu lösen sein und man erhält das Ergebnis 547 * 1601 kommen.

Das Produkt zweier Primzahlen ist einfach zu überprüfen, aber in der Praxis sehr schwer zu zerlegen. **Für eine Zerlegung eines 400-stelligen Produktes würden auch die besten heute verfügbaren Supercomputer ca. 10 Milliarden Jahre benötigen. Der Quantencomputer immerhin noch etwa 3 Jahre**!

2.8.2 Erhöhung der Suchgeschwindigkeit

Eines der Haupthindernisse bei der technischen Verwirklichung des Quantencomputers: die Einrichtung so genannter Gates bzw. Gatter. Um in Zukunft komplexere Operationen durchführen zu können, müssten Photonen zusammengeführt werden. Mit 20, 40, 100 Lichtteilchen können Geschwindigkeiten für den Quantencomputer erzielt werden die jeden konventioneller Rechner schlagen.

Für eine Suchoperation in einer Datenbank mit zwei Millionen Einträgen muss eine Million Mal nachgefragt werden, um einen bestimmten Eintrag zu finden. Der Quantencomputer braucht dagegen nur 1400 Anfragen.

3 Aktuelles

Gegenwärtig gibt es noch keinen funktionsfähigen Quantencomputer, der den klassischen Rechner ablösen könnte, sondern lediglich eine große Anzahl an Theorien und wirklich erfolgversprechende Ansätze(z.B. Zeilinger).

Bis zum "Quanten-Laptop" ist es noch ein weiter Weg. Er hat mit einem Bürogerät noch sehr wenig zu tun. Es handelt sich dabei um eine Anordnung von Spiegeln, Linsen und Strahlteilern, um einen Labortisch. Die Notwendigkeit sehr niedriger Temperaturen für den Betrieb ist auch nicht gerade alltagstauglich.

Im November 2005 gelang es Rainer Blatt am Institut für Experimentalphysik der Universität Innsbruck erstmals, ein Quantenregister mit 8 verschränkten Qubits zu erzeugen. Die Verschränkung aller acht Qubits musste durch 650.000 Messungen nachgewiesen werden und dauerte 10 Stunden

Im Februar 2007 meldete die Firma D-Wave Systems, den weltweit ersten funktionsfähigen Quantencomputer entwickelt zu haben. Im November des gleichen Jahres meldete die Firma sogar, einen Quantencomputer mit 28 Qubits entwickelt zu haben. Nach eigenen Angaben soll die Zahl der Qubits in einigen Monaten auf 512 erhöht werden. Von der akademischen Welt werden diese Meldungen jedoch mit Skepsis betrachtet. Dies liegt daran, dass die Firma D-Wave Systems nicht erklärt, wie ihr Quantencomputer funktioniert, so dass eine unabhängige Überprüfung nicht stattfinden kann [Quelle: http://de.wikipedia.org/wiki/Quantencomputer].

Bis jetzt taugen alle Ergebnisse nicht um einen Quantencomputer mit einer großen Anzahl von Qubits zu realisieren. Erst mit ein einigen hundert Qubits kann einen Quantenrechner wirklich schneller rechnen als sein klassisches Gegenstück Das Hauptproblem bei der Realisierung ist die spontane, ungewollte Dekohärenz, welche man durch verschiedene Fehlerkorrekturmethoden eindämmen hofft.

3.1 Quantengase, Bose-Einstein-Kondensat,etc.

Einige Forschungsgruppen arbeiten mit kalten Quantengasen, die sie in optischen Gittern platzieren. Das Team um den Innsbrucker Wittgenstein-Preisträger Rudolf Grimm leistet hier wegweisende Arbeit. Im Jahre 2002 gelang der Arbeitsgruppe die weltweit erste Erzeugung eines Bose-Einstein-Kondensats aus Cäsium-Atomen. Im Jahr darauf stellten die Forscher erstmals ein Bose-Einstein-Kondensat aus Molekülen her. Die Gruppe um Rudolf Grimm untersucht auch Möglichkeiten zur Steuerung der Wechselwirkung in Quantengasen und befasst sich mit Fragen der Suprafluidität in ultrakalten Teilchensystemen. Indizien für die reibungsfreie Strömung von Teilchen in einem Fermi-Kondensat konnte Grimm 2004 erstmals finden, als er die ultrakalte Quantenwolke durch Radiowellen untersuchte. Inzwischen sind die Wissenschaftler in der Lage, auch komplexe Moleküle aus Bose-Einstein-Kondensaten herzustellen.

Für die sichere Übertragung nutzten Quantenphysiker verschränkte Photonen. Auch hier hat Österreich mit dem ersten Teleportationsexperiment von Anton Zeilinger eine Vorreiterrolle übernommen. Inzwischen ist es seiner Arbeitsgruppe gelungen, die verschlüsselten Daten unter der Donau und über den Dächern Wiens zu übertragen. Auch die erste mit

Quantentechnologie verschlüsselte Banküberweisung konnte sein Team demonstrieren. Nun arbeiten die Wiener Forscher sogar daran, die abhörsichere Kommunikation im Weltraum zu erproben.

Die mathematischen Grundlagen für die Informationstechnologie der Gegenwart wurden in der ersten Hälfte des 20. Jahrhunderts entwickelt. Ähnliches geschieht derzeit für die Quantentechnologie. Das Verstehen der Verschränkung und die Entwicklung von neuen Quantenalgorithmen stellt dabei eine große Herausforderung dar. Auch in diesem Bereich ist Österreich mit dem Innsbrucker Theoretiker Hans Briegel, dem Erfinder des "Einweg-Quantencomputers" federführend vertreten

[Quelle:. www.monitor.co.at/index.cfm/storyid/9098/pagenr/2

3.1.1 Spitzenforschung in Österreich

Möglich sind diese Spitzenleistungen der österreichischen Quantenphysiker nur durch enge Kooperation sowohl untereinander, als auch mit internationalen Partnern. Über mehrere Generationen hinweg ist in Österreich eine "kritische Masse" von Forschern herangewachsen, die heute über einen Spezialforschungsbereich des Österreichischen Wissenschaftsfonds (FWF) sowie das Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften (ÖAW) verbunden sind. Auch seitens des Landes Tirol, der Städte Wien und Innsbruck und der Industrie erfahren die Wissenschaftler Unterstützung. Darüber hinaus sind die einzelnen Arbeitsgruppen sehr gut in die internationale wissenschaftliche Gemeinschaft eingebunden. Ein Beweis dafür ist die 2006 in Tirol abgehaltene 20. Internationale Konferenz für Atomphysik, die über 800 Experten aus aller Welt nach Innsbruck brachte, darunter acht Physik-Nobelpreisträger und viele herausragende Vertreter dieses zukunftsträchtigen Fachs. Um diese Entwicklungen auch für die Zukunft zu sichern, widmen die österreichischen Quantenphysiker dem Nachwuchs ein besonderes Augenmerk (Quelle: http://www.monitor.co.at/index.cfm/storyid/9098/pagenr/2).

3.1.2 EU-Projekt zur Quantenverschlüsselung

Für die Präsentation des weltweit ersten integrierten Quantenkryptographie-Netzwerks werden Teile der bestehenden Glasfaser-Infrastruktur von Siemens verwendet. Darauf haben sich die Projektpartner des europäischen Projekts SECOQC (Development of a global network for secure communication based on quantum cryptography) geeinigt. Die Präsentation wird im September 2008 in Wien stattfinden. Das Netzwerk ermöglicht die Erzeugung und Weiterreichung von Schlüsseln und könnte in Zukunft etwa Filialen von großen Firmen mit bisher nicht erreichbarer Sicherheit miteinander verbinden.

Die Arbeit erfolgt in zwei Teilen, von denen einer die quantenphysikalischen Geräte zur Schlüsselerzeugung abdeckt, der andere das neuartige Design und den Aufbau der Infrastruktur. Darüber hinaus bildet auch die Zertifizierung der Geräte und Infrastrukturen einen wesentlichen Teil des Projekts, das von der Gruppe Quantentechnologien der Austrian Research Centers GmbH - ARC geleitet wird.

Das Projekt hat eine Laufzeit von vier Jahren und wird von der EU mit 11,4 Millionen Euro gefördert. Projektstart war im April 2004. Insgesamt beteiligen sich 41 Teilnehmer aus zwölf Ländern (Österreich, Belgien, Kanada, Tschechische Republik, Dänemark, Frankreich, Deutschland, Italien, Russland, Schweden, Schweiz und Großbritannien). Das Konsortium besteht aus drei KMUs, 25 Universitäten, fünf nationalen Forschungszentren und acht Privatunternehmen. (Quelle: www.secoqc.net)

3.1.3 D-Wave

Das auf Quanten-Computing spezialisierte Unternehmen D-Wave Systems hat in der dritten Fundraising-Runde von verschiedenen Investitionsfirmen 17 Millionen Dollar erhalten, um seine Forschungen vorantreiben zu können. Mit Quanten-Computern wird schon einige Zeit experimentiert. Vor etwa einem Jahr hatte D-Wave seinen Orion-Computer vorgestellt. Bislang haben diese Rechner den Weg aus den Laboren heraus jedoch noch nicht gefunden

Orion basiert auf einem Silizium-Chip mit 16 miteinander verbundenen Qubits - dem Äquivalent der Bits in einem herkömmlichen Computer. Jedes Qubit besteht aus Pünktchen des Elementes Niobium, die von Drahtspulen umgeben sind.

Wenn elektrische Ladung durch den Draht fließt, entstehen magnetische Felder, woraufhin sich der Status des Qubits verändert. Da die Forscher wissen, wie das Niobium auf magnetische Felder reagiert, können sie das exakte Muster und Timing der magnetischen Felder berechnen.

D-Waves Computer eignen sich vor allem für das Berechnen von komplexen und aufwändigen Simulationen. Beispielsweise berechnen sie, wie unterschiedliche Proteine mit verschiedenen Kunststoffen interagieren)[Quelle: http://www.zdnet.de/news/hardware/]

Doch manche Wissenschaftler sehen die Technologie mit Skepsis: *Im letzten Jahr hatte D-Wave nie eine Antwort darauf, was sie eigentlich Neues erreicht haben. Vielmehr scheinen sie sich immer mehr in Kleinkrämerei zu verzetteln* [**Zitat Scott Aaronson**, Assistenz-Professor für Informatik am Massachusetts Institute of Technology].

3.1.4 Rupert Ursin

2007 gelang ihm die Verteilung von verschränkten Photonen zwischen den Kanarischen Inseln La Palma und Teneriffa über eine Distanz von 144 km in Zusammenarbeit mit der Europäischen Raumfahrtsagentur ESA.

3.1.5 Wiener Physiker demonstrieren ein abhörsichere Netzwerk

Unangreifbar durch Quantentrick: Forscher haben in Wien das erste vollständig abhörsichere Computer-Netzwerk vorgestellt.

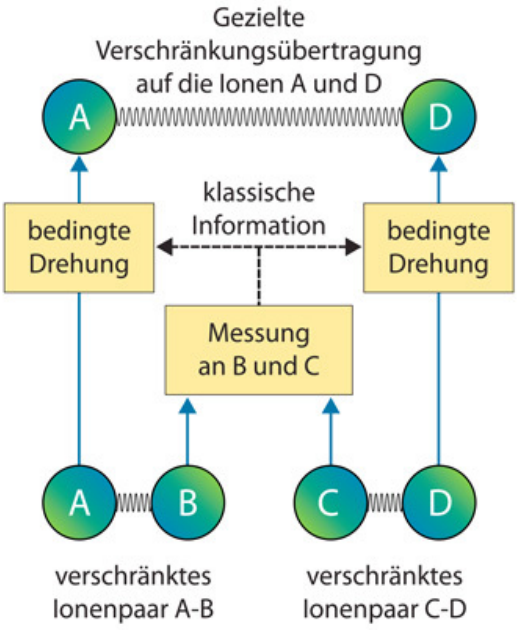
Die teure Technik soll eines Tages Banken-Militär- oder Unternehmensnetze absichern. Wie gut das schon funktioniert, demonstrierten Physiker und Techniker in Wien, indem sie über ein derart gesichertes Netzwerk telefonierten. Die Gesprächsdaten wurden dabei durch ein Verfahren aus der Quantenphysik verschlüsselt und über handelsübliche Glasfaserkabel verschickt [Quelle: Spiegel Online 9.10.2008].

3.1.6 Quanteninformation gezielt übertragen

Einem Forscherteam ist es gelungen, eine deterministische Übertragung von Verschränkungen zwischen Ionen im Labor zu verwirklichen.

Die Wissenschaftler um Rainer Blatt, Markus Hennrich und Mark Riebe vom Institut für Experimentalphysik der Universität Innsbruck berichten über ihre Variante des Entanglement Swapping Protokolls in der Online-Ausgabe der Fachzeitschrift Nature Physics.

Sie hoffen, damit die Implementierung von Quantenrepeatern voranzubringen und die Weiterleitung verschränkter Zustände in Ionenfallen-Quantencomputern zu erleichtern. [Quelle: Heise Online 4.11.2008].



Die Innsbrucker Forscher können mit diesem Verfahren den Zustand verschränkter Ionen gezielt steuern.
Bildquelle: Universität Innsbruck

4 Quellenangabe

[1] M. Hormeister QUATUM COMPUTING verstehen .
[2] J. Stolze, D. Sutter QUANTUM COMPUTING
[3] O. Morsch QUANTUM BITS AND QUANTUM SECRETS
[4] R.Ursin QUANTENTELEPORTATION
[5] www.weltderphysik.de
[6] /www.spektrum.de/artikel/849265&_z=798888