

1

Eva-Maria Zimmermann
Pascál Bihler

mychen@web.de
pb@bi-on.de

Quanten-Computer und verschränkte Zustände



Vortrag im Rahmen der Sommerakademie
La Villa 2003

Quantencomputer und verschränkte Zustände
25.8.3 - La Villa Eva-Maria Zimmermann - Pascál Bihler



2

Grenzwissenschaften?

*Es gibt mehr zwischen Himmel und Erde,
als unsere Schulweisheit sich träumen lässt!*

- Quantenmechanik
- Quanteninformatik
- Quantencomputer

- Qubits
 - Superposition
 - Verschränkung
- Quantengatter
- Realisation & Probleme
- Quantenalgorithmien
- Quantenteleportation
- Quantenkryptographie





3

Herkömmliche Datenhaltung

Binäre Kodierung von Daten:

1423 = 10110001111

$1 \wedge 0 = 0$

$1 \vee 0 = 1$

Datenspeicherung:

- Magnetisch (Element ist nord/süd-gerichtet)
- Elektrisch (Kondensator geladen/nicht geladen)
- Optisch (Reflexion/Keine Reflexion)
- ...

=> Jedes Datenspeicherelement hat genau zwei Zustände



- Wahr/Falsch
 - 1 / 0
 - ...
- } 1 bit

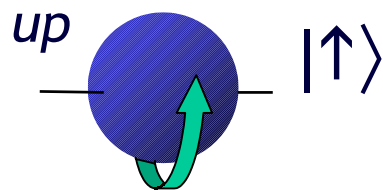
Mit n Einzelementen lässt sich genau einer von 2^n Zuständen speichern und weiterverarbeiten



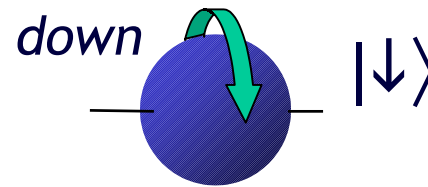
4

Elektronen-Spin

- Elektronen haben einen Spin, der zwei Zustände repräsentieren kann:



$|\uparrow\rangle$
 $|1\rangle$



$|\downarrow\rangle$
 $|0\rangle$



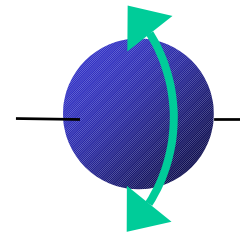
$$|s| = \sqrt{s(s+1)} \cdot \hbar$$

Qubits

- Superpositionszustände: $|\updown\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

z.B. $|\psi\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$

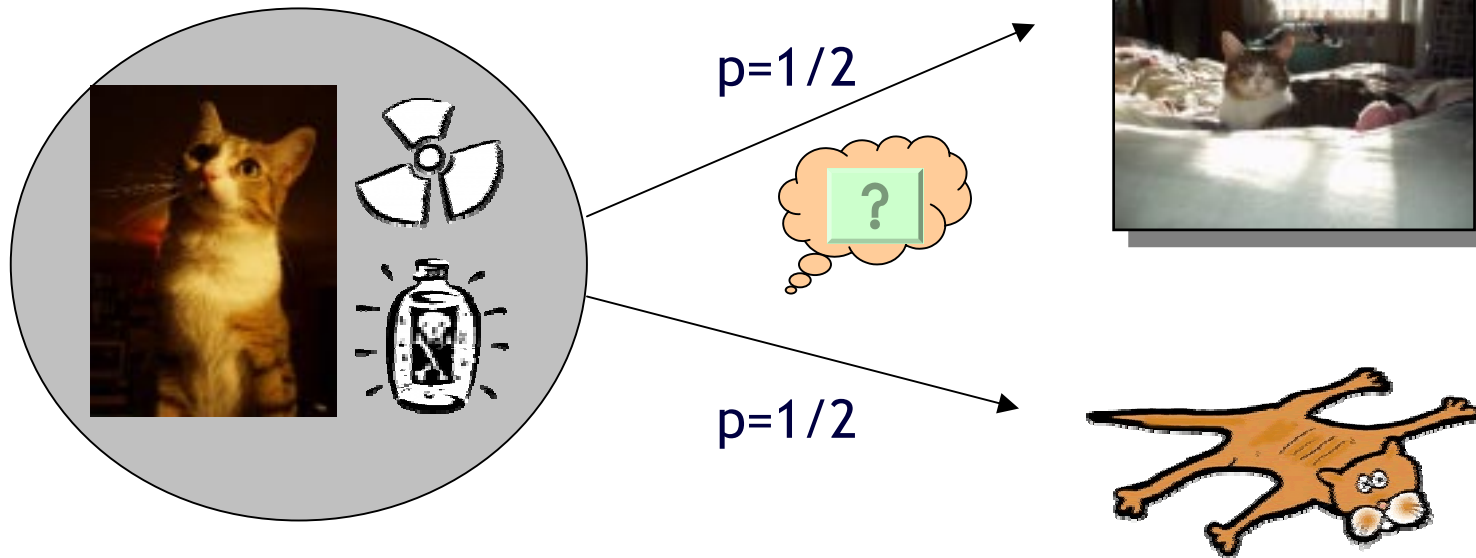




5

Schrödingers Katze

Das wohl bekannteste Beispiel für Überlagerung:
Schrödingers Katze



Katze im Superpositionszustand:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

1 = lebendig

0 = tot





6

Verschränkte Zustände

- System aus zwei Teilchen mit je zwei möglichen Zuständen:

A $|\psi_A\rangle \in H_A$ mit $|\psi_A\rangle = \alpha_A |\uparrow\rangle + \beta_A |\downarrow\rangle$

B $|\psi_B\rangle \in H_B$ mit $|\psi_B\rangle = \alpha_B |\uparrow\rangle + \beta_B |\downarrow\rangle$

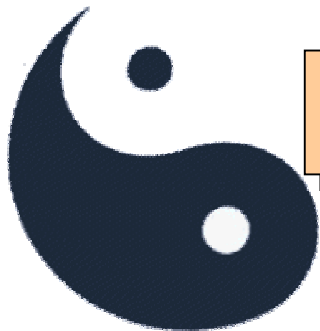
$|\psi_{AB}\rangle \in H_{AB}$

wobei $H_{AB} = H_A \otimes H_B$

- Somit ist ein bel. Gesamtzustand von der Form:

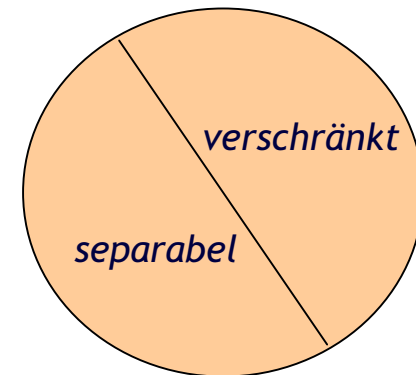
$$|\psi_{AB}\rangle = (\alpha_A |\uparrow\rangle + \beta_A |\downarrow\rangle) \otimes (\alpha_B |\uparrow\rangle + \beta_B |\downarrow\rangle)$$

- Separabilität: $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$



Verschränkung = nicht separabel

Superpositionen





7

Verschränkte Zustände

Eigenschaften von Verschränkung:

- Superposition
- Gesamtzustand \neq Einzelzustände
- Messung bei A \Rightarrow Zustand von B fest

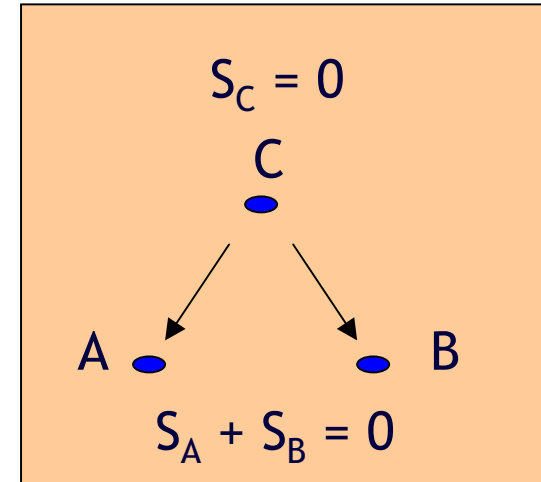
Kriterien für Separabilität:

- Schmidtzahl k

$|\Psi_{AB}\rangle = \sum_i c_i |u_i\rangle |v_i\rangle$ für Systeme aus zwei Teilchen zu je i Zuständen

- $k = \text{min. Summandenzahl}$
- $k=1 \Leftrightarrow \text{separabel} \Leftrightarrow \text{nicht verschränkt}$

- Peres-Horodecki-Kriterium (für 2x2 und 2x3 Systeme)



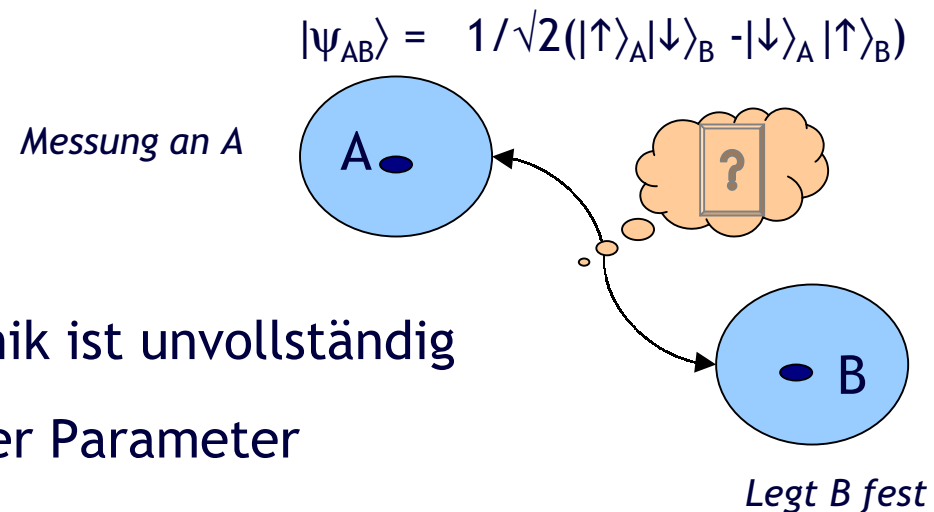
EPR-Paradoxon

Grundannahmen des EPR-Paradoxon (Einstein, Podolsky und Rosen, 1935):

- Die Voraussagen der Quantenmechanik sind korrekt
- Die Quantenmechanik ist eine lokal-realistische Theorie
- Keine Information breitet sich schneller aus als mit Lichtgeschwindigkeit

Folgerungen EPRs:

- Die Quantenmechanik ist unvollständig
- Existenz verborgener Parameter

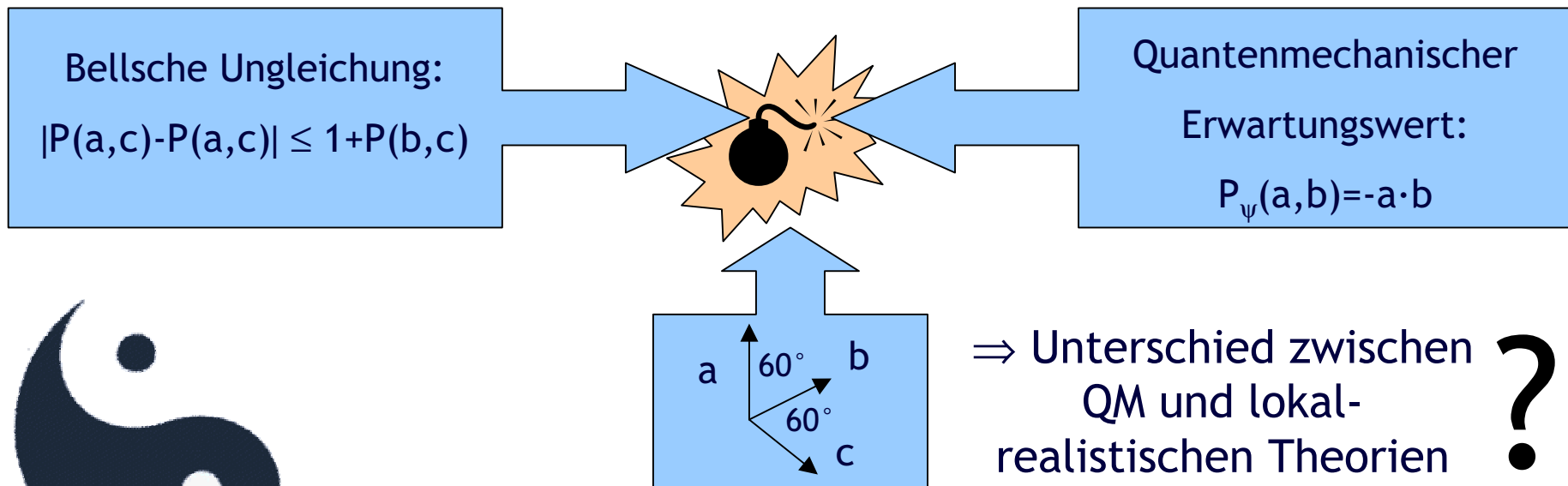


Die Bellsche Ungleichung

Bells Idee [1964]:

- Rekapitulation des Arguments von EPR
- Vollständigere Beschreibung durch „verborgene Parameter“

$$|\psi_{AB}\rangle = 1/\sqrt{2}(|\uparrow\rangle_A |\downarrow\rangle_B - |\downarrow\rangle_A |\uparrow\rangle_B)$$



Weitere Ergebnisse

- GHZ-Gedankenexperiment:

Greenberger, Horne und Zeilinger führen mit drei unterscheidbare spin-1/2 Teilchen die Annahmen des EPR ad absurdum

- CHSH-Ungleichung:

Verallgemeinerung der Bellschen Ungleichung, die aussagt, dass auch stochastische lokale Theorien mit verborgenen Parametern die quantenmechanischen Korrelationen nicht reproduzieren können.



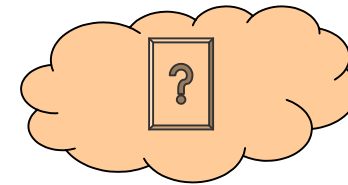
Schwierigkeit: Gedankenexperimente in die Realität umzusetzen

Konsequenzen

- Sind die lokal-realistischen Theorien falsifiziert?

Wenn ja, welches Konzept verwirft man:

- Lokalität ?
- Realität ?
- Beide ??



- Keine Informationsübertragung ist schneller als Licht

- Anwendungen:

- Teleportation von Quanten
- Quantencomputer
- Quantenkryptographie



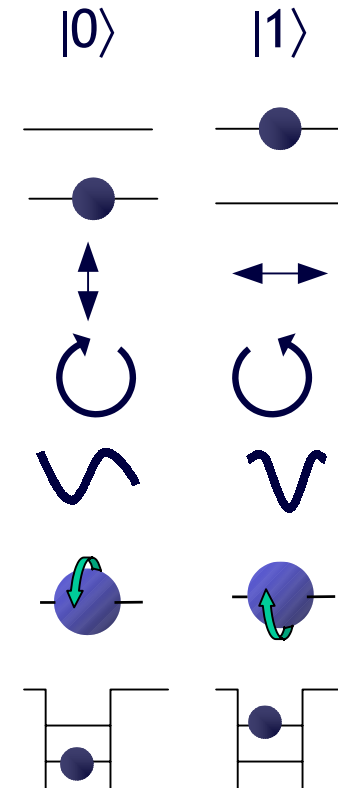


12

Quanten-Information

- Verschiedene Möglichkeiten zur Qubit-Speicherung:

- Energieniveaus der Schale
(Ionen, Atome)
- Polarisation
(Photonen)
- Phase
(Photonen)
- Spin
(Neutronen, Elektronen, Atomkerne)
- Energieniveaus
(Quantenpunkte)



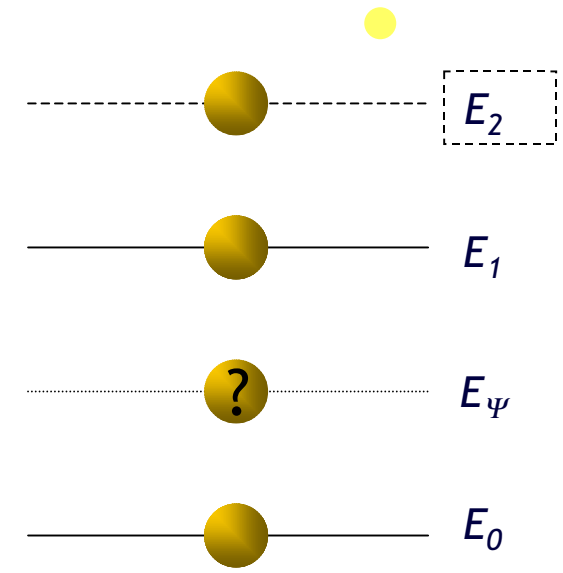


13

Lesen, Schreiben, ...

- Beispiel: Wasserstoffatom

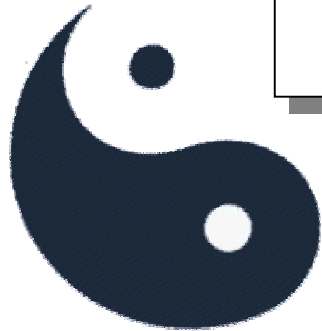
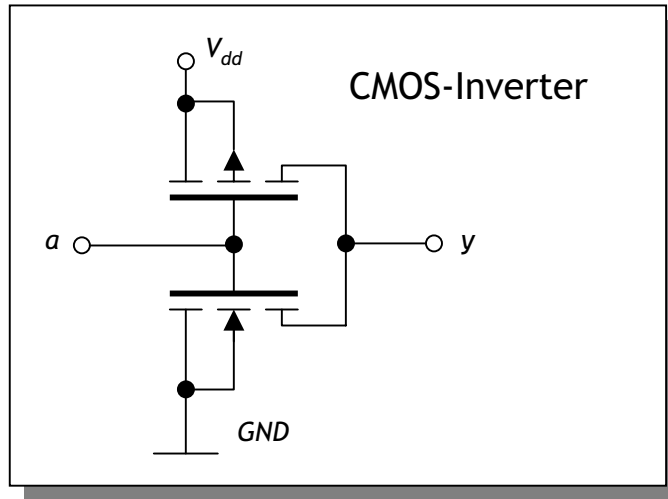
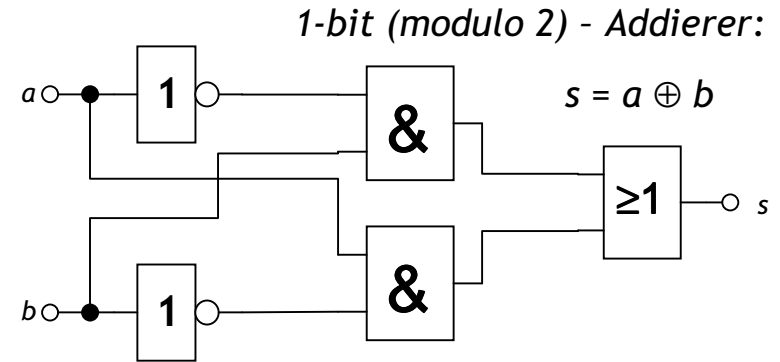
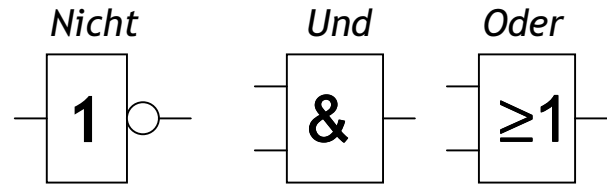
- Grundzustand: $E_0 = |0\rangle$
- Angeregter Zustand: $E_1 = |1\rangle$
- „Zwischenzustand“: $E_\Psi = |\Psi\rangle$
- Instabiler Zustand: E_2





... Rechnen

- Herkömmliche Logik: Rechnen mit Gattern:





15

... Rechnen

- Quantengatter:

- Es genügt eine Einzelqubit-Operation und eine Zwei-Qubit-Operation:
 - Hadamard-Transformation

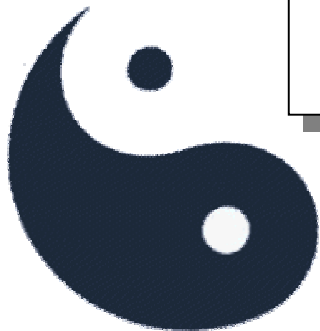
$$\hat{H} : \begin{array}{l} |0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2} \\ |1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2} \end{array}$$

- Kontrolliertes Quanten-NICHT-Gatter (**CNOT**)

$$\hat{C} : |\epsilon_1\rangle|\epsilon_2\rangle \rightarrow |\epsilon_1\rangle|\epsilon_1 \oplus \epsilon_2\rangle,$$

$$\hat{C} : \begin{array}{l} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{array}$$

$$\hat{C}_{12} : (a|0\rangle + b|1\rangle)|0\rangle \rightarrow a|0\rangle|0\rangle + b|1\rangle|1\rangle$$

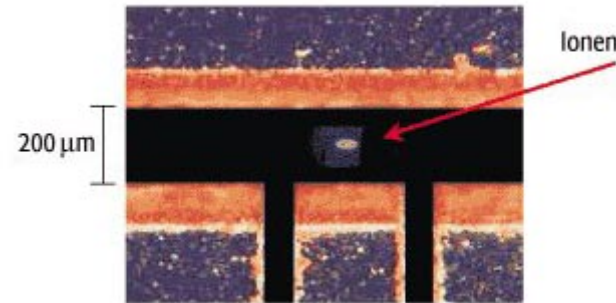




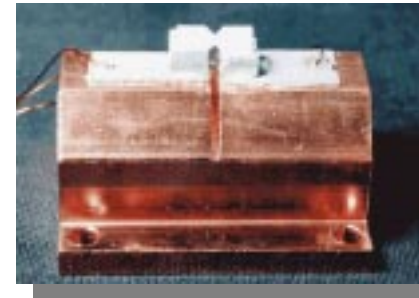
16

Realisierung der Gatter

- Lasergekühlte Ionen

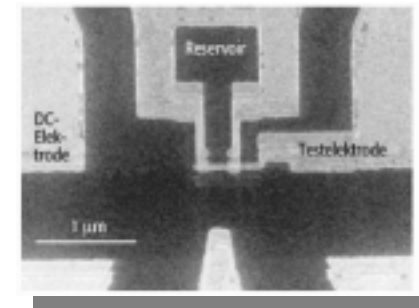


- Atome im Resonator



- supraleitender Metall-Halbleiter-Übergang

(Josephson-Kontakt)



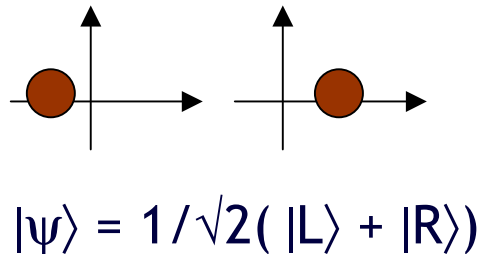
Quantencomputer und verschränkte Zustände

25.8.3 - La Villa

Eva-Maria Zimmermann - Pascál Bihler

Dekohärenz

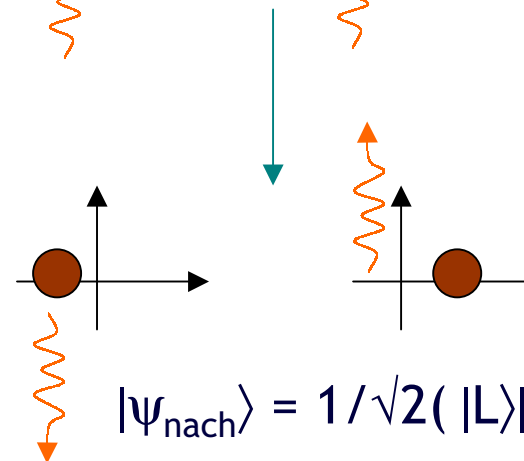
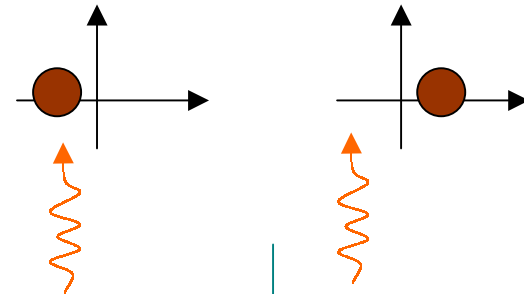
Dekohärenz - oder - Der Hang unserer Welt zu reinen Zuständen:



Durch die Wechselwirkung mit der Umwelt entsteht aus einer Superposition eine Verschränkung, die bei der „Messung“ auf einen reinen Zustand projiziert wird



$$|\psi_{\text{vor}}\rangle = 1/\sqrt{2}(|L\rangle|\uparrow\rangle + |R\rangle|\uparrow\rangle)$$



$$|\psi_{\text{nach}}\rangle = 1/\sqrt{2}(|L\rangle|\downarrow\rangle + |R\rangle|\uparrow\rangle)$$



18

Quantenalgorithmen

- Deutsch-Josza-Algorithmus (*Das Orakel*)

$f : \{0,1\}^n \rightarrow \{0,1\}$ Konstant oder balanciert?

- Aufwand klassisch: 2 bis $2^{n-1} + 1$ Schritte
- Mit Quantencomputer: $0,5*n + 1$ Schritte

⇒ *Exponentieller Speed*



- Grovers Suchalgorithmus (*Die Nähnadel finden*)

- Aufwand klassisch: $0,5*n$ Schritte
- Mit Quantencomputer: $\approx \sqrt{n}$ Schritte

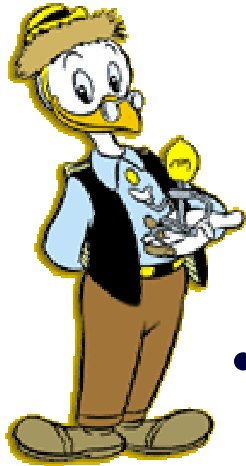
⇒ *Auch schneller*





Shor-Algorithmus

- *für Mathematiker(innen) ...*



Primfaktorzerlegung natürlicher Zahlen

- Aufwand klassisch: $e^{\left(\frac{64}{9}\right)^{1/3} (\log n)^{1/3} (\log \log n)^{2/3}}$ Schritte
- Mit Quantencomputer: $(\log n)^3$ Schritte



Peter W. Shor

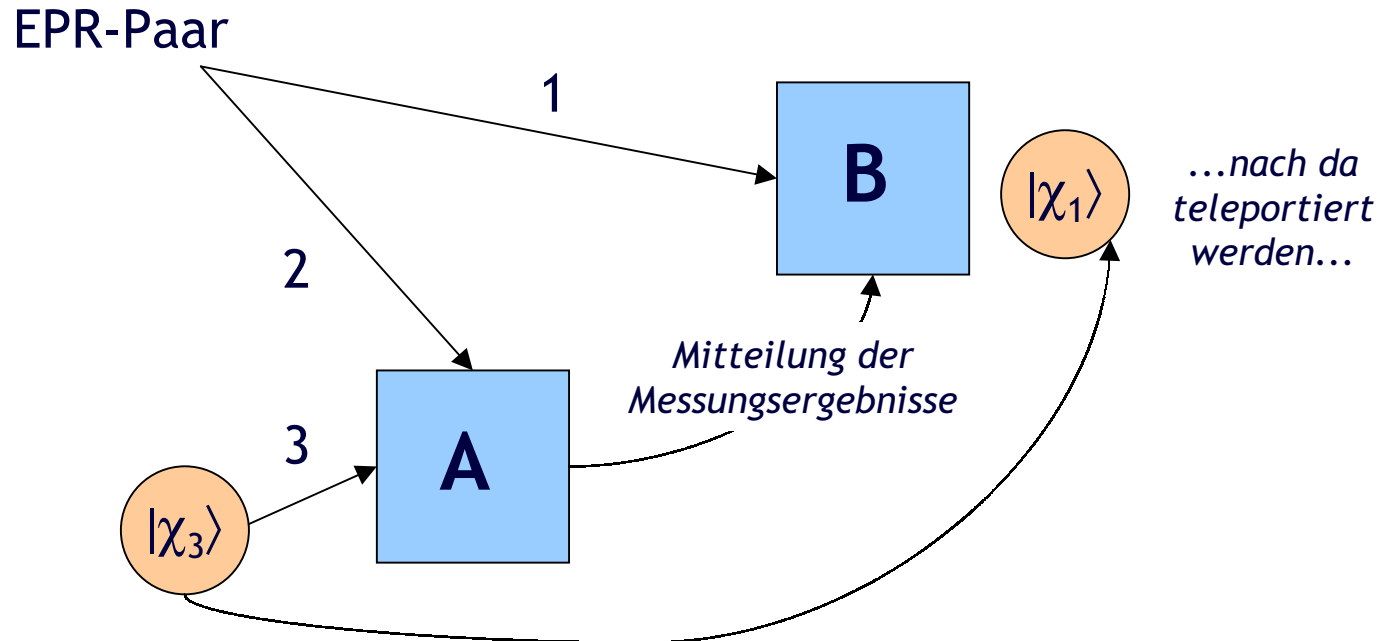
- *... und Panzerknacker*

Public-Key-Kryptografie:

- Verschlüsseln mit öffentlichem Schlüssel:
 $N = p * q, \dots$
- Entschlüsseln mit geheimen Schlüssel:
 $h = \varphi(N) = (p-1) * (q-1)$



Quantenteleportation



...soll von hier...

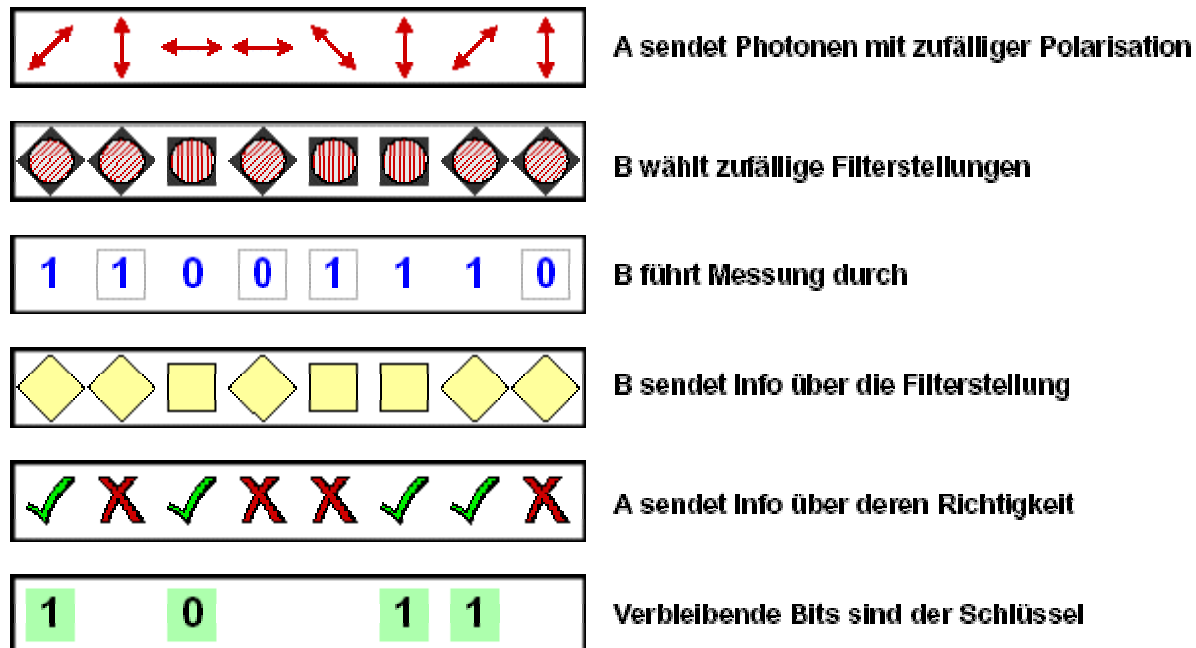
Quantenteleportation ist
Grundlage für
Quantenkryptographie



Quantenkryptographie

- Bisherige Kryptographie nicht mehr sicher wegen der Quantencomputer => Idee: Quantenkryptographie

BB84-Protokoll (nach Bennett/Brassard 1984)



Aus: Bernd Däne: Die ziemlich verrückte Welt der Quantencomputer



- Quantenmechanik bezieht sich auf...

... den Mikrokosmos

- Gibt es eine Verallgemeinerung/Erweiterung der Quantenmechanik auf...

... den Makrokosmos

und damit auf

... unsere Welt

?





23

Résumé 2

- Herkömmliche Datenverarbeitung

=> *Glockenspiel*



- Datenverarbeitung mit Superpositionen

=> *Symphonie*



Noch Fragen?

- Literatur:

- Online-Lexikon der Physik, Wissenschaft Online, Heidelberg
- Arnd Bäcker: Die Bellsche Ungleichung, Proseminar zur Quantenmechanik II
<http://www.ap.univie.ac.at/users/fe/Quantentheorie/Dekohaerenz/>
- Franz Embacher
- Bernd Däne: Die ziemlich verrückte Welt der Quantencomputer
http://www.theoinf.tu-ilmeneau.de/ra1/ver/quant_gi02.pdf
- Christian Hillmann: „Einführung und Charakterisierung von Verschränkung“
- Seth Lloyd: Quanten-Computer - Spektrum der Wissenschaft 12/1995, S. 62
- Popescu, Brims, Rohrlich: „The joy of entanglement“
- Alexander Rieth: Quantenalgorithmen I
<http://maitre.physik.uni-kl.de/~rieth/Projekte/Hauptseminar.htm>

- Grafiken:

- http://edition.cnn.com/TECH/9712/10/beam.me.up.ap/t1_beam.up.jpg
- <http://interconnecte.org/home/more/dome/images/quantu.jpg>
- <http://www.1zu1.ch/img/orakel.gif>
- <http://www.clipsahoy.com/clipart2/as2280.gif>
- <http://www.curiosius.ch/fasi02/knacktanz.jpg>
- <http://www.flensburg-online.de/comics/daniel-duesentrieb.gif>
- <http://www.helmut-block.de/hahn.gif>
- http://www.kirchdorf.at/rathaus/vereine/page_logo/kreisel1.gif
- http://www.nfpa.org/sparky/images/cool_poison_hunt/poison.gif
- <http://www.playandlearn.de/instrumente/abbildungen/produkte/03glockenspiel.gif>
- <http://www.quarks.de/castor/bilder/radio.gif>
- <http://www.research.att.com/pics/shor.gif>
- <http://www.tire-covers.com/catalog/images/yingyang.jpg>

