

Die ziemlich *verrückte* Welt der Quantencomputer

Ein Einblick

Bernd Däne

TU Ilmenau, Fakultät I/A

Tel.: 03677-69-1433

Bernd.Daene@TU-Ilmenau.de

Gliederung

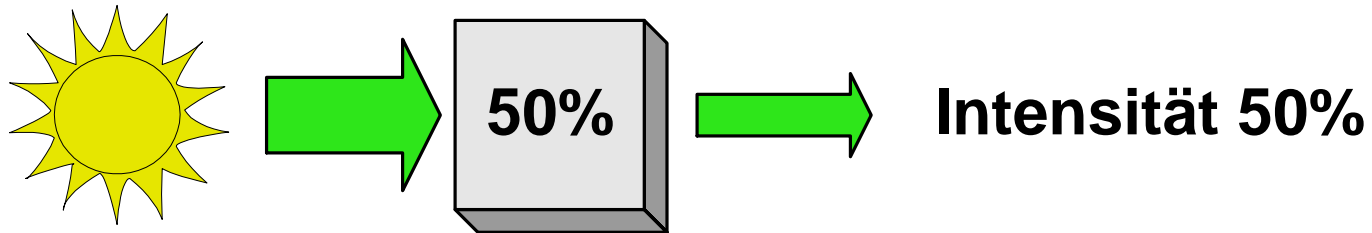
1. Quanteneffekte sind überall
2. Quantenbits und weiteres
3. Quantenalgorithmien
4. Realisierungen
5. Kryptographie mit Quanten
6. Ein Fazit
7. Literatur und Links

1. Quanteneffekte sind überall

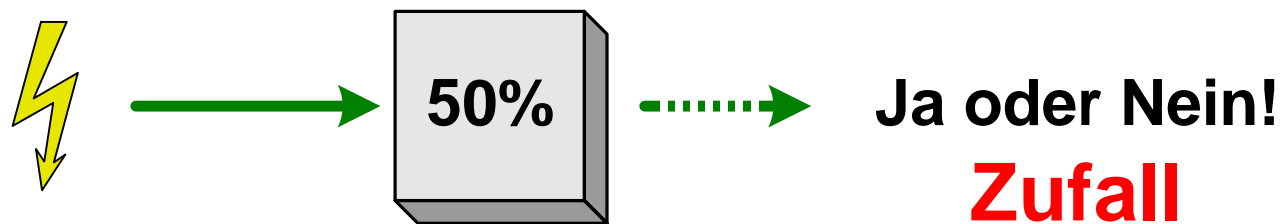
- Photonen
 - Energie
 - Polarisation
- Elektronen
 - Ladung
 - Energieniveau (in der Atomhülle)
- Spins von Teilchen
- Quanten-Hall-Effekt
- Radioaktiver Zerfall
-

Zum Beispiel: Licht

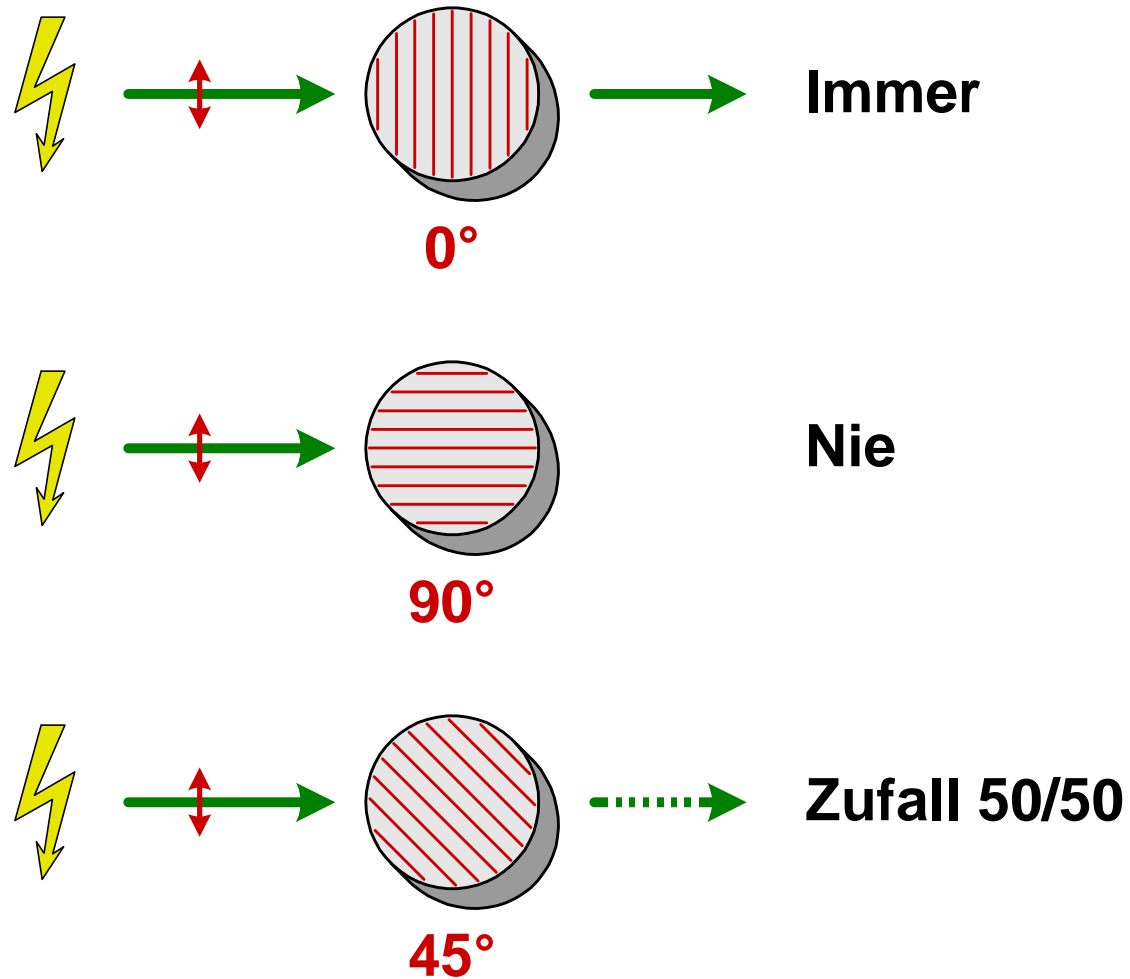
Viele Photonen:



Ein Photon:



Dasselbe mit Polarisation



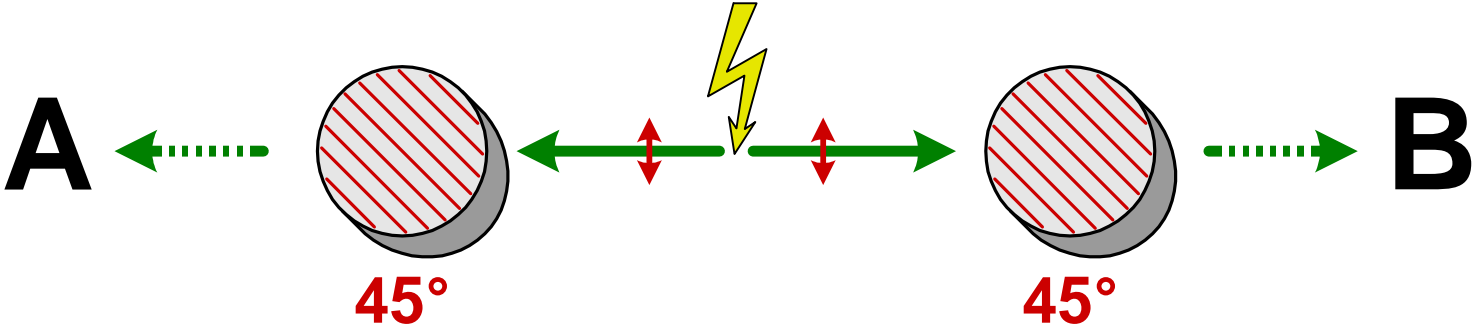
Eigenschaften der Quanten

- Unteilbar
- Diskrete Zustände
- Stochastisch
- Mikroskopisch
- *Intuitiv schwer erfassbar*
- **Das Wichtigste kommt noch!**

Nochmal die Photonen

Beispiel: EPR-Photonen

(nach Albert Einstein, Boris Podolsky und Nathan Rosen, 1935)



A	B	Klassisch	Quantentheorie	Experiment
0	0	25 %	50 %	~ 50 %
0	1	25 %	0 %	~ 0 %
1	0	25 %	0 %	~ 0 %
1	1	25 %	50 %	~ 50 %

Zwei weitere Eigenschaften

- **Verschränkung:**

- Gegenseitige Abhängigkeit von Quantenereignissen
- Stochastischer Charakter

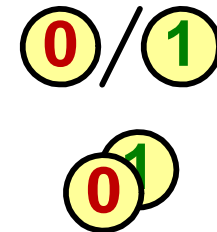
- **Superposition:**

- Unbestimmter (unscharfer) Zustand
- Enthält alle möglichen Zustände
- Wird durch jede Interaktion („Messung“) zerstört!

2. Quantenbits und weiteres

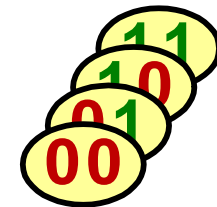
- **1 qubit:**

- Quantenereignis mit zwei Zuständen
- Superposition: beide Zustände **gleichzeitig**



- **Quantenregister mit n qubit:**

- Verschränkung aus n solchen Ereignissen
- Superposition: 2^n Zustände **gleichzeitig**

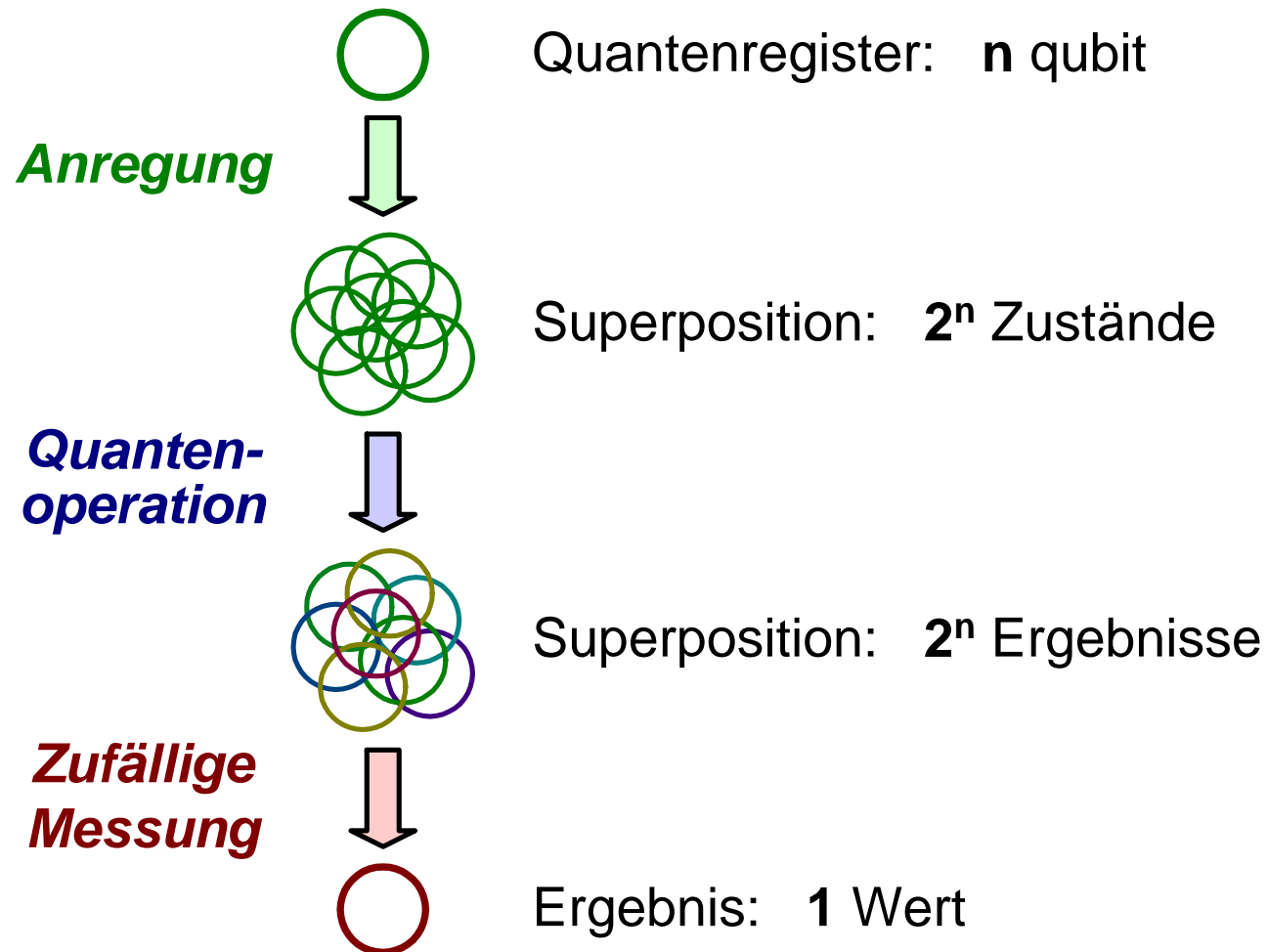


➔ Parallelität 2^n mit **n** Elementen!

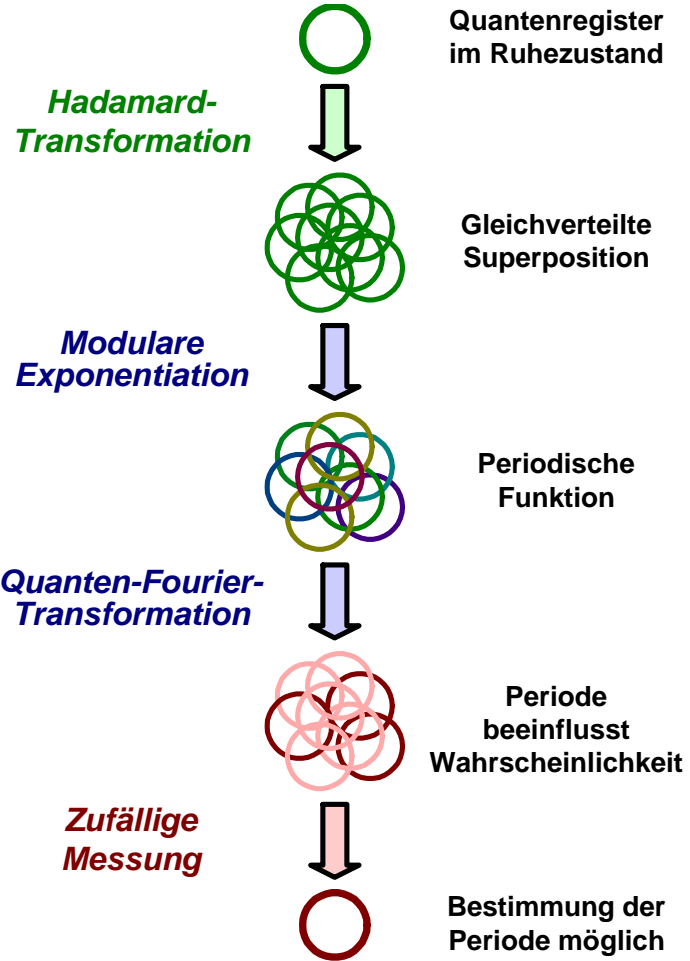
Probleme mit Quantenbits

- **Stabilität:**
 - Äußerer Einfluss zerstört die Superposition
- **Messung:**
 - Nur eine Messung
 - Zufällige Auswahl
- **Registerbreite:**
 - Passend zur Aufgabe
- **Fehler:**
 - Zufällige Fehler bei jeder Operation

3. Quantenalgorithmen



Faktorisierung nach Shor



Beispiel: Argument $N = 15$
Zufallszahl $a = 7$

x	0	1	2	3	4	5	6	...
$a^x \bmod N$	1	7	4	13	1	7	4	...

Graph showing a periodic function with period p on the x-axis.

$r = 4$

$\text{ggT}(a^{r/2}+1, N) = \text{ggT}(7^2+1, 15) = 5$
 $\text{ggT}(a^{r/2}-1, N) = \text{ggT}(7^2-1, 15) = 3$

Effizienz des Shor-Algorithmus

- Zeitbedarf: $O((\log N)^2 (\log \log N) (\log \log \log N))$
- Registerbreite: $\geq 2 \cdot \lg N - 1$
(qubit)

Fiktives Zahlenbeispiel		
Länge des Arguments (bit)	Heutiger Supercomputer (10^6 MIPS)	Hypothetischer Quanten- computer (10^7 Op/s)
512	3 Tage	15 Tage 1023 qubit
1024	60 000 Jahre	80 Tage 2047 qubit
2048	70 Bill. Jahre	400 Tage 4095 qubit

Quantengatter

- Umkehrbarkeit
- Erhaltungssätze und Symmetriebedingungen
- Basissystem

Toffoli-Gatter

Input	Output
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	0 1 0
0 1 1	0 1 1
1 0 0	1 0 0
1 0 1	1 0 1
1 1 0	1 1 1
1 1 1	1 1 0

"gesteuertes NOT"
 NAND

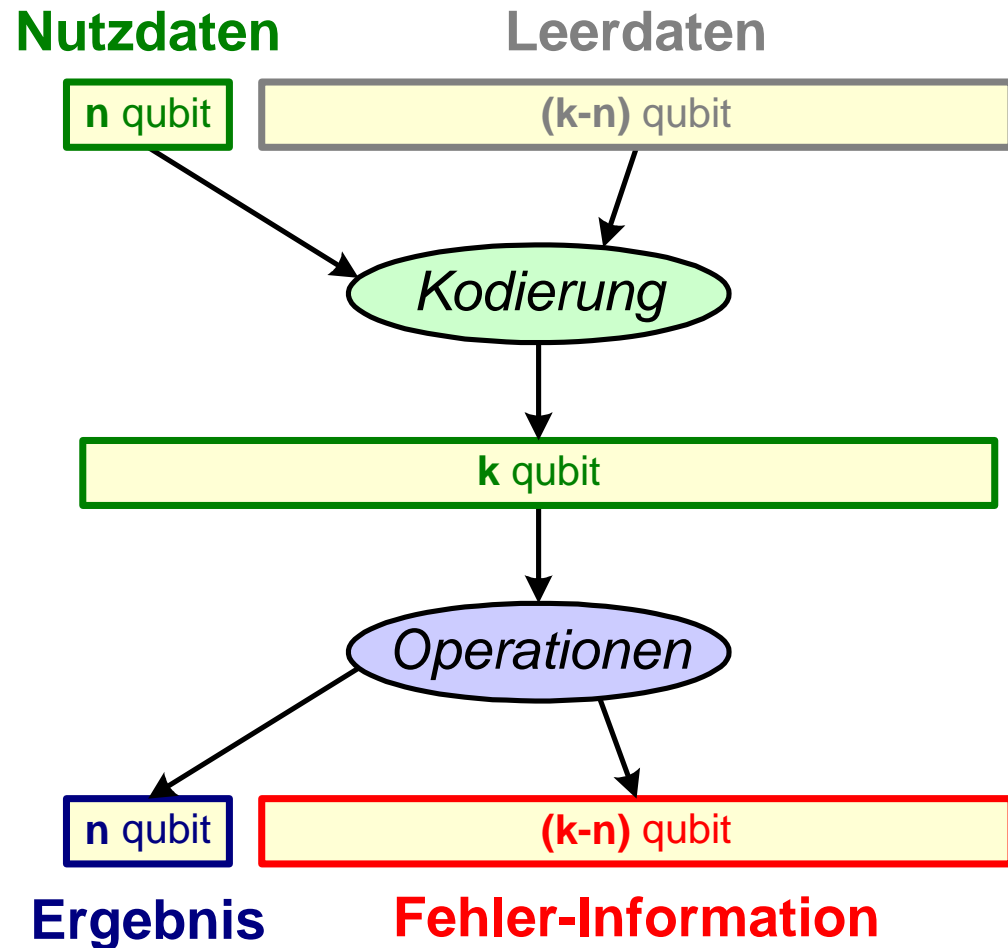
Fredkin-Gatter

Input	Output
0 0 0	0 0 0
0 0 1	0 1 0
0 1 0	0 0 1
0 1 1	0 1 1
1 0 0	1 0 0
1 0 1	1 0 1
1 1 0	1 1 0
1 1 1	1 1 1

Tausch
 NOT
 AND

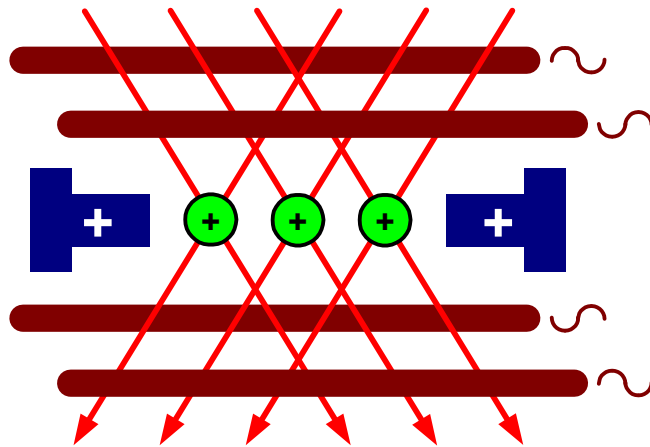
Fehlerkorrektur

- **[k,n] - Code:**
 - Nutzdaten **n qubit**
 - verteilt auf **k qubit**
- Fehlerauswertung:
 - Messung
 - Korrekturoperationen
- Beispiel:
 - **[5,1] - Code**
Optimum für Einzel-Qubit-Operationen



4. Realisierungen: Ionenfalle (MOT)

- Energiezustände in der Atomhülle
- Kopplung durch Vibration
- Anregung durch Laser
- Kurze Dekohärenzzeiten
- Aktuell:
 - Gatter 2 qubit
 - Rudimentäre Operationen bis etwa 10 qubit



Tauschoperation in der Ionenfalle:

<http://www.spectrum.ieee.org/WEBONLY/publicfeature/feb01/quantf4.gif>

Abbildung: IEEE Spectrum Feb. 2001, S. 46

Kernspin-Resonanz (NMR)

- Spins im Atomkern
- Kopplung im Molekül
- Anregung mit HF
- Viele Moleküle
- Aktuell:
 - Shor-Algorithmus für $N=15$ (mit 7 qubit)
- Beispiel:
 - CHCl_3 (2 qubit)

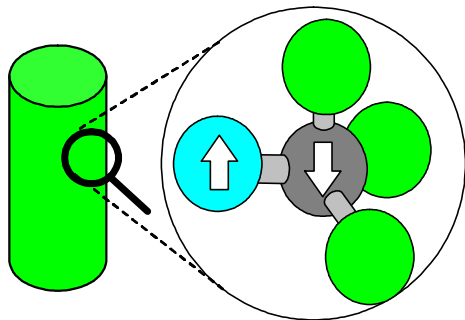


Abbildung: Torsten Koch

„Gesteuertes NOT“ mit Kernspin-Resonanz:

<http://www.spectrum.ieee.org/WEBONLY/publicfeature/feb01/quantf3.gif>

Abbildung: IEEE Spectrum Feb. 2001, S. 45

Quantenpunkte

- Diskrete Energieniveaus von Elektronen in kleinen Leiterstrukturen
- Abmessung: ≤ 20 nm
- Elektrostatische Kräfte und Tunneleffekte
- Auch für „konventionelle“ Logik

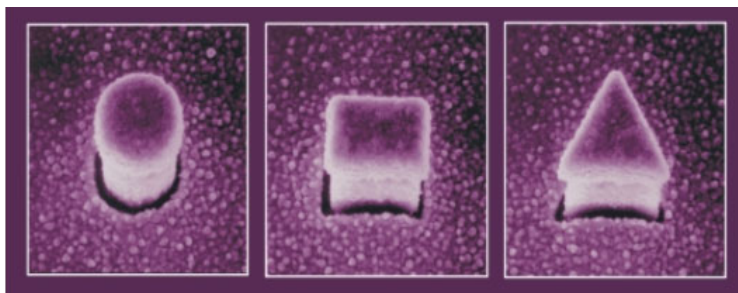
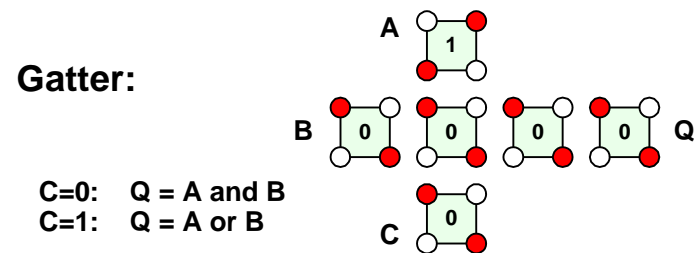
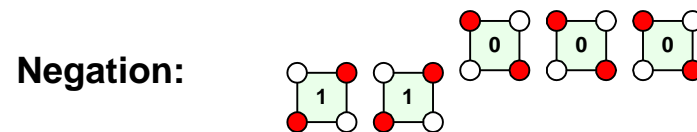
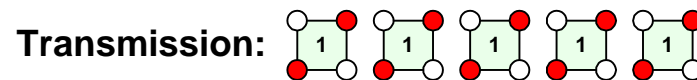
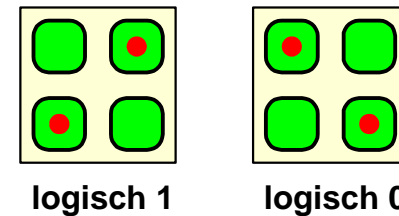


Abbildung: TU Delft

Logikzelle aus vier Quantenpunkten:



Weitere Kandidaten

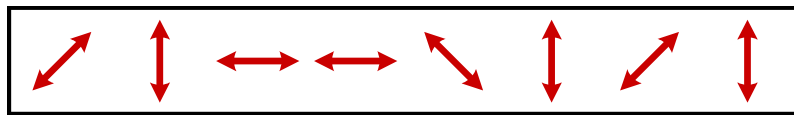
- Kristalline Atomfalle
 - Atome eingesperrt in Festkörpern
- Molekülkaskade
 - Moleküle „kleben“ auf einer Fläche
- Nanoröhren
 - Winzige Strukturen aus Kohlenstoff
- Supraleitende Ringe
 - Kreisende Elektronen tragen Information
- Bose-Einstein-Kondensate
 - Atome im „Gleichschritt“
- EPR-Photonen für Teleportation und Klonen

5. Kryptographie mit Quanten

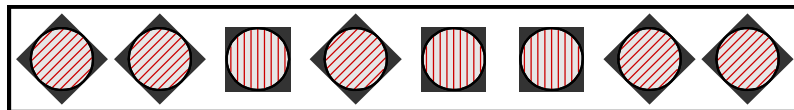
- Grundproblem:
 - Sicherer Transport von Geheimnissen
- Derzeitiger Ansatz:
 - Rechenoperationen, deren Umkehrung extrem zeitaufwendig ist
 - Gefährdet durch Quantencomputer
- Quantenkryptographie:
 - Echter Zufall
 - Messung zerstört Info
 - **Quantenparallelität nicht benötigt**

Protokoll zur Schlüsselerzeugung

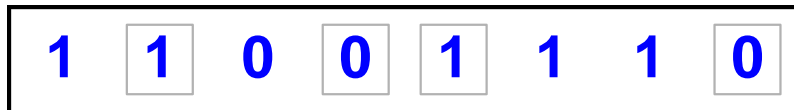
BB84-Protokoll (nach Bennett/Brassard 1984)



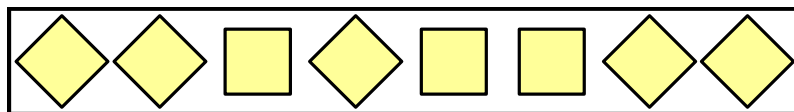
A sendet Photonen mit zufälliger Polarisation



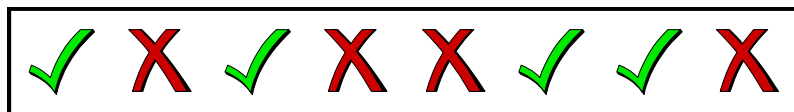
B wählt zufällige Filterstellungen



B führt Messung durch



B sendet Info über die Filterstellung



A sendet Info über deren Richtigkeit

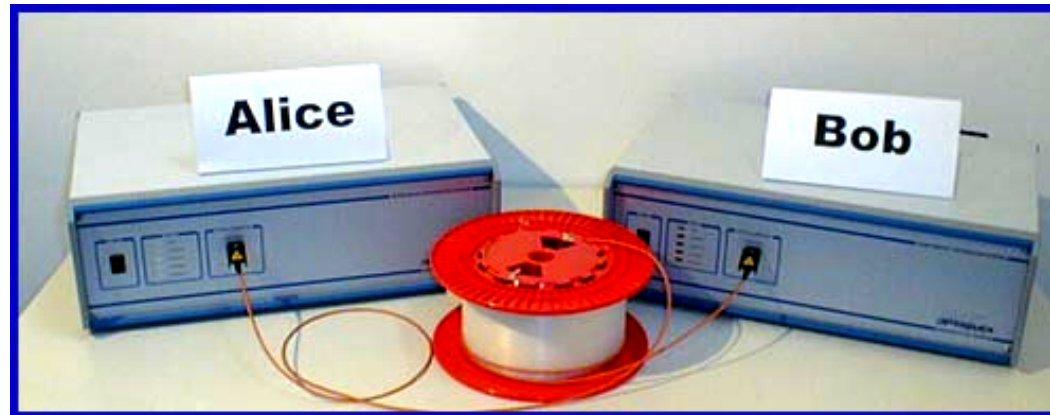


Verbleibende Bits sind der Schlüssel

Ergebnis und Probleme

- Braucht zwei Kanäle:
 - Optische **Direkt**verbindung
 - Beliebiger öffentlicher Kanal
- Abweichungen im geheimen Schlüssel:
 - Hinweis auf Spionage
 - Erkennung durch Hash oder Testübertragung
- Problem:
 - Fehler bei Übertragung und eigener Messung
 - Müssen toleriert werden
 - Müssen von Spionage unterscheidbar sein

Das erste Produkt



- **Hersteller:** id Quantique (Genf, Schweiz)
- **Faserlänge:** bis 70 km (nur Punkt-zu-Punkt)
- **Preis:** etwa US-\$ 90.000,-
- **Konkurrenz:** Quantum Confidential Inc. (Lacanada, USA)
- **Zukunft:** Optische Netze mit „quantentauglichen“ Routern

6. Ein Fazit

- **Wann?**
 - In 5 bis 100 Jahren ...
- **Wer?**
 - Forscher, Geheimdienste, Militär, Verbrecher, ..., alle.
- **Wie?**
 - Technologie noch nicht entschieden.
 - Mikroelektronik zwangsweise betroffen.
- **Wozu?**
 - Kryptographie
 - Naturwissenschaften
 - Datenbanken
 - ...

7. Literatur und Links

- **P. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.**
SIAM J.Sci.Statist.Comput. 26 (1997) pp. 1484-1509
- **J. Rink: Quäntchen für Quäntchen.**
c't Magazin für Computertechnik 16/1998, S. 150 ff.
- **A. Steane, E. Rieffel: Beyond Bits. The Future of Quantum Information Processing.**
IEEE Computer, Jan. 2000, pp. 38-45
- **R. Sietmann: Kleine Sprünge, große Wirkung.**
c't Magazin für Computertechnik 25/2000, S. 118-133
- **J. Mullins: The Topsy Turvy World of Quantum Computing.**
IEEE Spectrum, Febr. 2001, pp. 42-49
- **J. Mullins: Making Unbreakable Code.**
IEEE Spectrum, May 2002, pp. 40-45

- **Dieser Foliensatz und weitere Quellenhinweise:**
<http://tin.tu-ilmenau.de/ra/ver/#q02>