Vortrag über

QUANTENCOMPUTER

gehalten von
Marcus HARRINGER, Gregor KÖNIG,
Michael POBER, Klaus WERDENICH

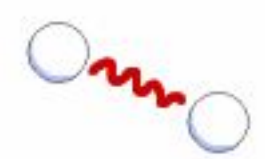
24.01.2002

Einleitung

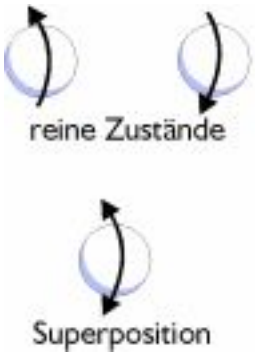
- massive Parallelrechner und absolut sichere Kodierungssyteme
- Erweiterung der Informationstechnologie um die Quantentheorie
- Idee 1982 von Richard Feynman: Nutzung von Quanteneffekten in Computern
- erfolgreichste und umstrittene physikalische Theorie

Zustände

- Verschränkung

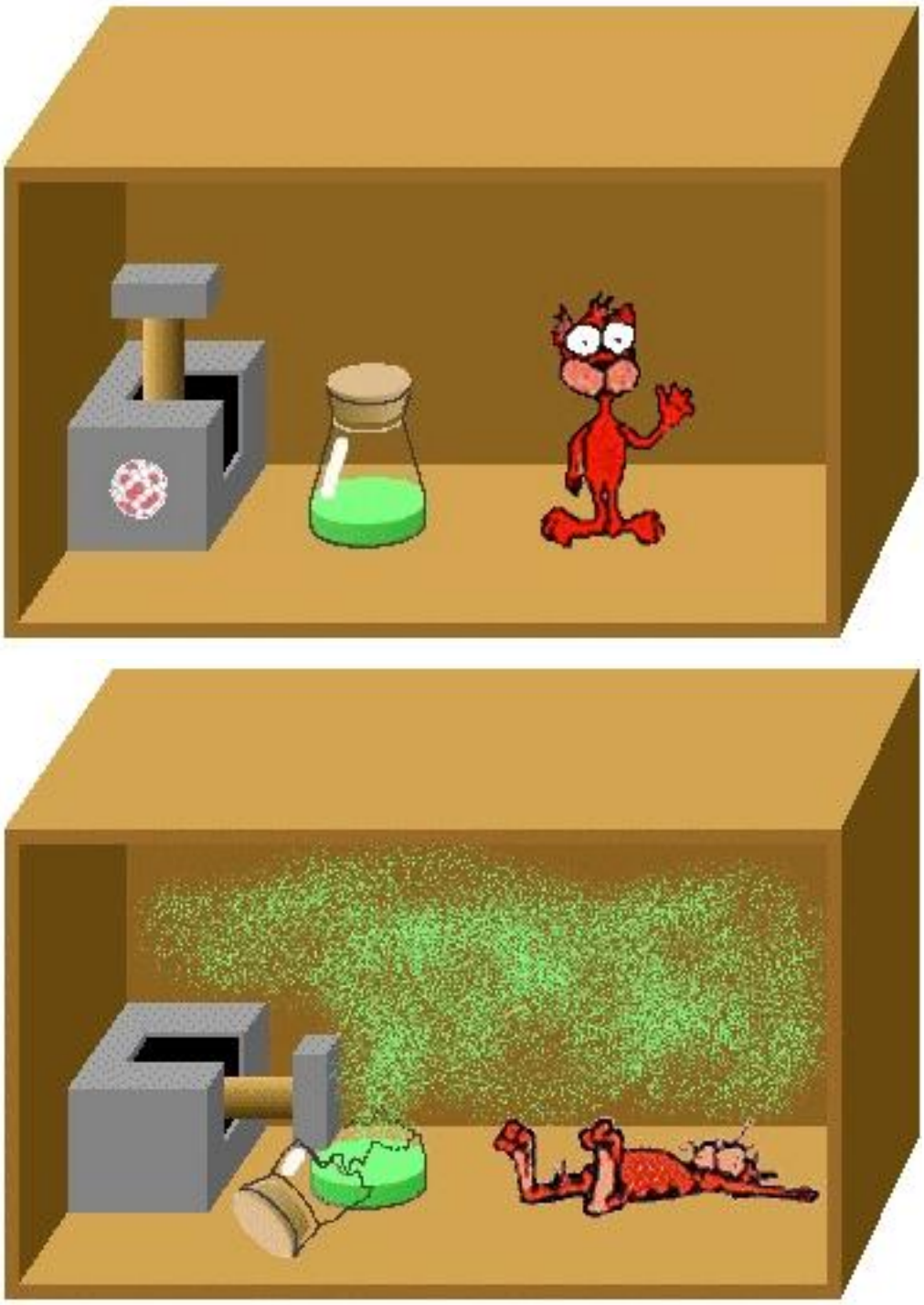


- Superposition



- Dekohärenz

Schrödingers Katze



Messung

- Messung zerstört komplett und unwiderruflich die Superposition
- Wahrscheinlichkeitsamplitude
- Quantenalgorithmen
- Qubits beeinflussen sich gegenseitig
- Operatoren so einsetzen, daß der richtige Zustand Wahrscheinlichkeit 1 hat und alle anderen durch Interferenz den Wert 0

Algorithmen

Algorithmen

- N=pq
- Standardalgorithmus: expontentiell viele Rechenschritte
- Kryptoverfahren (RSA)
- Quantenrechner: simultan N durch Zahlen teilen
- Problem: Überlagerung der Ergebnisse
- Zufällige Wahl des Ergebnisses
- Wieder Exponentiell

- Peter Shor Algorithmus
- $$f(a) := x^a mod N$$
- Klassischer Computer kann Periode r nicht effizient berechnen
- Ziel: kleinste Periode berechnen

1. Quantenregister mit 2 Teilen
2. Teil 1: Superposition aller ganzen Zahlen für die Funktion
3. f auf Teil 1 anwenden

4. Ergebnis in Teil 2 speichern

5. Messung von Teil 2 liefert k mit

$$x^a mod N = k$$

6. Durch Messung ist Teil 1 kollabiert

7. Messung mit gleicher Wahrscheinlichkeit - zweite Messung nötig.

8. Trick: Auf Teil 1 jetzt eine diskrete Fouriertransformation anwenden

9. Ergebnis: Superposition mit 'Peaks' genau bei Vielfachen von 1/r

10. Heisst: Messung mit hoher Wahrscheinlichkeit in der Nähe eines solchen Vielfachen

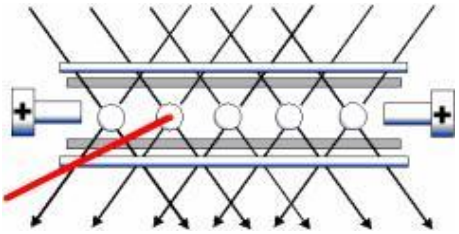
11. Ein paar Wiederholungen

12. Algorithmus ist probabilistisch

Realisierung von Quantenrechnern

Ionenfalle

- Quanten: Kette lasergekühlter Ionen



- Qubits: Anregungszustand der Ionen

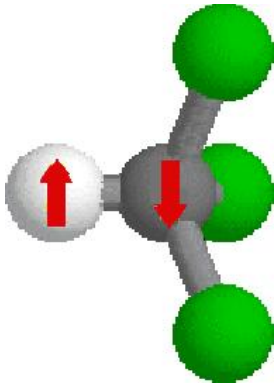
- Operationen und Messungen: Durch Laserimpulse bei Resonanzfrequenz

- Kriterien:
  - Kühlung der Ionen
  - Absolutes Vakuum
  - Präzise Laserimpulse

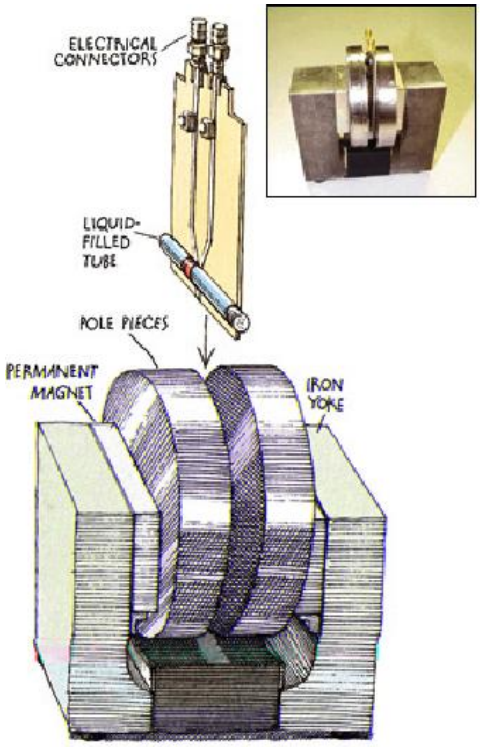
NMR - Nuclear Magnetic Resonance

- Quanten: Atomkerne von Flüssigkeits - Molekülen

- Qubits: Spin der Atomkerne



- Operationen und Messungen: Durch Radiowellen spezifischer Frequenz



- Vorteile:
  - Bei Zimmertemperatur realisierbar
  - Kein Vakuum notwendig
  - Etablierte Technik

qUanTenkRyptogrAPhiE

Begriffdefinition

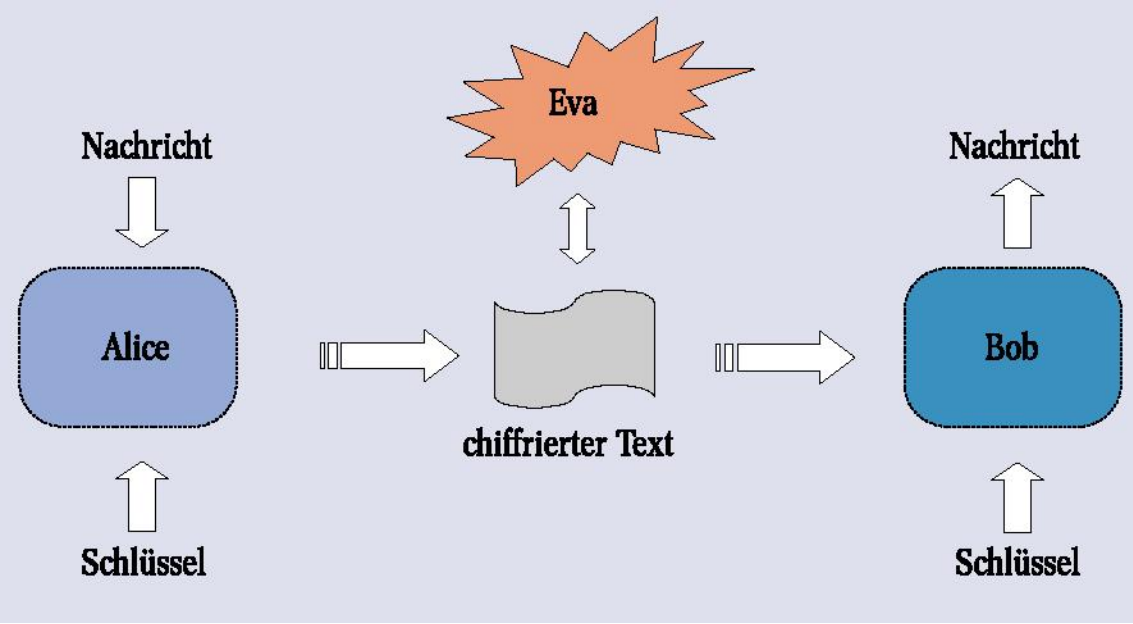
Was ist Kryptographie? Kryptographie ist die Kunst, eine Nachricht so zu verschlüsseln, dass sie fuer unbefugte Personen unlesbar und ohne jeglichen Informationsgehalt ist.

Was ist Quantenkryptographie? Anwendung im Gebiet der Quantenkommunikation, deren Aufgabe es ist sichere Verschlüsselungen mit Hilfe der Eigenschaften der Quantenmechanik zu generieren.

one time pad

- Verschlüsselung durch private Schlüssel

- Sicherheit ist mathematisch bewiesen



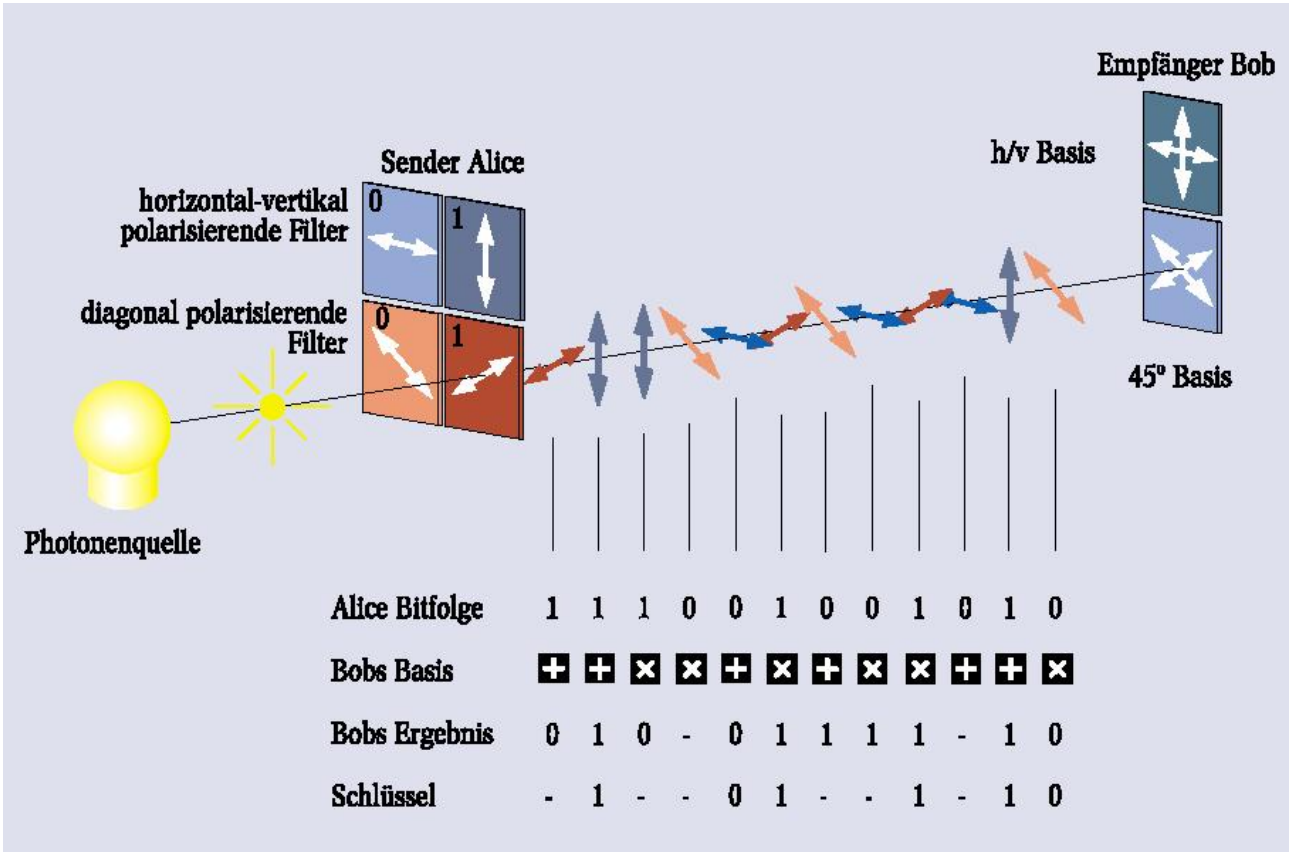
Funktionsweise der Quantenkryptographie

- I. Die quantenmechanische Schlüsselübertragung durch Einteilchensysteme

  - Polarisationskodierung einzelner Photonen

  - Photonen mit 4 Zuständen werden 2 Werte zugewiesen

    horizontal sowie unter -45 Grad polarisierte Photonen mit dem Bitwert 0 und vertikal sowie +45 Grad polarisierte mit dem Wert 1.

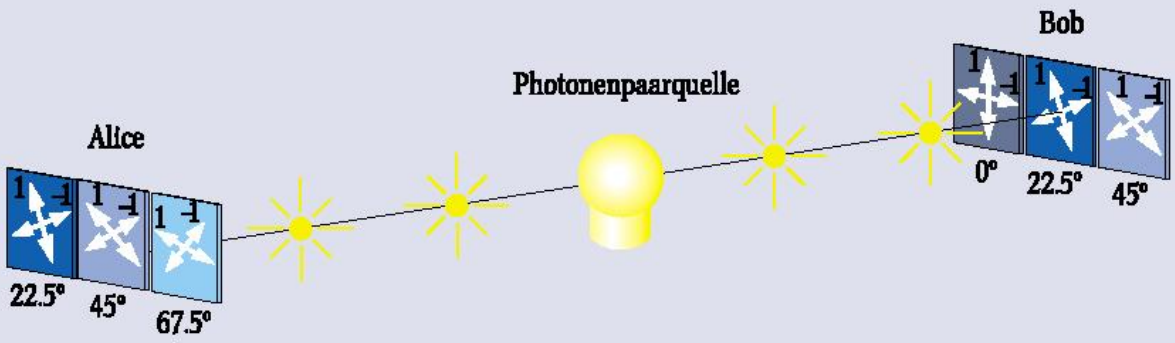

Empfänger Bob
h/v Basis
Sender Alice
horizontal-vertikal polarisierende Filter
0
1
diagonal polarisierende Filter
0
1
45° Basis
Photonenquelle
Alice Bitfolge 1 1 1 0 0 1 0 0 1 0 1 0
Bobs Basis + + × × + × + × × + + ×
Bobs Ergebnis 0 1 0 - 0 1 1 1 1 - 1 0
Schlüssel - 1 - - 0 1 - - 1 - 1 0

Schritt für Schritt

- Sender: Photon in Polarisationszustand versetzen
- Sender: Protokollieren des Zustands
- Empfänger: Wahl des Analysators
- Empfänger: Wahl des Analysators und Ausrichtung des Photons protokollieren
- Vergleich der Listen zwischen Sender und Empfänger

- II. Die quantenmechanische Schlüsselübertragung durch Zweiteilchensysteme

  - Polarisationskodierung mit verschränkten Photonen



Alice Basis	22.5°	67.5°	45°	22.5°	67.5	45°	45°	45°	67.5°	67.5°	22.5°	45°
Alice Ergebnis	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
Bobs Basis	45°	0°	45°	0°	22.5	45°	22.5°	22.5°	0°	45°	22.5°	22.5°
Bobs Ergebnis	1	-1	-1	1	-1	-1	1	-	1	1	-1	1
Differenz	22.5°	67.5°	0°	22.5°	45°	0°	22.5°	22.5°	67.5°	22.5°	0°	22.5°
Klasse	Bell	Bell	Code	Bell	-	Code	Bell	-	Bell	Bell	Code	Bell
Schlüssel	-	-	0	-	-	0	-	-	-	-	0	-

- 3 Ergebnisse der Messungen:

  1. perfekte korrelierte Ergebnisse

  2. gewählten Orientierungen ermöglichen einen Test der Bell-Ungleichungen.

  3. nichtkompatible Orientierungen

Probleme der Praxis

- perfekt Korrelation der Bitabfolgen in Abwesenheit eines Spions ist nicht Realität

- Absorption von Photonen durch Transmissionsverlust in Glasfaser

heute und morgen

- es ist bereits möglich die sichere Übertragung von Nachrichten zu garantieren

- Verbesserungsbedarf besteht vor allem in der Distanz sowie der Übertragungsrate