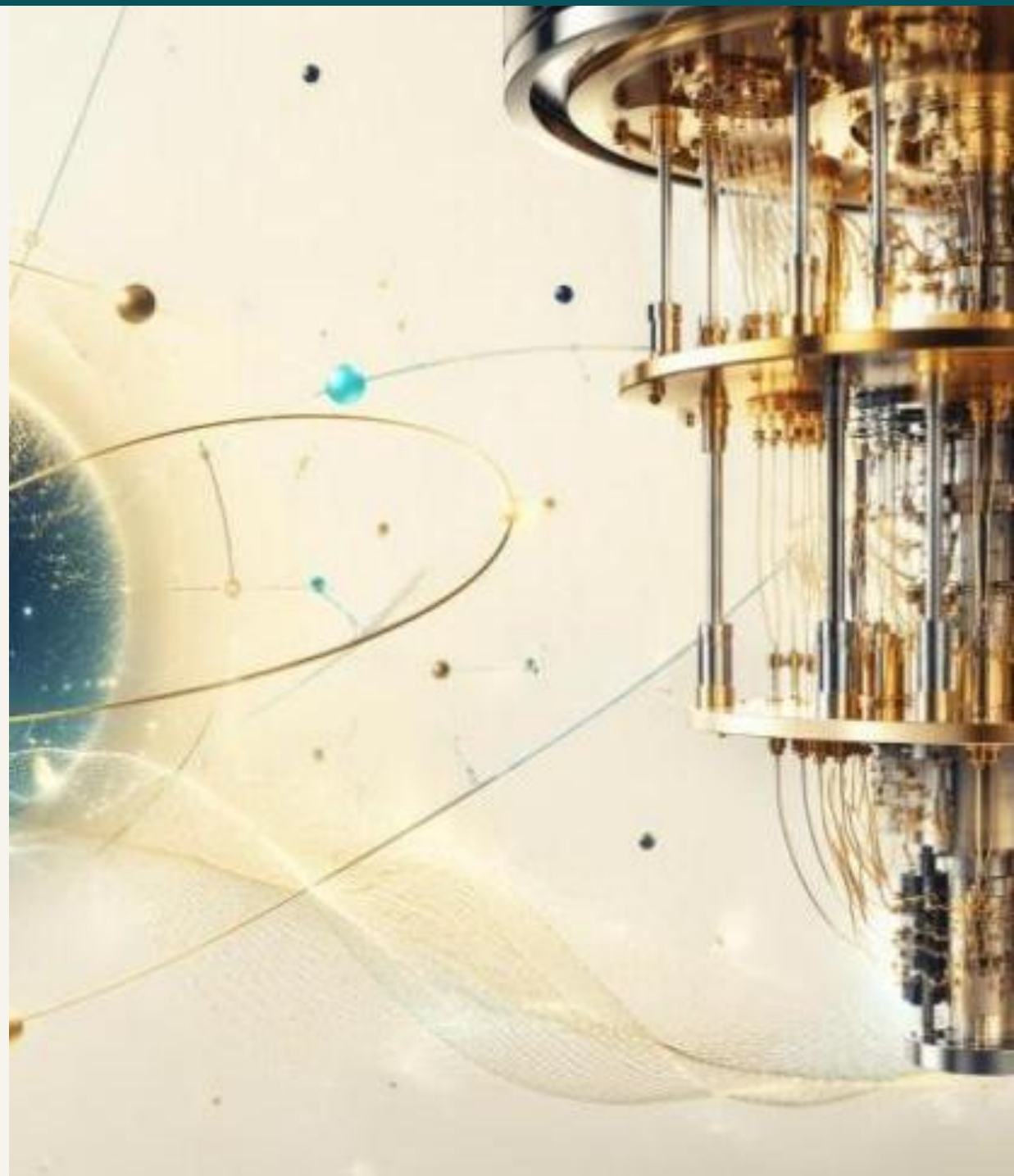
Was ist Quanteninformation und warum können Quantencomputer sie effizient verarbeiten?

Barbara Kraus



Überblick

1. Klassische Information
2. Quanteninformation, Anwendungen der Quanteninformation
3. Wie funktionieren Quantencomputer?
4. Fortschritte & Herausforderungen

1. Klassische Information: Von Symbolen zu Bits

Vom Zählen per Hand zu Symbolen, Zahlensystemen, Bits und klassischen Computern.

Zählen

Hierogl. Schrift

Abakus

XIV

Römische Zahlen

123.45

Dezimal-zahlen

Bits + Computer

Was führte zu diesem Übergang?

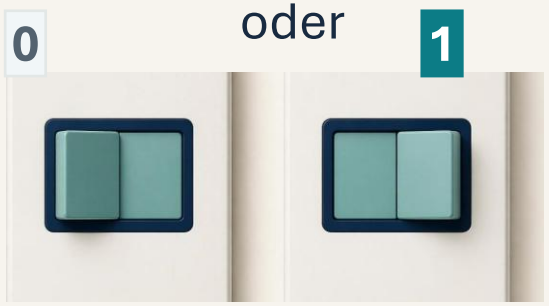
- Effizienter rechnen
- Neugier
- Neue Technologien

Klassische Information: Bits

Ein Bit ist eine 0/1-Entscheidung; jede klassische Nachricht kann als Bitfolge kodiert werden.

Bit
wie ein Lichtschalter

entweder
oder



Bitfolge = klassische Information

0	1	0	1	1	0	1	0	0	1

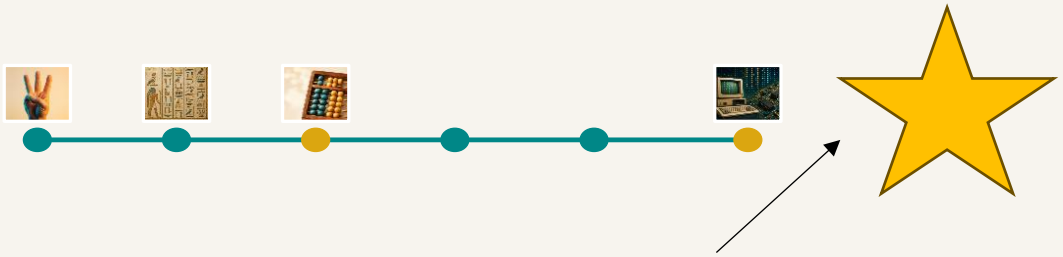
Beispielkodierung: A → 0001, B → 0010,
…

Ein klassisches Bit hat einen eindeutigen Wert: entweder 0 oder 1

Klassische Computer verarbeiten lange Bitfolgen

Klassische Information wird als Bits dargestellt; Rechnen transformiert Bitfolgen.

Ein Bit ist die Grundeinheit der klassischen Information



Der nächste Schritt ist nicht „ein kleineres Bit“
sondern eine völlig neue Theorie!

?

Warum?

Atome und Licht verhalten sich nicht wie winzige klassische Objekte.

Wir brauchen eine neue Theorie, die Quantenphysik, um sie zu beschreiben

⇒ neue Art von Information möglich.

Neue Theorie: Quantenphysik

Auf atomaren Skalen gelten andere Regeln.

Um 1900: neue Technologie ⇒

einzelne Atome, Elektronen und Photonen

Die klassische Physik konnte ihr Verhalten nicht erklären.

Alltagswelt (>10^{-3} m)

Klassische Physik funktioniert gut

Mikroskopische Welt (<10^{-9} m): Atome, Elektronen, Photonen

Klassische Physik beschreibt sie nicht mehr korrekt

Benötigen eine neue Theorie: Quantenphysik

Quantenphysik ist keine kleine Korrektur zur klassischen Physik - sie ist eine völlig neue Theorie zur Beschreibung von Materie und Licht

2. Quanteninformation: Von Bits zu Qubits

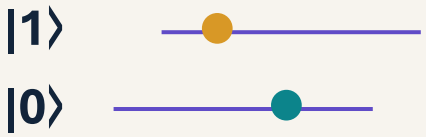
Klassisches Bit

entweder

0 oder 1

Ein klassisches Bit hat einen eindeutigen Wert
(vor und nach dem Ablesen).

Qubit



Energieniveaus
(z. B. Atom)

Superposition

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

In $|0\rangle$ und $|1\rangle$ gleichzeitig

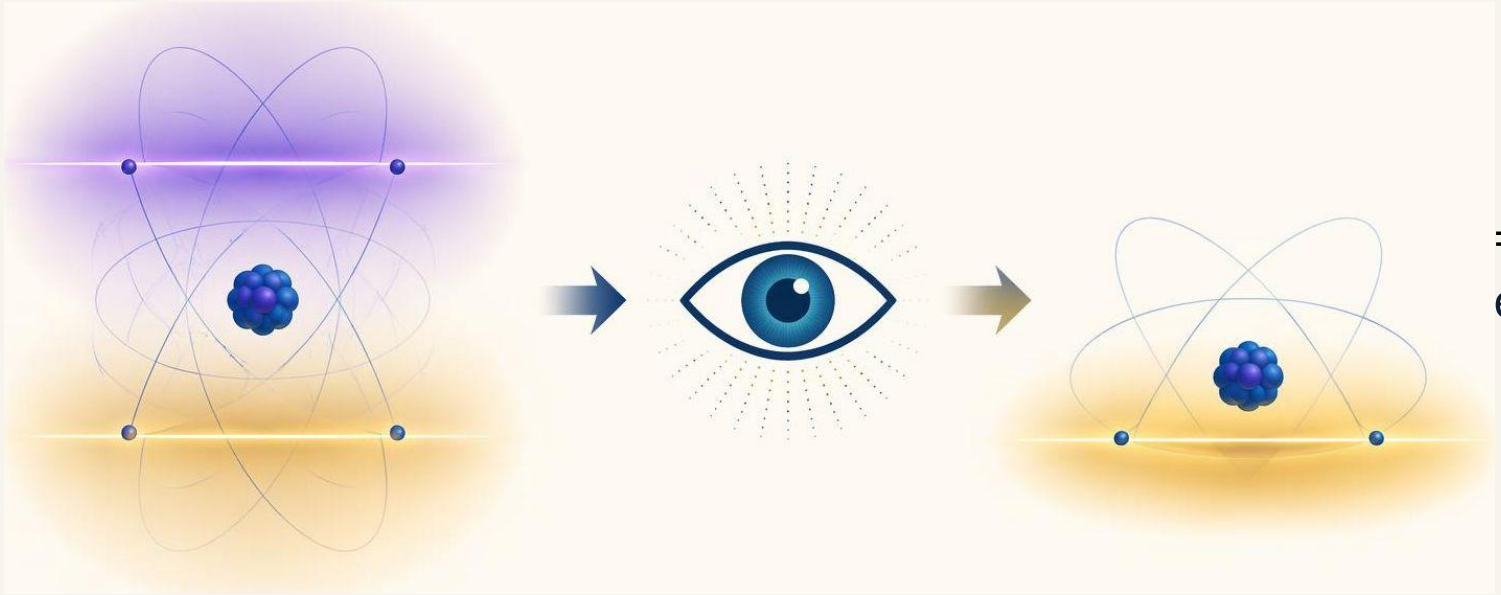
Ein Qubit (quantenmechanisches Bit) kann gleichzeitig im Zustand 0 und 1 sein (und in allen möglichen Superpositionen).

Messung verändert den Zustand

„Hinschauen“ in der Quantenwelt verändert im Allg. den Zustand des Systems

Superposition **Messung** **Ergebnis**

vor der Messung:
Superposition
von „0“ und „1“



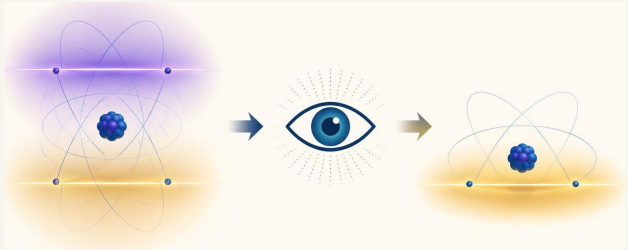
⇒nach der Messung:
ein Ergebnis, 0 oder 1

Eine Messung liefert klassische Information und verändert den Quantenzustand.
⇒ Man kann nicht einfach „in“ den Quantenzustand hineinschauen.

Verschränkung: Korrelationen ohne klassisches Gegenstück

1 · Superposition

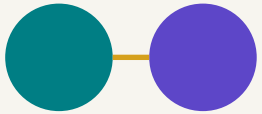
einzelnes Qubit



$$|0\rangle + |1\rangle$$

2 · Verschränkung

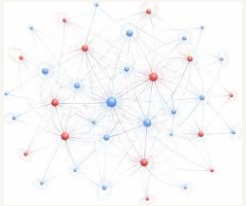
zwei Qubits, starke Quantenkorrelationen



$$|00\rangle + |11\rangle$$

3 · Mehr-Qubit-Verschränkung

Starke Korrelationen, der gemeinsame Zustandsraum wächst exponentiell



$$\mathcal{H} = 2^n$$

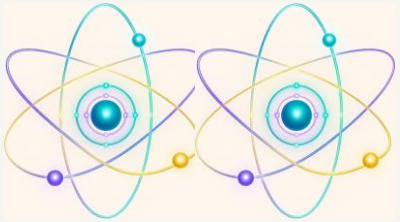
$$|000\ldots0\rangle + |111\ldots1\rangle$$

$$\sum_{i_1,i_2,\ldots i_n=0}^{1} c_{i_1,i_2,\ldots i_n} |i_1, i_2, \ldots i_n\rangle$$

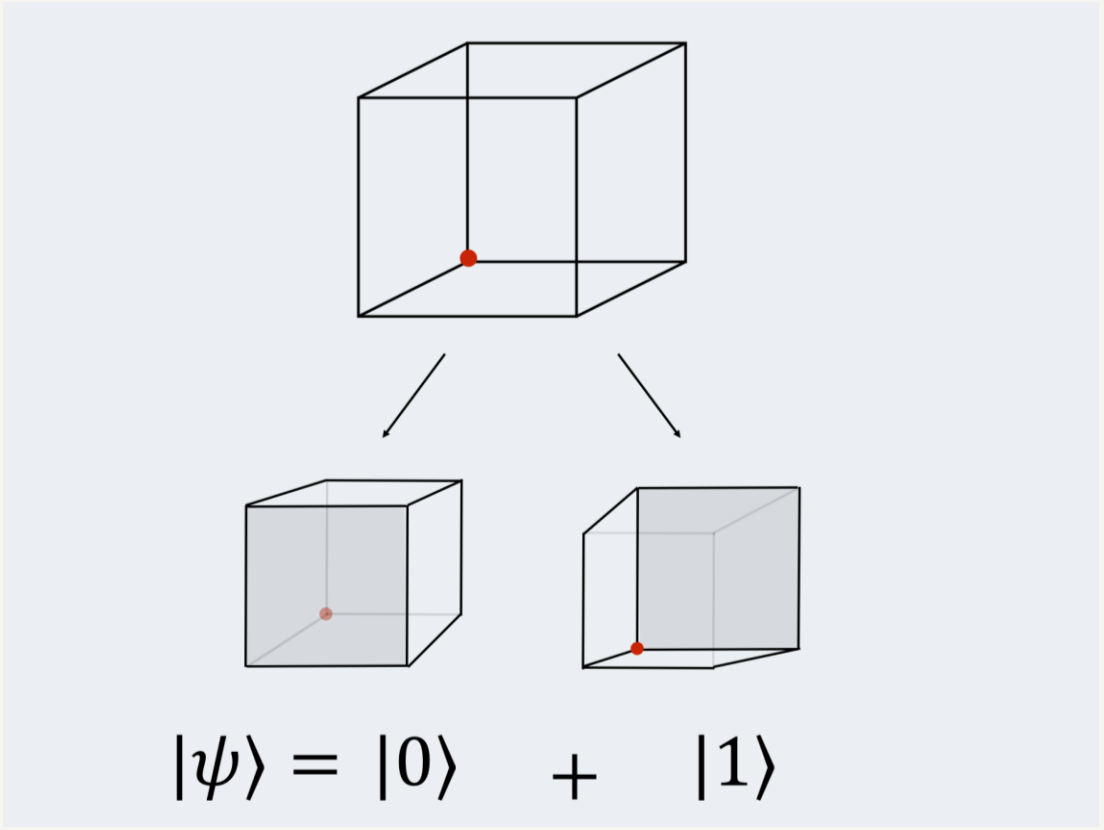
Verschränkung ist eine zentrale Ressource für Quantencomputing.
Der Zustandsraum wächst exponentiell mit der Zahl der Quantensysteme.

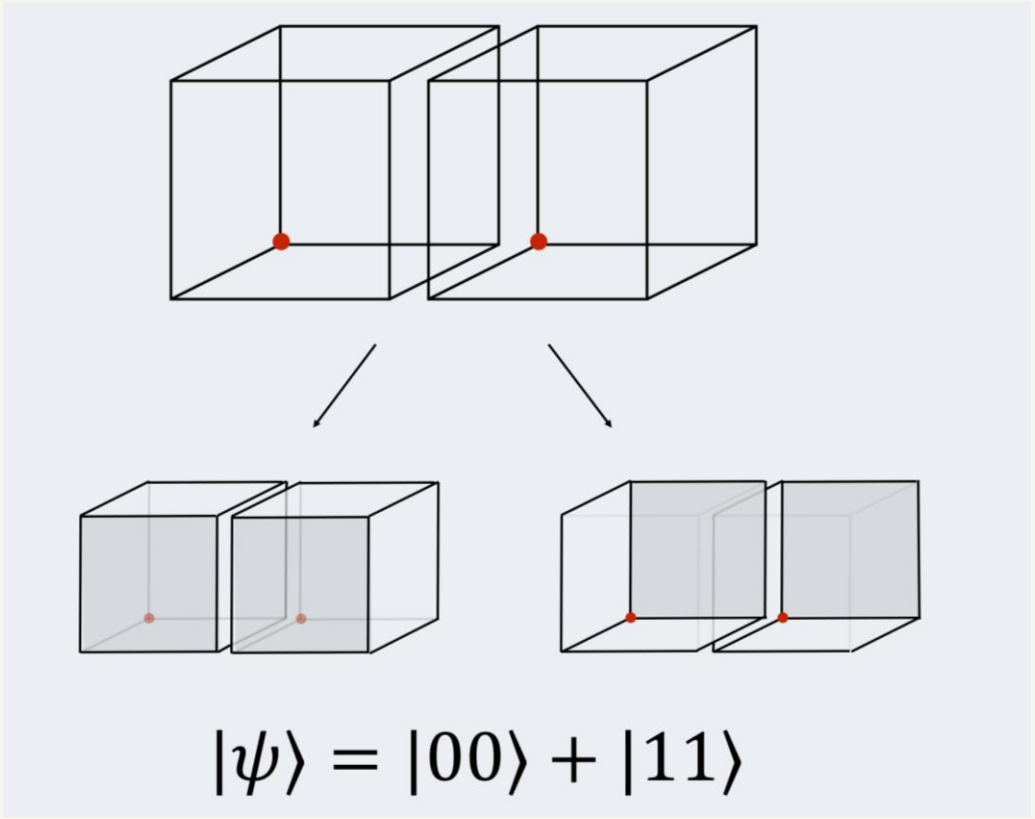
Verschränkung – starke quantenmechanische Korrelationen ohne klassisches Gegenstück

Superposition



Verschränkung





Anwendungen

Quanten-kryptographie

Satelliten
Langstrecken
Repeater

Quanten-computing

Klassische Algorithmen

Simulation / Berechnung
quanteninspiriert

Präzisions-messungen

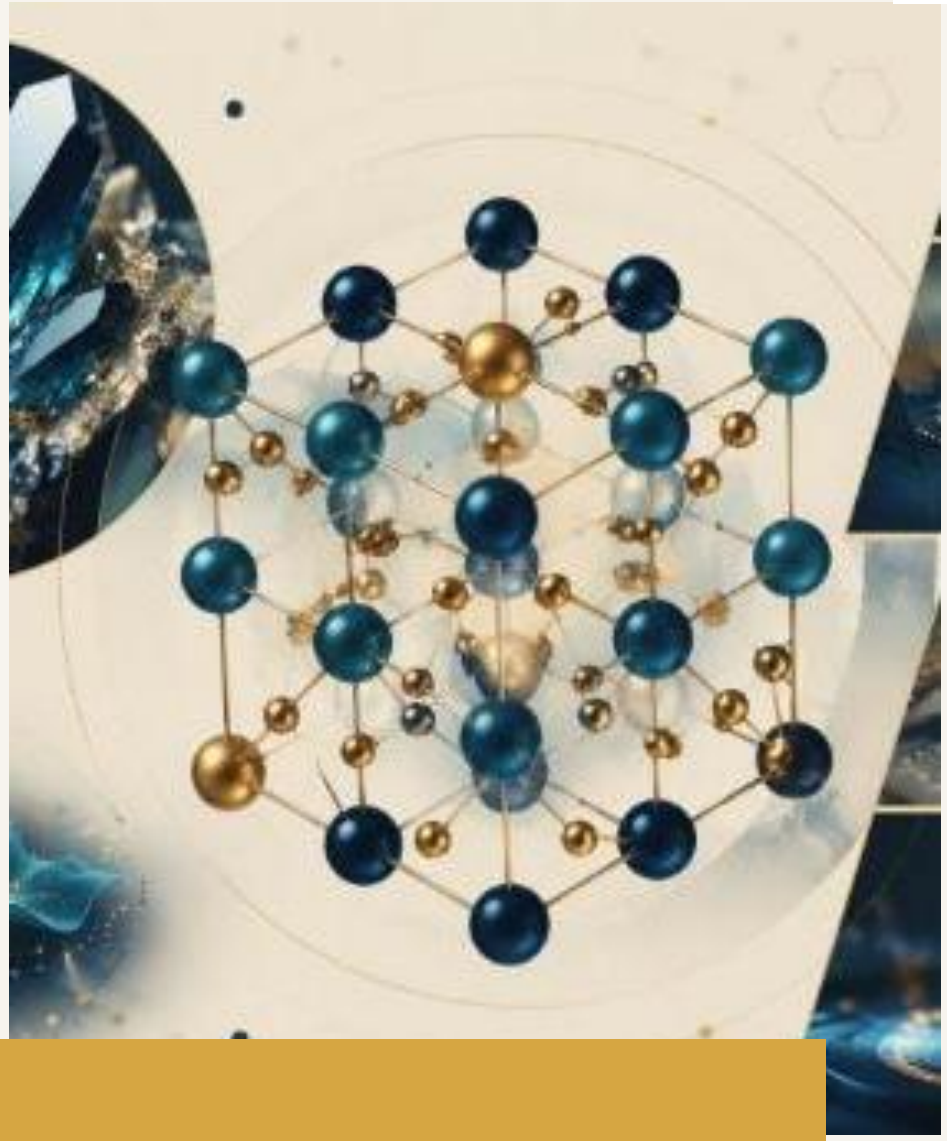
sehr hohe Genauigkeit,
z. B. Atomuhren

Quanten-simulationen

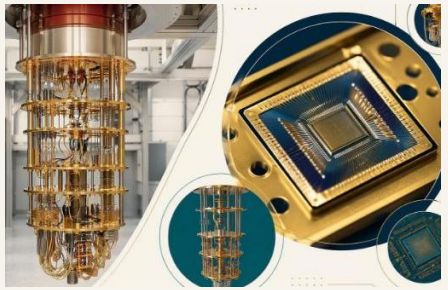
Erfolg der Quanteninformationswissenschaft und -technologie

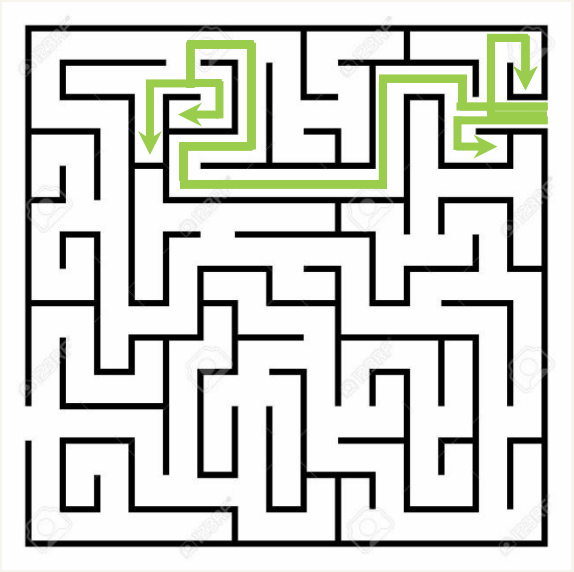
3

Wie funktionieren Quantencomputer?



Idee, warum Quantencomputer effizienter sein könnten



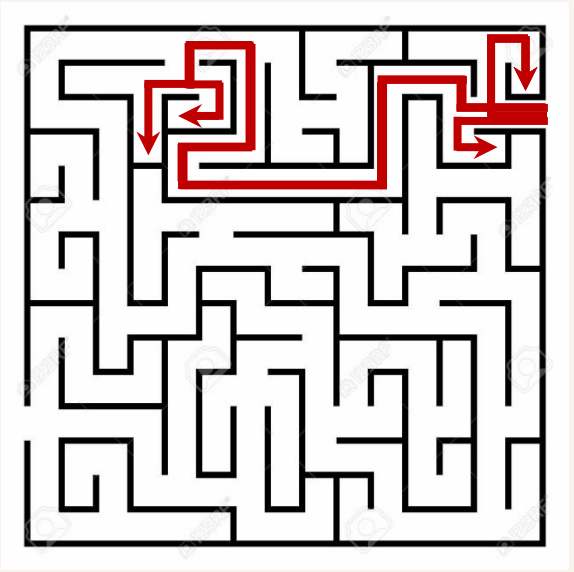


$|0\rangle|0\rangle$

$|0\rangle|1\rangle$

$|1\rangle|0\rangle$

$|1\rangle|1\rangle$



$|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle$

Superposition kann genutzt werden, um Dinge parallel zu tun, aber das reicht nicht aus! Wir müssen Informationen auslesen können (Messung!)

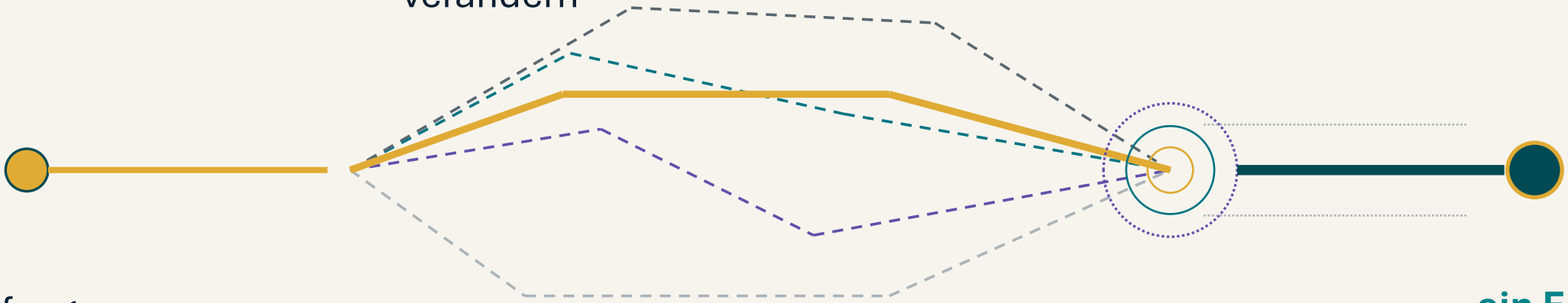
Wie ein Quantenalgorithmus funktioniert

1 **Vorbereiten**
Qubits im Startzustand

2 **Gatter**
QI verarbeiten, Zustand kontrolliert verändern

3 **Interferenz**
nützliche Teile verstärken, andere auslöschen

4 **Messen**
klassisches Ergebnis auslesen



Anfangs-zustand

viele mögliche Pfade

Interferenz

ein Ergebnis wird verstärkt

Ein Quantenalgorithmus nutzt Superposition, Interferenz und Verschränkung, sodass gewünschte Ergebnisse verstärkt werden.

Beispiel: Grover-Algorithums mit 4 Möglichkeiten (2 bits)

Aufgabe: Unter vier möglichen Antworten ist genau eine richtig.

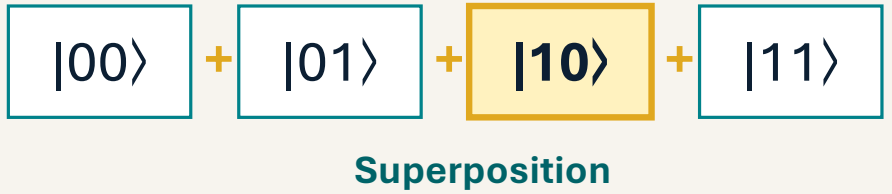
Klassisch

Man kann Kandidaten nacheinander prüfen:

die klassische Komplexität ist linear:
N Kandidaten ⇒ ~N Prüfungen

Quantenalgorithmus

Zwei Qubits in Superposition aller vier Basiszustände :



nicht alle vier Antworten werden geprüft
Q. Algorithmus transformiert Q. Information so, dass **|10⟩** am Ende wahrscheinlicher gemessen wird.

Q. Algorithmus: Interferenz schwächt falsche Wege ab und verstärkt die gesuchte Antwort.

Grover-Algorithmus: Schritt für Schritt

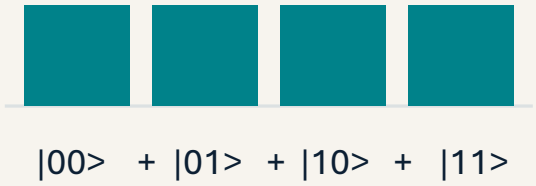
vier Möglichkeiten, eine davon ist die Lösung |10⟩.

1 Start

Alle vier Zustände sind gleich wahrscheinlich.

Superposition

Aller möglichen Zustände



alle Zustände gleichwahrscheinlich

2 Oracle

Die richtige Antwort wird markiert (z.B. hat spez.Eigenschaft)

Mit Phase markieren

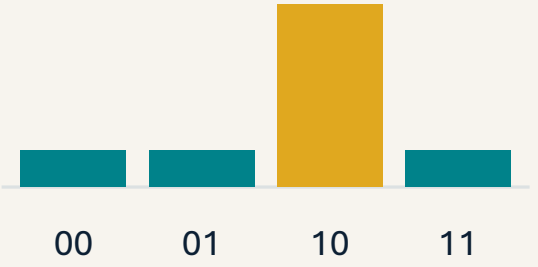
Lösung |10⟩ bekommt ein Minuszeichen

markiert, aber noch nicht messbar

3 Interferenz

Da anderes Vorzeichen -> kann Messwahrscheinlichkeit für |01> verstärken

Interferenz verschiebt Gewicht zur Lösung



Lösung |10⟩ wird mit hoher Wahrscheinlichkeit gemessen

Merksatz: Grover sucht nicht durch schnelleres Ausprobieren, sondern durch gezieltes Verstärken der richtigen Amplitude.

Anwendungen von Quantencomputern

1

1 · Spezielle Algorithmen

Shor: Faktorisierung
Grover: Suche

⇒Kryptographie muss quanten-sicher werden

Quantenkryptographie
Post-quantum secure Kryptofraphie

2

2 · Optimierung

Optimierung: effizienter lösen?

Beispiele:
Traveling salesman problem, Grover, Heuristiken

3

3 · Simulation

Moleküle und Materialien sind selbst Quantensysteme

Klassische Simulation sehr schwierig ($\mathcal{H} = 2^n$)

→ Untersuchung von Materialien & Chemie

4

Fortschritte und Herausforderungen

Quantum supremacy – Quantenvorteil

DURCHBRUCH

nature

View all jou

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature › articles › article

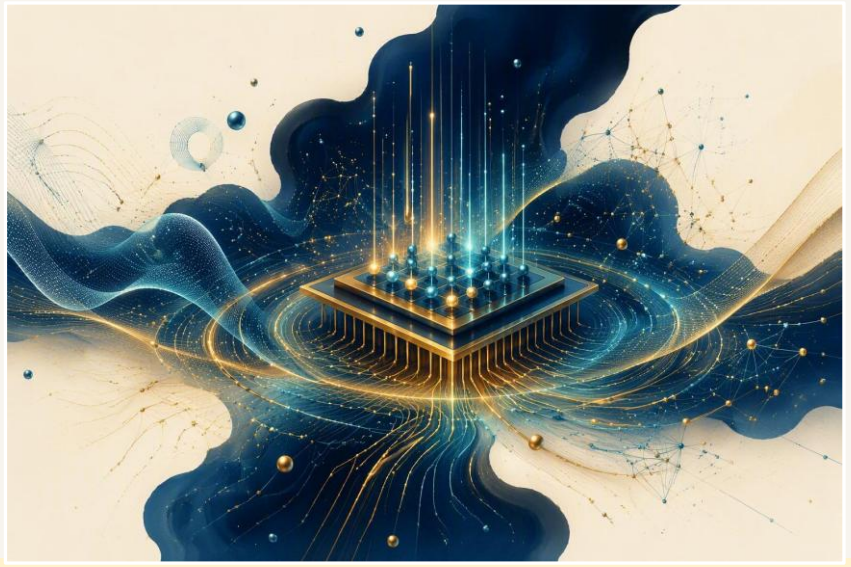
Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, ... John M. Martinis ✉ + Show authors

Nature **574**, 505–510 (2019) | Cite this article

Google, 2019



Quantencomputer hat klassischen Computer übertroffen!
Behauptung: klassischer Computer braucht ~10.000 Jahre

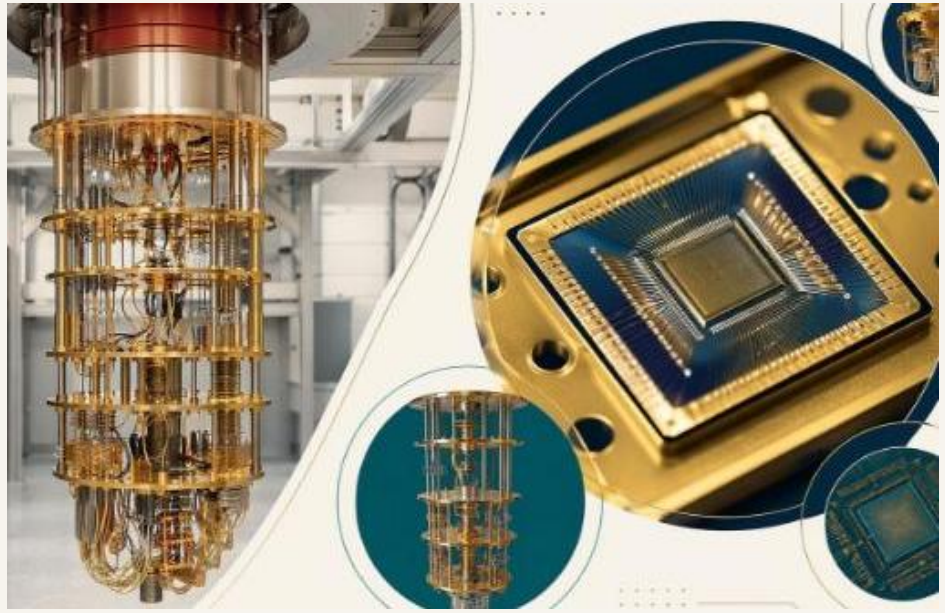
Problem war nebensächlich,
jetzt: wichtiges, praktisches Problem lösen und klassischen Computer übertreffen.

Plattformen: viele Wege, Qubits zu bauen

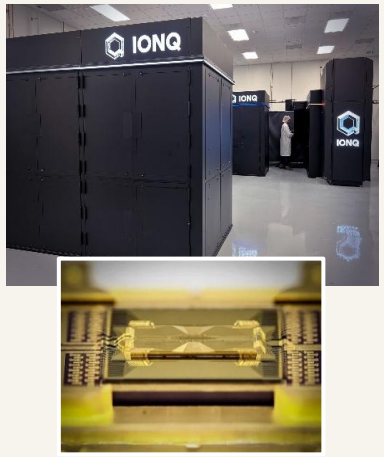
Gefangene Ionen

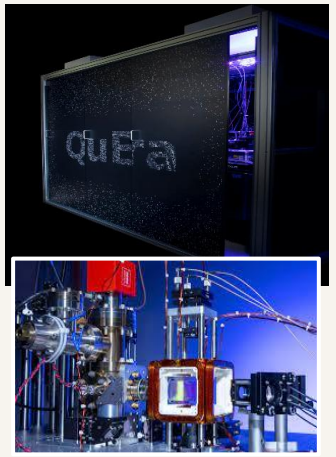
Supraleitende Qubits

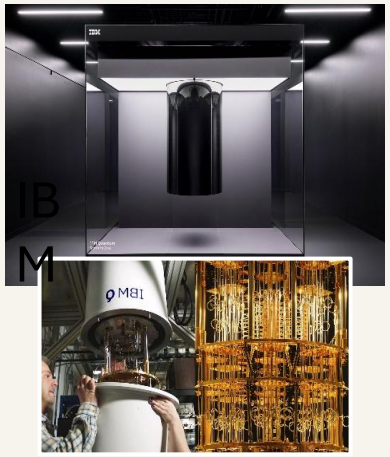
Neutrale Atome



Weitere Plattformen
Photonen, Halbleiter-Spins, ...







Herausforderung: Fehler und Skalierung

Quanteninformation ist fragil

Wechselwirkung mit Umgebung → Rauschen, Fehler

Kohärenz und Verschränkung gehen verloren

Berechnung kann fehlschlagen

Skalierung?

Es braucht größere Systeme. Aber „einfach“ mehr Qubits reichen nicht; auch niedrige Fehlerraten sind nötig

NISQ (rauschende Quantencomputer mittlerer Größe)

10–500+
Physikalische Qubits

≈1000+
Operationen, bevor Fehler dominieren

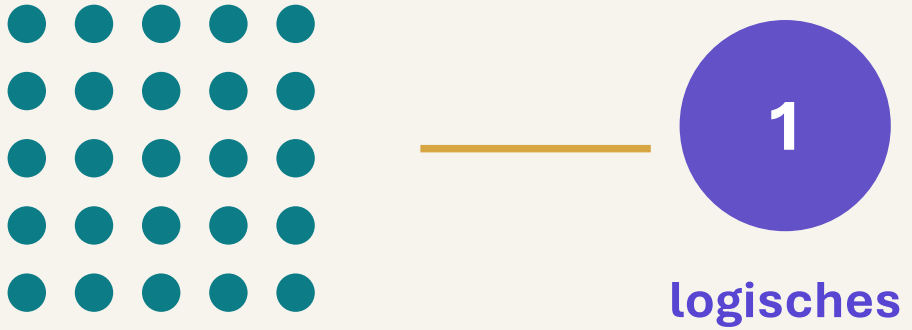
⇒Für Quantenberechnung im großen Maßstab braucht es beides: mehr Qubits und niedrige Fehlerraten -> Fehlerkorrektur

Quantenfehlerkorrektur

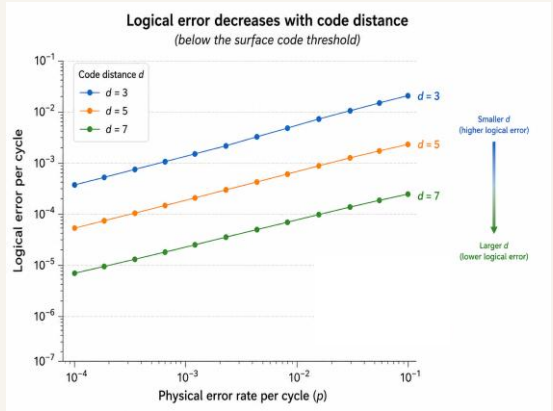
Viele physikalische Qubits für ein logisches Qubit

Vielteilchenverschränkung nutzen, um Quanteninformation zu schützen

Ziel: logische Fehlerraten kleiner als physikalische Fehlerraten.

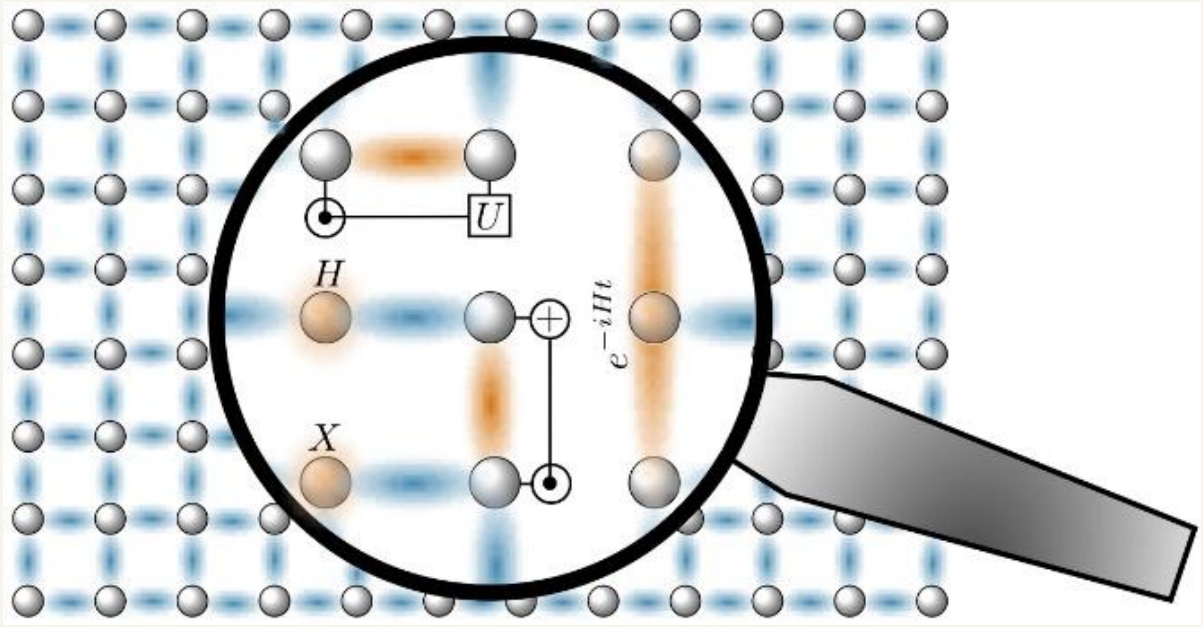


Durchbruch



Verhalten unterhalb der Schwelle wurde experimentell gezeigt!

Herausforderung: Verifikation



können nicht einfach hineinschauen: Messung verändert den Zustand

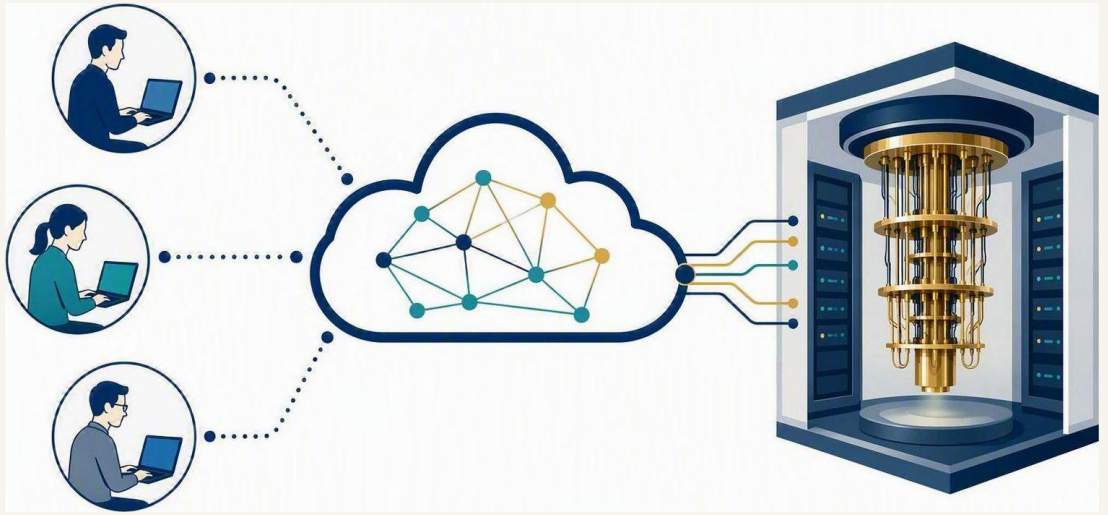
wollen QC verwenden um Probleme zu lösen, die klassisch schwer zu prüfen sind

brauchen Tests, die Fehler abschätzen, ohne die Berechnung zu zerstören

Verschiedene Szenarien des QC

Direkter Zugriff

Cloud-Computer



Wie können wir Quantenberechnungen verifizieren?

Klassisches Rechnen	Quantencomputing
Tracing	Messung verändert den Zustand
Berechnungen ausführen deren Ergebnisse wir kennen, oder leicht prüfen können,	Berechnungen ausführen deren Ergebnisse wir kennen, oder leicht prüfen können
	kleinere Systeme, crossplatform Verifizierung

Fazit

1. **Klassische Information - Bits**

   Rechnen transformiert Bitfolgen

2. **Quanteninformation ist sehr anders**

   ⇒ Superposition, Messung und Verschränkung
   neue Anwendungen.

3. **Quantencomputer**

   Wie wird Quanteninformation verarbeitet, Algorithmen, Optimierung, Quantensimulation

4. **Fortschritte & Herausforderungen**

   Rasche Entwicklung, Fehler, Skalierung, Fehlerkorrektur, Verifikation.

Danke

Where Quantum and Fluids entangle

PASQuanS2

Munich Quantum Valley