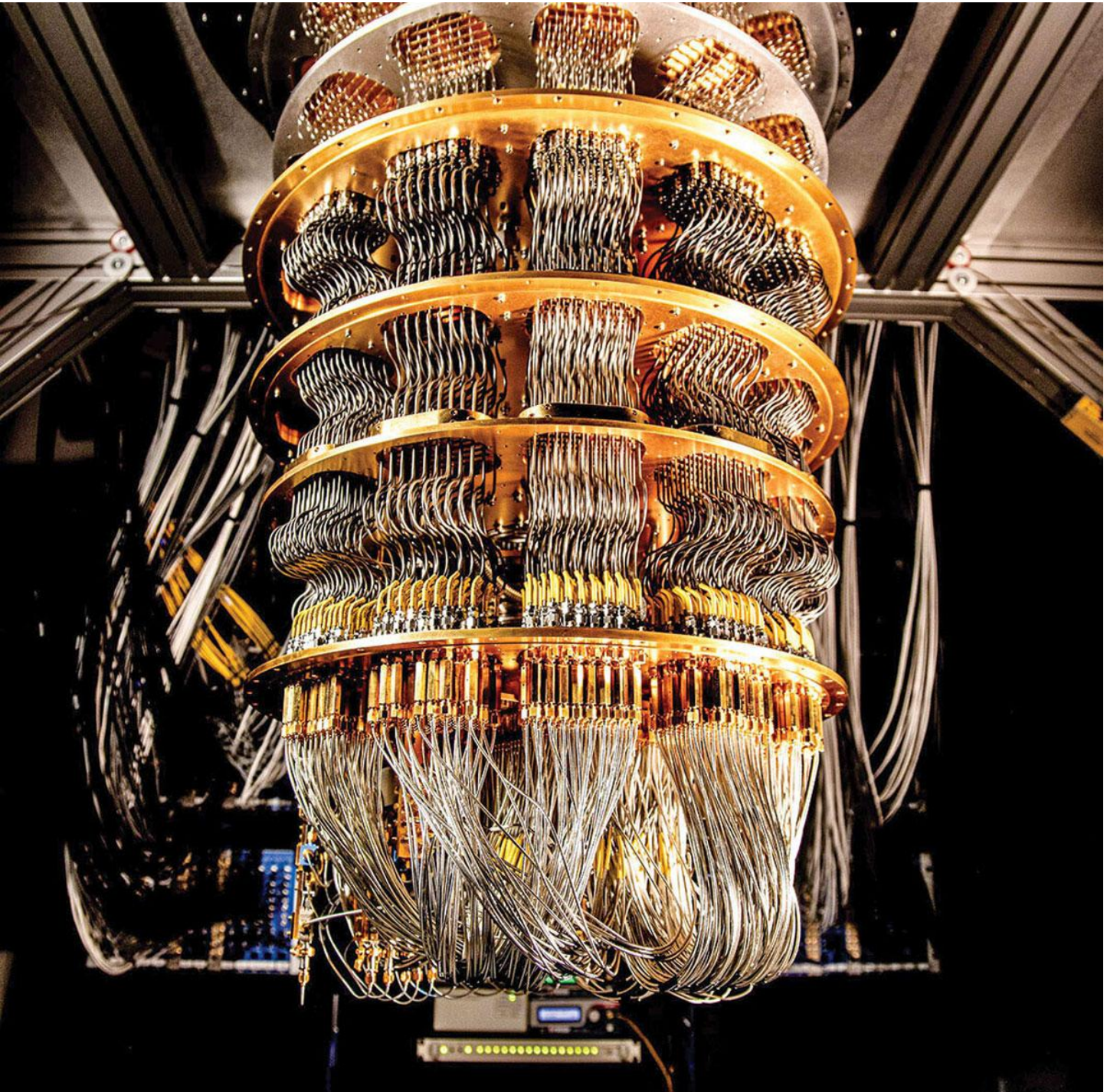
Quantentechnologie

Wie die Physik des Allerkleinsten die Welt von morgen revolutioniert

21. 1. 2026 Gunter Eger



Inhalt

- Erste und zweite Quantenrevolution
- Quantencomputer: Der Heilige Gral
  - Wie funktioniert ein Quantencomputer?
  - Anwendungen und prinzipielle Einschränkungen
  - Technologische Herausforderungen
  - Entwicklungsstand QC heute
- Quantenkommunikation
  - Quanteninternet
  - Quantenteleportation
- Quantenkryptographie
- Quantensensorik
- Quantensimulation
- Quantenchemie

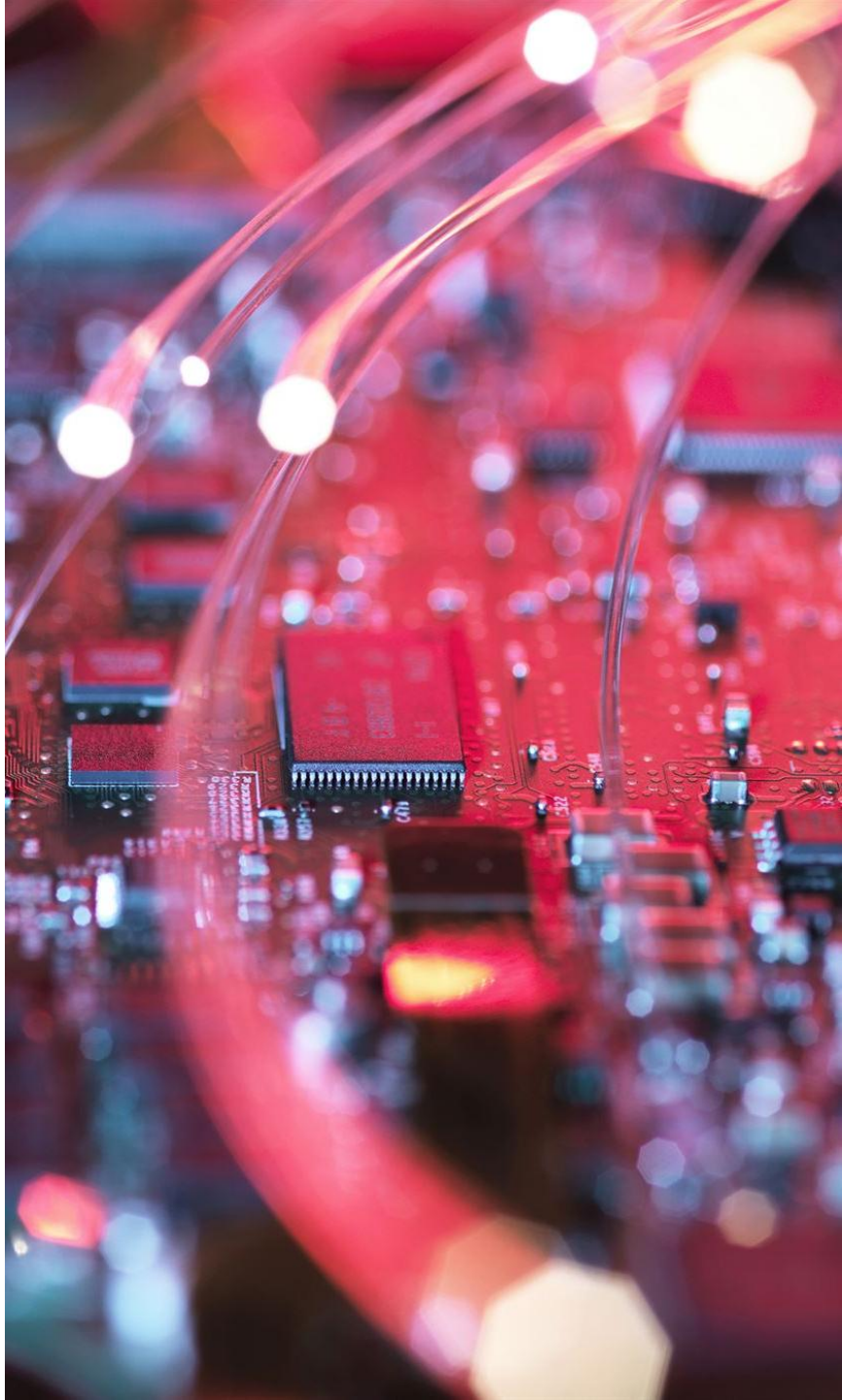
Die erste Quantenrevolution

Im 20. Jahrhundert erblickte eine ganze Reihe von Technologien das Licht der Welt, die nur mit einem grundlegenden Verständnis der Quantenphysik entwickelt werden konnten. Diese Technologien sind heute nicht mehr aus unserem Alltag wegzudenken

- Alles begann mit der Entdeckung der Quantennatur von Licht und Materie
- Verständnis
  - der Atomkerne und der Energieniveaus von Teilchen und deren Wechselwirkungen
  - Energiequelle der Sonne
- Entdeckung von Halbleitern
  - darauf aufbauend Transistoren und Computerchips
- Atomuhren - hochpräzise Zeitmessung
- LEDs, Leuchtmittel, Flachbildschirme, Touchscreens
- Mikrowellentechnologie
- Glasfasertechnologie
- Solarzellen, Radar, Laser
- Atomreaktoren und Atombomben
- Kernfusion

Die zweite Quantenrevolution

- Während bei der ersten Quantenrevolution die Wirkung von Myriaden von kleinsten Teilchen hervorgebracht wurde,
- werden bei der zweiten Quantenrevolution, vor der wir jetzt stehen, einzelne Quantenzustände und Quanteneffekte genutzt, um klassische Grenzen zu überwinden
  - bis zur hinunter zur untersten, prinzipiellen physikalischen Messgrenze - der Heisenberg‘schen Unschärferelation
- Quantenphysik verspricht eine technologische Entwicklung mit gigantischem Potential
  - ermöglicht vollkommen neue Technologien
    - die zum Teil kurz vor ihrer Realisierung stehen
    - zum Teil aber auch in weiterer Zukunft liegen
- Quantencomputer sprengen die Grenzen bisheriger Berechnungsmöglichkeiten



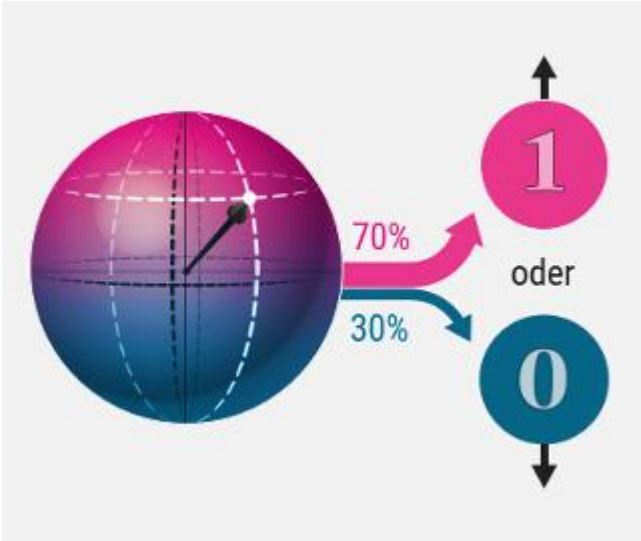
QC sind der Heilige Gral der Quantentechnologie

Wann kommt der Quantencomputer?

- Folgt man den Nachrichten mit immer neuen Rekordmeldungen entsteht leicht der Eindruck, dass der Durchbruch bei Quantencomputern unmittelbar bevorsteht oder dass sie bereits in etlichen Bereichen zum Einsatz kämen.
- Die hohe öffentliche Aufmerksamkeit geht auf das Potential der Quantencomputer zurück, eine begrenzte Klasse von Problemen deutlich schneller zu lösen, als es klassischen Computern jemals möglich sein wird.
- Quantencomputer wurden schon seit Anfang der 2000er Jahre mit Vorschusslorbeeren überhäuft. Seit Jahrzehnten arbeiten Physiker an Quantencomputern, die klassische Rechner überflügeln sollen.
- Darin gleichen sie dem Fusionsreaktor, der uns ein glorreiches Zeitalter unerschöpflicher Energiemengen bescheren soll, von dem seit Jahrzehnten versprochen wird, dass er in absehbarer Zeit zur Verfügung steht.

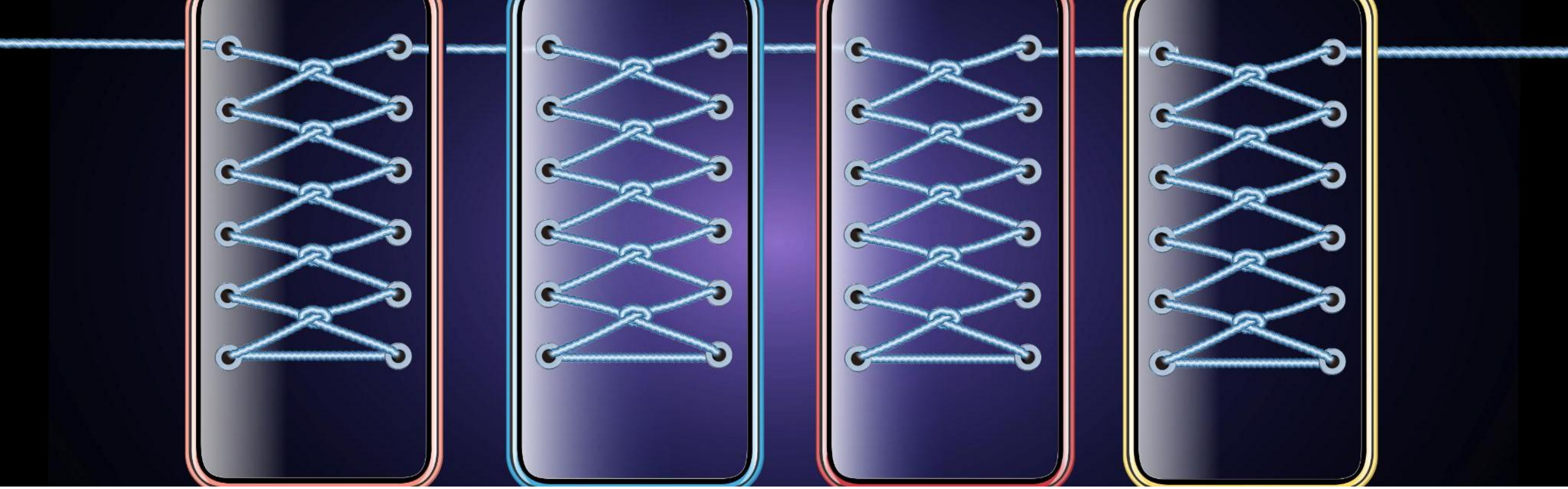
Quantencomputer arbeiten mit Qubits

Klassisches Bit



Qubit

- Konventionelle Computer arbeiten mit **Bits**
  - Zustand 0 oder 1
- Quantencomputer arbeiten mit **Qubits**
  - Als Qubits dienen die allerkleinsten Materieteilchen
  - Überlagerung der Zustände von 0 und 1: Superposition
    - Eine Mischung 0 und 1: gleichzeitig
      - Bsp.: 70% 1 und 30% 0
      - 0 und 1 existieren parallel in *allen* Mischungsverhältnissen
      - dies ermöglicht die enorme Rechenleistung
      - erst bei der Messung "entscheidet" sich das Qubit für einen der klassischen Zustände
      - die Superposition kollabiert: Dekohärenz
  - Mathematische Darstellung
    - $|\Psi\rangle = \alpha\ |0\rangle + \beta\ |1\rangle$
    - In $\alpha\ und\ \beta$ steckt die Wahrscheinlichkeit für 0 oder 1
    - QC funktionieren wie ein riesiges Mischpult mit tausenden Schiebereglern mit denen die Werte von α und β für die einzelnen Qubits „aufgezogen“ werden
  - Eine große Herausforderung bei der Entwicklung war es lange Zeit, überhaupt Qubits herzustellen und zu kontrollieren
    - für große Mengen ist das bis heute die zentrale Herausforderung



QC rechnen anders

QC nutzen Verschränkung

- ein Qubit allein genügt nicht
- QC arbeiten mit Verschränkung von sehr vielen Qubits
- mehrere Qubits bilden einen gemeinsamen Überlagerungszustand
- eine einzige unteilbare Einheit
- nicht auflösbar in Einzelzustände

- Niemand weiß wirklich genau, wie oder warum diese Verschränkung funktioniert
  - faszinierend und rätselhaft
- Wir verstehen aber genug davon, um damit Computer zu bauen, die sich diesen Effekt zunutze machen

Die Magie der verschränkten Qubits

Messgerät 1

Messgerät 2

Was bedeutet Verschränkung?

- Die Wahrscheinlichkeit am Messgerät links eine 0 zu messen beträgt ½
- Die Wahrscheinlichkeit am Messgerät rechts eine 1 zu messen beträgt ebenso ½
- Das Gleiche gilt, wenn wir 0 und 1 vertauschen
- **Wenn aber, am Messgerät 1 (links) eine 0 *gemessen* wurde, ist die Wahrscheinlichkeit am Gerät 2 (rechts) eine 1 zu messen 100%**. - Antikorrelation
- Das Wunderbare: Diese Umkehr geschieht exakt im Moment der ersten Messung (instantan)
  - unabhängig davon, wie weit die beiden Messgeräte voneinander entfernt sind
    - quasi mit „Überlichtgeschwindigkeit“
- „Spukhafte Fernwirkung“ - Albert Einstein

Zwei verschränkte Qubits

Verblüffende Eigenschaften von QC

Parallelität

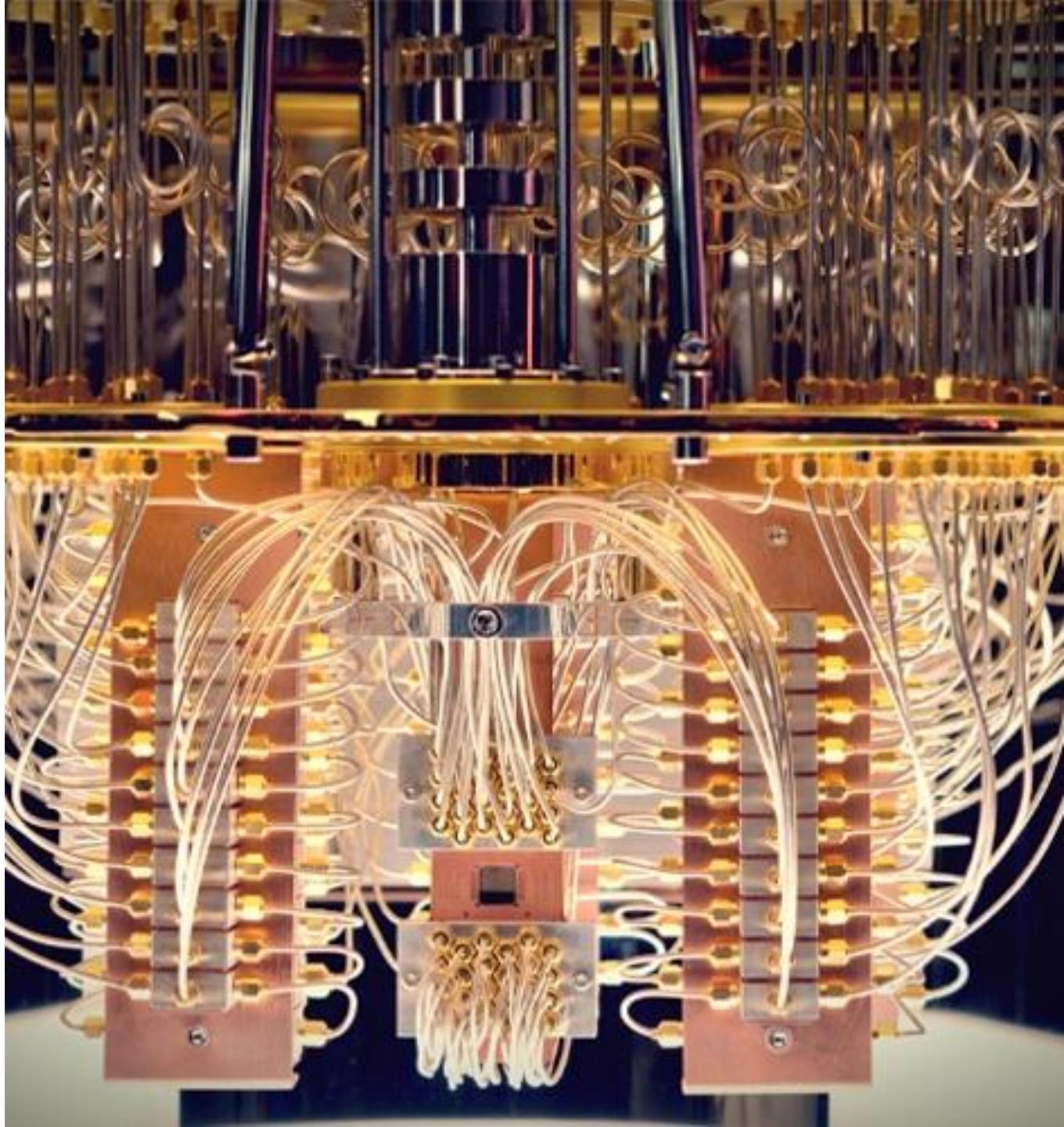
- In einem QC existieren **alle Lösungen** zu einem Problem **zur gleichen Zeit**
  - Man kann aber immer nur genau eine Lösung auslesen
  - Oberflächlich betrachtet wirkt es, als rechneten die Qubits in einem Quantencomputer parallel.

Unterschiede zwischen klassischem und Quantencomputer

- Es gibt **keine if-then-else Strukturen** in der Programmierung
  - alle Alternativen werden gleichzeitig berechnet
- Ein Quantencomputer hat **keine Taktfrequenz**
- mit 50 klassischen Bits kann man jeweils **einen von 2^{50}** möglichen Zuständen darstellen.
- mit 50 Qubits kann man **alle 2^{50}** verschiedenen **Zustände gleichzeitig** darstellen und speichern.
- $2^{50} \approx 10^{15}$ eine Billiarde, 1 mit 15 Nullen oder eine Million Milliarden
- Bei einem Quantencomputern verdoppelt sich die Rechenleistung mit jedem zusätzlichen Qubit. Exponentielles Wachstum.
- Deshalb ist der Unterschied zwischen einer Maschine mit 5 Qubits und einer mit 50 Qubits so gewaltig.
- Quantencomputer könnten ungeheure Datenmengen speichern

Einschränkungen

- Es ist nicht möglich, beliebige Algorithmen parallel durchzuführen
- Ein Quantencomputer eignet sich nicht für numerische Berechnungen!



Wie funktioniert ein QC?

In drei Schritten zur Lösung

1. **Verschränkung erzeugen**

- d.h. Input für QC präparieren
- Die Präparierung ist sehr aufwändig
- Verschränkung möglichst lange aufrecht erhalten
- mehr als nur ein paar Millionstel Sekunden

2. **Überlagerung zwischen den Qubits manipulieren**

- um einen Lösungsalgorithmus auf die Qubits anzuwenden
- mittels Laser- oder Mikrowellenpulsen

3. **Die Lösung auslesen: „zu messen“**

- aus der Unmenge an möglichen Lösungen, die parallel existieren, die richtige finden
- man kann nur eine Lösung auslesen
- dabei wird die Überlagerung zerstört
- man muss die Messung u.U. millionenfach wiederholen, bis man ein Messergebnis erhält, das sich von einem Zufallsergebnis unterscheidet

Zwei Anwendungen

Primzahlzerlegung

- Bekannteste Anwendung: jene beiden Primzahlen zu finden, die eine große Zahl restlos teilen: **Faktorisierung**
- Ein akademisches Problem? Keinesfalls!
- Wenn die Zerlegung großer Zahlen in Primzahlen durch QC gelingt
  - stellt das eine riesig große Bedrohung für unsere sichere Verschlüsselung im Internet dar
    - das heute meistgenutzte Verschlüsselungsverfahren RSA kann mit QC gebrochen werden
  - die übliche Schlüssellänge beträgt heute 2048 oder 4096 bits
  - Zahlen mit 600 bzw. 1.200 Dezimalstellen
  - 1994 entwickelte der US-Mathematiker Peter Shor einen nach ihm benannten Quantencomputer-Algorithmus, der die Faktorisierung viel schneller lösen kann als konventionelle Rechenprogramme

Schnelle Suche in unstrukturierten Datenbanken

- Grover Algorithmus

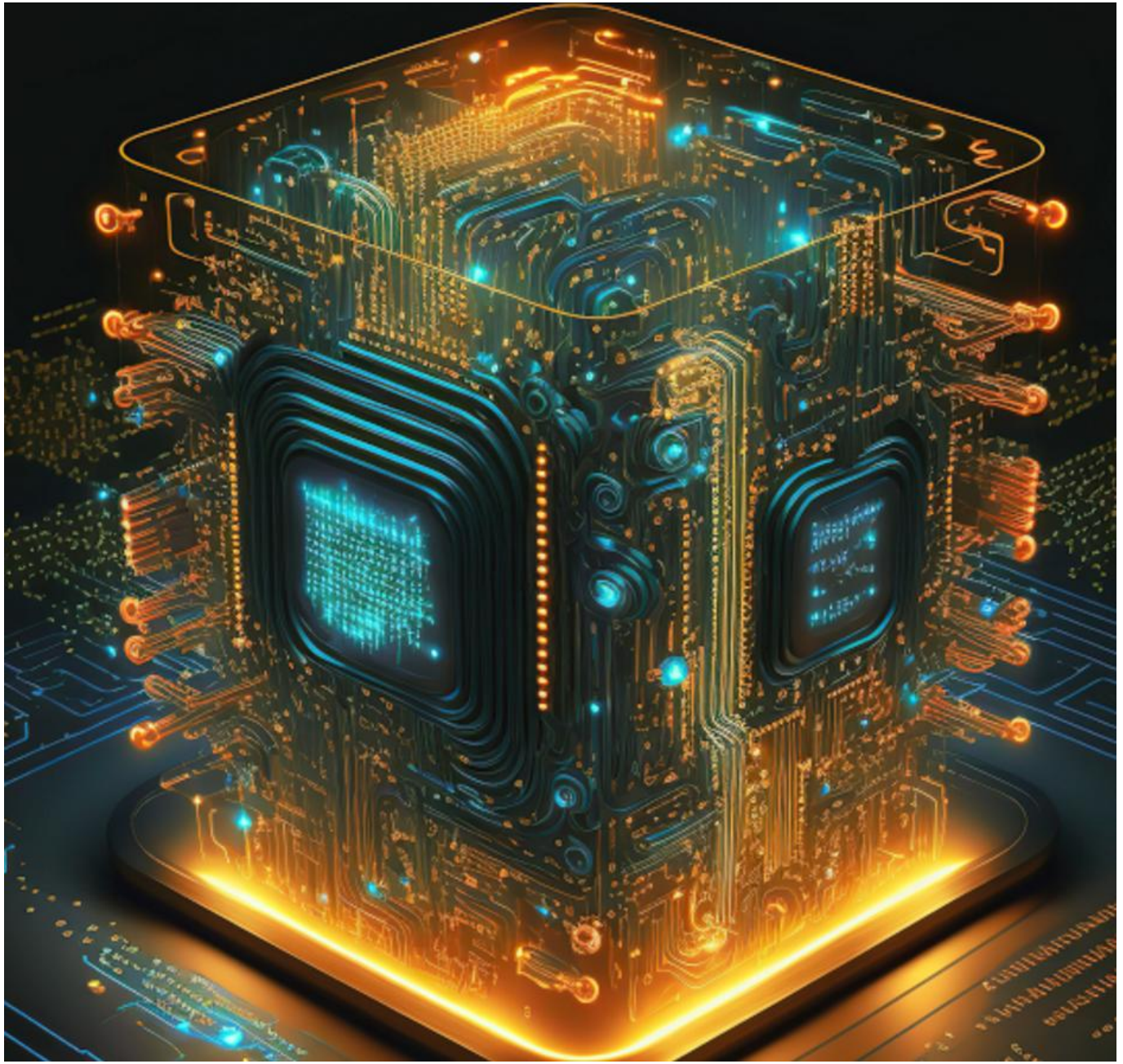
Es fehlt an Anwendungen für QC

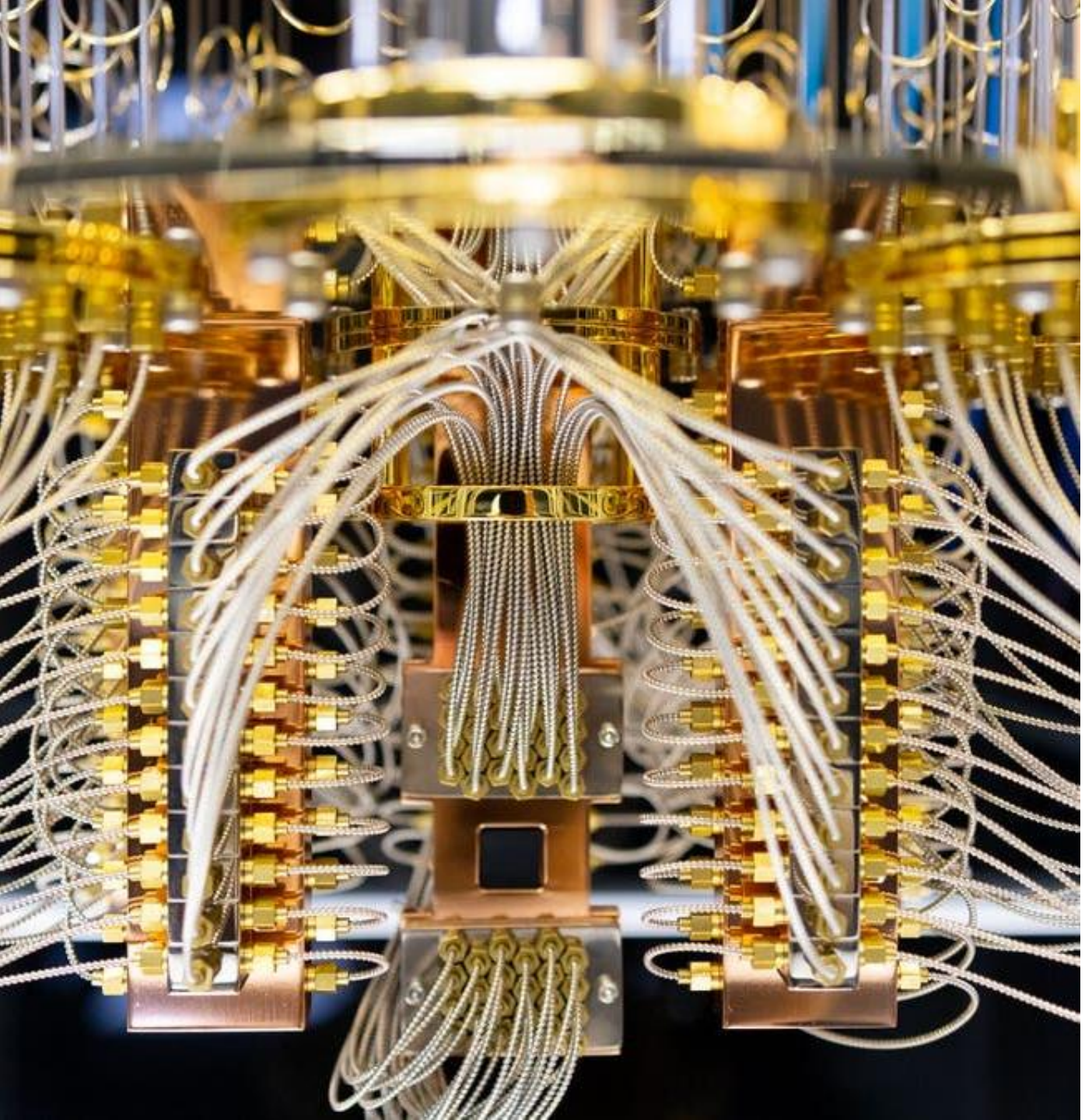
Wissenschaftler kennen bisher nur wenige Rechenaufgaben, die von Quantencomputern schneller gelöst werden würden als von herkömmlichen Computern.

- 2020 waren es 64 Algorithmen für echt akademische Probleme

Mögliche Anwendungen

- Kombinatorische Optimierungsprobleme in der Logistik: Problem des Handlungsreisenden
- Probleme der Steuerung von Verkehrsflüssen
- Berechnungen in der Quantenchemie
  - Ziel neue Materialien und Medikamente mit genau definierten Eigenschaften designen.
- Quanten simulieren durch QC (Richard Feynman) – die Natur ist quantenmechanisch!
- Beschleunigung des Lernens von KI Modellen
  - Leistungssteigerung durch Analyse großer Datenbestände (hybrid)
- effiziente Suche in riesigen unstrukturierten Datenbanken
- Herkömmliche Hochleistungsrechner und Algorithmen werden im Wettbewerb mit QC immer leistungsfähiger





Prinzipielle Einschränkungen

- Ein Quantencomputer ist keine Universalrechenmaschine, **kein Allzweckcomputer**
- bei weitem nicht jedes Problem ist geeignet, mit einem Quantencomputer gelöst zu werden
- umgekehrt: nicht jedes komplexe, heute ungelöste Problem ist potenziell mit QC lösbar.
- Quantenalgorithmen sind denselben fundamentalen, komplexitäts-theoretischen Limitierungen unterworfen wie klassische Algorithmen.
- Industrie und Hersteller suchen fieberhaft nach passenden Anwendungsfällen für die heutige Generation der QC.
- Bisher führten Quantenrechner nur triviale oder irrelevante Aufgaben aus, die allenfalls für Zahlentheoretiker interessant sind.
  - Proof-of-concept Demonstrationen
  - Maximale Leistung ist bisher die Primzahlzerlegung von 21 = 3 * 7

Technologische Herausforderungen

- **Kohärenz aufrechterhalten**
  - Um Quantenberechnungen durchzuführen, müssen alle Qubits kohärent sein, d.h. möglichst lange in ihrem magischen Zustand der Superposition verbleiben. Und das ist nicht einfach.
    - Diese Herausforderung wächst mit der Anzahl der Qubits.
  - Die geringste Störung führt zum Zusammenbruch der Kohärenz: Dekohärenz.
  - Dekohärenz ist einer der effizientesten und am schnellsten ablaufenden Prozesse der Physik: in einem Milliardstel einer Milliardstel Sekunde
- **Rauschen unterdrücken**
  - fundamentale quantenmechanische Prozesse führen immer wieder dazu, dass der Zustand eines Qubits umklappt oder völlig zufällig wird.
- **Fehler korrigieren**
  - Quantencomputer benötigen sehr aufwändige Fehlerkorrekturmechanismen.
  - Zum Brechen eines 2048 Bit langen Schlüssels bräuchte man einen QC mit geschätzt einer Million Qubits.
    - 100 QuBits für die Berechnung
    - den Rest für die Fehlerkorrektur
- **Miniaturisierung**
  - Entwicklung eines „Quantentransistors“

Fehlerkorrektur

Wie erkennt man unbekannte Fehler?
Wie korrigiert man sie?

ohne dass man sicher sein kann, wo und ob überhaupt ein Fehler aufgetreten ist und ggf. welcher?

Lösung: Redundanz und Mehrheitsentscheid

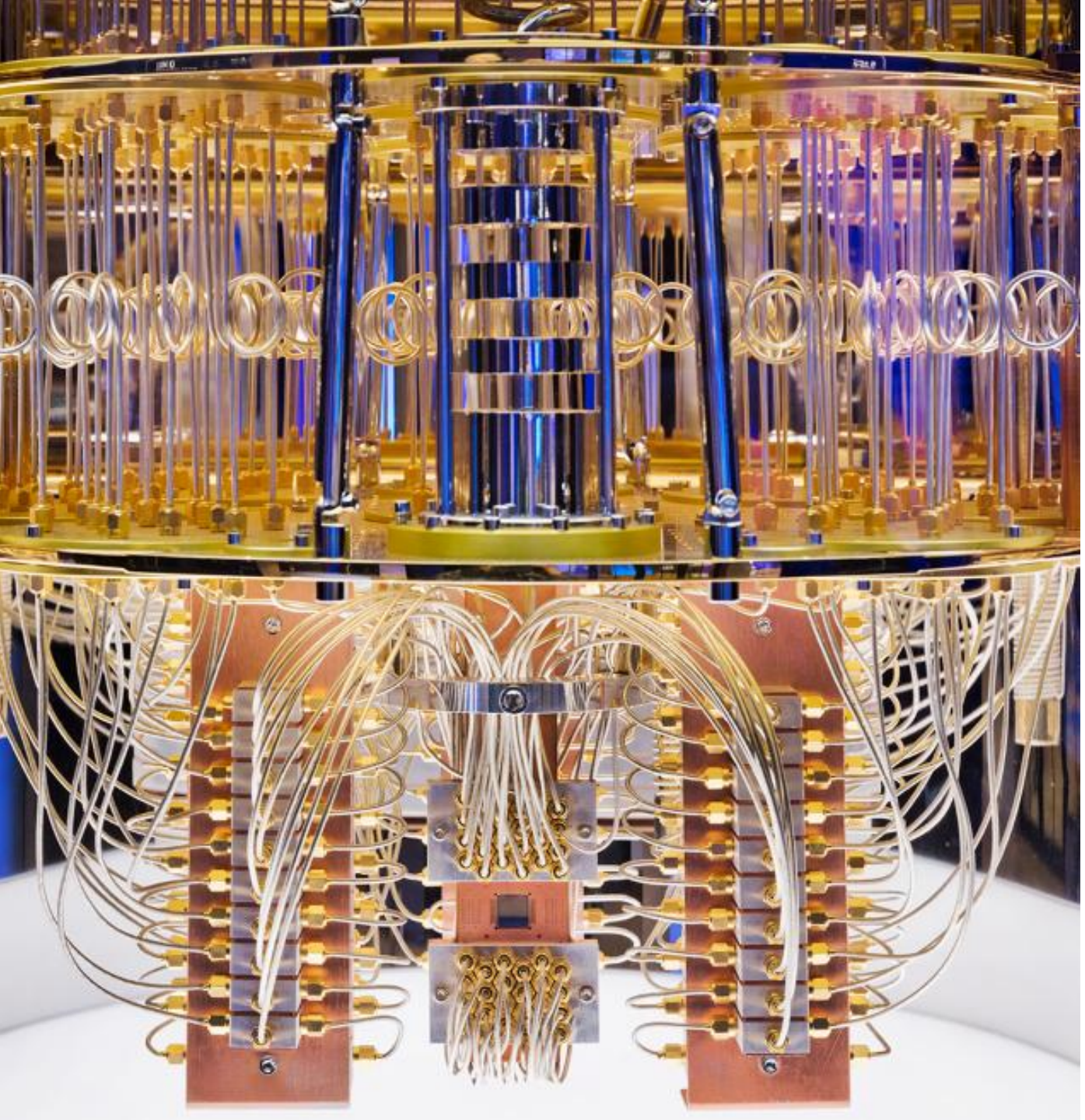
- Statt mit einem Qubit zu rechnen präpariert man zahlreihe Inputbits und rechnet die gleiche Rechnung mit diesen Hilfs-Qubits (Ancillas) parallel.
- Man spricht dann von einem logischen Qubit
  - 2,5 facher Lebensdauer eines physikalischen Qubits
- Wenn die Ergebnisse vorliegen „prüft“ man, ob es Abweichungen gibt und korrigiert das Ergebnis so, wie es der Mehrheit der Ergebnisse entspricht.
  - das kann natürlich auch falsch sein
- Wichtig dabei: keines der Qubits darf dabei jemals ausgelesen und sein genauer Wert bestimmt werden
  - → Dekohärenz
- Man verwendet eine Schaltung, die alle Ergebnisse untereinander verrechnet und die von der Mehrheit abweichenden Qubits auf den Wert der Mehrheit setzt.
- Dabei ist es zu keinem Zeitpunkt notwendig, exakt zu wissen, ob das Ergebnis eine 0 oder eine 1 war
- Das Geheimnis der Qubits (die Kohärenz) bleibt gewahrt.
- Erst ganz am Ende des Algorithmus wird gemessen und das Ergebnis bestimmt.
- Offensichtlich braucht man dafür große Mengen von Hilfsbits
  - Qubits wie alle anderen und damit gleich mimosenhaft

Uncomputing

BACK

Quantencomputer rechnen „rückwärts“

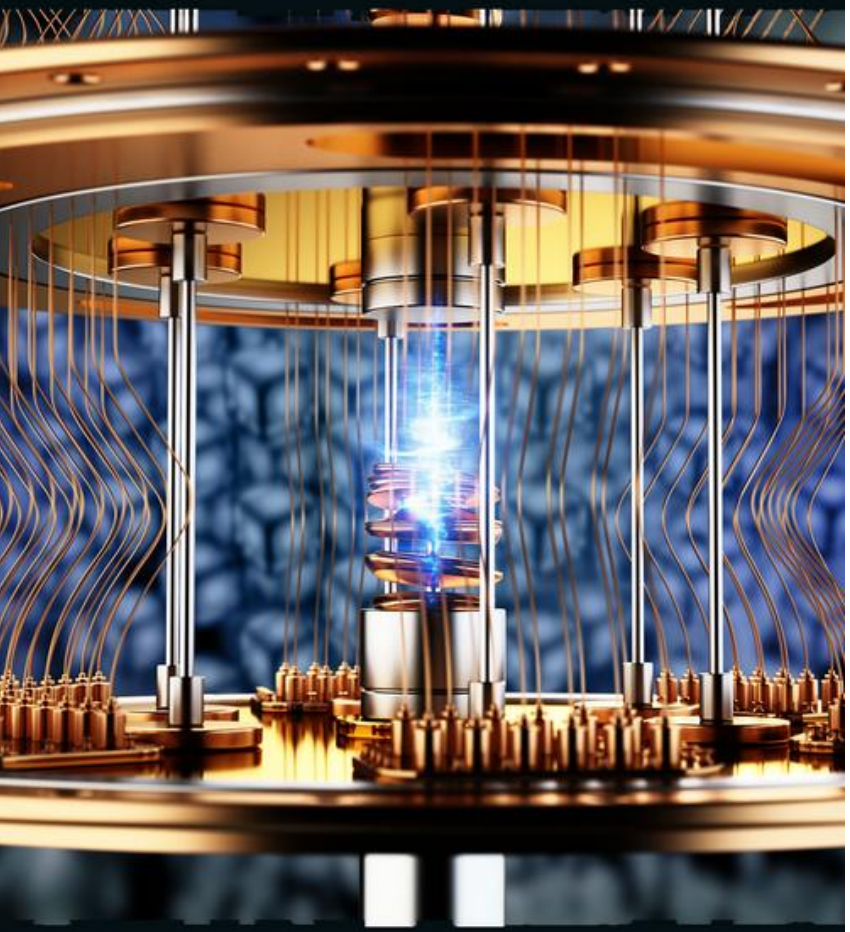
- Bis zu 90% seiner Zeit ist der fehlerkorrigierende QC damit beschäftigt „rückwärts“ zu rechnen.
- In der Quantenwelt gibt einen keinen eindeutigen Zeitpfeil. Alle Vorgänge sind reversibel: sie können genauso gut rückwärts stattfinden wie vorwärts.
- Das muss der QC berücksichtigen. Alle Berechnungen müssen auch „rückwärts“ ablaufen können. Qubits dürfen nicht einfach gelöscht werden.
  - Dies würde die Verschränkung mit den Ergebnis-Qubits zerstören
- Die Hilfs-Bits für die Fehlerkorrektur (die Ancillas) müssen für den nächsten Rechenschritt wieder ohne Nebenwirkungen auf den Ausgangszustand zurückgestellt werden.



Wettbewerb um Quantum Supremacy

Supremacy – Überlegenheit, Vormachtstellung

- ursprünglich: Punkt, an dem ein Quantencomputer eine Aufgabe schneller lösen kann als der beste klassische Supercomputer
- Quantum Supremacy ist längst zu einer geopolitischen Frage geworden
  - nicht nur Firmen (wie Google, IBM, Amazon, ..) liegen im Wettstreit
  - sondern ganze Staaten
    - USA und China investieren Milliardenbeträge
    - weltweit 35 Milliarden Dollar in 2022
  - in Erwartung eines riesigen wirtschaftlichen Potentials
    - mutmaßlich 700 Milliarden Dollar in 2035
- Es gibt erste Klagen über Behinderung des offenen wissenschaftlichen Austauschs
- Es ist sicher damit zu rechnen, dass die Verfügbarkeit eines allgemein nutzbaren Quantencomputers nicht sofort öffentlich kommuniziert werden wird.
- Es geht um die Nutzung strategischer Vorteile
  - das Entschlüsseln vertraulicher Daten
  - heute bereits wird verschlüsselte Kommunikation mengenweise aufgezeichnet
  - mit der Perspektive sie eines Tages entschlüsseln zu können.



Entwicklungstand heute

- Wir befinden uns heute in der NISQ Ära dem Zeitalter der noisy-intermediate-scale-Quantum Computer (Rauschbehaftete mittelgroße QC) - mit zahlreichen Einschränkungen
- NISQ-Technologie ist nicht geeignet für Quantenfehlerkorrekturen
- die klassischen Quantenalgorithmen sind damit noch nicht sinnvoll implementierbar
- selbst wenn die nominelle Qubit-Zahl für die Implementierung des Grover- oder Shor-Algorithmus vorhanden wäre, könnte man das Resultat aufgrund des starken Rauschens von einem Zufallsergebnis nicht unterscheiden
- Stattdessen heute: Einsatz von weniger fehleranfälligen NISQ-Algorithmen.
  - Hybride Hardware: Klassische Hochleistungs-Hardware im Verbund mit QC.
- Die führenden Cloudprovider bieten die Nutzung von QC an
  - Eigene Programmiersprachen für QC wurden bereits entwickelt
  - Ziel: Übertragbarkeit von QC-Algorithmen auf andere QC-Hardware

Durchbruch bei Googles Willow Chip

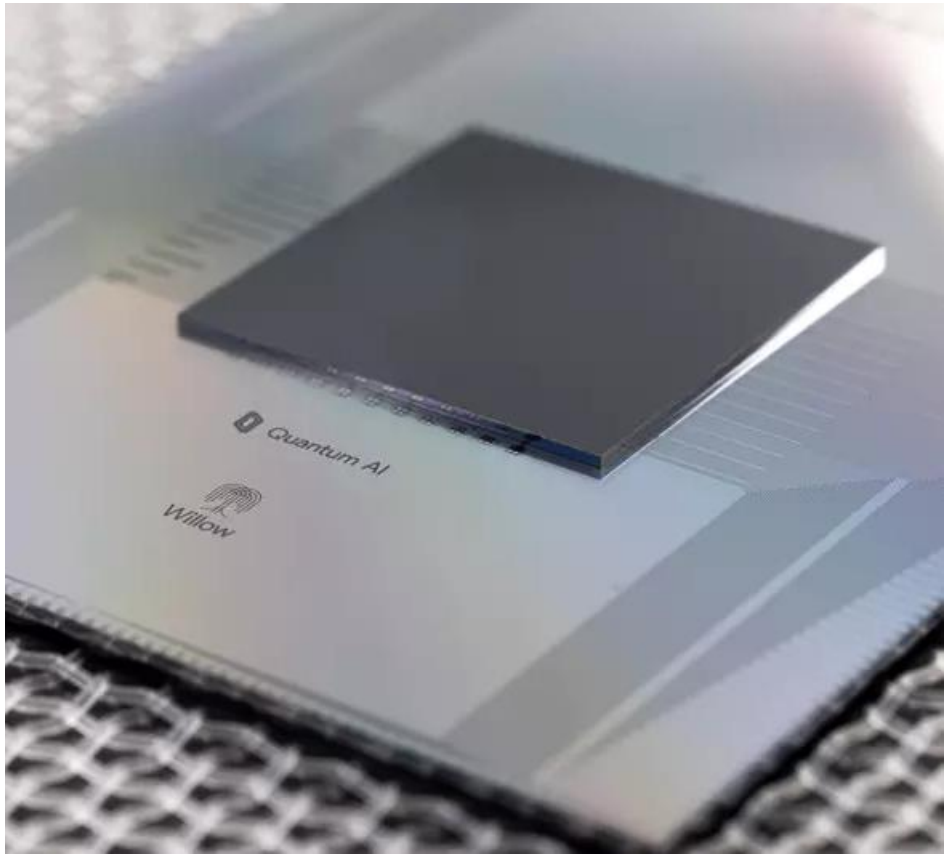
Googles Willow Quantencomputer Dez 2024

Riesiger Fortschritt bei Miniaturisierung und Fehlerfreiheit

- Willow verfügt über 30 – 105 Qubits
- die besonders stabil und fehlerarm sind
- Durchbruch bei der Kohärenzzeit
  - mit Kohärenzzeiten bis zu 100 µs ~ 10.000 Berechnungen pro Sekunde
  - Ein-Qubit-Fehlerrate: 3,5 Fehler bei diesen 10.000 Berechnungen
  - Milliarden Korrekturzyklen
  - Meilenstein bei fehlerkorrigierten, skalierbaren QC
- Willow benötigt Kühlung knapp über dem absoluten Nullpunkt

Sensationeller neuer Algorithmus Okt. 2025

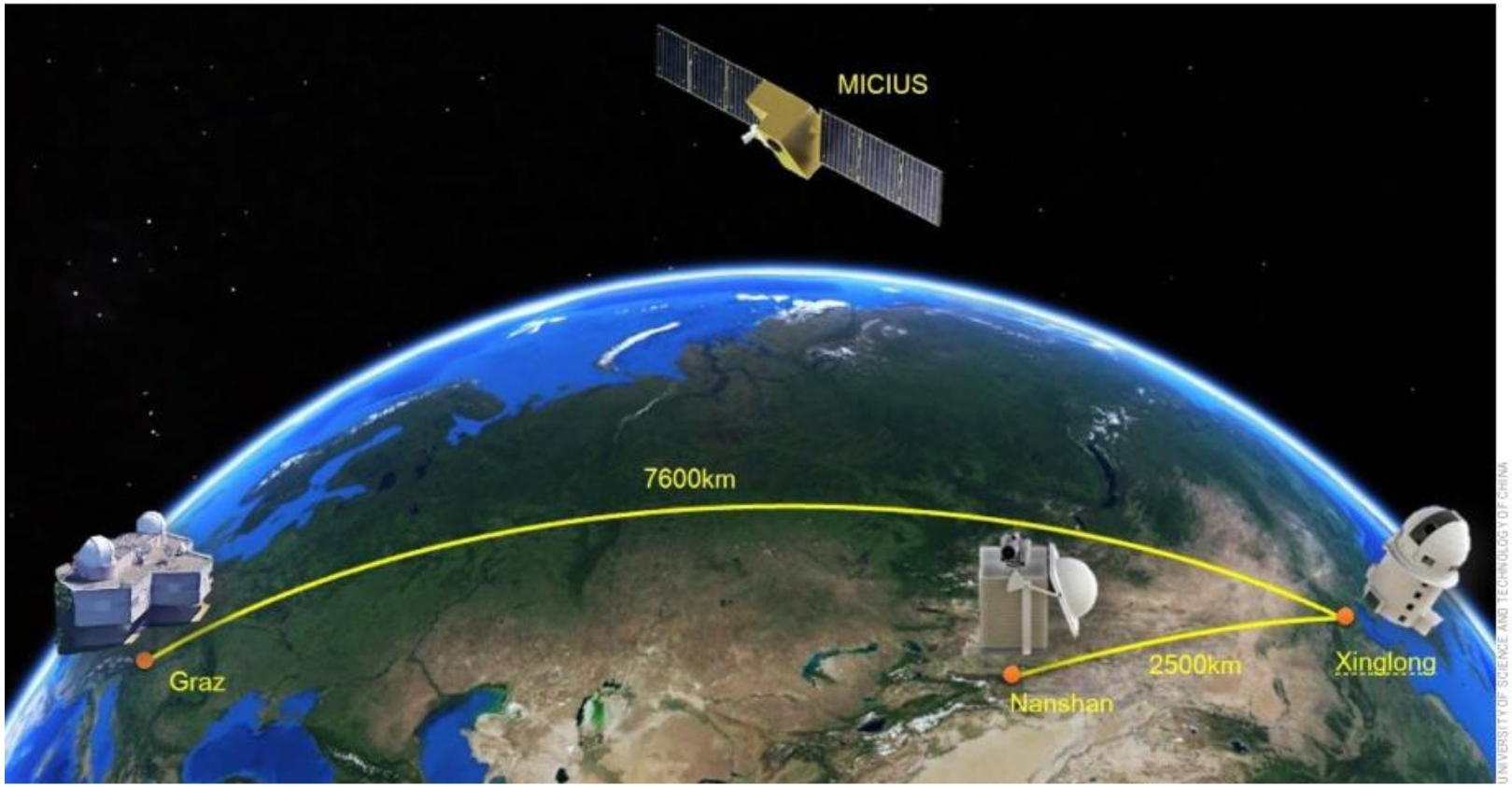
- löst Drei-Jahres Aufgabe in zwei Stunden
- geschätzt 13.000-mal schneller als der beste bekannte klassische Algorithmus auf den schnellsten Supercomputern
- Simulation des Verhaltens von Molekülen mit 15 bzw. 28 Atomen
- Algorithmus kann erstmalig auf anderen QC wiederholt und geprüft werden



Googles Quantum Chip „Willow“ Dezember 2024

Quanten-Kommunikation

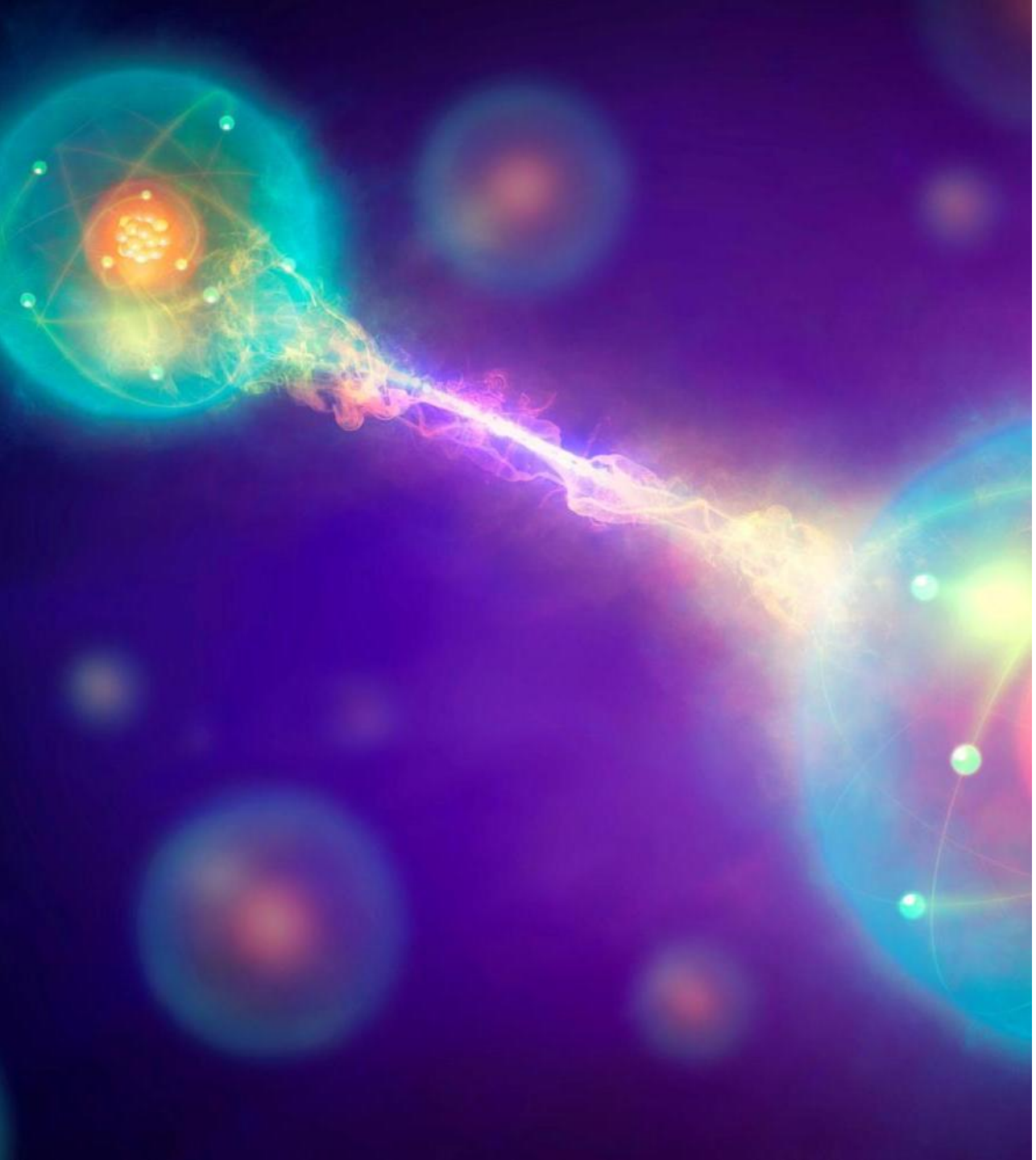
- Quanteninternet
- Quantenteleportation
- Quantenkryptografie



Zwei Reichweiten-Rekorde für Quanten-kommunikation

- 2017 **Quantenvideoübertragung** über den chinesischen Micius Satellit
  - zwischen zwei wissenschaftlichen Arbeitsgruppen in China und in Österreich
  - mit konventionellem Code verschlüsselt (AES)
  - Verbindungslänge 7.600 km
    - Kosten 50 Millionen Euro.

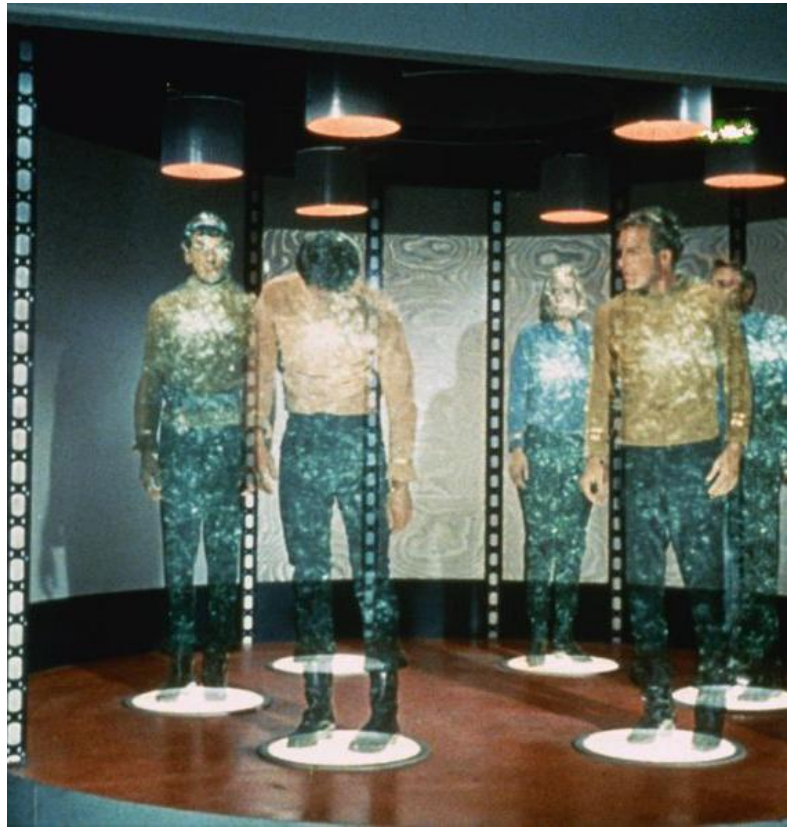
- **Distanzrekord für verschränkte Photonen**
- Von einem Satelliten aus konnte ein Paar verschränkter Photonen zu zwei verschiedenen Bodenstationen geschickt werden, die 2500 km voneinander entfernt lagen.
  - Sie waren noch immer verschränkt.



Technische Hürde: Quantenrepeater

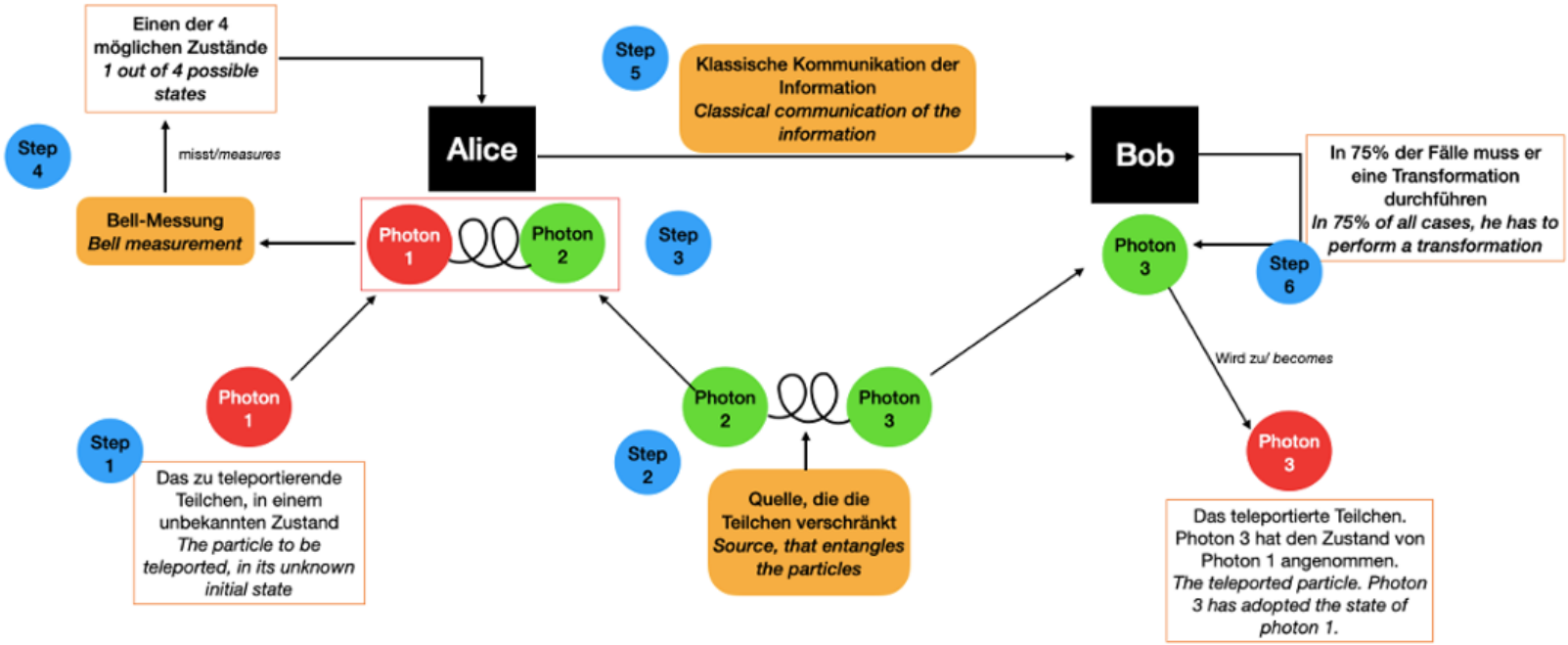
- **unvermeidliche Verluste** bei der Glasfaserübertragung
  - terrestrisch nur einige hundert Kilometer
- Quanten können nicht wie herkömmliche Signale in Glasfasern nach ein paar Kilometern wieder verstärkt werden.
  - deshalb vorzugsweise Satellitenverbindungen
  - geringe Störungen im Vakuum des Weltraums
- **No-cloning Theorem**
  - Verschränkte Quantenzustände können nicht kopiert werden, ohne sie zu zerstören
    - Quantenobjekte können niemals kopiert werden
    - keine Messung ohne Störung
    - es kann keinen Quantenkopierer geben
    - Garantie für abhörsichere Übertragung
  - **Quantenrepeater** sind möglich
    - dabei werden die ausgesandten Quanten zerstört
  - Quantenrepeater sind technisch ausgesprochen anspruchsvoll
  - Ihre Entwicklung wäre ein technologischer Durchbruch

Quantenteleportation



so funktioniert es nicht !

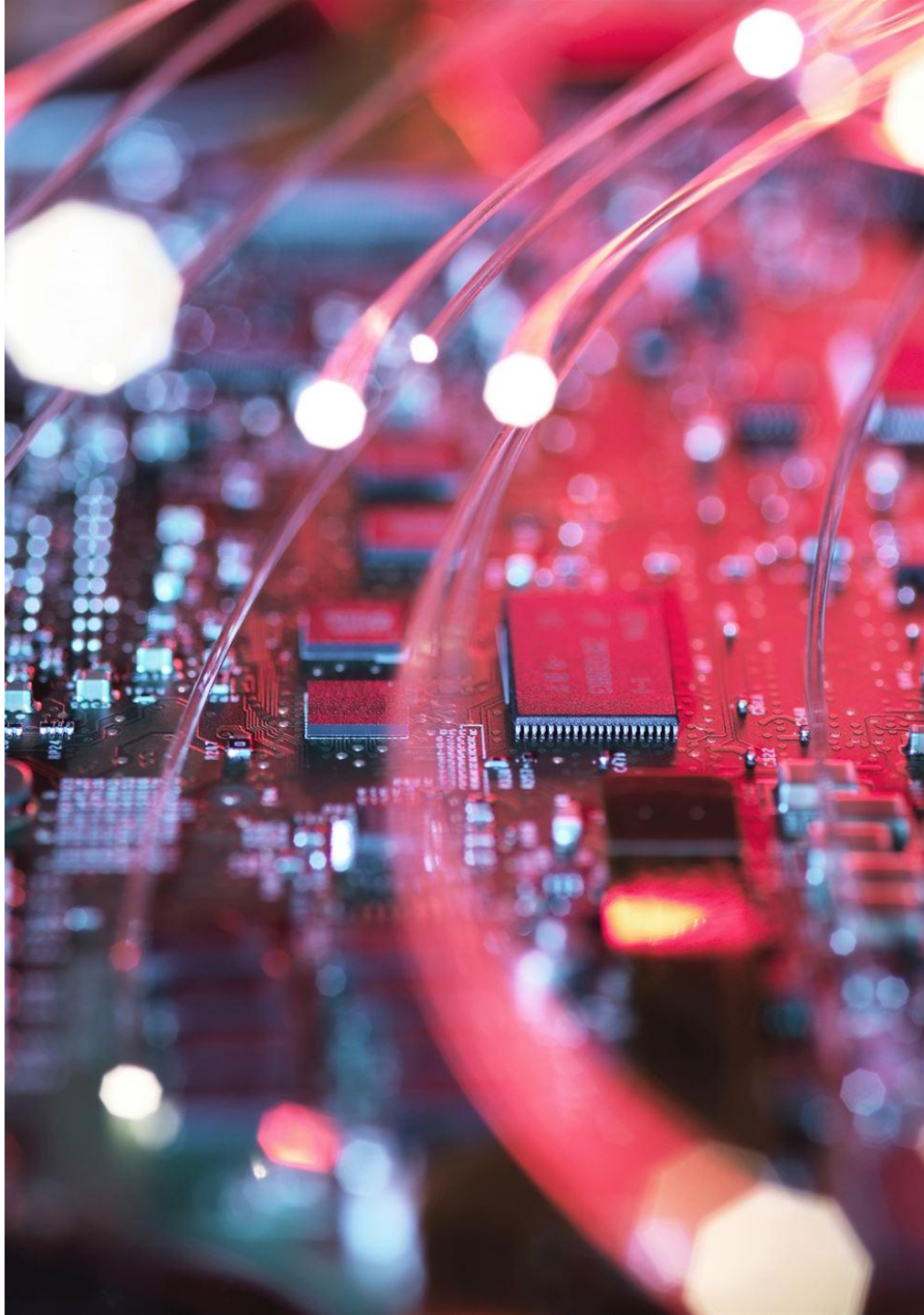
- eines der faszinierendsten Konzepte der Quanteninformationstheorie
- bedeutet, den *Zustand eines Qubits* – also die gesamte quantenmechanische Information – von einem Ort zum anderen zu übertragen, *ohne dass das Qubit selbst physisch transportiert wird*.
- geschieht mittels dreier **verschränkter Qubits** und zusätzlicher **klassischer Kommunikation**.



Quanteninternet

Das Quanteninternet verspricht mindestens drei verschiedene attraktive Dienste, die sich in Teilen kurz vor der Marktreife befinden

- **Quantenkryptografie** für hochsichere Datenübertragung
- **blindes Cloudcomputing**
  - Verschlüsselte Datenspeicherung in der Cloud und verschlüsselte Verarbeitung
    - sehr rechenintensiv
- garantiert abhörsicheres, **unbeobachtetes Suchen** im Netz
  - wer könnte etwas dagegen haben?
  - Google ??? NSA ???



QUBE Projekt

Deutschland hat mit dem Projekt **QUBE** den ersten Kleinstsatelliten für Quantenkommunikation ins All gebracht

Ziel: weltweite, abhörsichere Kommunikation durch Quantenschlüsselverteilung (QKD) via Kleinstsatelliten

CubeSat (Größe etwa wie ein Schuhkarton, 3,5 kg) mit hochmoderner Quanten- und Laserkommunikationstechnologie ausgestattet

am 16. August 2024 mit einer SpaceX Falcon-9-Rakete ins All gebracht.

Kommunikation erfolgt über optische Freistrahlverbindungen zwischen dem Satelliten und Bodenstationen (z. B. DLR in Oberpfaffenhofen).

Quanteninternet der Zukunft

- Quantenkommunikationsnetzwerke
  - Netzwerke von zahlreichen Knoten mit sicherer Kommunikation
- Verteilte Quantenserver
  - die gemeinsam an Problemen arbeiten
  - zur Vernetzung von QC mit ihren unterschiedlichen Technologien
  - Übergänge zu klassischen Computern
  - Glasfaser- und Satellitentechnologie
- direkter Austausch von (verschränkten) Quantenzuständen in für heutige Verhältnisse ungeahnten Größenordnungen.
- Netzwerke von Quantensensoren
- Dauerhafte Quantenspeicher
  - Quantum Vault Datenbanken (quantentechnologisch abgesicherte Datenbanken – Tresore), die ein Maximum an Sicherheit garantieren.
  - z.Zt. nur für Millisekunden

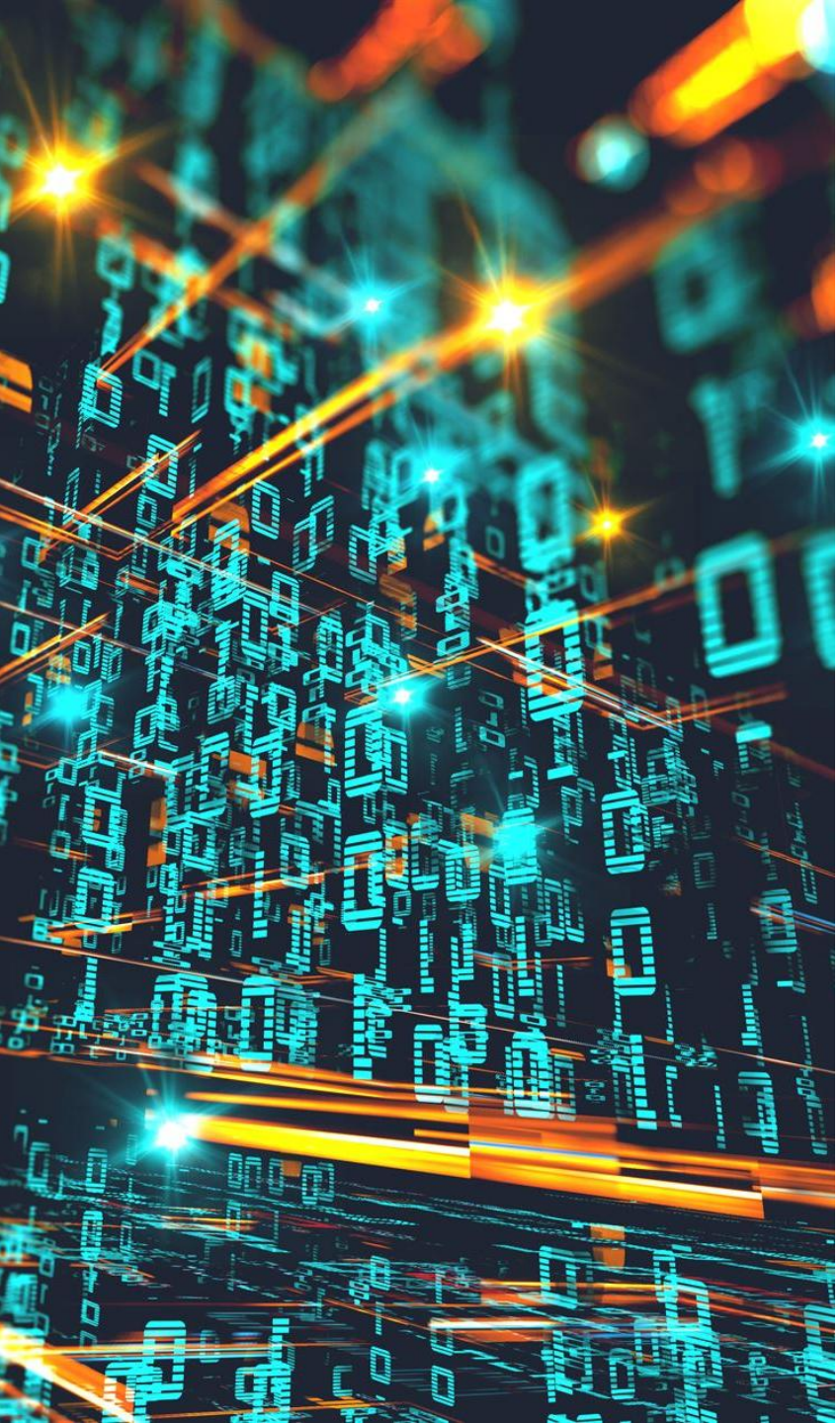
Quantenkryptografie

Sichere Verschlüsselung ruht auf drei Säulen

1. Generierung eines zufälligen, regellosen Schlüssels zum Ver- und Entschlüsseln.
2. Garantiert abhörsicherer Austausch des Schlüssels – Geheimnis bleibt gewahrt
3. Die Gewähr, dass der *öffentlich bekannte* Verschlüsselungsalgorithmus nicht gebrochen werden kann.

Alle drei Anforderungen kann die Quantenkryptografie sicherstellen

- Quantenkryptografie lässt sich auch durch einen Quantencomputer nicht brechen.



Sicherheit durch Quantenkryptographie

- Sicherheit basiert auf dem grundlegenden Zufallscharakter der Quantenphysik
  - Superposition und Verschränkung

Eine vollkommen zufällige erzeugte Bitfolge als Schlüssel

- Lässt sich mit Quantentechnologie vergleichsweise einfach und zuverlässig erzeugen: Quantum Random Number Generator **(QRNG)**
  - Schlüssel darf nur einmal verwendet werden
  - Schlüssel muss mindestens doppelt so lang sein wie die zu übertragende Nachricht, um Lauscher zu erkennen und auszusperren
- Mit Quantum Key Distribution (**QKD**) erzeugte Schlüssel sind auf unbeschränkte Zeit sicher, unabhängig von den Rechenkapazitäten, den mathematischen Kenntnissen oder den algorithmischen Innovationen etwaiger künftiger Mithörer

Sicherer Schlüsselaustausch – mit verschränkten QuBits

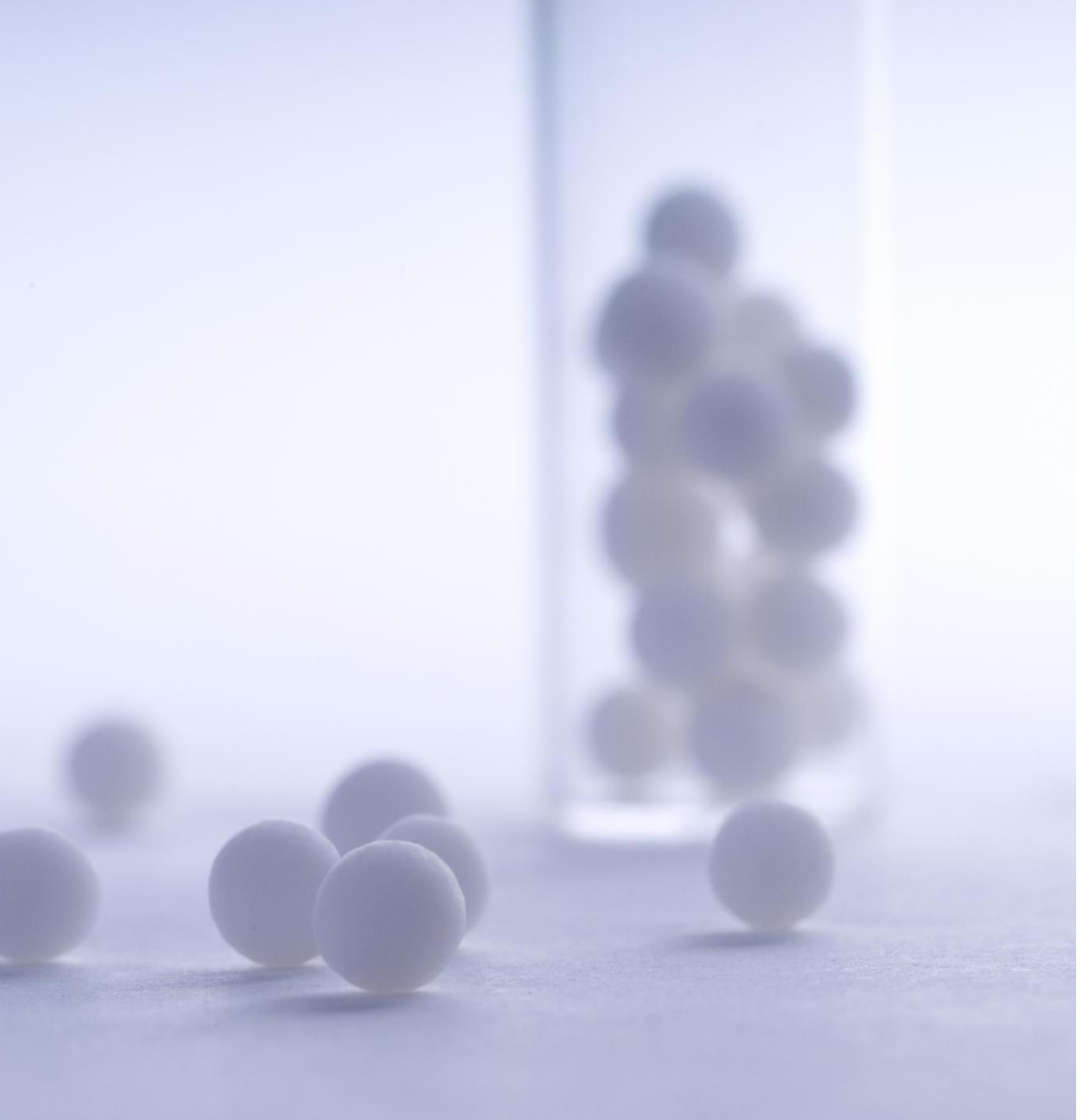
- Lauschangriffe beim Schlüsselaustausch werden sicher erkannt
  - zusätzliche konventionelle Kommunikation nötig
    - ohne Weiteres auch über eine unsichere Verbindung

Ein absolut nicht zu brechender Verschlüsselungsalgorithmus

- Das heute verwendete (symmetrische) Verschlüsselungsverfahren AES 256 ist recht kompliziert aber effizient zu berechnen
  - gilt bisher als sicher gegenüber Quantentechnologie
- Quantenkryptographie nutzt ein vollkommen simples Verfahren (XOR)
- Nicht zu brechen: die Verschlüsselung erfolgt durch den erzeugten echt zufälligen Schlüssel. Der gleiche für Ver- und Entschlüsselung.

Aktueller Entwicklungsstand

- Erste Unternehmen produzieren Mikrochips basierend auf Quantentechnologie für den Einsatz in Massenprodukten wie Mobiltelefonen, Druckern und anderen vernetzten Geräten.
- QRNG-Chips (Quantum Random Number Generation) erzeugen Zufallszahlen in höchster Qualität.
- echte Zufallszahlen sind ungeheuer vielfältig einzusetzen
  - Authentifizierung und Verschlüsselung auf höchstem Niveau
  - Schutz für elektronische Währungen
  - Schutz für Transaktionen wie z.B. Geldtransfers
    - entsprechende Regularien sind zu erwarten
- ein Massenmarkt für Consumer Geräte - Handys ("in den nächsten fünf Jahren")

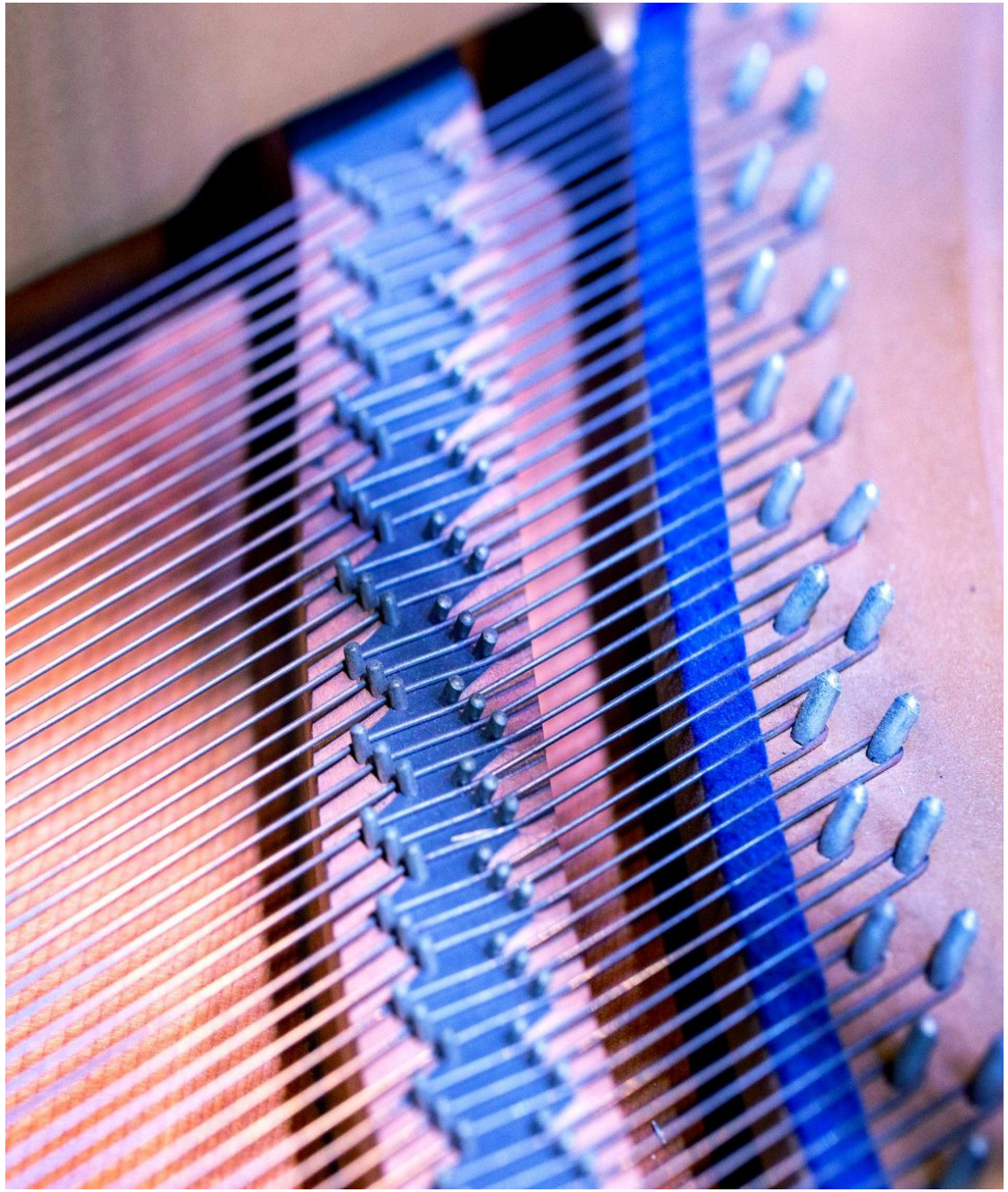


Quantensensorik und Quantenchemie

Anwendungen und Potenzial

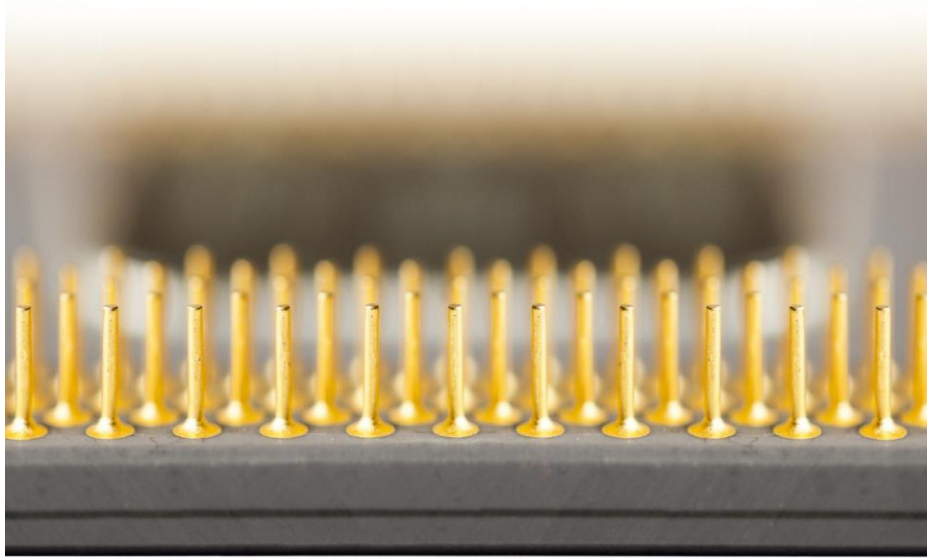
Quantensensorik

- Nutzung quantenmechanischer Effekte (Superposition und Verschränkung)
  - äußerst empfindliche Reaktion auf Änderungen in der Umgebung
  - aus Schwäche (Störanfälligkeit der Qubits) wird eine Stärke (Empfindlichkeit)
- **extrem genaue Messungen** physikalischer Größen, die klassischen Messverfahren deutlich überlegen sind
  - Magnetfelder, Beschleunigungen, Rotationen, Zeit oder Schwankungen im Gravitationsfeld
- Quantengravimeter und Quantenbeschleunigungssensoren
  - eine 50-fache Stabilität gegenüber klassischen Beschleunigungssensoren, bei erheblich höherer Präzision.
  - GPS-unabhängige Navigation
  - Revolutionierung der geophysikalischen Exploration
    - Erkennung von Substrukturen im Boden
    - Veränderungen des Gravitationsfeldes der Erde
- Erschließung neuer Spektralbereiche für die es keine Kameras gibt
- zerstörungsfreie Messungen



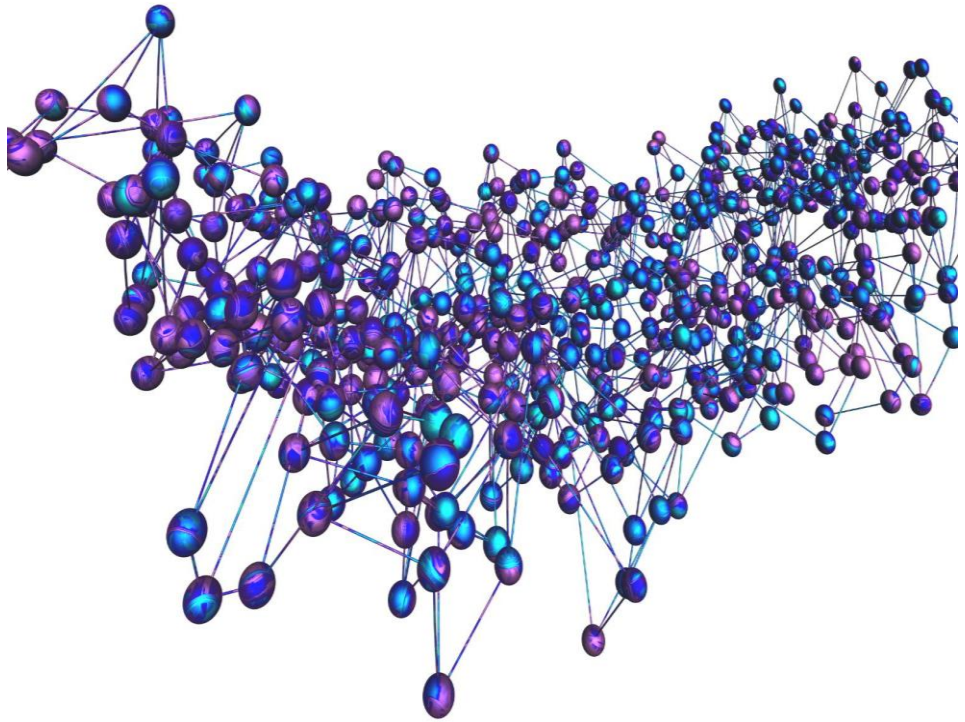
Quantensensoren in der Medizin

- stark gesteigerte Empfindlichkeit und Auflösung bildgebender Verfahren
  - Magnetresonanztomographie
- verbessertes Signal-Rausch-Verhältnis
- geringere Strahlungsintensität / -Belastung
- präzisere und schnellere Diagnostik und Therapiemonitoring
  - Krebsfrüherkennung, Blutanalyse
  - Magnetoenzephalographie (Hirnströme), Magnetokardiographie
- Qualitätskontrolle bei Arzneimitteln



Quantensimulation in der Chemie

- Simulation von Molekülen ist ein dynamisches Forschungsgebiet
  - Mit Nuclear Magnetic Resonance (NMR) kann der Aufbau komplexer Moleküle präzise dargestellt werden - Quantenlineal
  - chemisch bedeutungsvolle Simulationen ab 20 - 100 Qubits
    - heute noch oft im Verbund mit Hochleistungsrechnern
- Erforschung neuer Materialien wie Polymere und Katalysatoren
  - Modellierung leistungsfähigerer Batteriekomponenten
  - Nachhaltige und umweltfreundliche Materialien
- erstmals Analyse ultraschneller chemischer Prozesse
- Entwicklung neuer wirkungsvoller Medikamente
- Erfassen des Vorkommens gefährlicher Substanzen (PFAS)
  - Suche nach ungefährlichen Alternativen



Entwicklungsstand und Herausforderungen

- Quantensensorik Systeme
  - sind heute bereits praxistauglich für spezialisierte, missionskritische Anwendungen
  - noch voluminös und teuer
- werden schrittweise industriell nutzbar
- der breite Einsatz in Standardgeräten wird in den kommenden Jahren folgen
- Deutschland verfügt mit seiner Photonikindustrie über einen außergewöhnlich innovativen Industriezweig
- startet von einer exzellenten internationalen Wettbewerbsposition
  - hat beste Voraussetzungen, um sich mit neuen quantentechnologiebasierten Produkten neue Märkte zu erschließen.
- Intensiver Austausch der KMUs mit den Universitäten notwendig

Herausforderungen

- Miniaturisierung - Chipentwicklung
- Systemintegration
- gesteigerte Robustheit

Fazit und Ausblick

Beginn einer neuen Ära

Quantentechnologie markiert den Start einer technologischen Revolution mit großem Potenzial für viele Bereiche.

Herausforderungen

Eingehende Forschung und die Entwicklung neuer Technologien sind notwendig für den Durchbruch in der Quantentechnologie

Nachhaltige Veränderung

Diese Technologien werden unsere Welt langfristig verändern und völlig neue Möglichkeiten schaffen.

Vielen Dank

für Ihre Aufmerksamkeit

Quellen

Bilder

- spektrum.de
- Microsoft 365-Inhaltsbibliothek
- John D/Getty Images

Internetquellen

- Zu Quantum-Echoes
- Zu Willows Chip

Literatur

- Knörzer, Edmonts **Ein Quantum Zukunft**
  - Springer Verlag
- Rainer Müller, Franziska Greinert **Quantentechnologien**
  - De Gruyter Studium
- Wilms, Neukart **Chancen und Risiken von Quantentechnologie**n
  - Springer Gabler Verlag
- Christian Meier Eine kurze Geschichte vom Quantencomputer
- Spektrum der Wissenschaft kompakt: Quantencomputer