

# Quantenkommunikation

# Gliederung

1. Was sind Quanten?
2. Grundlegende Konzepte der Quantenmechanik
3. Was ist Quantenkommunikation?
4. Warum ist sie wichtig?
5. Anwendungen
6. Herausforderungen und Zukunftsaussichten
7. Ausblick Quantenkryptographie?

# 1. Was sind Quanten?

- Quant= lat. „quantum“, was „wie groß“ bzw. „wie viel“ bedeutet → Messbares, „Quantifizierbares“
- Idee elementarer Grundbausteine schon im antiken Griechenland → Demokrit: Materie kann nicht unendlich geteilt werden, sondern dass man irgendwann auf Atome, auf unteilbare Stücke stoßen
- mehr als 2000 Jahre später bestätigt mit Frage nach der Natur des Lichts (Welle oder Teilchen?)
- Thomas Young: Doppelspaltversuch → Licht = Wellen mit typischen Überlagerungsmuster
- Photoeffekt: Licht löst Elektronen aus Metalloberflächen → Stromfluss nicht abhängig von Helligkeit, sondern Farbe
- Albert Einstein löste Problem, indem er ein ursprünglich rein theoretisches Konzept von Max Planck aufgriff, dass Licht in Paketen auftritt, wobei die Energie eines solchen Photons nur von der Wellenlänge, also der Farbe, abhängt
- Auch einzelne Elektronen wechselwirken mit sich selbst

## → **Wellen-Teilchen-Dualismus**

### → **Beispiele:**

- Elektronen und Quarks
- Photonen und Gluonen
- Gitterschwingungen in einem Kristall

## 2. Grundlegende Konzepte der Quantenmechanik

### Was ist Quantenmechanik und welche Phänomene beschreibt sie?

- Phänomene auf der atomaren und subatomaren Ebene zu erklären
- **Probleme mit klassischer Physik:** Klassische physikalische Gesetze, insbesondere die Newtonsche Mechanik und die elektromagnetische Theorie von Maxwell, konnten nicht alle experimentellen Ergebnisse auf mikroskopischer Ebene erklären. Insbesondere die Eigenschaften von Atomen und subatomaren Partikeln konnten nicht konsistent beschrieben werden.
- **Plancksches Strahlungsgesetz (1900):** Ein Schlüsselereignis, das zur Entwicklung der Quantenmechanik führte, war die Arbeit von Max Planck. Er führte 1900 das Plancksche Strahlungsgesetz ein, um Phänomene im Zusammenhang mit der Emission von elektromagnetischer Strahlung durch schwarze Körper zu erklären. Dabei wies er nach, dass die Energie nicht kontinuierlich, sondern in Einheiten (Quanten) aufgenommen oder abgegeben wird.
- **Photoelektrischer Effekt (1905):** Albert Einstein trug mit seiner Erklärung des photoelektrischen Effekts ebenfalls zur Entwicklung der Quantenmechanik bei. Er schlug vor, dass Licht nicht nur als Welle, sondern auch als Teilchen (Photonen) betrachtet werden sollte. Dies war ein wichtiger Schritt in Richtung der Quantenansicht der Natur.
- **Bohrsches Atommodell (1913):** Niels Bohr entwickelte ein Modell des Wasserstoffatoms, das erfolgreich bestimmte spektrale Linien erklärte, indem er Quanten einbezog. Bohrs Modell war jedoch begrenzt und konnte nicht alle Beobachtungen erklären. Heute gilt es als überholt und wird den semiklassischen Quantentheorien zugerechnet.
- **Welle-Teilchen-Dualismus:** Die Entdeckung des Welle-Teilchen-Dualismus von Materie, insbesondere von Elektronen, zeigte, dass Materie sowohl Wellen- als auch Teilcheneigenschaften aufweist. Dies führte zu weiteren Entwicklungen in der Quantenmechanik.

Mittels Quanten lässt sich eine Vielzahl von Phänomenen auf der mikroskopischen Ebene erklären, darunter:

- **Quantelung der Energie:** Energie wird in diskreten Einheiten (Quanten) übertragen
- **Unschärferelation:** Es gibt Grenzen für die gleichzeitige Messung von beispielsweise Ort und Impuls eines Teilchens
- **Quantenverschränkung:** Teilchen können miteinander verschränkt sein, und der Zustand eines Teilchens kann den Zustand eines anderen beeinflussen, unabhängig von der Entfernung
- **Zustände und Wahrscheinlichkeiten von Quanten:** Die Beschreibung von Teilchen erfolgt oft durch Wellenfunktionen, die Wahrscheinlichkeitsverteilungen repräsentieren

# Wellen- und Teilcheneigenschaften

- Teilchen wie Elektronen sowohl Wellen- als auch Teilcheneigenschaften
  - klassischen Physik : diskrete Punktteilchen mit definierten Positionen und Geschwindigkeiten → Quantenmechanik: Elektronen, die als grundlegende Bausteine der Materie gelten, zeigen eine Art „Doppelnatur-Verhalten“
  - bestimmten Ort zu einer bestimmten Zeit lokalisiert = Teilchen
  - über Raum erstrecken & Interferenzmuster erzeugen = Welle (z.B. Lichtwelle)
  - grundlegende Unsicherheit in die Vorhersagbarkeit von Eigenschaften subatomarer Teilchen
  - nicht gleichzeitig exakte Informationen über Ort und Impuls
- Notwendigkeit, die Natur der Realität auf quantenmechanischer Ebene durch Wahrscheinlichkeitsverteilungen und Wellenfunktionen zu beschreiben

# Berühmte Experimente

- **Doppelspaltexperiment:** Das Doppelspaltexperiment ist ein Schlüsselexperiment, das den Welle-Teilchen-Dualismus von Teilchen wie Elektronen und Photonen nachweist. Es zeigt, dass Teilchen sowohl als Wellen als auch als Teilchen auftreten können und gilt dank seines Spiels mit Licht als eines der schönsten physikalischen Experimente aller Zeiten.
- **Stern-Gerlach-Experiment:** Das Stern-Gerlach-Experiment demonstriert die Quantisierung von Drehimpulsen. Es zeigt, dass der Drehimpuls eines quantenmechanischen Systems nur bestimmte diskrete Werte annehmen kann, was einen Bruch mit der Kontinuität der klassischen Physik darstellt. Dieses Experiment trug unter anderem zur Entwicklung des medizinischen Kernspin-Verfahrens und zur hochpräzisen Zeitmessung mit Atomuhren bei.
- **EPR-Paradoxon:** Das EPR-Paradoxon, vorgeschlagen von Albert Einstein, Boris Podolsky und Nathan Rosen beschäftigt sich mit dem Phänomen der Quantenverschränkung. Das Gedankenexperiment befasst sich mit der „Fernwirkung“, bei der der Zustand eines Teilchens den Zustand eines anderen Teilchens unmittelbar beeinflussen kann, selbst wenn die beiden Teilchen Lichtjahre voneinander entfernt sind. Die Ergebnisse dieser Experimente widersprechen den klassischen Gesetzen von Lokalität und Realismus.
- **Davisson-Germer-Experiment:** Das Experiment von Clinton Davisson und Lester Germer demonstrierte die Wellennatur von Elektronen. Durch die Beobachtung von Elektronenbeugung an einem Kristallgitter bestätigte das Experiment, dass Elektronen nicht nur als Teilchen betrachtet werden können, sondern auch Welleneigenschaften aufweisen. Dies unterstützte die De-Broglie-Hypothese der Materiewellen.

# Grundlegende Konzepte

- **Superposition:** Zustand, in dem sich ein Quantenteilchen in mehreren Zuständen gleichzeitig befindet (z. B. ein Qubit kann gleichzeitig 0 und 1 sein)  
→ beispiel Doppelspaltexperiment
- **Verschränkung (Entanglement):** Zwei oder mehr Teilchen sind so miteinander verbunden, dass die Messung des Zustands eines Teilchens den Zustand der anderen sofort beeinflusst, unabhängig von der Entfernung.
- **No-Cloning-Theorem:** Ein unbekannter Quantenzustand kann nicht perfekt kopiert werden
- **Heisenbergsche Unsicherheitsprinzip / -relation:** unmöglich, bestimmte Paare von physikalischen Eigenschaften eines Teilchens gleichzeitig mit unendlicher Genauigkeit zu messen (Ort & Impuls)
  - Konkret : Je genauer sich der Ort eines Teilchens bestimmen lässt, desto unsicherer wird die Messung seines Impulses und umgekehrt.



# 3. Was ist Quantenkommunikation?

- Quantenkommunikation = Informationsübertragung mit Prinzipien der Quantenmechanik.
- Nutzt **Verschränkung** und **Superposition** zur sicheren Schlüsselverteilung.
- Abhörversuch → Manipulation durch Abweichungen in der statistischen Verteilung sofort erkennbar
- Wichtige Anwendung: **Quantenschlüsselverteilung (QKD)** → Schlüssel ist abhörsicher.
- Erste praktische Anwendungen: Pilotprojekte wie **QuNet** in Berlin, Forschung an **Quantenrepeatern** und **Satelliten** für größere Entfernungen.
- <https://www.youtube.com/watch?v=b4tHlckW8aY>
- [1] → siehe Word Dokument
- **Beispiel Alice/Bob:**
- Grundsätzlich läuft das so: Zwei Kommunikationspartner, in der Quantenliteratur für gewöhnlich "Alice" und "Bob" genannt, wollen sich eine Botschaft schicken. Alice verschlüsselt die Information in Frankfurt und schickt sie als Zahlenreihe aus Nullen und Einsen, also im Binärcode zu Bob nach Kehl. Den verwendeten Schlüssel, eine ebenso lange Zahlenreihe aus Nullen und Einsen, schickt Alice anschließend mittels Quantenteilchen, zum Beispiel Photonen, durch die Glasfaserleitung zu Bob. Die beiden machen sich messbare Zustände dieser Lichtquanten zunutze, üblicherweise deren Polarisierung – die Schwingungsrichtung des Lichts. Nach einem Abgleich kann Bob die ursprüngliche Botschaft entschlüsseln. Versucht nun eine dritte Person, üblicherweise "Eve" genannt, den Schlüssel in der Mitte der Leitung abzugreifen, können Alice und Bob das mit hoher Wahrscheinlichkeit feststellen. Die Regeln der Quantenphysik wollen es so: Bei jedem Versuch, die Polarisierung der abgefangenen Photonen unbemerkt zu messen, läuft Eve Gefahr, diese zu verändern und sich so zu verraten. [2]

# Wofür?

- **Abhörerkennung:** Manipulation zerstört die Verschränkung und wird statistisch sichtbar.
  - Verschränkte Zustände des Lichts sind ideal, um einen Quantenschlüssel für die Quantenkryptographie zu verteilen. Die Eigenschaft der Verschränkung liefert für Messungen bei „A“ und bei „B“ echte Zufälligkeit, gleichzeitig aber auch die Übereinstimmung der Schlüsselketten, und drittens die Möglichkeit potenzielle Abhörversuche zu erkennen. Letzteres wird dadurch möglich, dass Abhörversuche (zu einem Teil) die Verschränkung stören und dadurch Spuren hinterlassen.
- **Maximale Sicherheit:** Mathematisch beweisbar gegen heutige und zukünftige Angriffe.
  - Beispiel: Wir hatten 2015 die derzeit fortschrittlichste Quantenschlüsselverteilung basierend auf Amplituden- und Phasenmodulationen des Lichts demonstriert. Unsere Implementierung basiert auf stark Einstein-Podolsky-Rosen-verschränktes Licht [1] und ist absolut sicher gegen Abhörversuche, auch gegen solche, die möglicherweise erst zukünftig erfunden werden. Dieser Sicherheit liefert ein mathematischer Beweis auf Grundlage der Quantentheorie. Aus den Messdaten bei „A“ und „B“ wurde ein echt zufälliger und abhörsicherer Schlüssel mit einer Länge von über 108 Nullen und Einsen erzeugt. Das Besondere an unserer Implementierung war die Sicherheit gegen jegliche Angriffe auf den Kommunikationskanal (einschließlich Angriffe zukünftiger Technologien) sowie die Sicherheit gegen alle Angriffe auf die Geräte am Empfängerstandort [2]. → diese Quellen siehe Artikel
- **Abhörschutz:** Jeder Abhörversuch hinterlässt Spuren in den Messdaten.
- **Zukunftstechnologie:** Grundlage für sichere Kommunikationsnetze (z. B. Banken, Militär, Regierung).
- **Fortschrittliche Forschung:** z. B. Quantenrepeater, Photonenmessungen, Verschränkungs-Destillation
  - Zurzeit wird umfangreiche Forschung im Rahmen der Quantenkommunikation betrieben. Ein wesentliches Problem ist die Dekohärenz, die bei der Übertragung die Verschränkung reduziert und Quantenkommunikation schließlich unmöglich macht. 2008 konnten wir erstmalig eine Zwei-Kopien-Destillation von Verschränkung zeigen [3]. Auch die Grundlagenforschung an der Natur von verschränkten Systemen zeigt nach wie vor überraschende Ergebnisse. In unserer Arbeit [4] konnten wir zeigen, dass es verschränkte Systeme gibt, die Schrödingers „Steering“-Effekt nur in einer Richtung erlauben. Ob dieses Ergebnis zu einer Anwendung in der Quantenkommunikation führen wird, ist derzeit noch Gegenstand der Forschung. In [5] haben wir erstmalig die Quasiwahrscheinlichkeitsdichteverteilung der elektrischen Feldstärke eines Ein-Photonen-Fockzustands bei der Telekommunikationswellenlänge von 1550 nm gemessen. Wie von der Quantentheorie vorhergesagt, ergeben sich negative(!) Werte (Abb.). In [6] haben wir aus einer großen Zahl nur wenig-gequetschter Zustände, eine geringe Zahl stärker gequetschter Zustände „destilliert“. Zum Einsatz kam eine hocheffiziente Photonenzählanlage.
- [3] → siehe Word Dokument

# Anwendungen

- **Quantenschlüsselverteilung (QKD):** Nutzung von Quantenmechanik, um einen sicheren kryptografischen Schlüssel zwischen zwei Parteien zu erzeugen → Quantenkryptographie
  - Beispielprotokoll: **BB84** (Bennett-Brassard 1984).
- **Quanten-Teleportation:** Übertragung eines Quantenzustands von einem Ort zu einem anderen ohne den physischen Transport des Teilchens selbst.
- **Quantennetzwerke:** Visionen und Herausforderungen für zukünftige, vernetzte Quantensysteme.

# Mögliche weitere Quellen

- <https://www.helmholtz.de/glossar/begriff/quantenkommunikation/>
- Arxiv :
  - Continuous-Variable Quantum Key Distribution with Gaussian Modulation -- The Theory of Practical Implementations
  - The Security of Practical Quantum Key Distribution
  - Gaussian Quantum Information
- Max-Planck-Institut: Ein Impuls für abhörsichere Quantenkommunikation
- <https://www.nist.gov/quantum-communications>
- <https://pages.jh.edu/rrynasi1/HealeySeminar/literature/Nielsen+Chuang2010QuantumComputation+QuantumInformation.FirstTwoChapters.pdf>
- [https://www.researchgate.net/publication/328336776\\_Quantum\\_Processes\\_Systems\\_and\\_Information\\_by\\_Benjamin\\_Schumacher\\_Michael\\_Westmorel\\_and](https://www.researchgate.net/publication/328336776_Quantum_Processes_Systems_and_Information_by_Benjamin_Schumacher_Michael_Westmorel_and) --> mögliche Übungsaufgaben