Karlsruhe Institute of Technology

Von abhörsicherer Kommunikation zum Quanteninternet

Prof. David Hunger

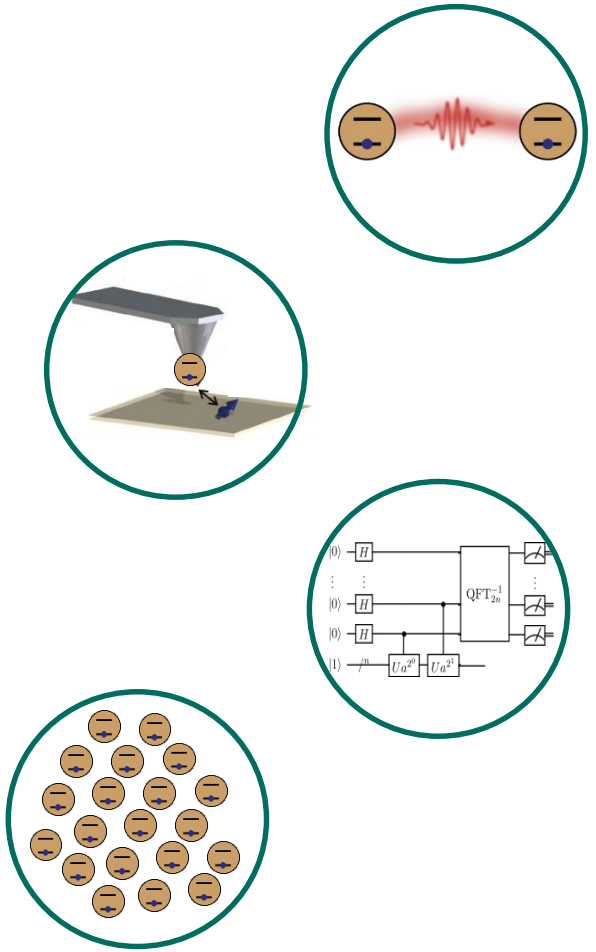
Physikalisches Institut, KIT Fakultät für Physik

Die 2. Quantenrevolution: Quantentechnologien

- einzelne Quantensysteme als Bausteine
- Superposition & Verschränkung als Ressource

Anwendungsgebiete

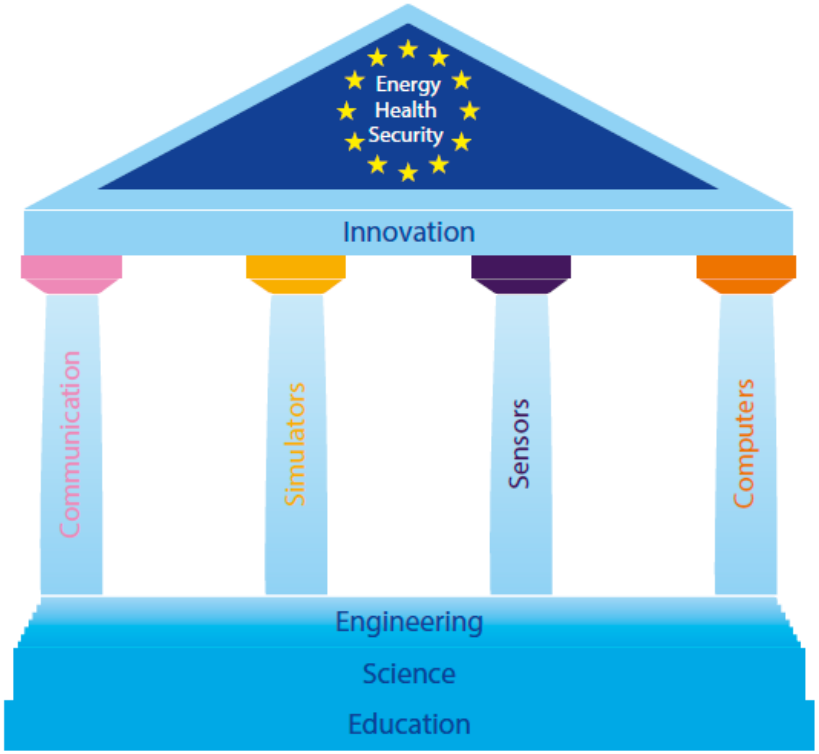
- Quantenkommunikation
- Quantensensorik & -metrologie
- Quantencomputer
- Quantensimulatoren

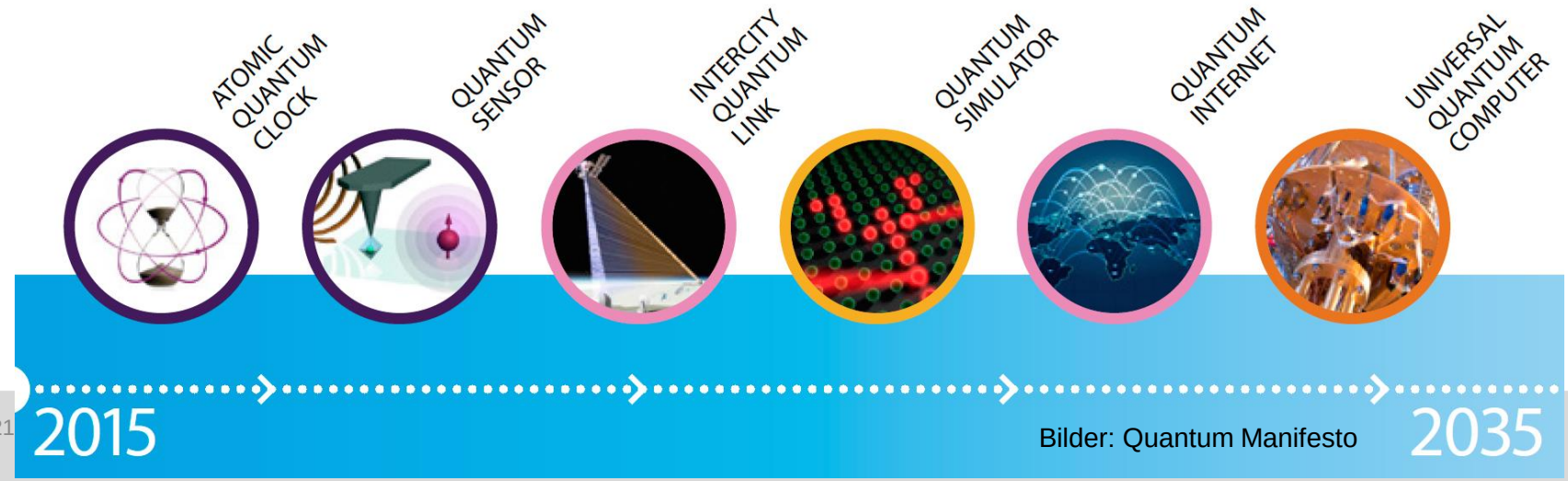


Weltweite Förderaktivitäten

- Europäische Union: 1Mrd €
  Quantentechnologie Flaggschiff

- England: ~ 500 M€
- China: > 10 Mrd €
- USA: > 1 Mrd €
- Deutschland: > 2 Mrd €





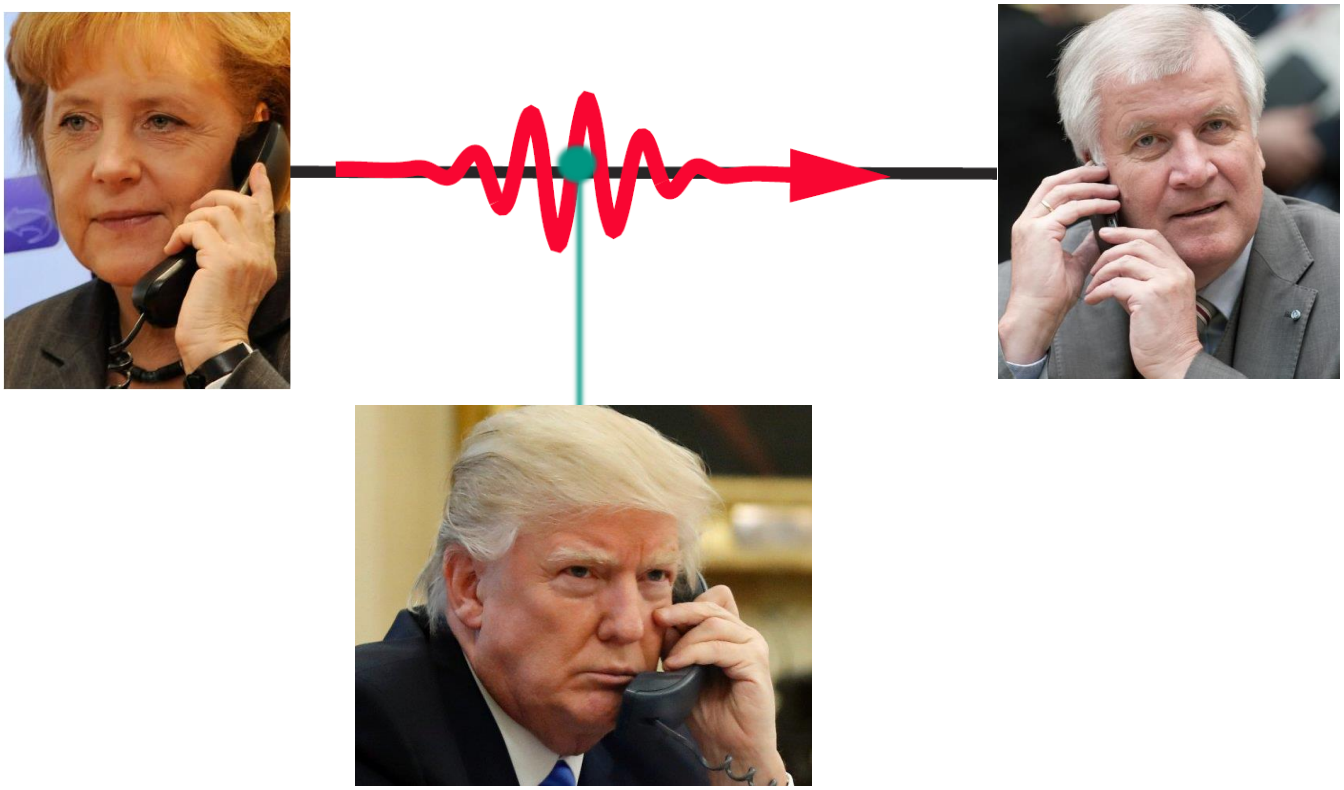
Bilder: Quantum Manifesto

Quantennetzwerke

Anwendungsszenarien

- **Q**uantum **K**ey **D**istribution über große Distanzen
- Verknüpfung von Quantensensoren & Atomuhren
- Verteiltes Quantencomputing

Quantenkryptographie



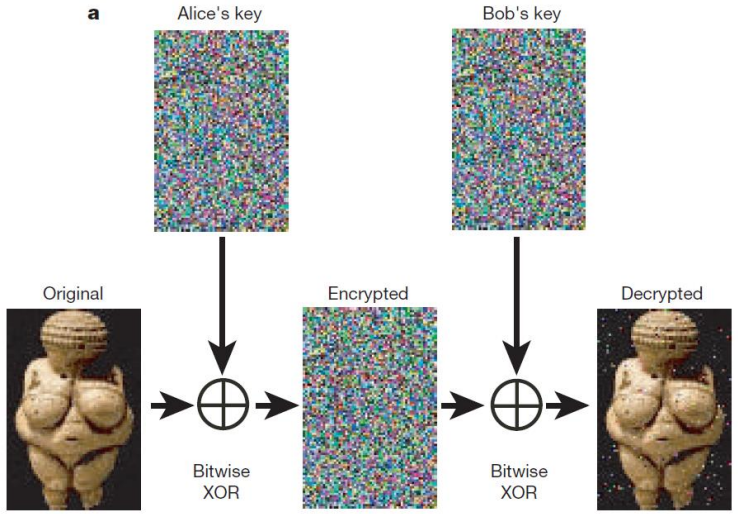
Quantenkryptographie

Kryptographie

teile geheimen, zufälligen Schlüssel

Gefahr:

- Abhören beim Schlüsselaustausch
- Quantencomputer können klassische Verschlüsselung knacken



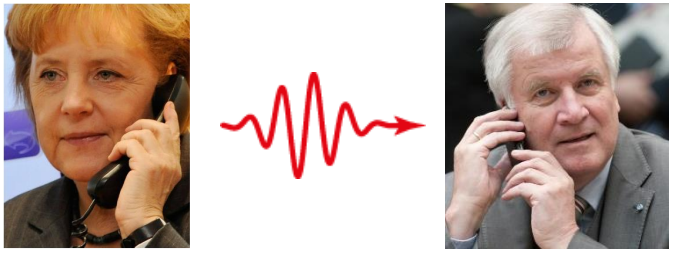
PRL 84, 4729 (2000)

Quantenkryptographie

- Quantenzustände können nicht kopiert werden (No-Cloning-Theorem)

  → absolut abhörsicher

einzelne Photonen um Schlüssel zu teilen

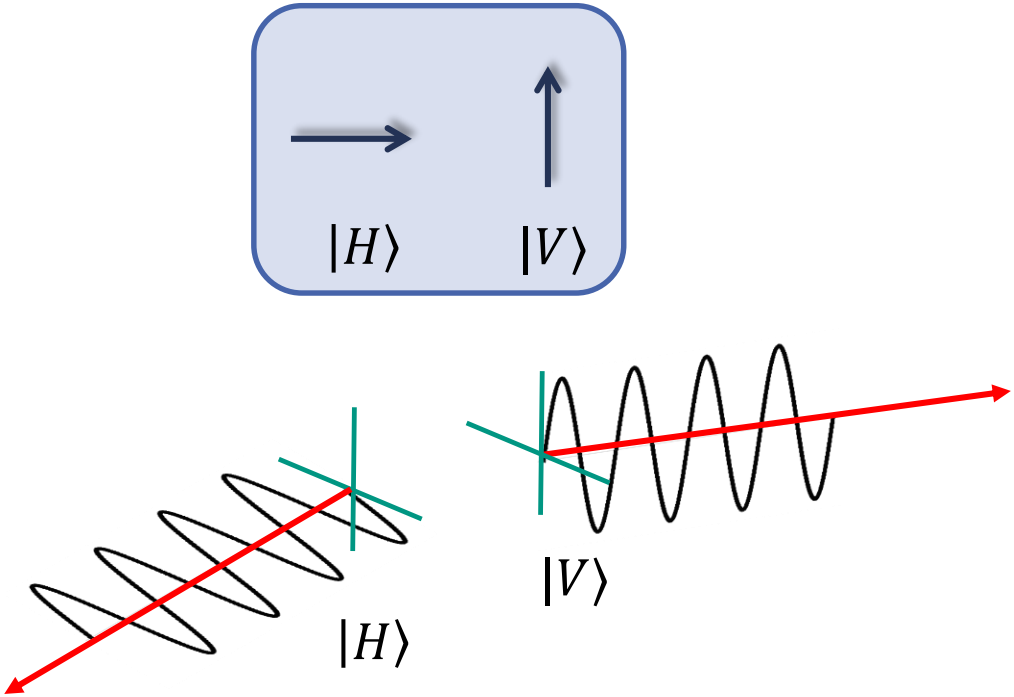


Quantenkryptographie

Implementierung:

Polarisation einzelner Photonen

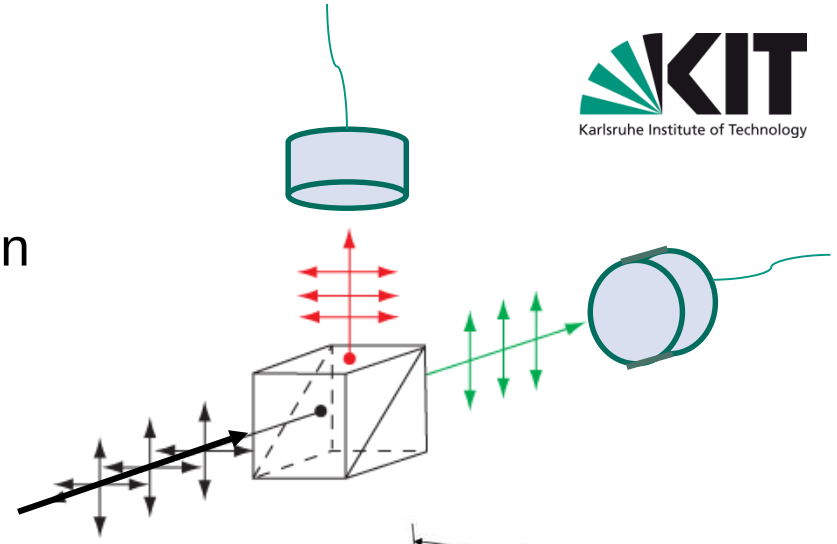
- Zustände $|0\rangle, |1\rangle$ entsprechen Polarisation $|H\rangle, |V\rangle$



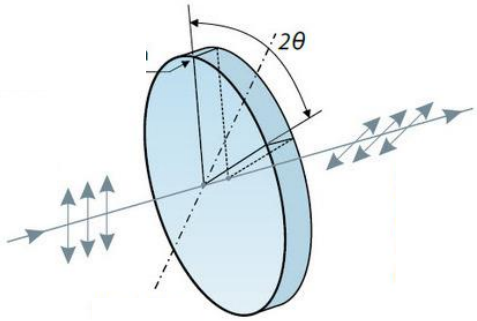
Detektion

Detektion & Manipulation der Polarisation

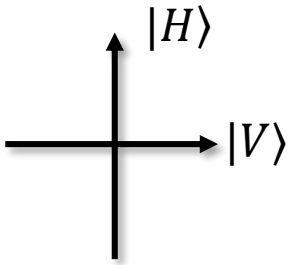
- Polarisationsdetektion:
  - Strahlteilerwürfel
  - Einzelphotonzähler

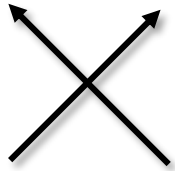


- Polarisationsdreher ($\lambda/2$-Plättchen)



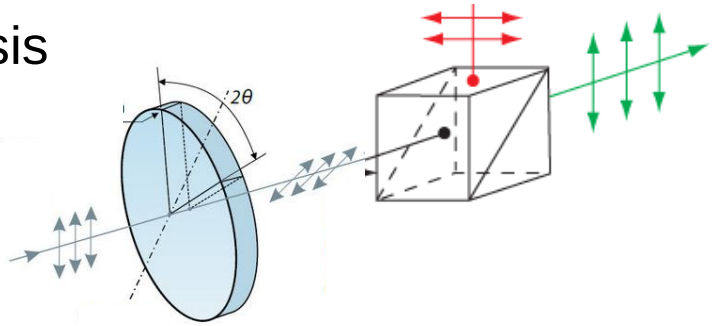
- Transmission zufällig für gedrehte Messbasis





$|+\rangle = |+45°\rangle$

$|-\rangle = |-45°\rangle$



Basis Wahl und Schlüsselerzeugung

Quantenkommunikationsnetzwerke

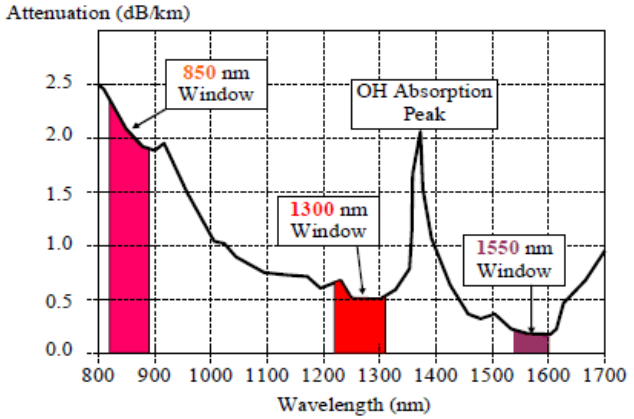
Optische Glasfasern

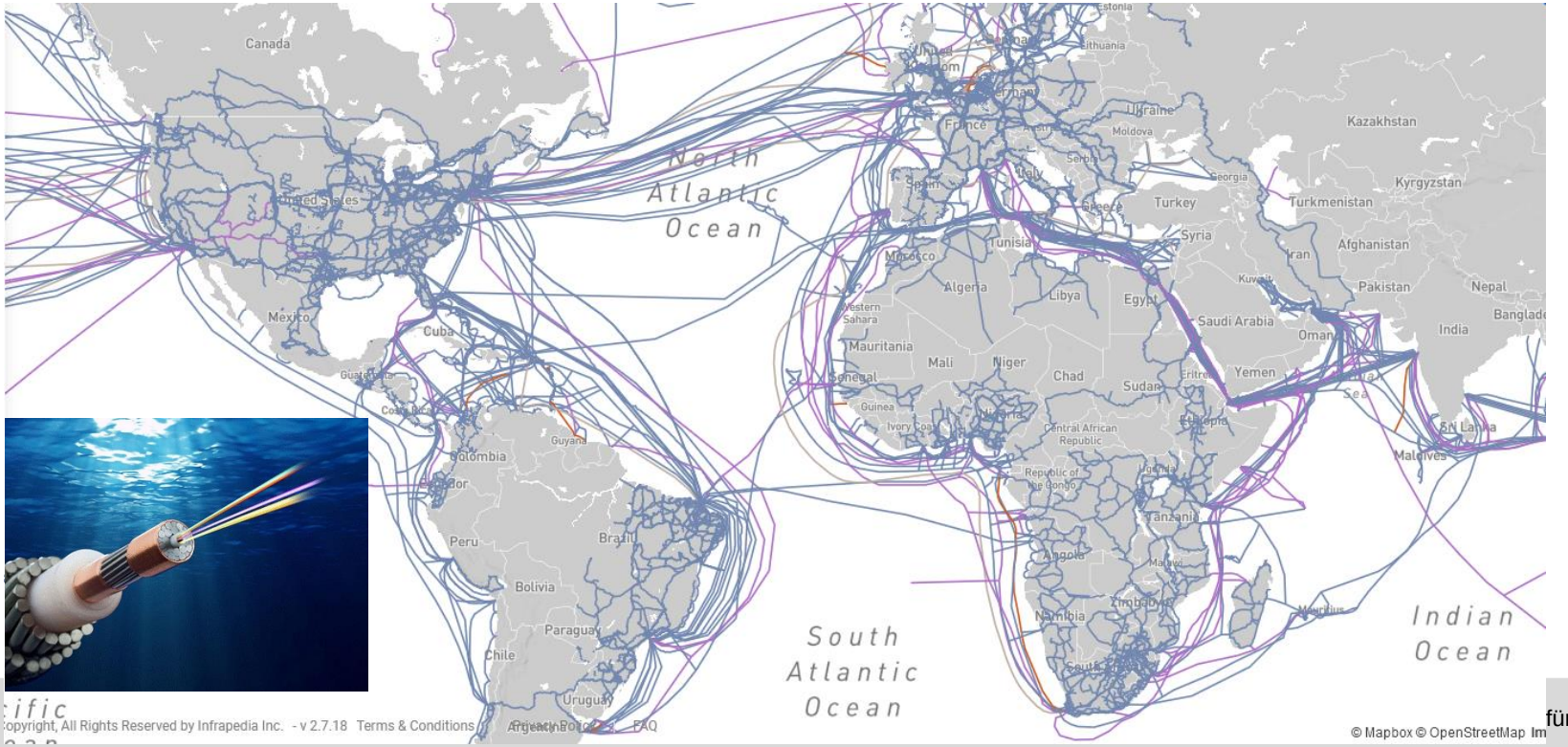
- Problem 1: Dämpfung (0.2dB/km)

  > 97% Verlust nach 100km

- Problem 2: keine direkte Verstärkung

  (no cloning)

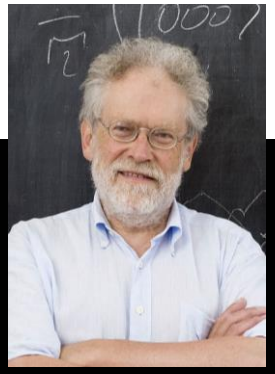




www.infrapedia.com

Quantenkryptographie

- Überbrückung weiter Strecken via Satellit

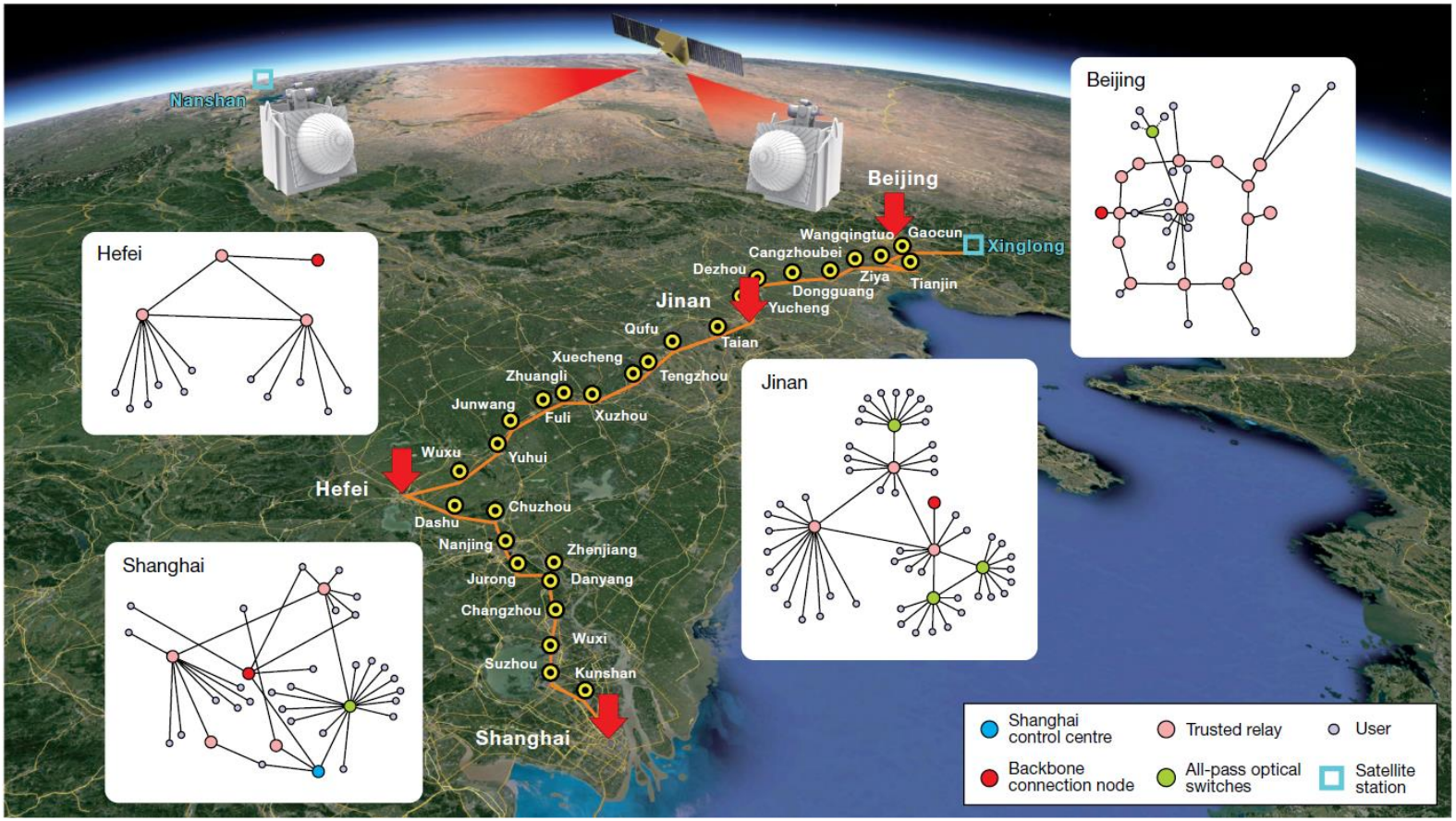


Anton Zeilinger

Jianwei Pan

Nature 549 (2017), PRL 120, 030501 (2018)

Quantenschlüsselaustausch mit sicheren Zwischenstationen



- 2000km Backbone, 32 Zwischenknoten
- 2600km Satellitenverbindung
- Verschiedene lokale Topologien
- 150 Nutzer

Quantenkryptographie kommerziell verfügbar seit ~ 20 Jahren

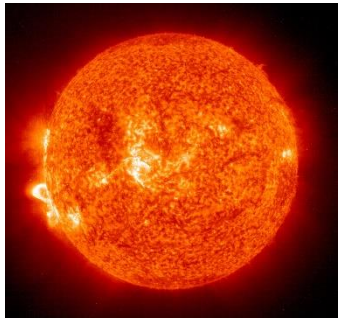
Erste Nutzer

- Quantenverschlüsselung der Wahlen in Genf (2007)
- Banken
- Militär
- Behörden

Wie geht es weiter? Verschränkungsverteilung!

Ein Teilchen: Superposition $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Zwei Teilchen: Verschränkung $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle)$

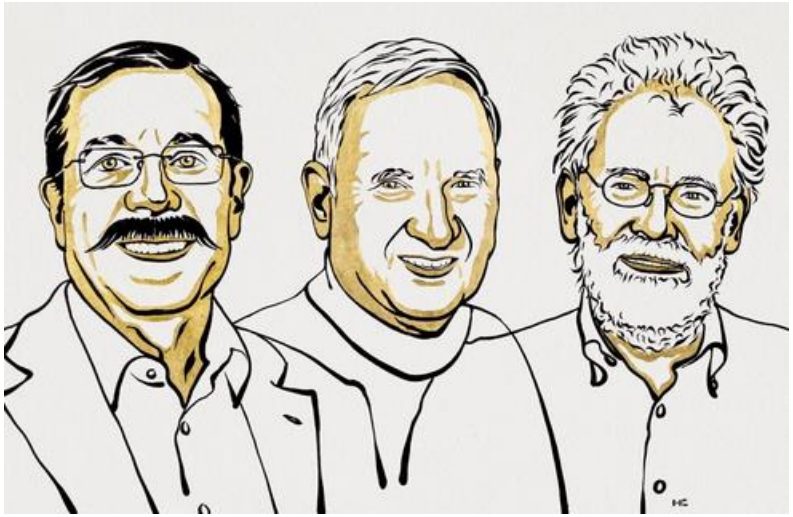


„Spukhafte Fernwirkung“
(Einstein)

Bilder: Internet

Nobelpreis 2022

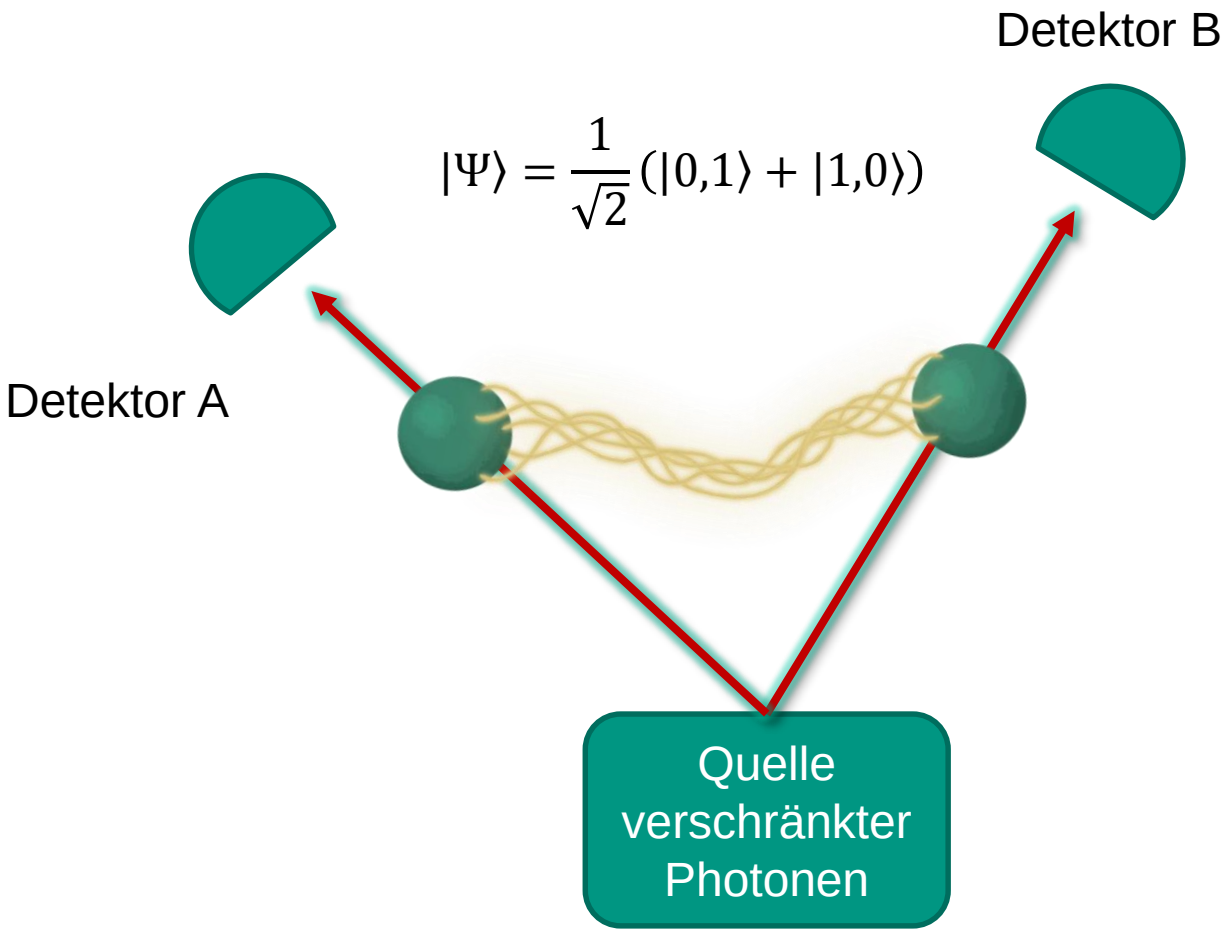
„für Experimente mit verschränkten Photonen, Nachweise der Verletzung der Bell‘schen Ungleichung und Pionierarbeiten auf dem Gebiet der Quanteninformation”



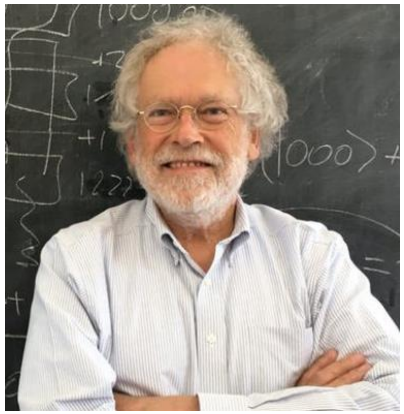
Alain Aspect John Clauser Anton Zeilinger

Niklas Elmehed © Nobel Prize Outreach

Quantenschlüsselaustausch mit verschränkten Photonen



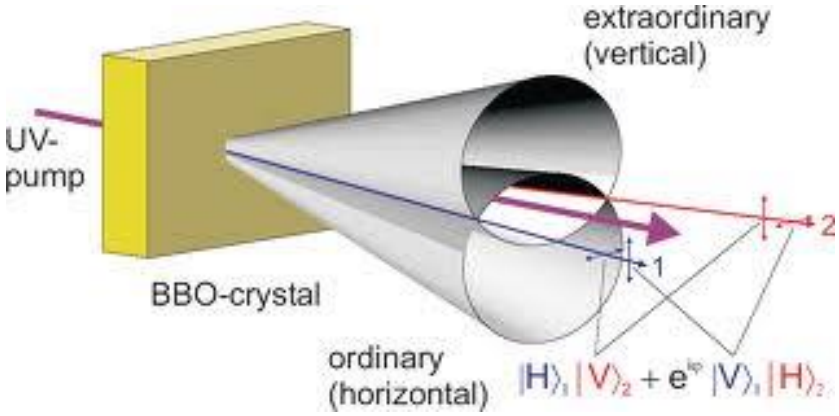
Einfache Quelle verschränkter Photonen

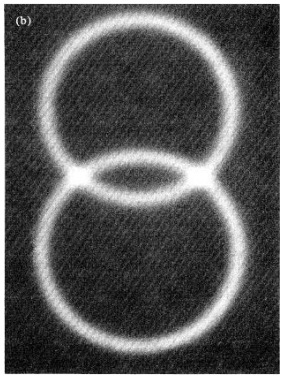


Anton Zeilinger (*1945, Ried im Innkreis, Österreich)

Professor an der Universität Wien

nichtlinearer Optik: parametrische Frequenzkonversion, Paarerzeugung





$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)$$

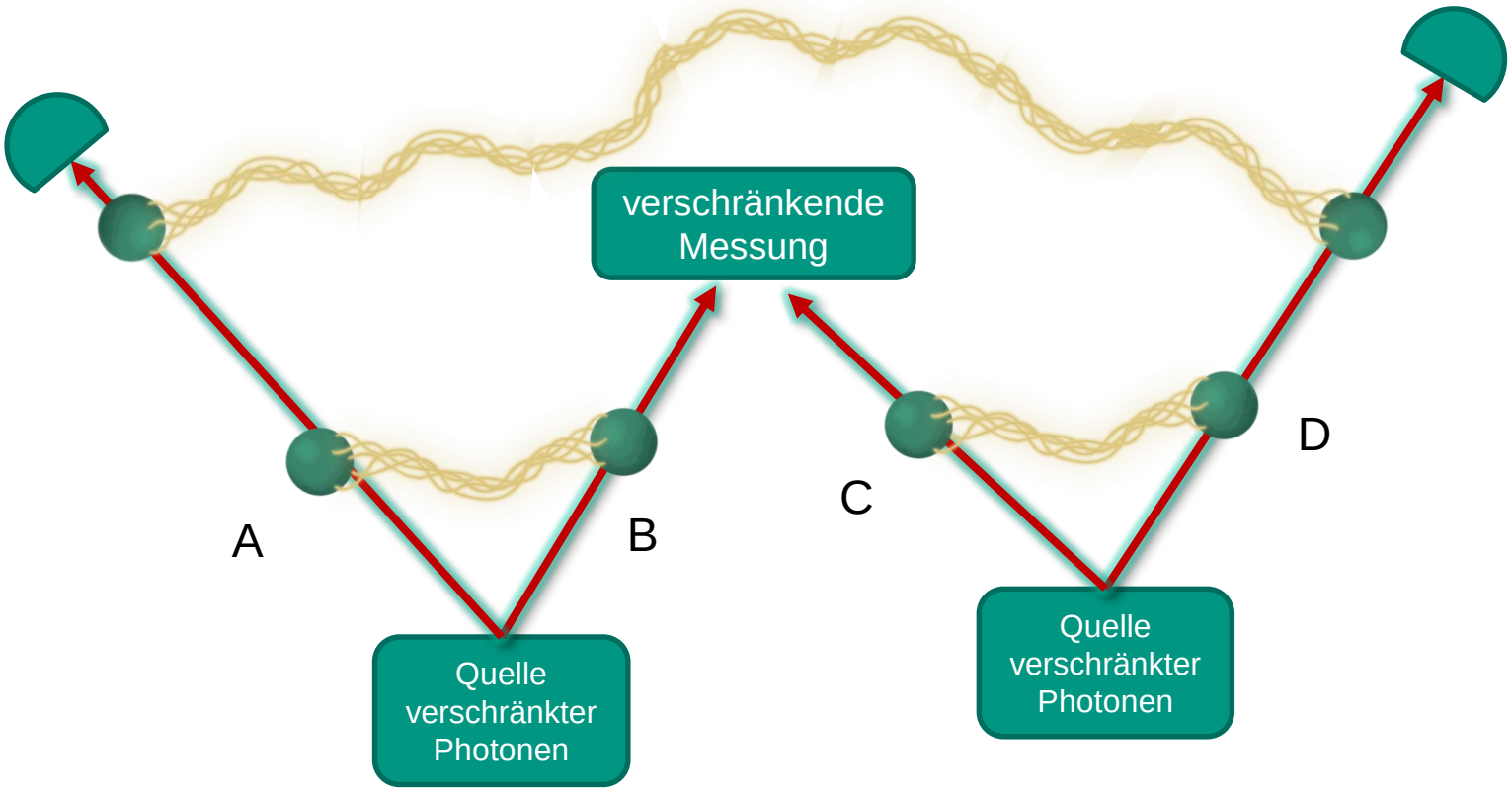
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)$$

verschränkter Zustand: Korrelation unabhängig von Messbasis

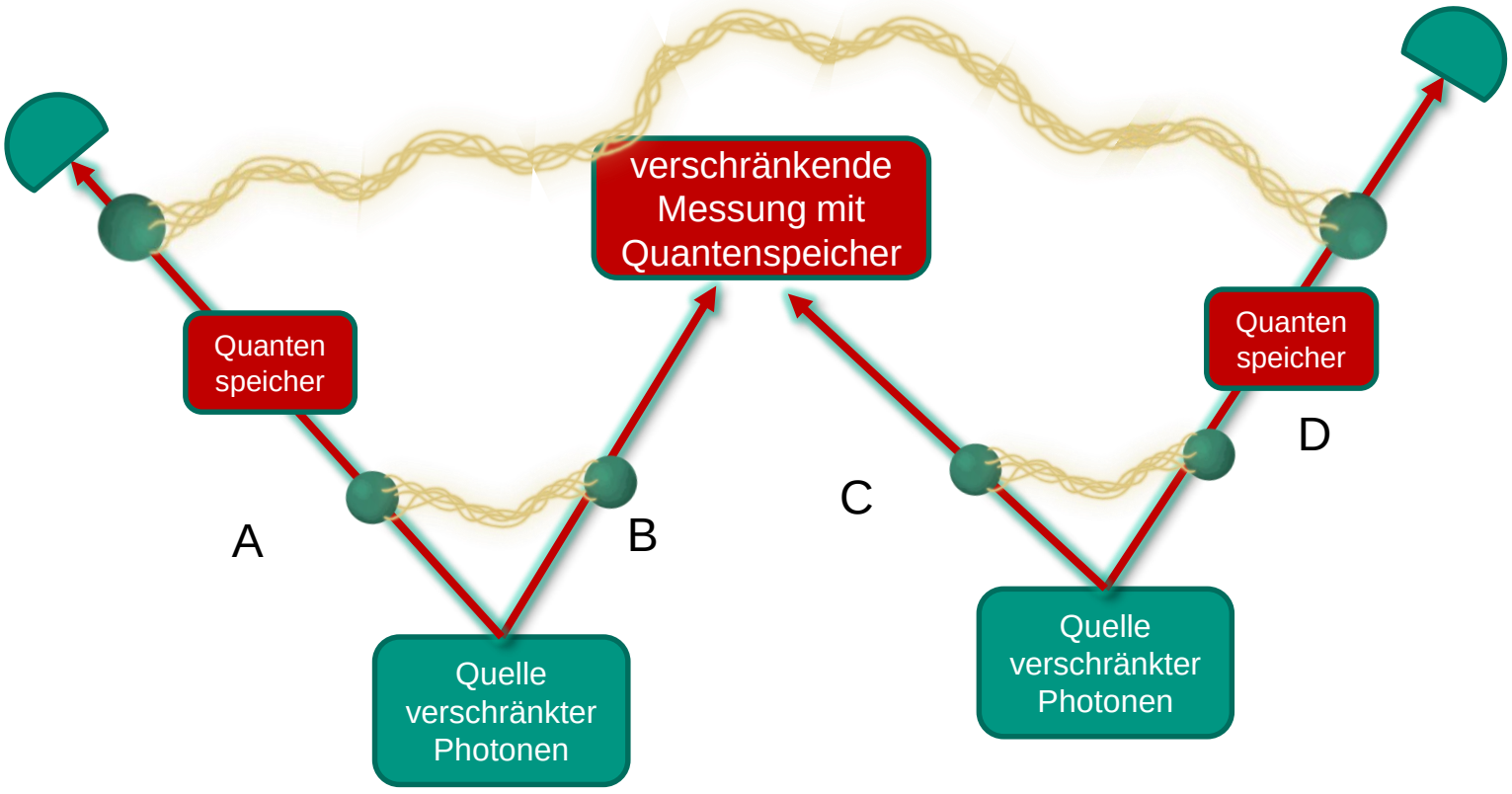
$$|HH\rangle + |VV\rangle = |++\rangle + |--\rangle$$

Phys Rev Lett 75, 4337 (1995)

Die Zukunft: Netzwerke mit Verschränkungstausch

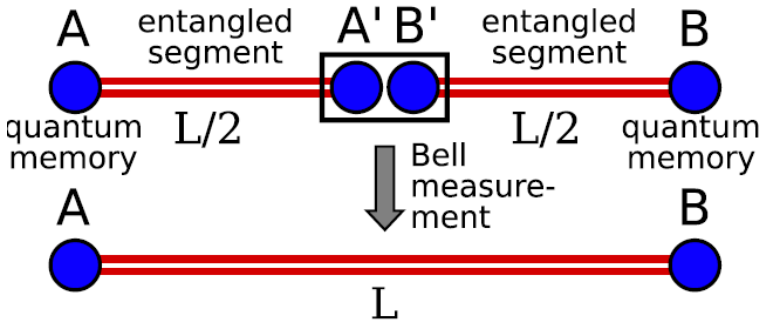


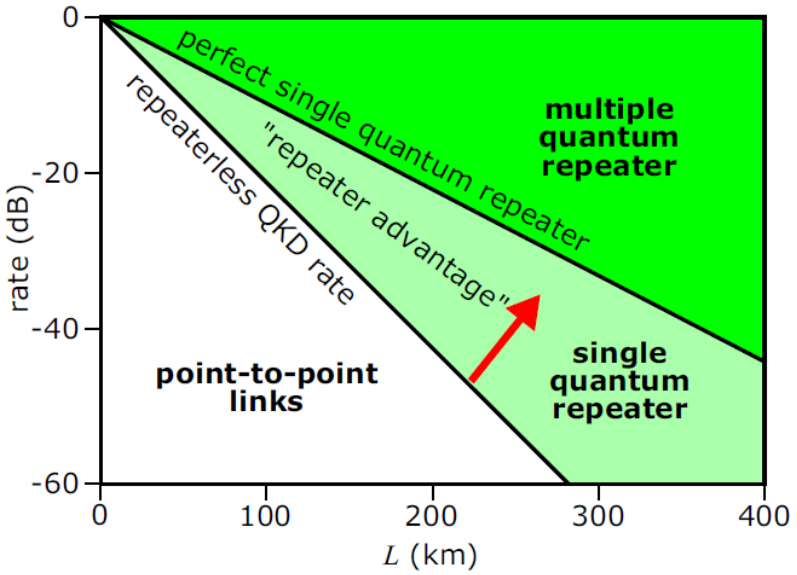
Verschränkungstausch mit Speichern



Quantenrepeater

Verschränkungsverteilung
durch Verschränkungstausch
und Distillation



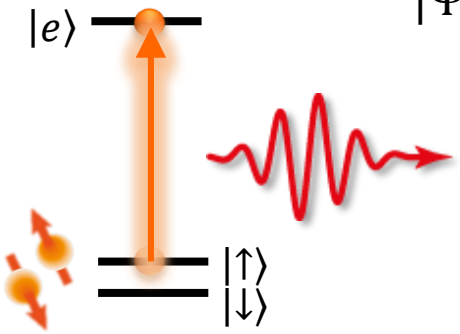


erfordert
- Mehrere Speicherknoten
- Quantenfrequenzkonversion
- Effiziente Detektoren
- …

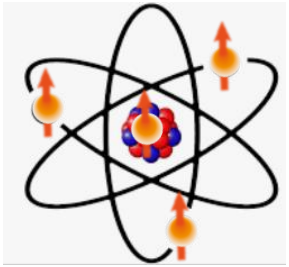
van Loock et al., Adv. Quantum Technologies 3, 1900141 (2020)

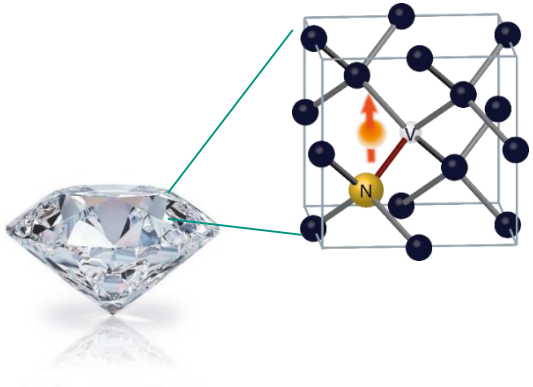
Verschränkung von Speicher Qubits

Langlebige Qubits: **Spins**



$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow, 1\rangle + |\downarrow, 0\rangle)$$

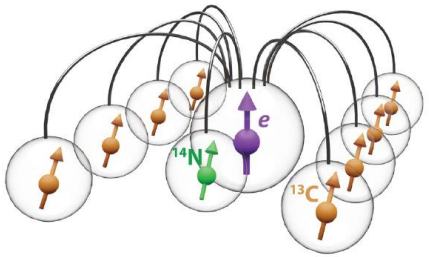




NV Zentren in Diamant

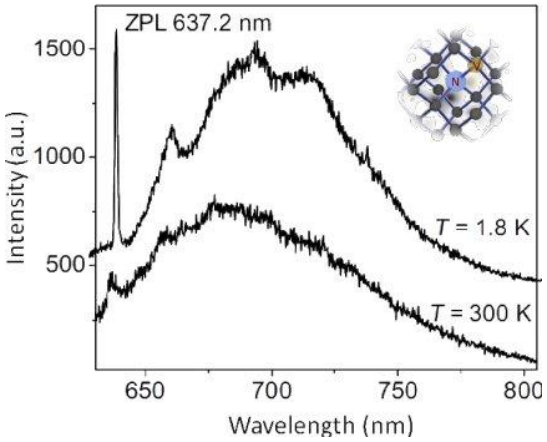
Exzellente Spinkohärenz

- Elektronspin T_2 > 1s at 4K
- ^{13}C Kernspin T_2 ~1 Minute
- Verschränkung über 10s
- Bis zu ~10 Qubits



Fourier limitierte optische Emission

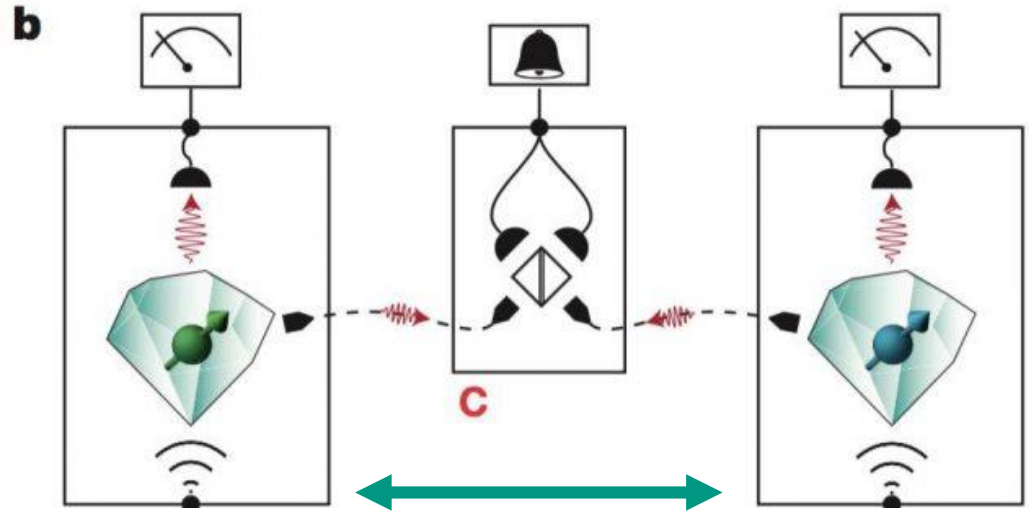
- Spin-Photon Schnittstelle
- Aber nur 3% kohärenter Anteil
- Empfindlich auf el. Störfelder

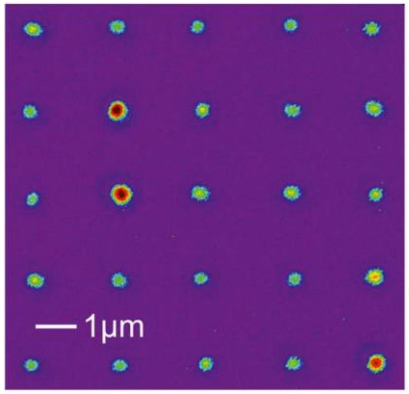


Bernien et al., Nature 497, 86 (2013)
Bradley et al., PRX 9, 031045 (2019)
Hensen et al., Nature 682, 526 (2015)
Humphreys et al., Nature 558, 269 (2018)
Pompili et al., Science 372, 259 (2021)

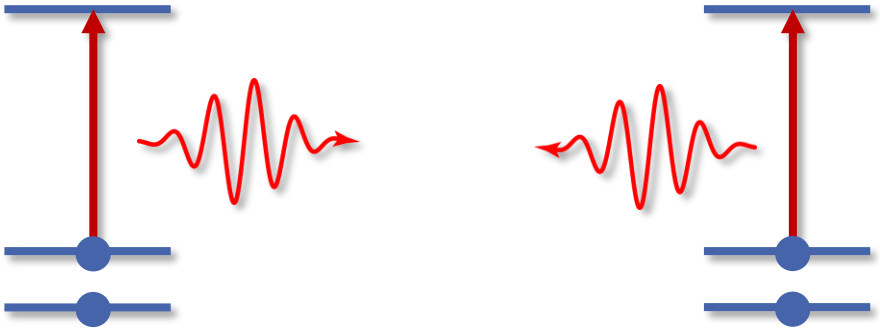
Zwei verschränkte „Atome“ in Diamant

Ronald Hanson





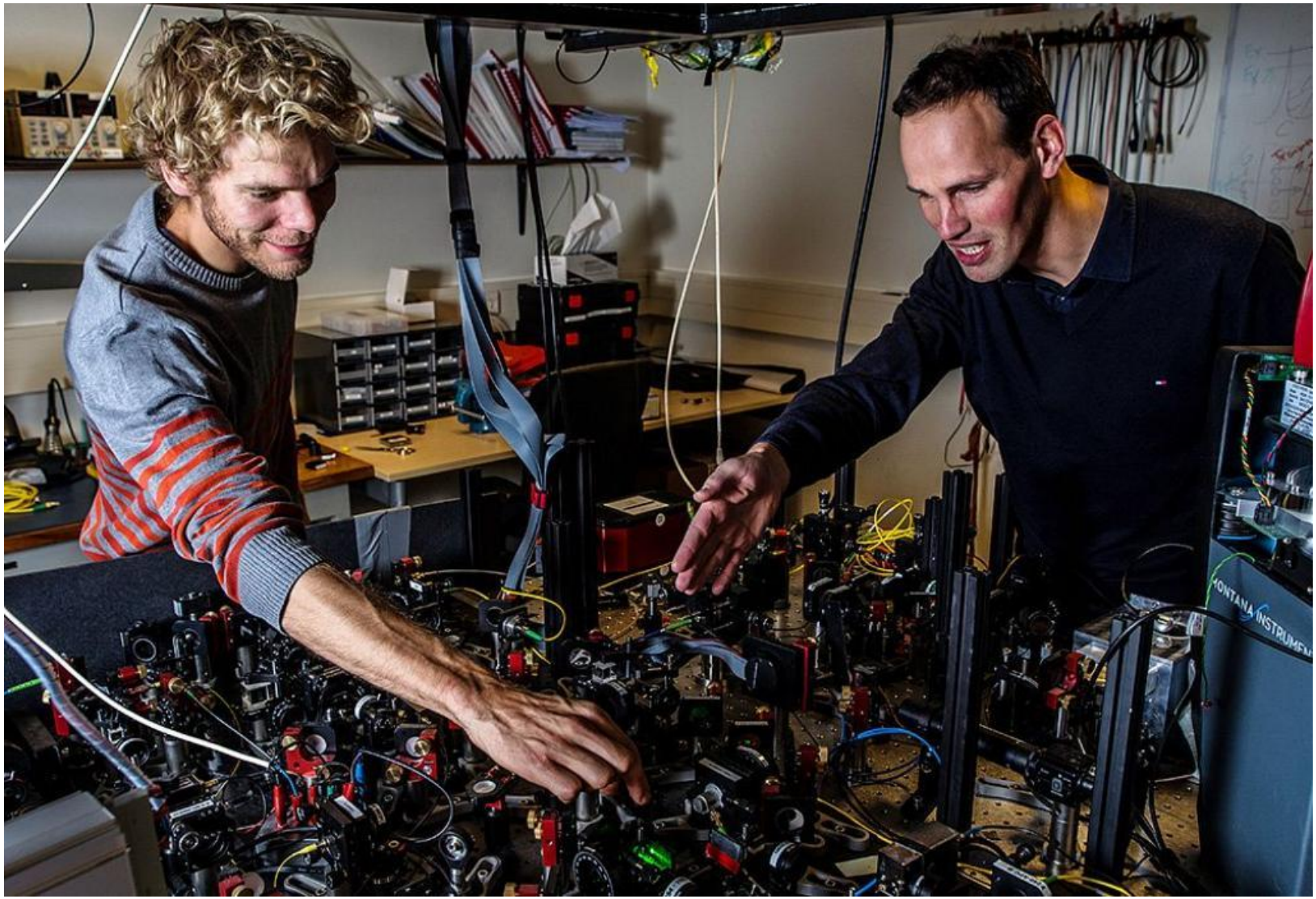
Chen et al, Optica 6, 662 (2019)



$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle)$$

Hensen et al, Nature 526, 682 (2015)

Im Labor

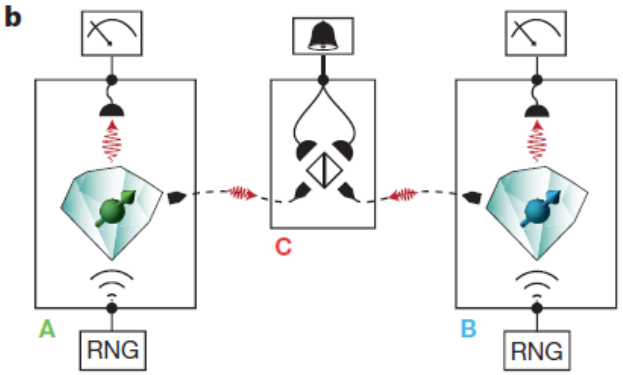


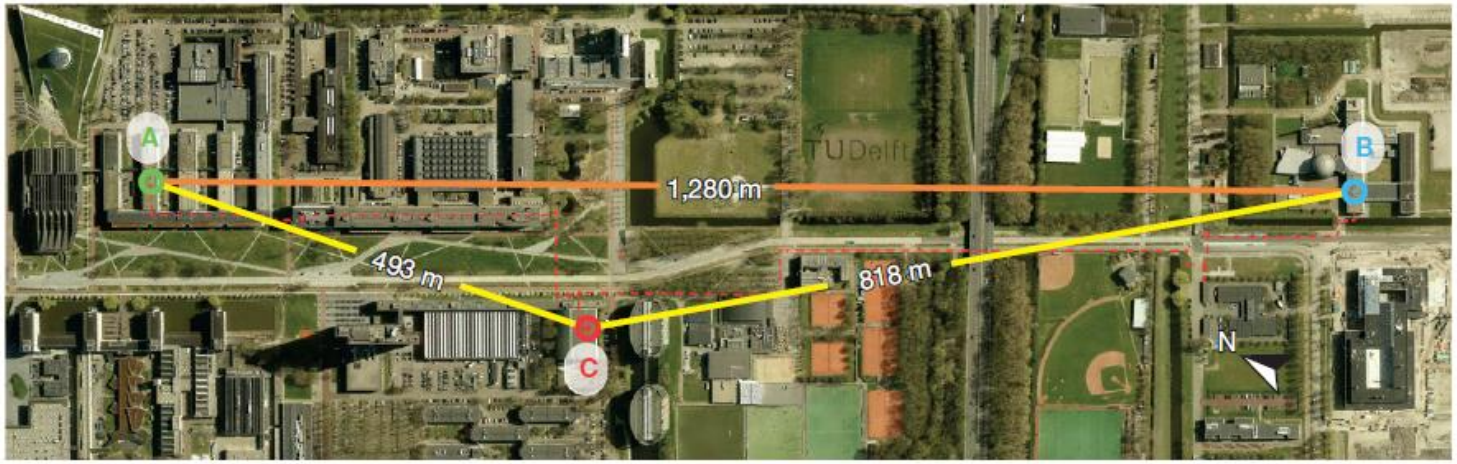
Loop-hole free Bell Test

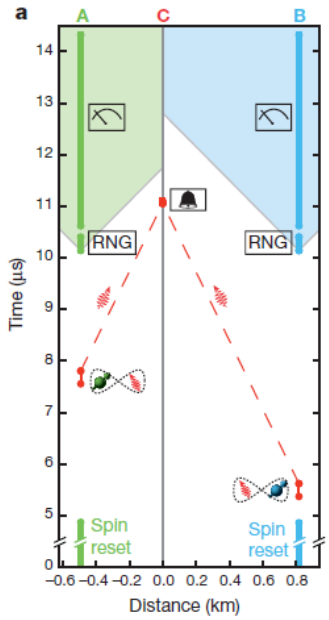
- Korrelationen sind stärker als klassisch möglich
- Nicht kompatibel mit Lokalitätsprinzip und Kausalitätsprinzip

Schlupflöcher:

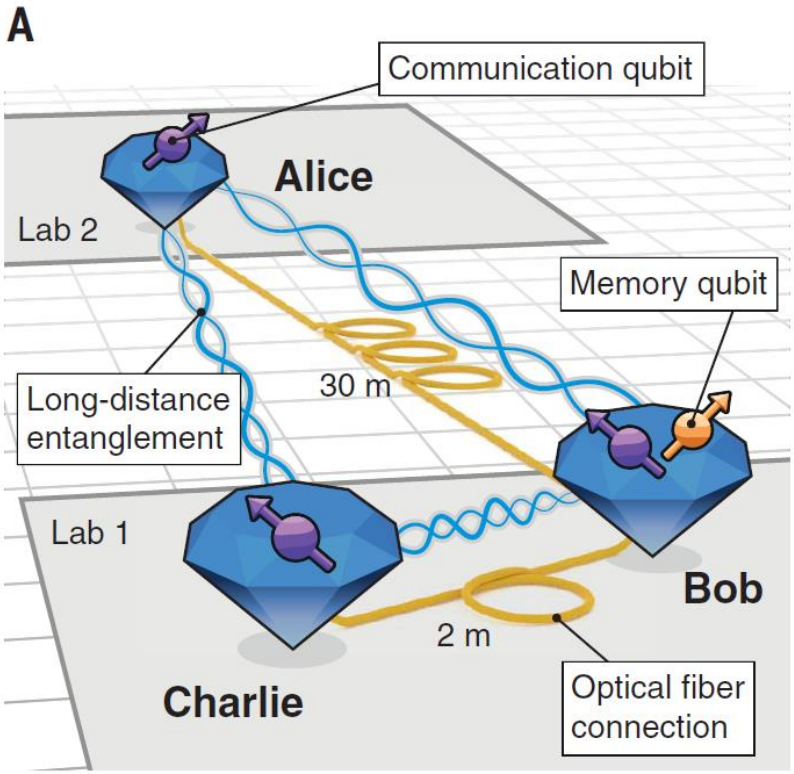
- Lokalität
- Fair sampling
- Wahlfreiheit







Drei-Knoten Quantennetzwerk



Verschränkung von 2 und 3 Knoten

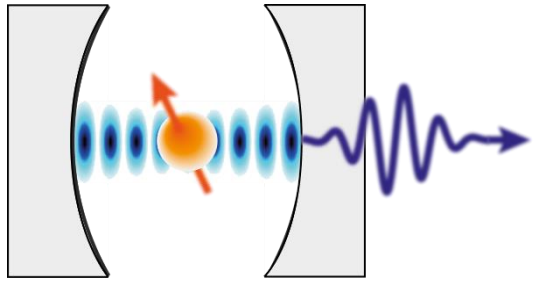
Verschränkung schneller erzeugt als sie zerfällt

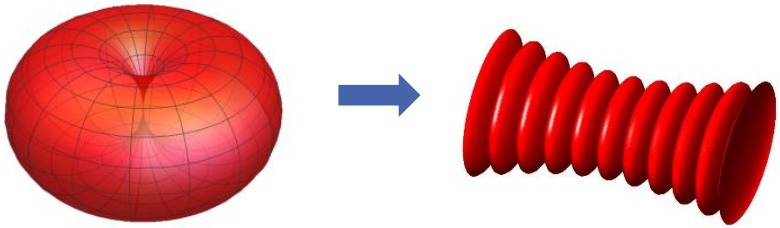
Problem: niedrige Effizienz (10^{-4} pro link)

Pompili et al., Science 372, 259 (2021)

Effiziente Atom – Photon Schnittstelle

Optische Mikroresonatoren
- hochreflektive Spiegel ~ Q
- kleines Volumen ~ V

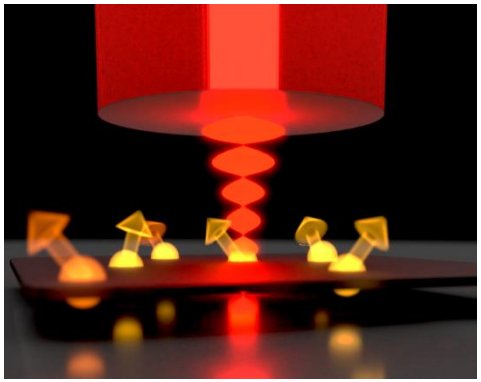




Purcell Effekt
beschleunigte Emission in Resonator

$$\gamma_c = C\,\gamma$$

$$C \sim \frac{Q}{V_m} \sim 10 - 1000$$



Das Quanteninternet

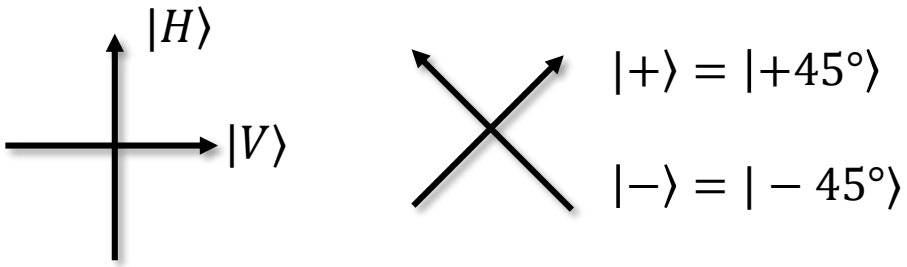
- Verknüpfung kleiner Quantenknoten für Kommunikation über große Distanz
- Verteiltes Quantencomputing für Skalierbarkeit
- Bereitstellung langlebiger Quantenspeicher z.B. für supraleitende Qubits
- Verknüpfte Quantensensoren für erhöhte Empfindlichkeit
- Verknüpfung von unterschiedlichen Quantensystemen

Interessante Webseiten

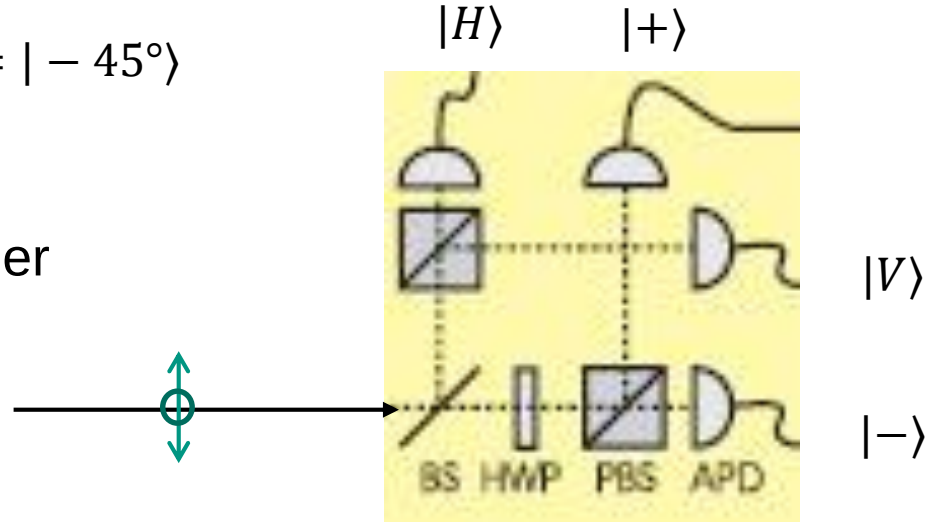
- milq.tu-bs.de (Quantenphysik für die Schule)
- play.quantumgame.io (Spiel – Quantenoptik mit Quantenlichtquellen, Spiegeln, Interferometer)
- www.scienceathome.org (diverse Spiele / app, Transport einer Wellenfunktion im Raum)
- helloquantum.mybluemix.net (IBM Quantenspiel)
- www.research.ibm.com/ibm-q (IBM quantum computing)
- www.meqanic.com/app/ (Quanten Puzzle)
- www.qt.eu (Website des europäischen Quanten Flagships)
- http://quantumalgorithmzoo.org (Überblick Quantenalgorithmen)
- www.qutools.com/quantum-physics-education-science-kits/ (Firma, stellt Quantenoptik Demonstrationsexperimente her)

Zufällige Basiswahl

- wähle zufällige Basis (H, V) / $(+, -)$



- Z.B. durch Zufall am Strahlteiler



Nature 433, 230 (2005)