“Ah”, “Oh” und “Ui”

Faszinierende Phänomene in Quantencomputer

Winterkongress, 21.02.2026

Daniel Rotzetter

whoami

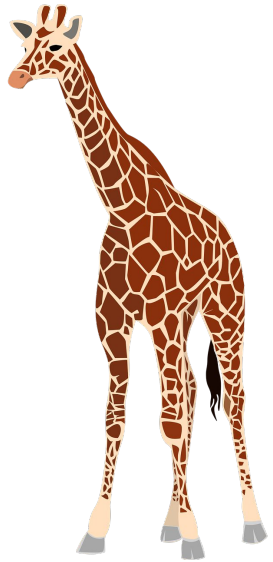
Daniel Rotzetter

Cyber Security Specialist, HSLU
Former Entrepreneur, CTO

https://www.linkedin.com/in/danirotzetter/

Agenda

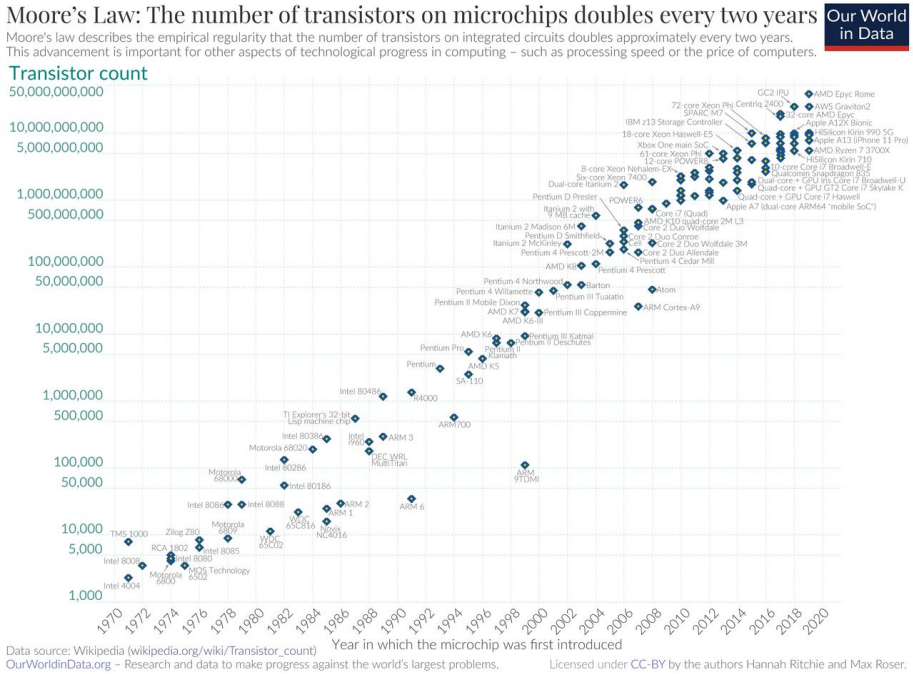
- Grenzen des Bits: klassische Computer am Limit
- Quantenmagie
- Kleine Teilchen, grosse Hürden
- Super-Influencer



Grenzen des klassischen Bits

Moore’sches Gesetz

- Anzahl Transistoren in integriertem Schaltkreis verdoppelt alle 18-24 Monate

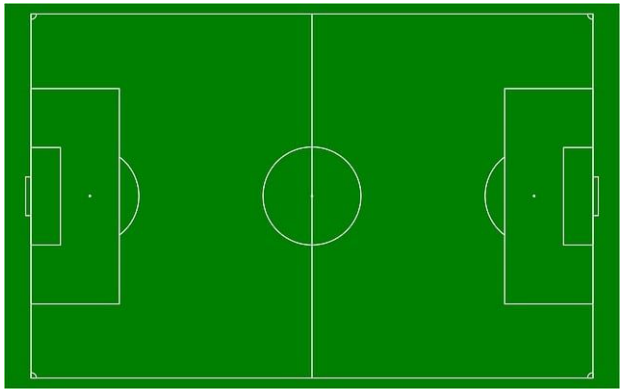


By Max Roser, Hannah Ritchie - https://ourworldindata.org/uploads/2020/11/Transistor-Count-over-time.png, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=98219918

Computer Skalierung

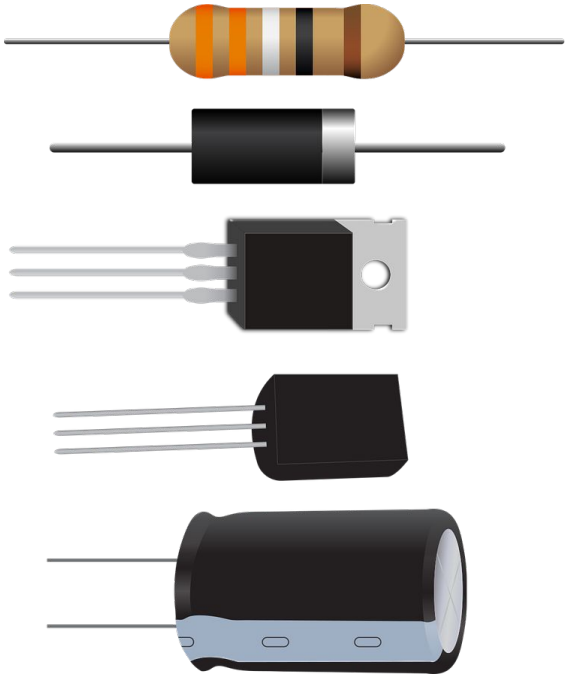
- 2025: “Jupiter”: Europas erster Exascale-Computer (3600 m^2)

0.5 Fussballfeld



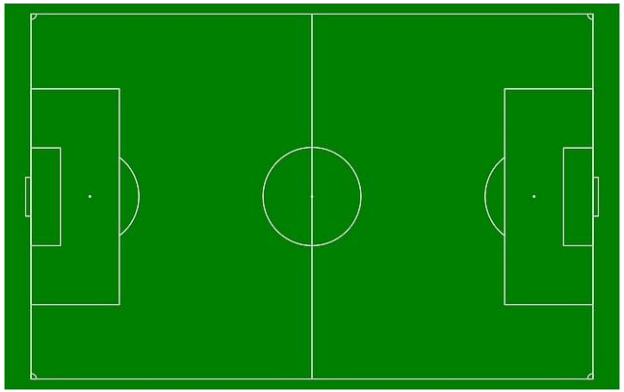
Grösse Transistoren

- 1965
  - 10-20 Mikrometer, ~600 μm^2



Grösse Transistoren

- 1965
  - 10-20 Mikrometer, ~600 μm^2
  - ~0.0000000000084 Fussballfelder



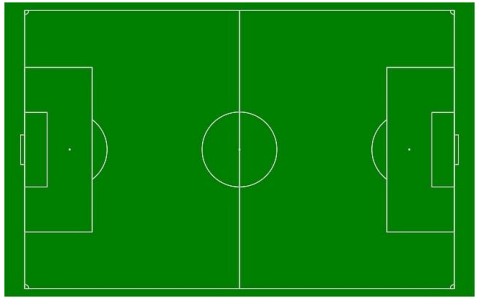
Grösse Transistoren

- 1965
  - 10-20 Mikrometer, ~600 μm^2
  - ~0.000000000084 Fussballfelder
- 2025
  - 2 Nanometer (TSMC)[1], ~0.004 μm^2

1 https://www.tomshardware.com/tech-industry/semiconductors/tsmc-begins-quietly-volume-production-of-2nm-class-chips-first-gaa-transistor-for-tsmc-claims-up-to-15-percent-improvement-at-iso-power (2026-02-07)

Grösse Transistoren

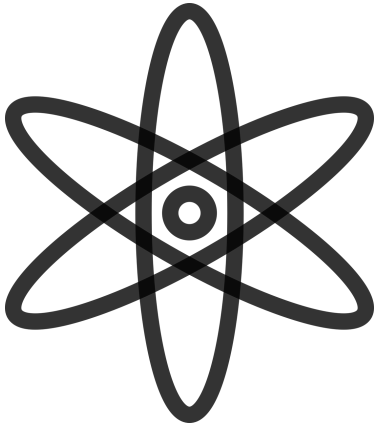
- 1965
  - 10-20 Mikrometer, ~600 μm^2
  - ~0.000000000084 Fussballfelder
- 2025
  - 2 Nanometer (TSMC)[1], ~0.004 μm^2
  - ~0.000000000000000056 Fussballfelder



1 https://www.tomshardware.com/tech-industry/semiconductors/tsmc-begins-quietly-volume-production-of-2nm-class-chips-first-gaa-transistor-for-tsmc-claims-up-to-15-percent-improvement-at-iso-power (2026-02-07)

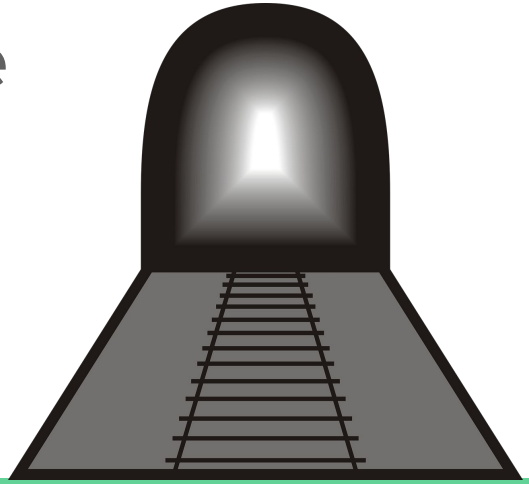
Probleme

- Wärmeabfuhr
- Wir sind auf atmoarer Ebene angelangt
  - Chip 2 Nanometer, Atom bis 0.3 Nanometer
    - falsch platzierte Atome



Probleme

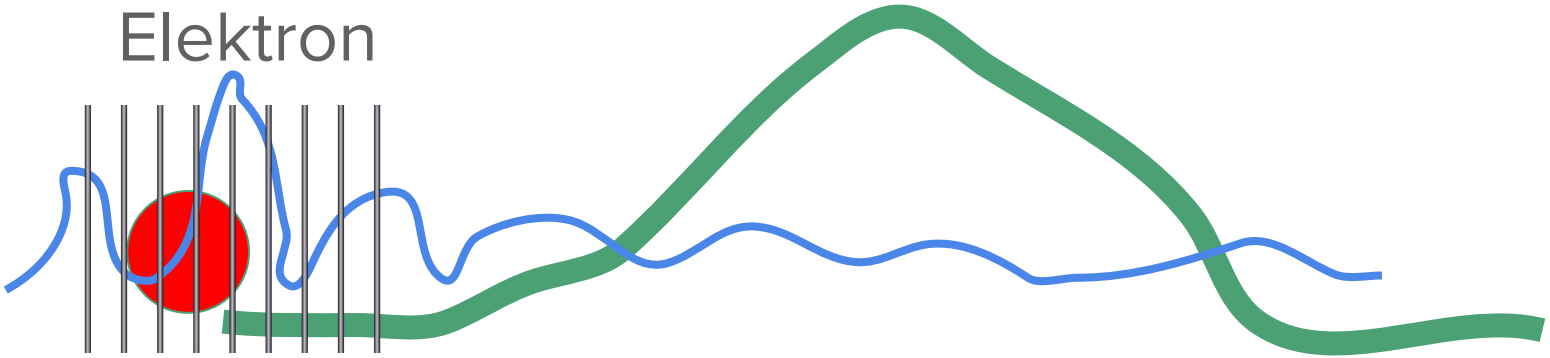
- Wärmeabfuhr
- Wir sind auf atmoarer Ebene angelangt
  - Chip 2 Nanometer, Atom bis 0.3 Nanometer
    - falsch platzierte Atome
- Tunneleffekt



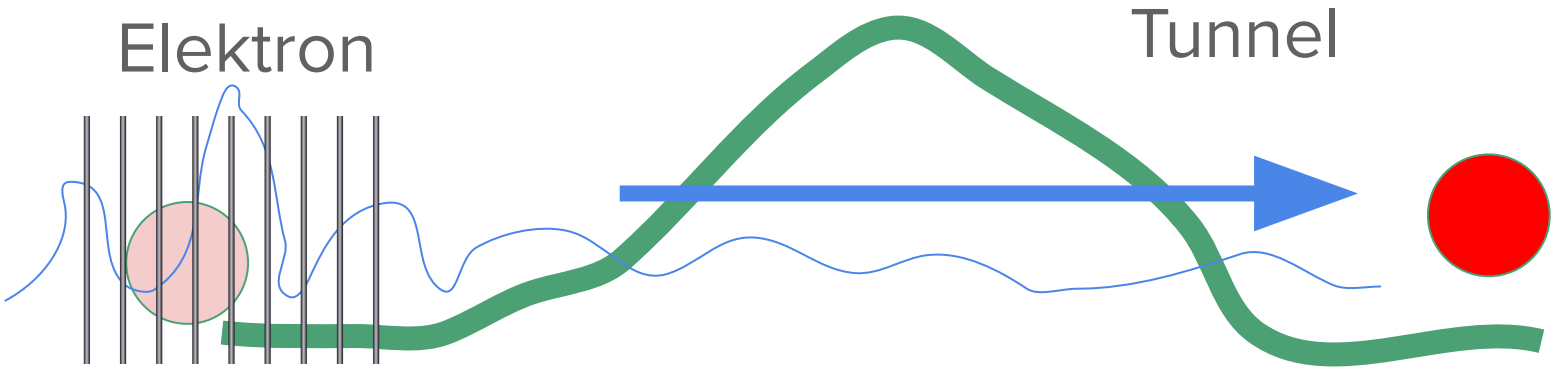
Quantenmagie

Tunneleffekt

Tunneleffekt



Tunneleffekt

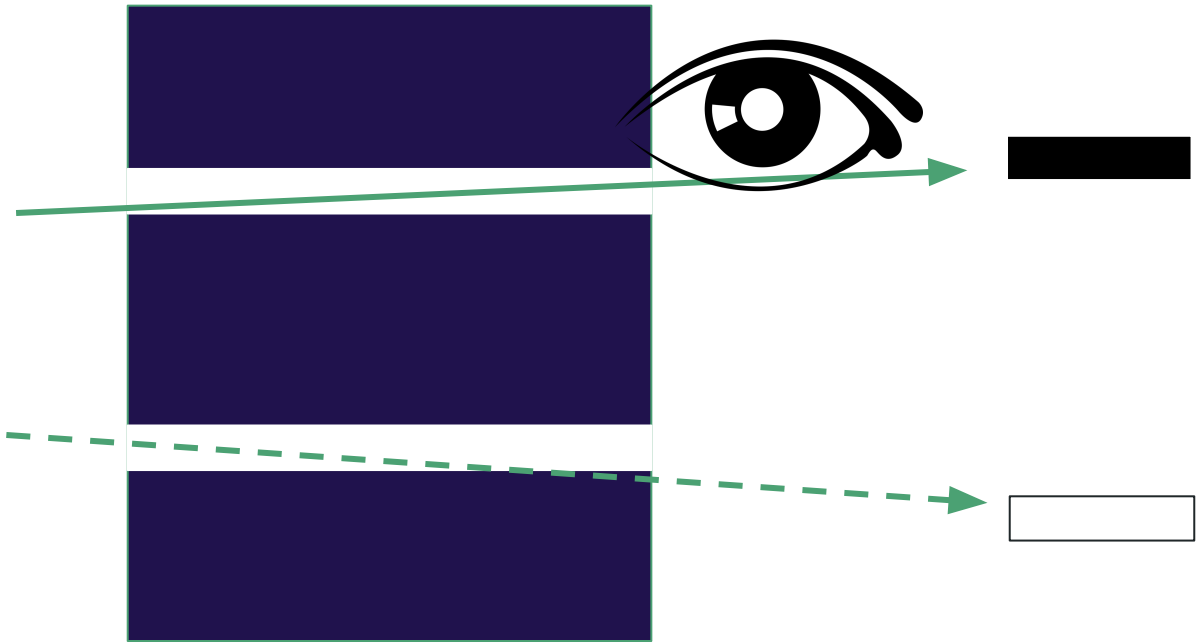


Isolierschicht (1-2 nm)

Quanteninterferenz: Doppelspaltexperiment

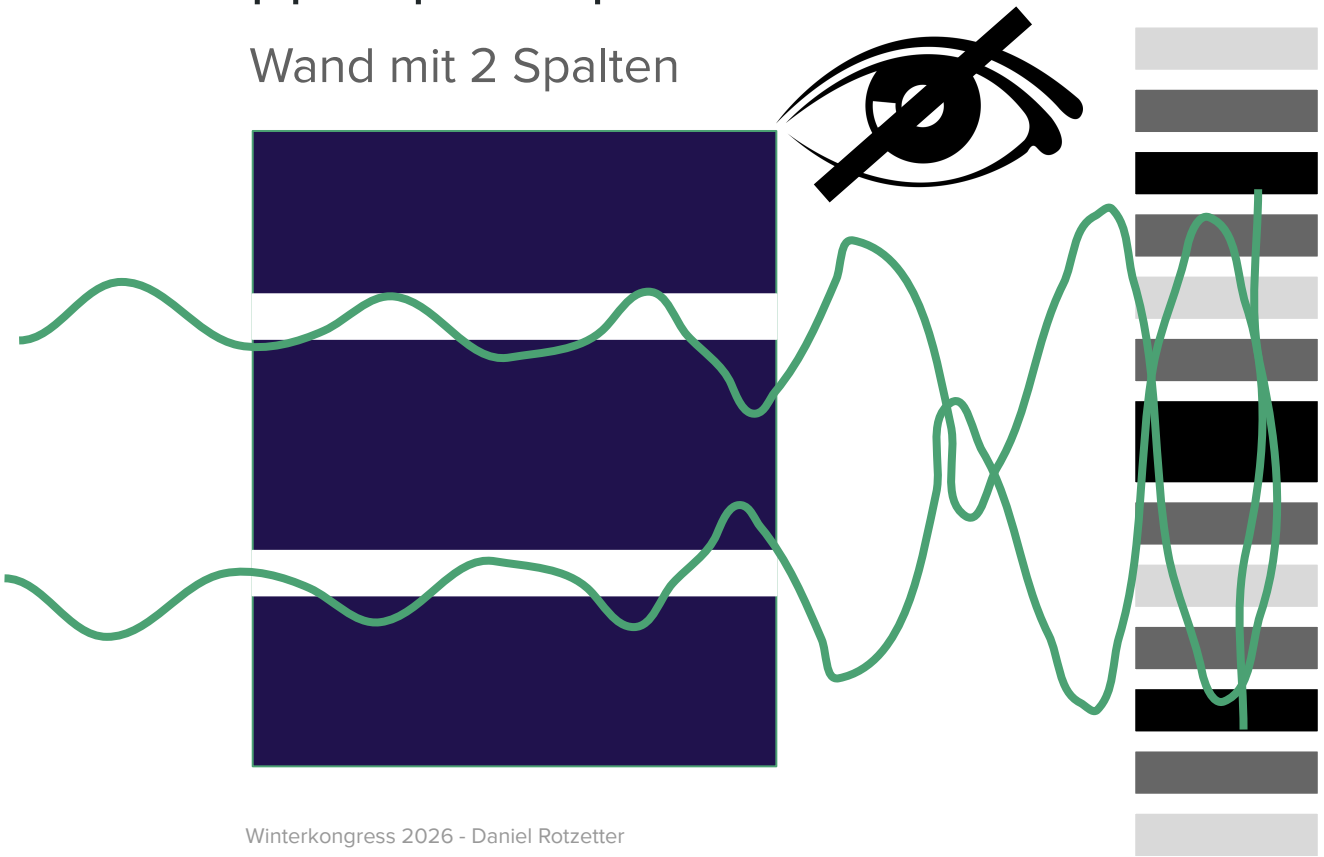
Photon

Wand mit 2 Spalten

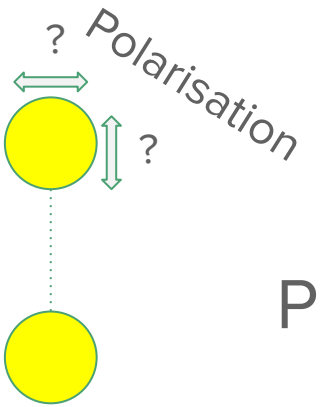


Quanteninterferenz: Doppelspaltexperiment

Photon



Verschränkung

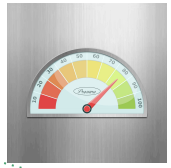


Photon

Verschränkung

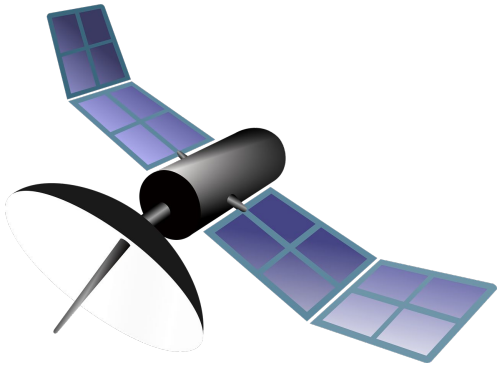
Verschränkung

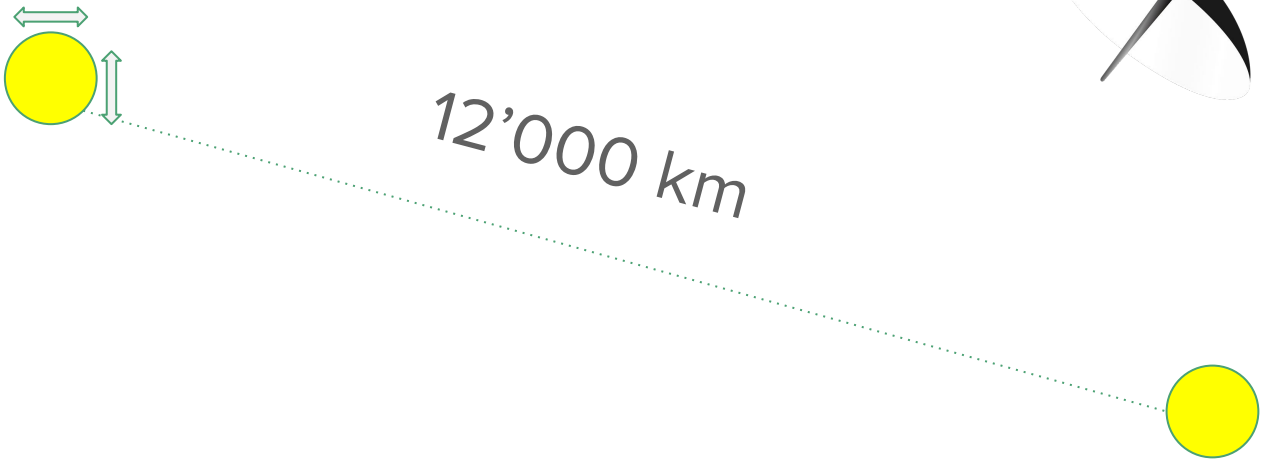
1. Messung



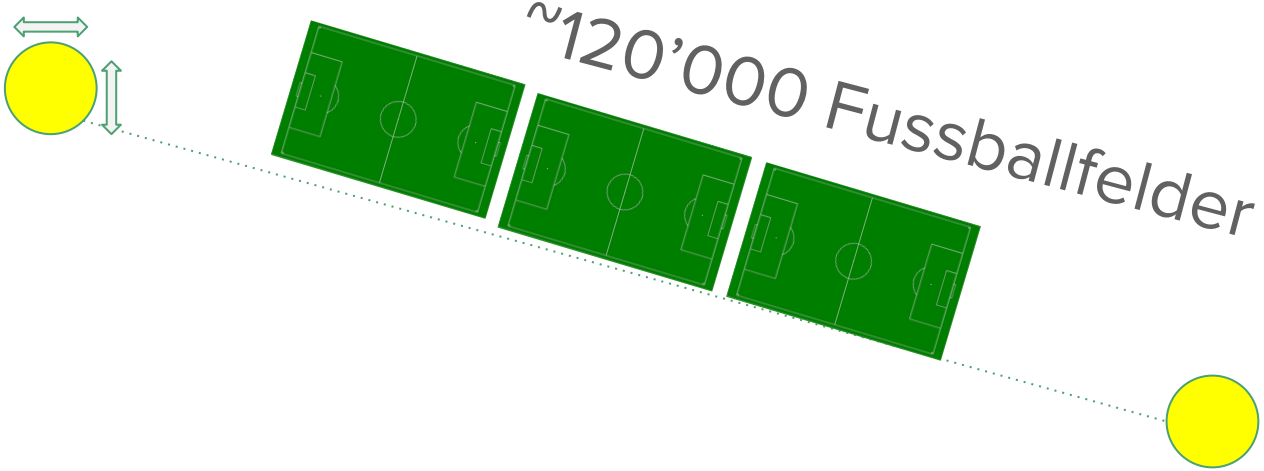
2. direkte Auswirkung

Verschränkung

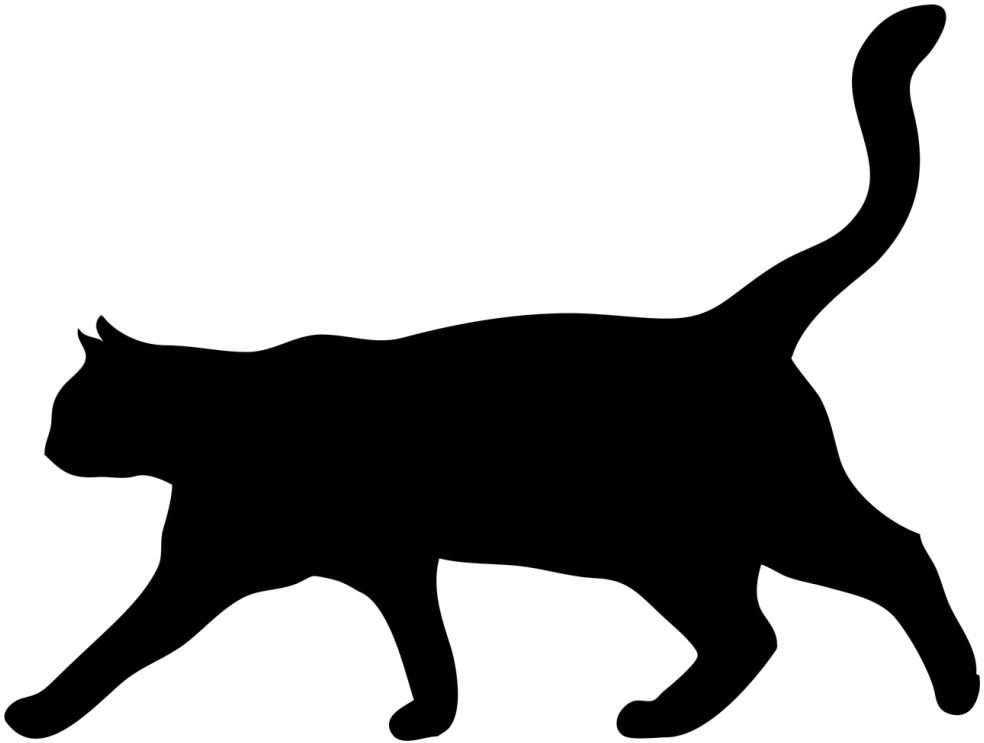




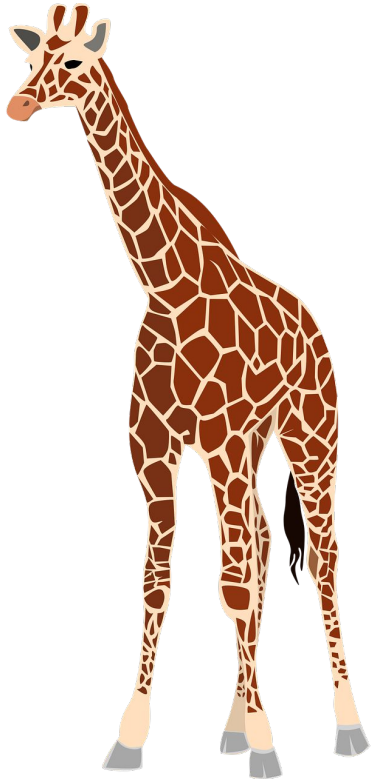
Verschränkung



Schrödinger’s Katze

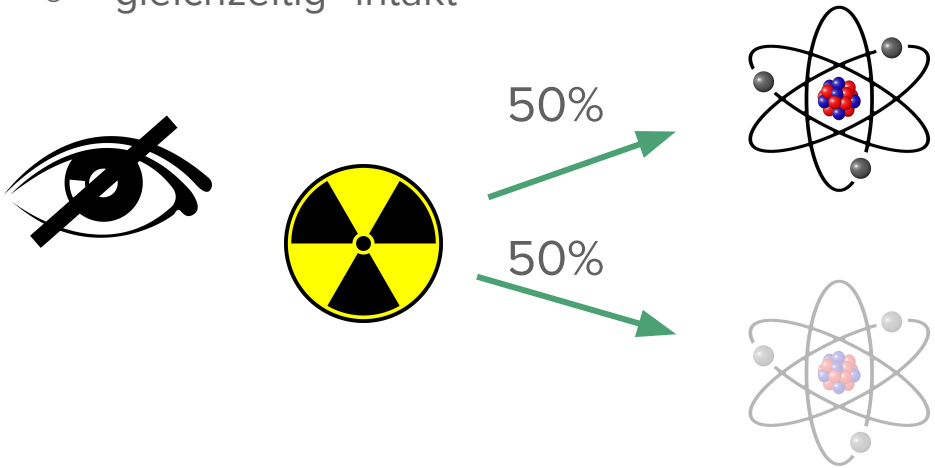


Schrödinger’s Giraffe



Schrödinger’s Giraffe

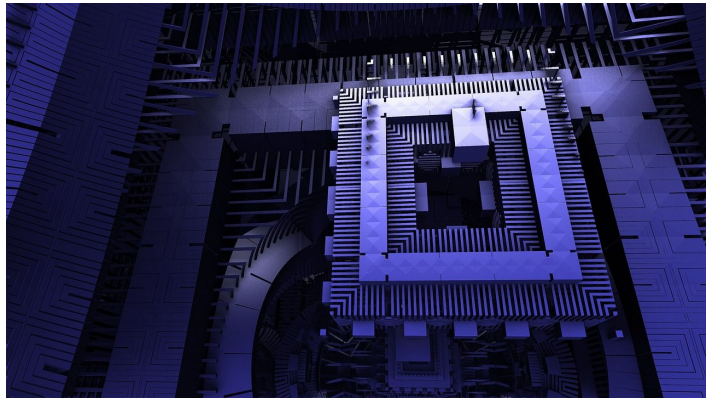
- Atom hat zwei Zustände gleichzeitig
  - sofern nicht nachgemessen (nachgeschaut)
- Radioaktives Atom
  - gleichzeitig “intakt”



Schrödinger’s Giraffe

Quantencomputer

- Superposition (Giraffe)
- Verschränkung (Lichtteilchen)
- Quanteninterferenz (Doppelspaltexperiment)



Quantumcomputer

Quantencomputer

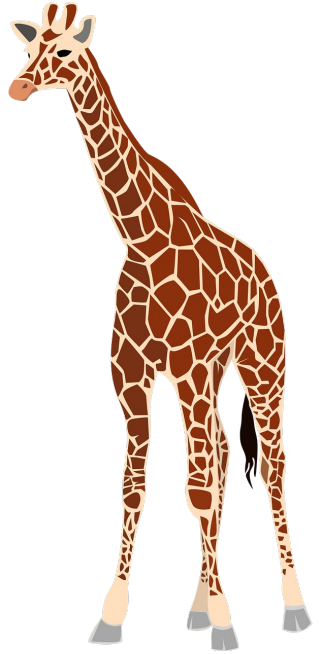
- Superposition (Giraffe)

- Superposition
  - Qubit: hat “Alle Werte zwischen 0 und 1”

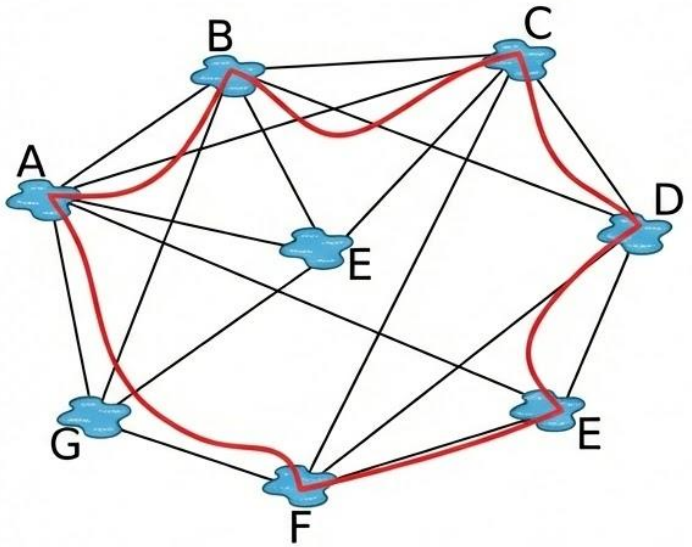
Super Influencer

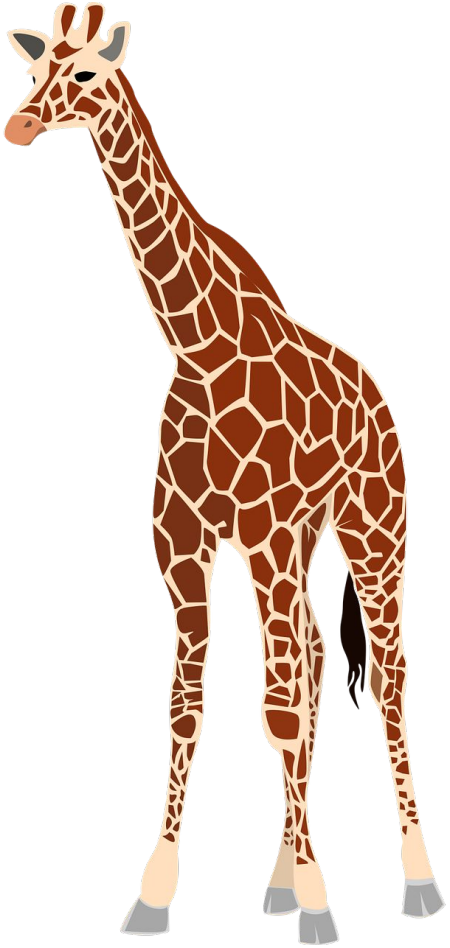
Travelling Sales Person Problem schnell lösen?

- Geschäftsperson muss alle (z.B. 50) Städte besuchen
- kürzester Weg gesucht



Travelling Giraffe’s Problem?





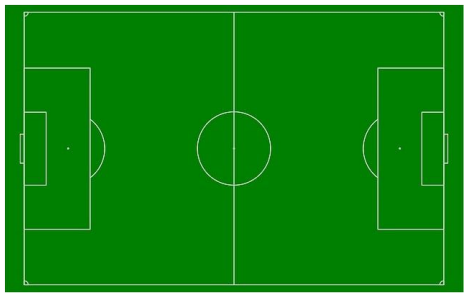
KI Generiert: Google Gemini
Ich hätte z.B. nicht 2x den “E” verwendet ;-)

RSA/ Asymmetrische Verschlüsselung knacken

- Verbreitet/ Standard im Web
  - TLS, PKI/ Zertifikate
    VPN, SSH, S-MIME
  - 2048 bit RSA Schlüssel
    klassisch knacken
    - Mindestens 20-30 Milliarden Jahre

RSA/ Asymmetrische Verschlüsselung knacken

- Verbreitet/ Standard im Web
  - TLS, PKI/ Zertifikate
    VPN, SSH, S-MIME
  - 2048 bit RSA Schlüssel
    klassisch knacken
    - Mindestens 20-30 Milliarden Jahre
      - ~ 11 Trillionen Fussballspiele à 90 min



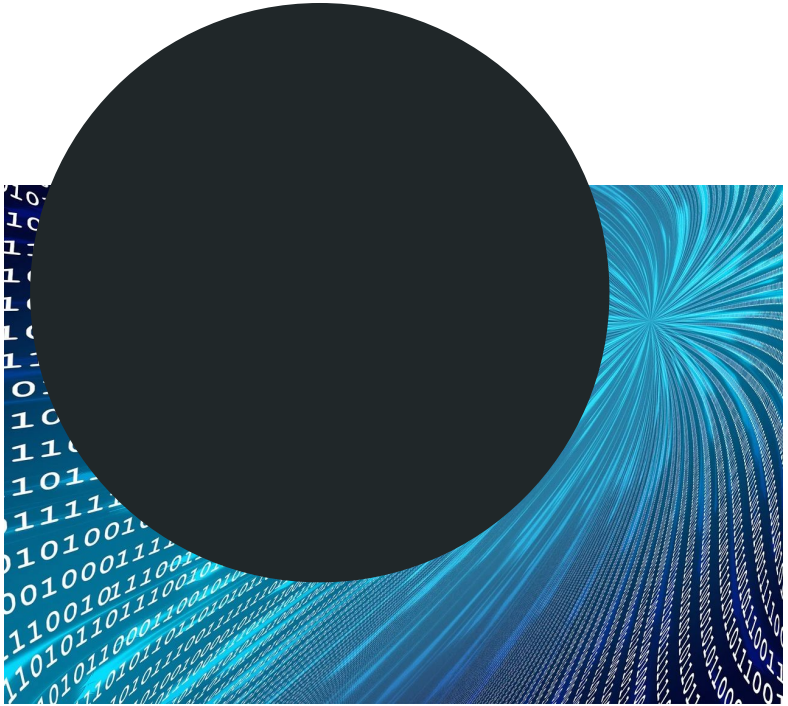
RSA/ Asymmetrische Verschlüsselung knacken

- Verbreitet/ Standard im Web
  - TLS, PKI/ Zertifikate
    VPN, SSH, S-MIME
  - 2048 bit RSA Schlüssel
    klassisch knacken
    - Mindestens 20-30 Milliarden Jahre
      - ~ 11 Trillionen Fussballspiele à 90 min
- Shor-Algorithmus mit Quantencomputer
  - Theoretisch “In Stunden” [1]
  - Harvest Now, Decrypt Later

[1] https://quantum-journal.org/papers/q-2021-04-15-433/

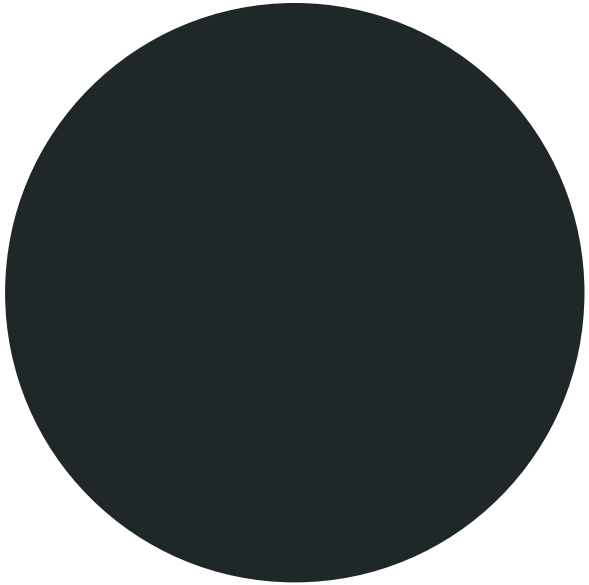
Post Quantum Verschlüsselung

- PQ Verschlüsselungs-Algorithmen
  - Gitterbasierte Kryptographie
  - multivariaten Polynomen
  - kryptologsiche Hashfunktionen
  - fehlerkorrigierenden Codes



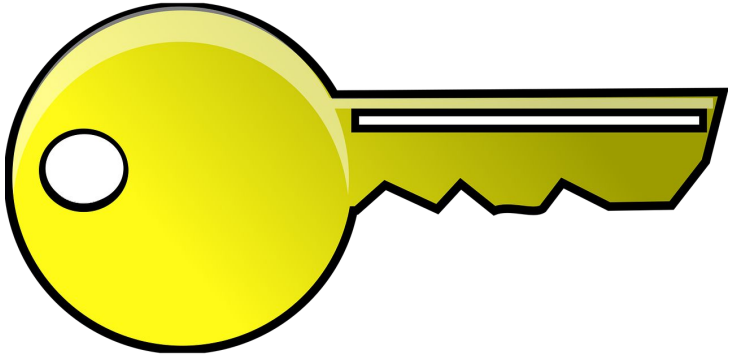
Post Quantum Verschlüsselung

- PQ Verschlüsselungs-Algorithmen
  - Gitterbasierte Kryptographie
  - multivariaten Polynomen
  - kryptologsiche Hashfunktionen
  - fehlerkorrigierenden Codes
- Krypto-Agilität



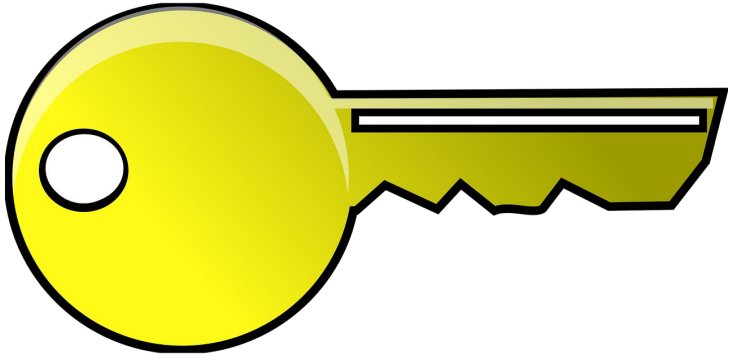
AES/ Symmetrische Verschlüsselung

- Anwendungsfälle
  - Dateien verschlüsseln, Backup
  - Messaging-Dienste
  - WLAN
  - Chipkarten…



AES/ Symmetrische Verschlüsselung

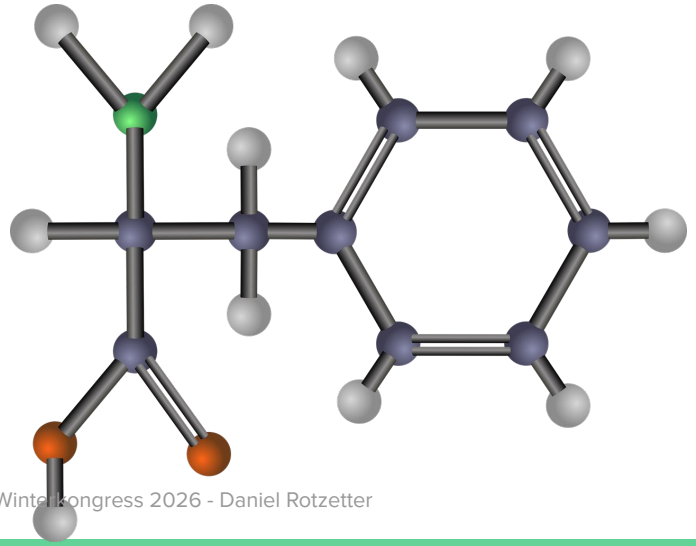
- Anwendungsfälle
  - Dateien verschlüsseln, Backup
  - Messaging-Dienste
  - WLAN
  - Chipkarten…
- Gegenmassnahmen
  - Längere Schlüssel nehmen/ verdoppeln
  - Dann noch relativ sicher[1]



[1] Solange Schlüssel nicht asymmetrisch verteilt werden
Disclaimer: keine generelle Nichthandlungsempfehlung

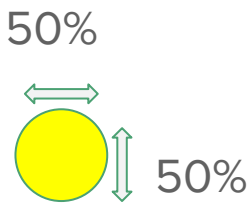
Simulationen & Optimierungen: viele Variablen

- Wetter- & Finanzsimulationen (kombinatorische Optimierungen)
- Chemie mit Einbezug von Quanteneffekten/ Teilchensimulationen
- Suchalgorithmen bei unstrukturierten Daten



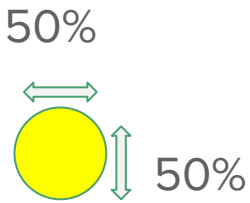
Abhörsichere[1] Leitung

- Superposition nutzen: bei Beobachtung (abhören) zerfällt der Zustand
  - [1]Abhörsicher => abgehörte Kommunikation wird bemerkt
- Quantum Key Distribution
  - Nur Schlüsselaustausch
  - Reichweite begrenzt (Fragilität, Hardwarefehler)

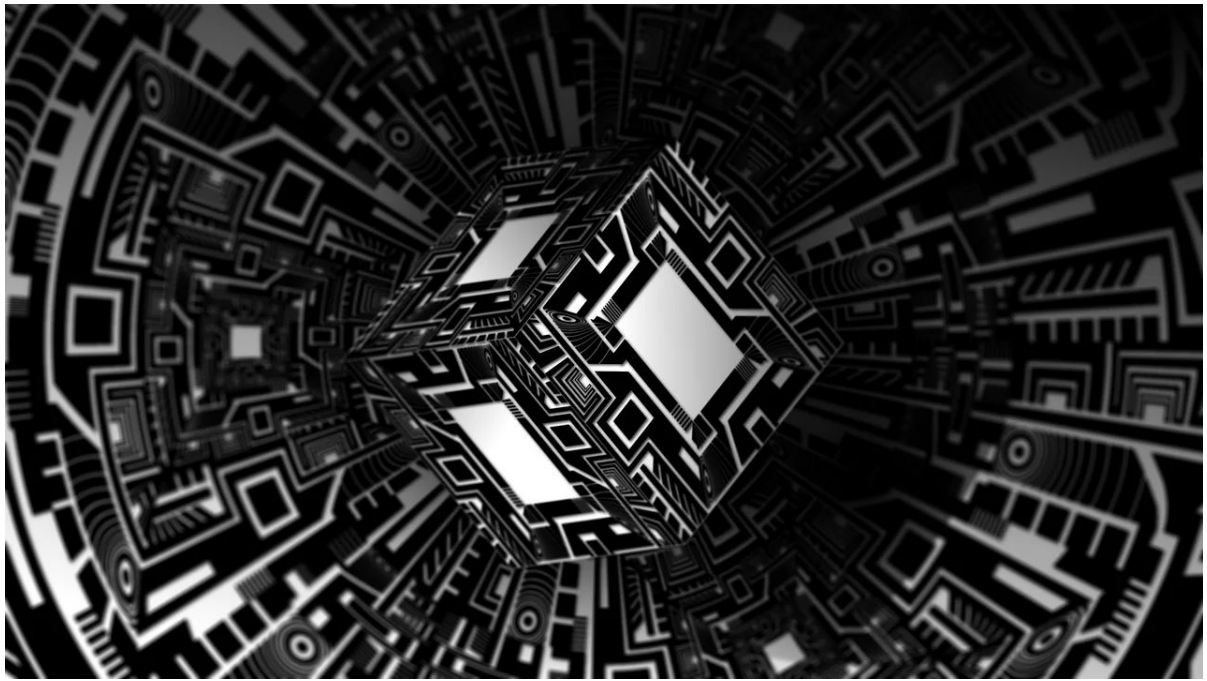


Echter Zufall

- Polarisation von Photonen
  - nacheinander reihen



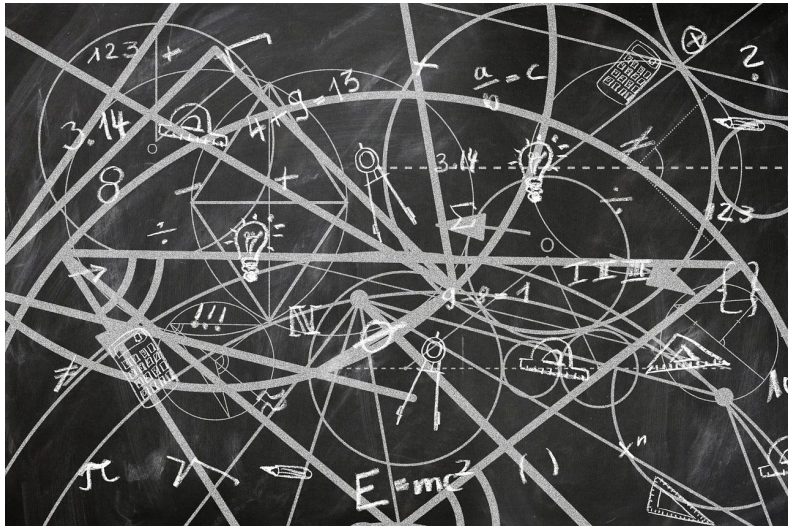
Noch unbekannte Anwendungsfälle



Kleine Teilchen, grosse Hürden

Anwendungsfälle

- Begrenzte Anwendungsfälle
- Quantencomputer rechnen
  - Addieren Wahrscheinlichkeiten, simulieren, optimieren…
  - und kommen zu einem *möglichen* Resultat
    - Überprüfung und/ oder Verknüpfung
    - mit klassischen Computern



Fragilität

- Quantenzustände verfallen sehr schnell

Fragilität

- Quantenzustände verfallen sehr, sehr, sehr, sehr schnell

Fragilität

- Quantenzustände verfallen sehr, sehr, sehr, sehr schnell
  - Umwelteinflüsse, Vibrationen
  - Dekohärenz bei Messung (Superposition verfällt)
  - => Fehlerkorrektur

Supraleiter

- Supraleiter
  - Nahe absoluter Nullpunkt (- 273°C)
- Hochtemperatur-Supraleiter

Supraleiter

- Supraleiter
  - Nahe absoluter Nullpunkt (- 273°C)
- Hochtemperatur-Supraleiter
  - Yttrium-Barium-Kupferoxid
  - Bismut-Strontium-Calcium-Kupfer-Oxid
  - Quecksilber-Barium-Calcium-Kupfer-Oxid

Supraleiter

- Supraleiter
  - Nahe absoluter Nullpunkt (- 273°C)
- Hochtemperatur-Supraleiter
  - Yttrium-Barium-Kupferoxid (-196°C)
  - Bismut-Strontium-Calcium-Kupfer-Oxid (-165°)
  - Quecksilber-Barium-Calcium-Kupfer-Oxid (-139°)

KI Generiert (Google Gemini)

Herausforderungen

- Dekohärenz: Instabilität
- Schwierige Skalierbarkeit: Fehlerkorrektur
- Kühlung und Infrastruktur
- Eingeschränkte Anwendbarkeit/ Anwendungsfälle: je nach Algorithmus

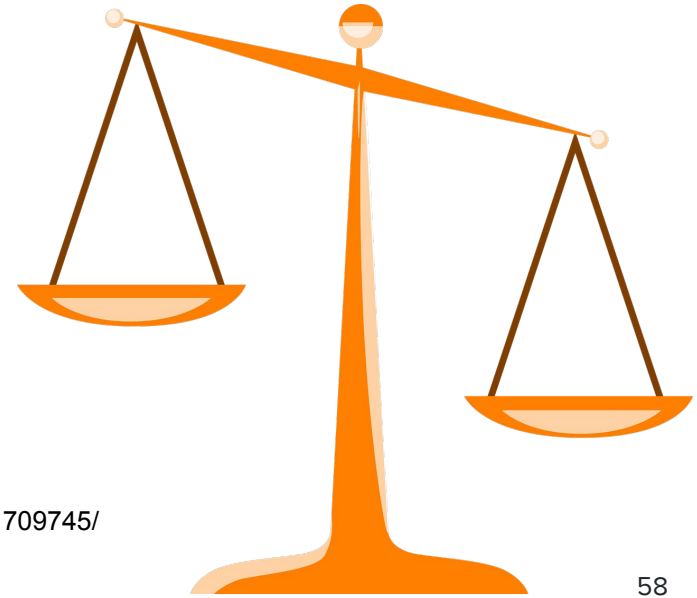
Stand Heute

- 2025: 6100 Qubits[1]

[1] https://t3n.de/news/quantencomputer-mit-6100-qubits-warum-13-sekunden-ein-riesenerfolg-sind-1709745/

Stand Heute

- 2025: 6100 Qubits[1]
- Schwierige Vergleiche: betrachtet müssen zudem
  - Architekturform
  - Stabilität (Kohärenzzeit)
  - Konnektivität zwischen Qubits
  - Verwendung für Fehlerkorrektur



[1] https://t3n.de/news/quantencomputer-mit-6100-qubits-warum-13-sekunden-ein-riesenerfolg-sind-1709745/

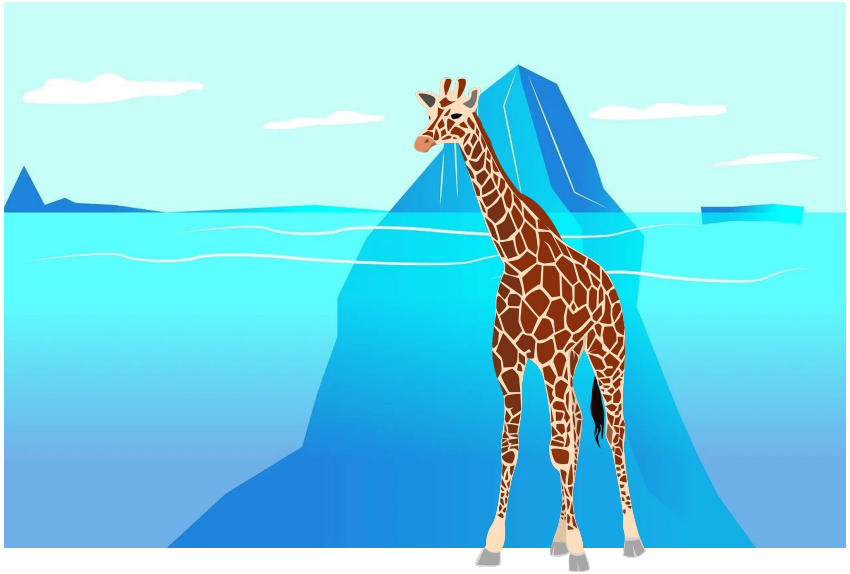
Zusammenfassung

Zusammenfassung

- Faszinierende Quantenwelt
- Gespannt bleiben, was alles noch kommt

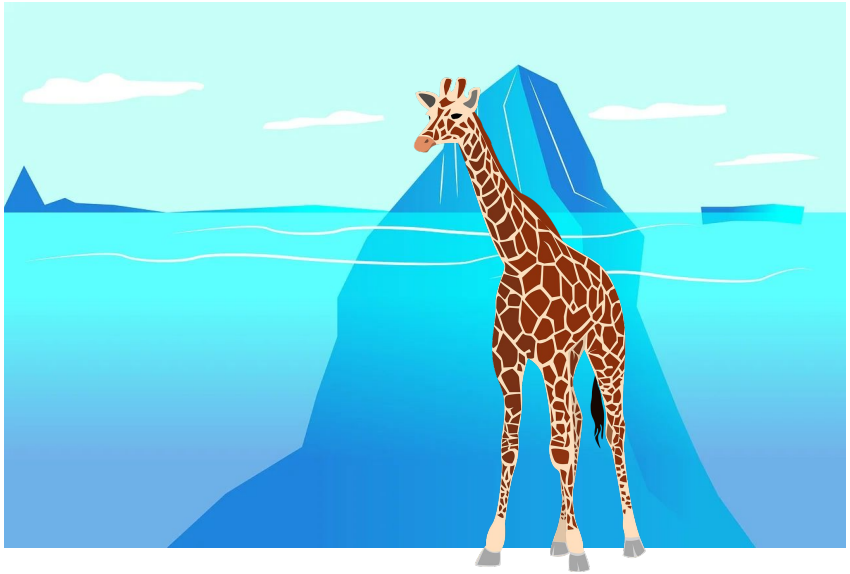
Zusammenfassung

- Faszinierende Quantenwelt
- Gespannt bleiben, was alles noch kommt
    - Spitze der Giraffe



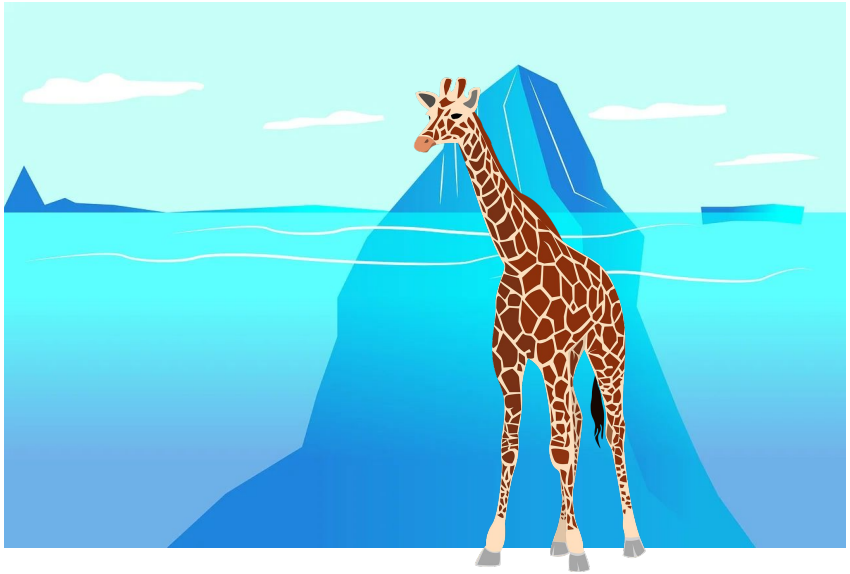
Zusammenfassung

- Faszinierende Quantenwelt
- Gespannt bleiben, was alles noch kommt
  - Spitze der Giraffe
- Don’t panic



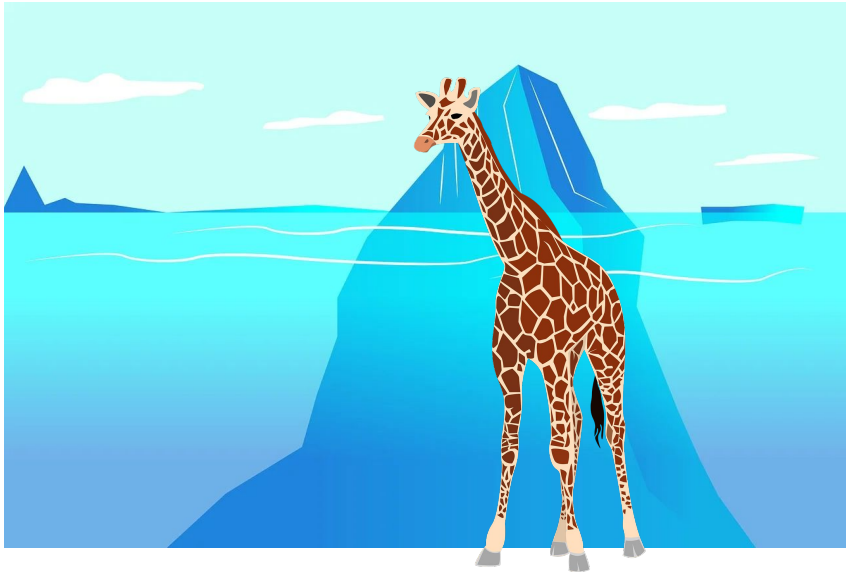
Zusammenfassung

- Faszinierende Quantenwelt
- Gespannt bleiben, was alles noch kommt
  - Spitze der Giraffe
- Don’t panic
  - but panic a little



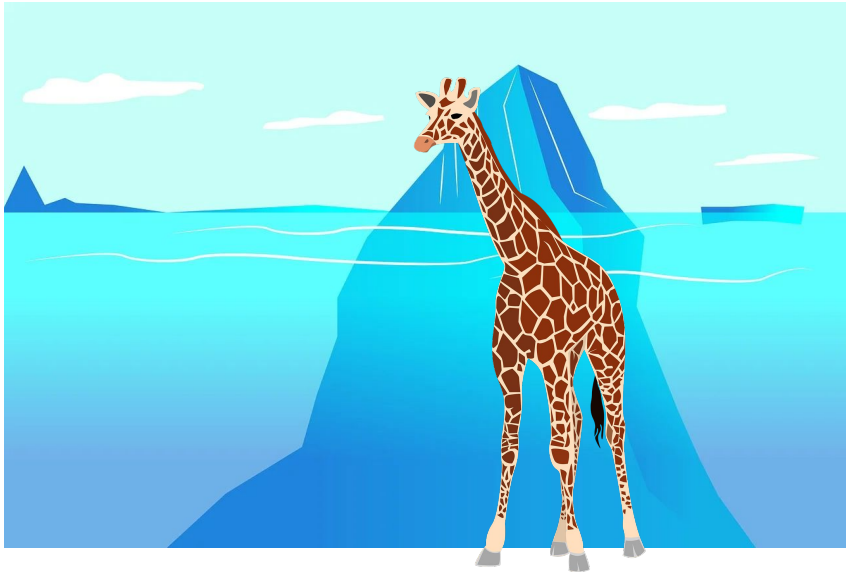
Zusammenfassung

- Faszinierende Quantenwelt
- Gespannt bleiben, was alles noch kommt
  - Spitze der Giraffe
- Don’t panic
  - but panic a little
- Klassische Computer bleiben



Zusammenfassung

- Faszinierende Quantenwelt
- Gespannt bleiben, was alles noch kommt
  - Spitze der Giraffe
- Don’t panic
  - but panic a little
- Klassische Computer bleiben
- Verschont die Giraffen



“Es ist nichts beständig(er) als die Unbeständigkeit.”

Immanuel Quant

Quellen: Inhalt

- https://www.itp.uni-hannover.de/fileadmin/itp/qinfo/Team_Tobias_Osborne/Bachelors_Theses/Lara_Lelakowski_Bachelors_Thesis.pdf (2026-02-01)
- https://people.phys.ethz.ch/~ihn/hlnano02(not%20in%20use%20any%20more)/oldSS05STUFF/Skript1.pdf (2026-02-01)
- https://de.wikipedia.org/wiki/Mooresches_Gesetz (2026-02-01)
- https://qarlab.de/speichereffiziente-quanten-optimierung-fuer-das-traveling-salesman-problem-ueber-binaere-kodierung-von-ganzzahligen-loesungen/ (2026-02-01)
- https://www.forschungsfabrik-mikroelektronik.de/de/presse--und-medien/fmd-impuls/4--fmd-impuls-qnc/Quanten.html (2026-02-01)
- https://www.studysmarter.de/studium/physik-studium/festkoerperphysik/hochtemperatur-supraleiter/ (2026-02-01)
- https://www.phonearena.com/news/tsmc-3nm-chips-will-contain-nearly-300-million-transistors-per-square-mm_id123963 (2026-02-07)
- https://www.chemie.de/lexikon/Caesium.html (2026-02-06)
- https://www.spektrum.de/magazin/die-zukunft-des-transistors/821019 (2026-02-06)
- https://www.it-daily.net/spezial/quantencomputer/quantencomputer-konzept-und-anwendungen (2026-02-06)
- https://www.spiegel.de/wissenschaft/technik/verschraenkte-photonen-chinesen-mit-rekord-bei-quanten-experiment-a-1152329.html (2026-02-06)
- https://www.fujitsu.com/de/about/resources/news/press-releases/2025/20250806.html (2026-02-06)
- https://www.ingenieur.de/technik/fachbereiche/ittk/quantencomputer-meilenstein-caltech-erreicht-6100-qubits/ (2026-02-06)
- https://www.isi.fraunhofer.de/de/presse/2025/presseinfo-09-quantenkommunikation_chancen_herausforderungen_anwendungsbereiche.html (2026-02-06)
- https://hub.hslu.ch/informatik/sicherer-kommunizieren-dank-quantenkryptographie/ (2026-02-06)
- https://rettenmund.com/en/2025/11/the-quantum-threat-how-post-quantum-cryptography-protects-the-web/ (2026-02-07)
- https://www.encryptionconsulting.com/de/Neue-Google-Studie-zeigt--dass-RSA-2048-fr%C3%BCher-als-erwartet-geknackt-werden-k%C3%B6nnte/ (2026-02-07)
- https://nordvpn.com/de/blog/post-quanten-kryptographie/ (2026-02-07)
- https://cvj.ch/fokus/hintergrund/quantencomputer-vs-bitcoin-ernste-bedrohung-oder-uebertriebene-panikmache/ (2026-02-07)
- https://www.tomshardware.com/tech-industry/semiconductors/tsmc-begins-quietly-volume-production-of-2nm-class-chips-first-gaa-transistor-for-tsmc-claims-up-to-15-percent-improvement-at-iso-power (2026-02-07)
- https://learnattack.de/schuelerlexikon/physik/schroedingers-katze (2026-02-07)
- https://www.weltderphysik.de/gebiet/teilchen/nachrichten/2017/das-ganze-ist-viel-mehr-als-die-summe-der-teile/ (2026-02-07)
- https://www.it-daily.net/spezial/quantencomputer/quantencomputer-konzept-und-anwendungen (2026-02-07)
- https://www.samaterials.de/content/list-of-superconductors-and-how-they-work.html (2026-02-08)
- https://www.spektrum.de/lexikon/physik/hochtemperatur-supraleiter/6805 (2026-02-08)
- https://www.quantencomputer-info.de/quantencomputer/quantencomputer-einfach-erklaert/ (2026-02-09)
- https://www.deutschlandfunk.de/supercomputer-offiziell-eingeweiht-was-kann-europas-schnellster-rechner-jupiter-100.html (2026-02-13)
- https://www.swb.de/ueber-swb/swb-magazin/swb-insider/erster-computer-der-welt (2026-02-13)
- https://news.hslu.ch/quantenkryptografie/ (2026-02-14)
- https://t2informatik.de/blog/5-missverstaendnisse-bei-quantencomputern/ (2026-02-14)
- https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2021.760783/full (2026-02-14)
- https://thequantuminsider.com/2026/02/13/new-architecture-could-cut-quantum-hardware-needed-to-break-rsa-2048-by-tenfold-study-finds/ (2026-02-14)

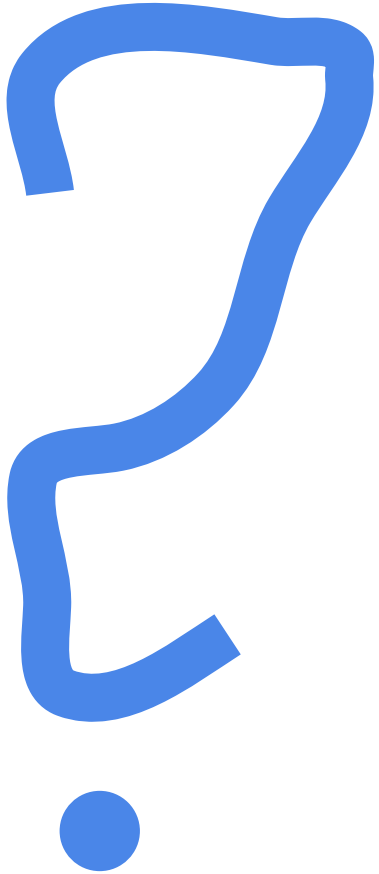
Quellen: Bilder

- Image by OpenClipart-Vectors from Pixabay Fussballfeld, ab Slide “Grösse Transistoren”)
- Image by Clker-Free-Vector-Images from Pixabay Atom, Slide “Probleme”)
- Image by Kate from Pixabay Katze, Slide “Schrödingers Katze”
- Image by Clker-Free-Vector-Images from Pixabay Giraffe, ab Slide “Schrödingers Giraffe”
- Image by OpenClipart-Vectors from PixabayHammer, Slide “Schrödingers Giraffe”
- Image by OpenClipart-Vectors from Pixabay Gift, Slide “Schrödingers Giraffe”
- Image by Andrea Baratella from Pixabay Messgerät, Slide “Schrödingers Giraffe”
- Image by Clker-Free-Vector-Images from Pixabay Atom, Slide “Schrödingers Giraffe”
- Image by Tomislav Jakupec from Pixabay Roulette, Slide “Echter Zufall”
- Image by 13smok from Pixabay Tunnel, Slide “Probleme”
- Image by Couleur from Pixabay Strommasten, Slide “Supraleiter”
- Image by Felix Mittermeier from Pixabay Wolken, Slide “Fragilität”
- Photon: habe ich selber gezeichnet, und ich bin sehr stolz darauf!
- Image by OpenIcons from Pixabay “Zerbrechlich” Symbol, Slide “Fragilität”
- Image by mohamed alava from Pixabay Zukunft, Slide “Noch unbekannte Anwendungsfälle”
- Image by Cedric Franchetti from Pixabay Zukunft, Slide “Noch unbekannte Anwendungsfälle”
- Image by Lumina Obscura from Pixabay Universum, Slide “Brute Foce”
- Image by Clker-Free-Vector-Images from Pixabay Offene Schatztruhe, Slide “Brute Foce”
- Image by skylarvision from Pixabay Browser, Slide “Asymmetrische Verschlüsselung”
- Image by Clker-Free-Vector-Images from Pixabay Schlüssel, Slide “Symmetrische Verschlüsselung”
- mage by Gerd Altmann from Pixabay Symbolbild “Algorithmen”, Slide “Post Quantum Kryptografie”
- Image by Clker-Free-Vector-Images from Pixabay Satellit, Slide “Verschränkung”
- Image by Gerd Altmann from Pixabay Atom, Slide “Atom”, Schrödingers Giraffe
- Image by OpenClipart-Vectors from Pixabay Molekül, Slide “Simulationen”
- Image by Gerd Altmann from Pixabay Berechnungen Wandtafel, Slide “Anwendungsfälle”
- Image by Mote Oo Education from Pixabay Eisberg, Slide “Zusammenfassung”
- Image by Sinisa Maric from Pixabay Transistor, Slide “Grösse Transistoren”
- Image by Perlinator from Pixabay Giraffe, Slide “Tunneleffekt”
- Image by Clker-Free-Vector-Images from Pixabay Auge, Slide “Doppelspaltexperiment”
- Image by Clker-Free-Vector-Images from Pixabay Waage, Slide “Stand heute”
- Image by Mohamed Hassan from Pixabay Climber, Slide “Herausforderungen”
- Smiley: Google Docs Emoji

Danke

- Max Planck (Begründung der Quantenphysik)
- Werner Heisenberg (Formulierung der Unschärferelation)
- Erwin Schrödinger (Entwicklung der Wellenmechanik)
- Erwin Schrödinger’s Katze
- Erwin Schrödinger’s Giraffe
- Publikum (Für Aufmerksamkeit)

Fragen



Daniel Rotzetter

https://www.linkedin.com/in/danirotzetter/

https://forms.gle/T8TPHWvQKRyUUiGY9