



Aufbruch ins Quanten-Zeitalter

Heute starten,
morgen profitieren
– mit Bechtle in die
Quanten-Zukunft

Quantentechnologien
Bechtle IT-Systemhaus Bonn/Köln

31.10.2024



Über uns

bechtle

1

2

3

4

Team Quantum Technologies Bechtle IT-Systemhaus Bonn/Köln

quantum.bonn@bechtle.com



**Fabian
Brings**

Quantum
Consulting



**Jonas
van Bebber**

Quantum
Application
Development



**Sebastian
Dittrich**

Program
Manager



**Experten &
Techniker**

Data Center



**Elena
Hofmann-Sauer**

Sales

Der Quanten-IT den Weg bereiten.

**Integration in
IT-Lösungen**

**QC Hub
& Cloud**

QC On-Premise

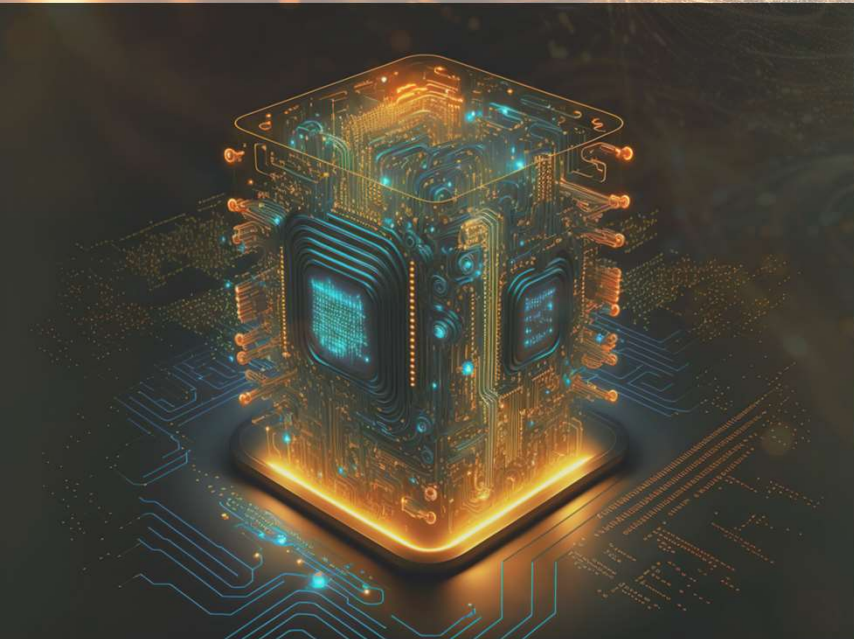
Beratung

Networking

**Quantum
Community**

Portfolio Quantentechnologien

- Bereitstellung von Quantenhardware (u. a. IQM Spark™, XeedQ XQ1)
- Quantum Technology Consulting
- Quantum Technology Services
 - Zugang zu QC-Systemen (u. a. IBM-Q, AWS Braket™, IQM Resonance™)
 - Aufwertung bestehender Lösungen
 - Konzipierung von Teststrecken
 - Use Case-Design, Integration, Begleitung
 - Benchmarking
- Marktstudien und -analysen
- Beteiligung an Ausschreibungen
- Quantum Education: Talks, Webinare, Workshops
- Events, White Paper, Social Media Influencing



Quanten- technologien für Ihre IT

6 Schritte für Ihre Quantum-Readiness.

Gestalten Sie mit uns die zukünftige Quanten-IT!

Das Team Quantum Technologies im Bechtle IT-Systemhaus Bonn/Köln bietet Ihnen umfassende Services in einem zukunftsweisenden Bereich, der die IT-Landschaft stark verändern wird.

Wissensvorsprung

Wir bringen Sie auf den aktuellen Stand und verschaffen Ihnen Überblick & Navigation im Bereich der Quantentechnologien.

Quantenkompetenz

Profitieren Sie von unserer Expertise und Kooperationen mit Hardware- & Softwareanbietern, Forschungsinstitutionen & Unis.

Einstieg in die Praxis

Sammeln Sie Erfahrung mit Quantensystemen. Wir bieten Ihnen Quantenhardware, Computing-Services und Beratung.

Use Case Design

Alles aus einer Hand. Konzeption, Design, Umsetzung, Tests, Integration – für optimierte und neuartige Anwendungen.

Performance steigern

Beschreiten Sie mit uns neue Wege für das zukünftige HPC – IT, die CPUs, GPUs und QPUs optimal kombiniert und auslastet.

Quantensicher & Kryptoagil

Wir helfen Ihnen bei der Anpassung von Sicherheitsstrategien & der Migration hin zur Quantum-Safe IT und zur Kryptoagilität.

Warum Quanten-Technologie?

bechtle

1

2

3

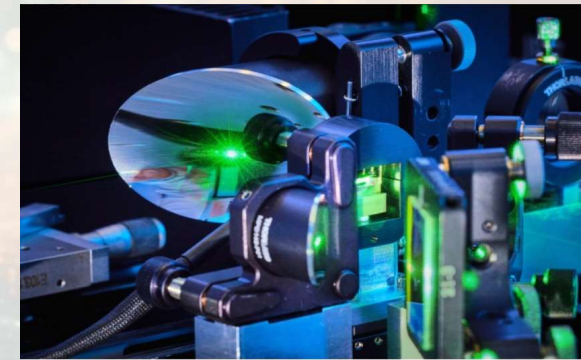
4

Quantentechnologien der 1. Generation

- Halbleiter
- OLED
- HEMT
- LASER
- Glasfaser
- NMR
- MRT
- Nuklearmedizin
- GPS
- Sattelitentechnik
-



1

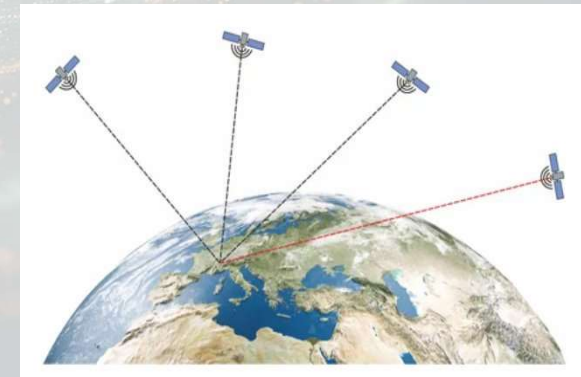


© Fraunhofer ILT, Aachen.

2



3

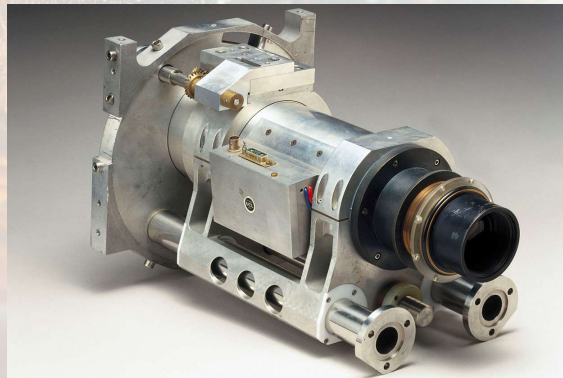


4

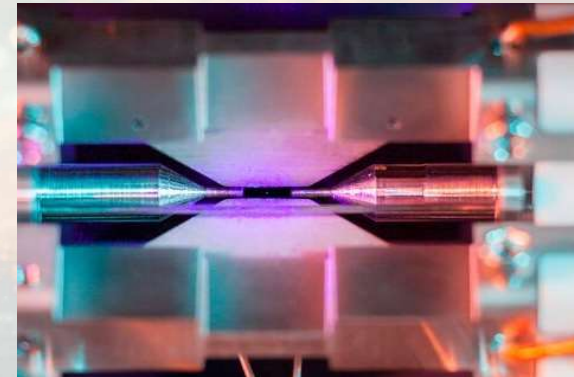
Bilderquellen:
1: Stiftung Warentest / Ralph Kaiser
2: Fraunhofer ILT, Aachen
3: Radiologie Ettlingen
4: Conrad Electronic SE

Quantentechnologien der 2. Generation

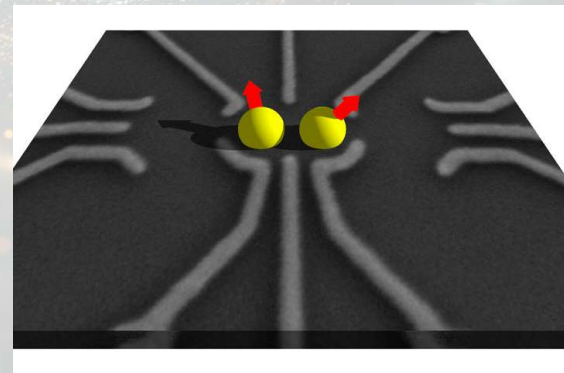
- Ionenfallen
- Einzel-Photon-Anwendungen
- Quantenpunkte



2



1



3

Bilderquellen:
1: David Nadlinger University of Oxford
2: Science Museum London / Science and Society Picture Library
3: D. E. F. Biesinger et al. Physical Review Letters 115 (2015)

Standort Baden-Württemberg

The logo for Quantum BW is displayed within a yellow and white rectangular frame. The word "Quantum" is in a large, bold, black sans-serif font, and "BW" is in a smaller, bold, black sans-serif font to its upper right.

Quantum^{BW}

- Top Standort
- Gute Verbindungen
- Lokale Forschung und Entwicklung

Der Prozess

bechtle

1

2

3

4

Vom Hype zur Roadmap



Quantenerfolg
statt
Quantenwinter



Quantensichere IT (Heute – 10 Jahre)

- Funktioniert ohne Quantencomputer
- Bietet neuartige Lösungen
- Ist zukunftssicher



Anwendungen: Langzeit Datenspeicherung, Medizinische Daten, Sicherer Datenaustausch

Verfügbare Hardware, Software, Tools

Quantum Safe Tools and Methods

- IBM Quantum Safe (Crypto Management)
- Patero (Secure Data)
- PQShield (Algorithms & Patterns)
- Quant-X Security (Consulting)

Quantum Safe Hard- and Software

- Cloudflare (Hybrid QS Handshake)
- Firefox (Hybrid QS Handshake)
- Secunet SINA (Boxes & Phones)
- IBM Z (Mainframe)
- Tuta / Tuta Mail (Secure Email)



Bilderquellen:
<https://newsroom.ibm.com/>,
<https://www.secunet.com/loesungen/sina-communicator-h>

Quantentechnologien, Bechtle IT-Systemhaus Bonn/Köln

KI + Quanten (2 Jahre – 10 Jahre)

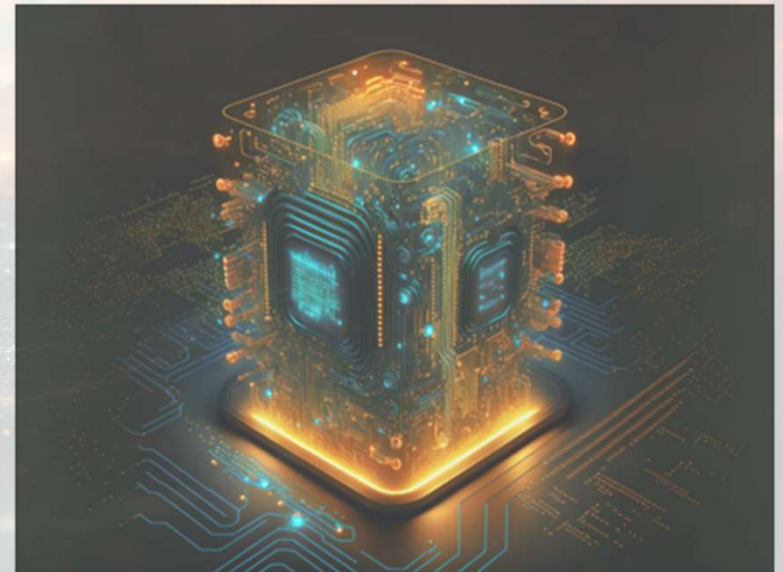


Beschleunigt Verarbeitung

- Verringert Hardware Anforderungen
- Erweitert Anwendungsmöglichkeiten

Generiert Code

- Verringert Einstiegsschwierigkeit
- Beschleunigt Entwicklung



Anwendungen: Verkehrsführung, Autonome Fahrzeuge, Logistik, Energienetzwerk Planung

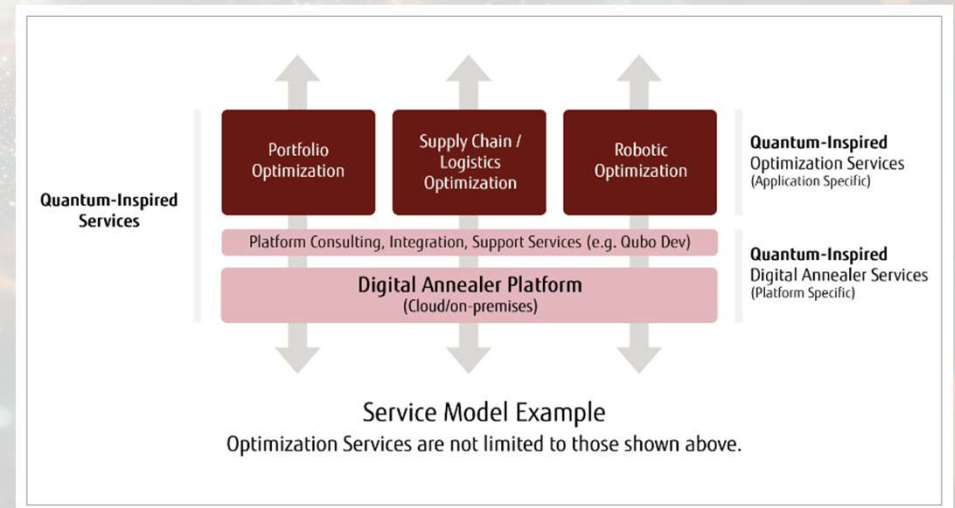
Quantensimulationen (Heute – 3 Jahre)

NVIDIA DGX H100

Der Goldstandard für KI-Infrastruktur.



**Anwendungen: Kompakte, kosteneffiziente,
quantum-ready Rechenzentren**

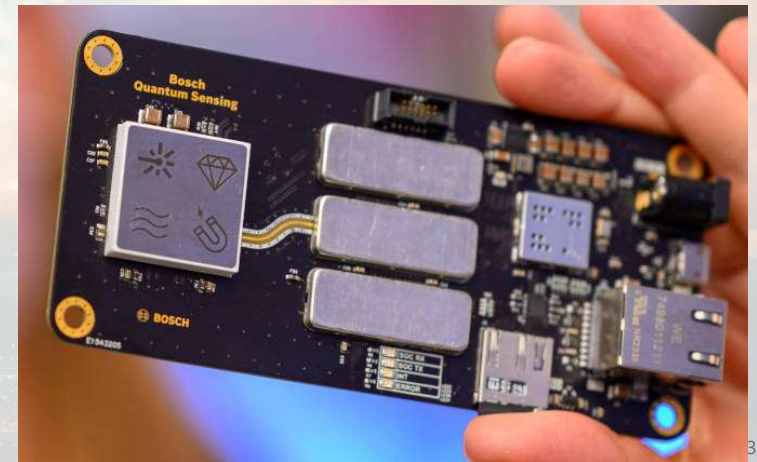


Bilderquellen:

Rechts: <https://www.nvidia.com/de-de/data-center/dgx-h100/>

Links: <https://www.fujitsu.com/global/services/business-services/digital-annealer/services/index.html>

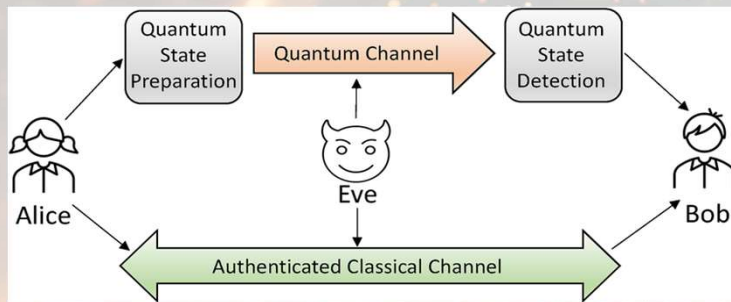
Quantensensorik (Heute – 4 Jahre)



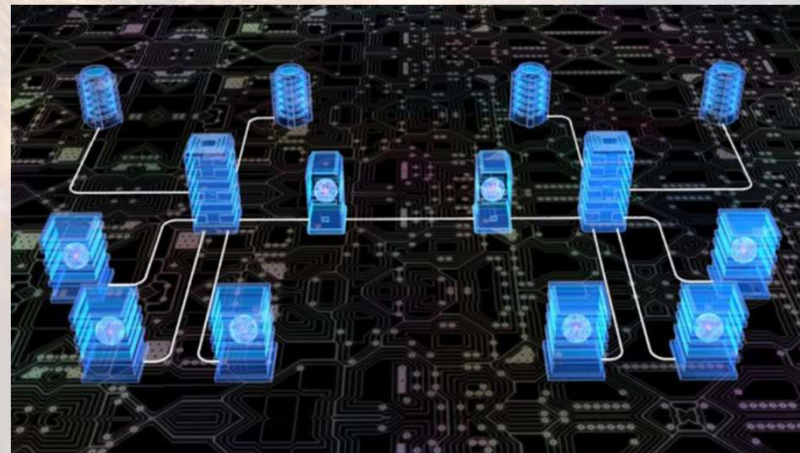
Anwendungen: Bodenbeschaffenheit, Echte Zufallszahlen, Prozessoptimierung, IoT

Bilderquellen:
1: Physikalisch-Technische
Bundesanstalt (PTB)
2: Elmos Semiconductor SE
3: Bosch Quantum Sensing

Quantenkommunikation (5 Jahre – 10 Jahre)



**Anwendungen: Metropole
Kommunikation, KRITIS,
Abhörsichere Verbindungen**



© Fraunhofer ILT, Aachen.

Am Fraunhofer ILT werden neue Komponenten für die Vernetzung von Quantencomputern erprobt.

Bilderquellen:

1: Liu et al. IET Quantum Communication June 2022 3(4)

2: www.unibw.de/muquanet

3: <https://www.ilt.fraunhofer.de/de/presse/pressemitteilungen/2023/5-16-photonische-technologien-fuer-quanteninternet.html>

4: <https://quantuminternetalliance.org/our-mission/>

Quantum Key Distribution (QKD)

KEEQuant



KEEQUANT

News | Technology | Products | Company

QKD is a paradigm shifting cryptographic key exchange method since it provides long-term security.

CV-QKD is a paradigm shifting implementation since it can be realized using components and processes that are widely adopted across the telecom industry. No exotic components like single photon detectors are necessary.

KEEQuant leverages the huge potential of **Photonic Integrated Circuits (PICs)**. 100% of the CV-QKD functionality will be hosted on a single PIC. The relevant technical properties such as size, weight, power consumption, environmental requirements, but especially producibility and cost of QKD systems will become similar to today's telecom devices.

Our long-term vision is to make CV-QKD an integral part of tomorrow's standard telecom transceivers – a true commodity with no extra hardware cost.

www.keequant.com

Quantum Optics Jena



Our «HD» product line stands for outstanding performance with highest entangled photon pair numbers to generate secure encryption keys, quantum imaging setups, or quantum technology experiments. Our customized system will generate polarization entangled photon pairs. The sources will be available for wavelengths around 800 nm, 1300 nm (O-Band), or 1500 nm (C-Band).

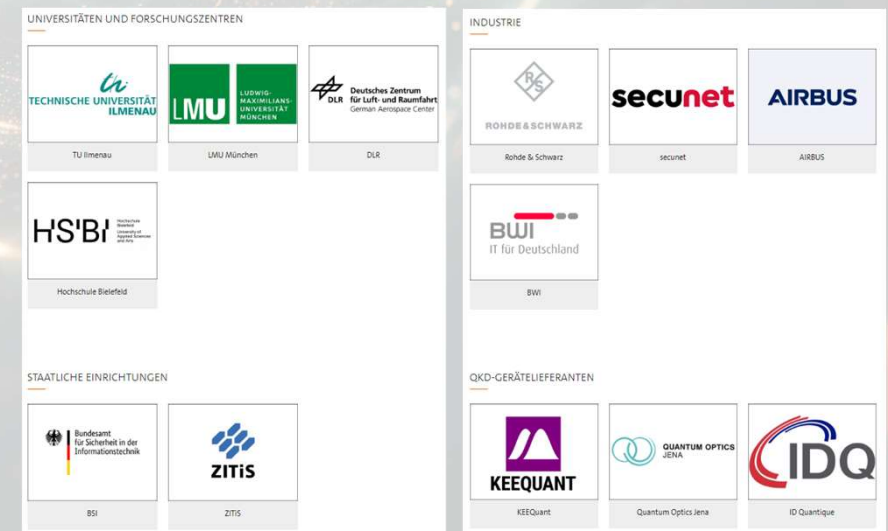
The «HD» products are characterized by a compact design, a high-precision fabrication and assembly on a thermo-mechanically stable platform. Our core technology covers the effective integration and deterministic assembly algorithms to achieve highest accuracies.

<https://qo-jena.com>

MuQuaNet

- Quantenkommunikationsnetzwerk im Raum München
- Entwicklung zukunftssicherer Kommunikationsinfrastrukturen
- Nutzung von QKD für Bereitstellung von Schlüsseln für die abhörsichere Kommunikation
- Umfasst zehn Knotenpunkte und integriert terrestrische und freie Raumstrecken zur Evaluierung von Quantenkommunikation
- Blaupause für die Entwicklung maßgeschneiderter, sicherer Netzwerke, etwa für Forschungseinrichtungen, Behörden und Militär

www.unibw.de/muquanet



Regionales Quantencomputing (7 Jahre - 15 Jahre)



Anwendungen: Quanten Kompetenz-Zentrum, High-Performance Computing, Cloud-Computing Hub, Energieeffizienz, Wachstumschancen



Bilderquellen:

1: <https://www.fz-juelich.de/de/ias/jsc/systeme/quantencomputing/juniq-infrastruktur>

2: Irekia Eusko Jaurlaritza - Gobierno Vasco :: Irekia (euskadi.eus)

3: Quantum Basel

Beispielhafte Timeline

2024

2040

Quantensichere IT

KI + Quanten

Quantensimulation

Quantensensoren

Quantenkommunikation

Quantencomputing

Vielen Dank! Zeit für Ihre Fragen.

Quantentechnologien, Bechtle IT-
Systemhaus Bonn/Köln



Anhang

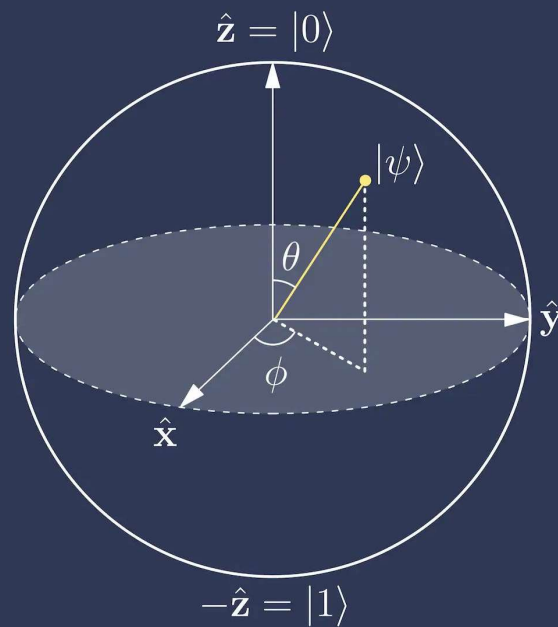
Quantum Computing

Was macht ein Quantencomputer?



Quantenmechanische Effekte für die
Informationsverarbeitung nutzen

Quantum Computing: Eine neue Art des Rechnens



Qubit

/ˈkjuːbɪt/

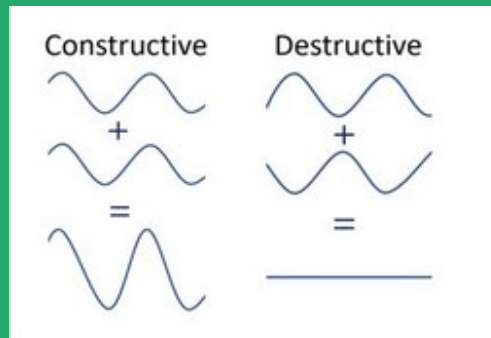
Basic unit of
quantum information

Quantum Computing: Essenzielle Effekte

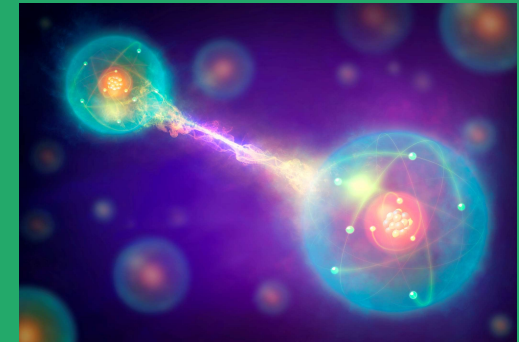
Superposition



Interferenz



Verschränkung

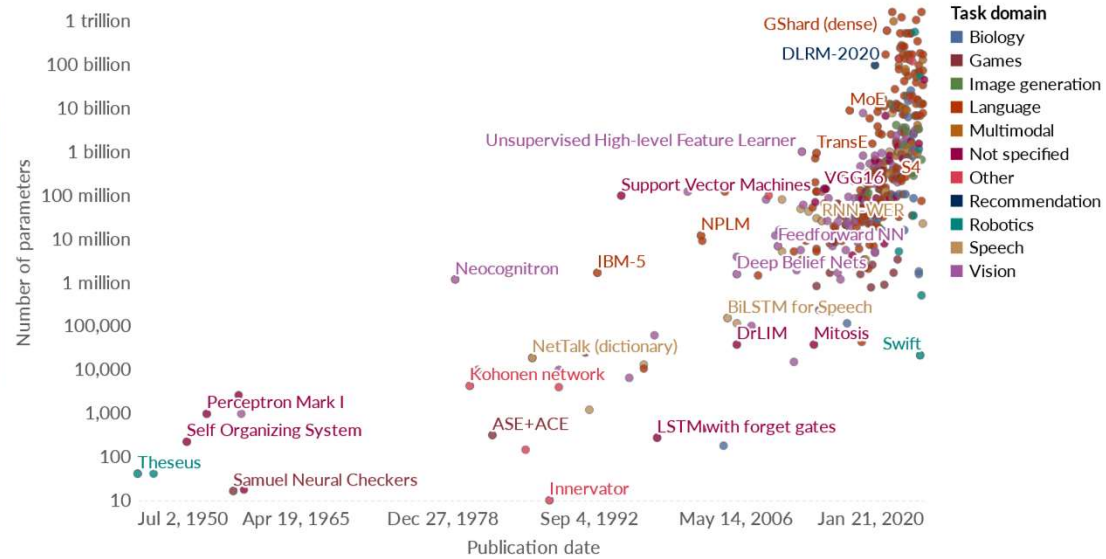


Exponentieller Parallelismus

Skalierbarkeit

Parameters in notable artificial intelligence systems

Parameters are variables in an AI system whose values are adjusted during training to establish how input data gets transformed into the desired output; for example, the connection weights in an artificial neural network.



Data source: Epoch (2023)

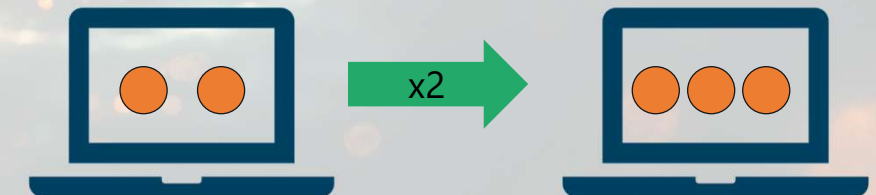
OurWorldInData.org/artificial-intelligence | CC BY

Note: Parameters are estimated based on published results in the AI literature and come with some uncertainty. The authors expect the estimates to be correct within a factor of 10.

Klassisches Rechenzentrum



Quantencomputer



Kryptografie

Symmetrisch



- Identischer Schlüssel für Ver- und Entschlüsselung
- Schlüssel muss geheim gehalten werden
- Z. B. genutzt bei Datenspeicherung

Hash-basiert

=

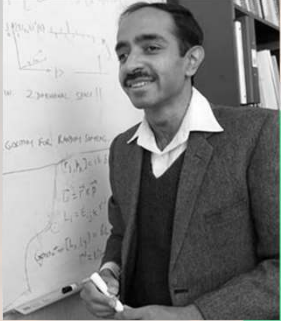
- Datenkonversion in Hashes bestimmter Länge
- Von Hashes auf Daten zurückzuschließen extrem schwer
- Z. B. genutzt für Verifizierung

Asymmetrisch



- Private- und Public-Schlüssel
- Sicherheit basiert auf Primfaktorzerlegung
- Essenziell für Kommunikation

Grover-Algorithmus / Shor-Algorithmus



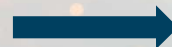
Lov Grover 1996:
**Algorithmus für Suche in
unstrukturierten Daten**



Geringer Vorteil beim Passwort-Raten



Peter Shor 1993:
**Algorithmus für effiziente
Dekomposition von großen
Zahlen in Primfaktoren**



**Ermittlung des privaten RSA-Schlüssels
mit Hilfe des Public Keys**

Shor-Algorithmus

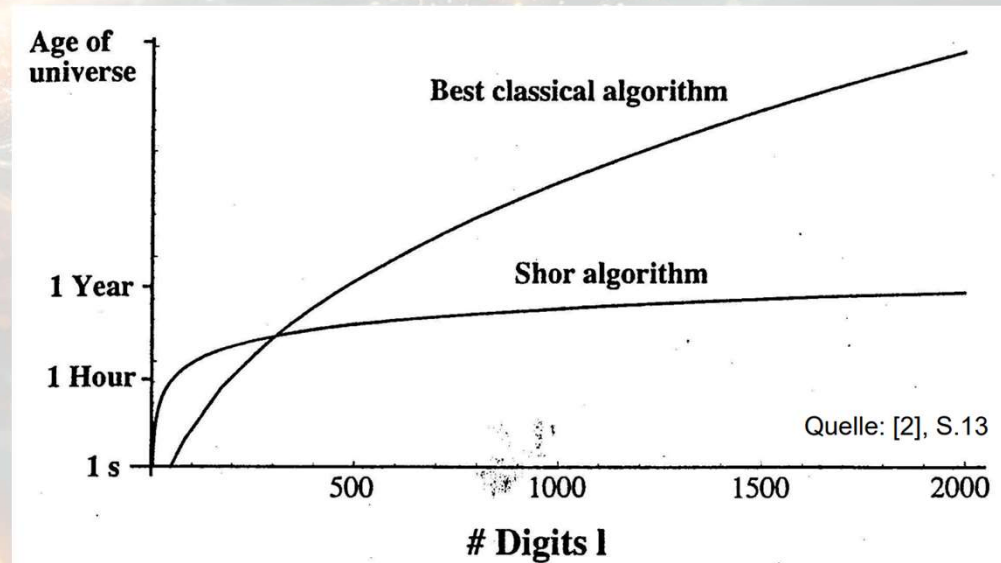
- ◆ Liefert zu einer natürlichen Zahl N einen nichttrivialen Faktor
- ◆ Klassische Faktorisierungsalgorithmen: Laufzeit nimmt exponentiell mit der Bit-Anzahl zu
- ◆ Shor-Algorithmus: Laufzeit nimmt polynomiell zu
 $\sim \mathcal{O}(\log_2 N)^3$
- ◆ Faktorisierung kann zurückgeführt werden auf Bestimmung der Periode einer Funktion
- ◆ Grundlegender Baustein ist die Quanten-Fourier-Transformation (QFT)

RSA beruht darauf, dass Faktorisierung großer Zahlen nicht effizient möglich ist. Wird verwendet, wo digitale Information sicher übertragen/ gespeichert werden sollen.

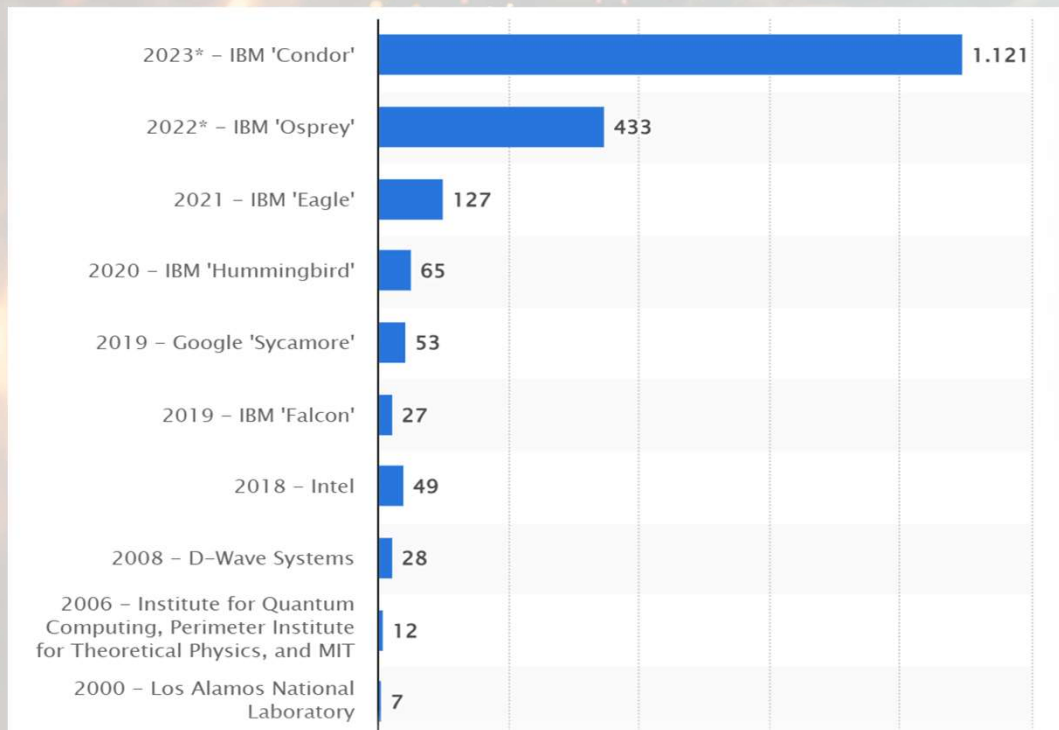


**Peter Shor 1993:
Algorithmus für effiziente
Dekomposition von großen
Zahlen in Primfaktoren**

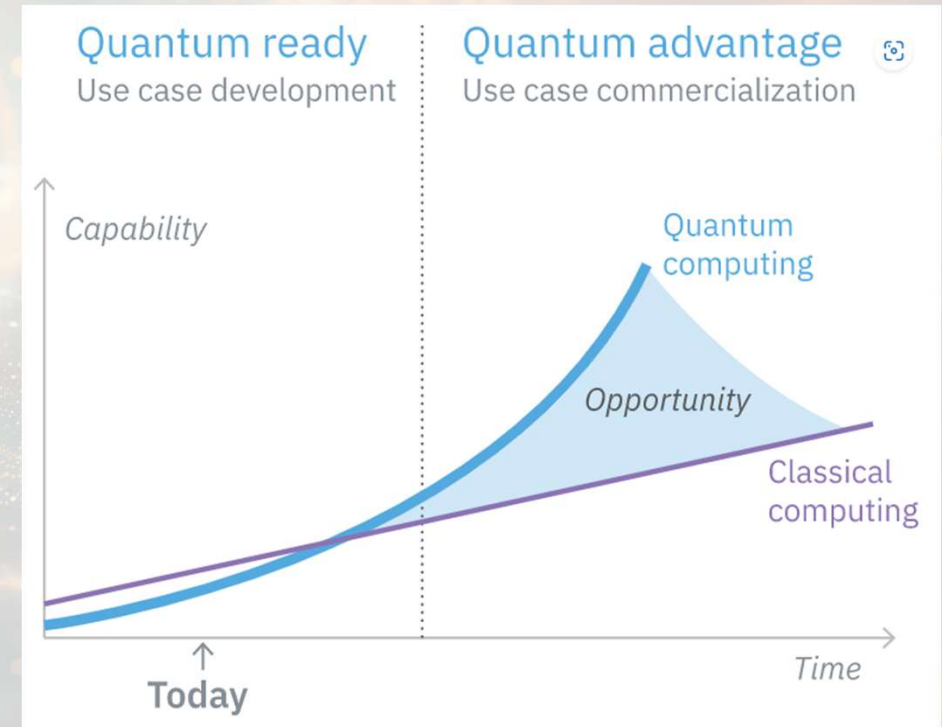
**Ermittlung des privaten
RSA-Schlüssels mit Hilfe
des Public Keys**



Quantum Computing: Perspektiven

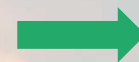


Quelle: <https://www.statista.com/chart/17896/quantum-computing-developments/>



Quelle: <https://www.ibm.com/thought-leadership/institute-business-value/report/quantumstrategy>

RSA 2048 Bit

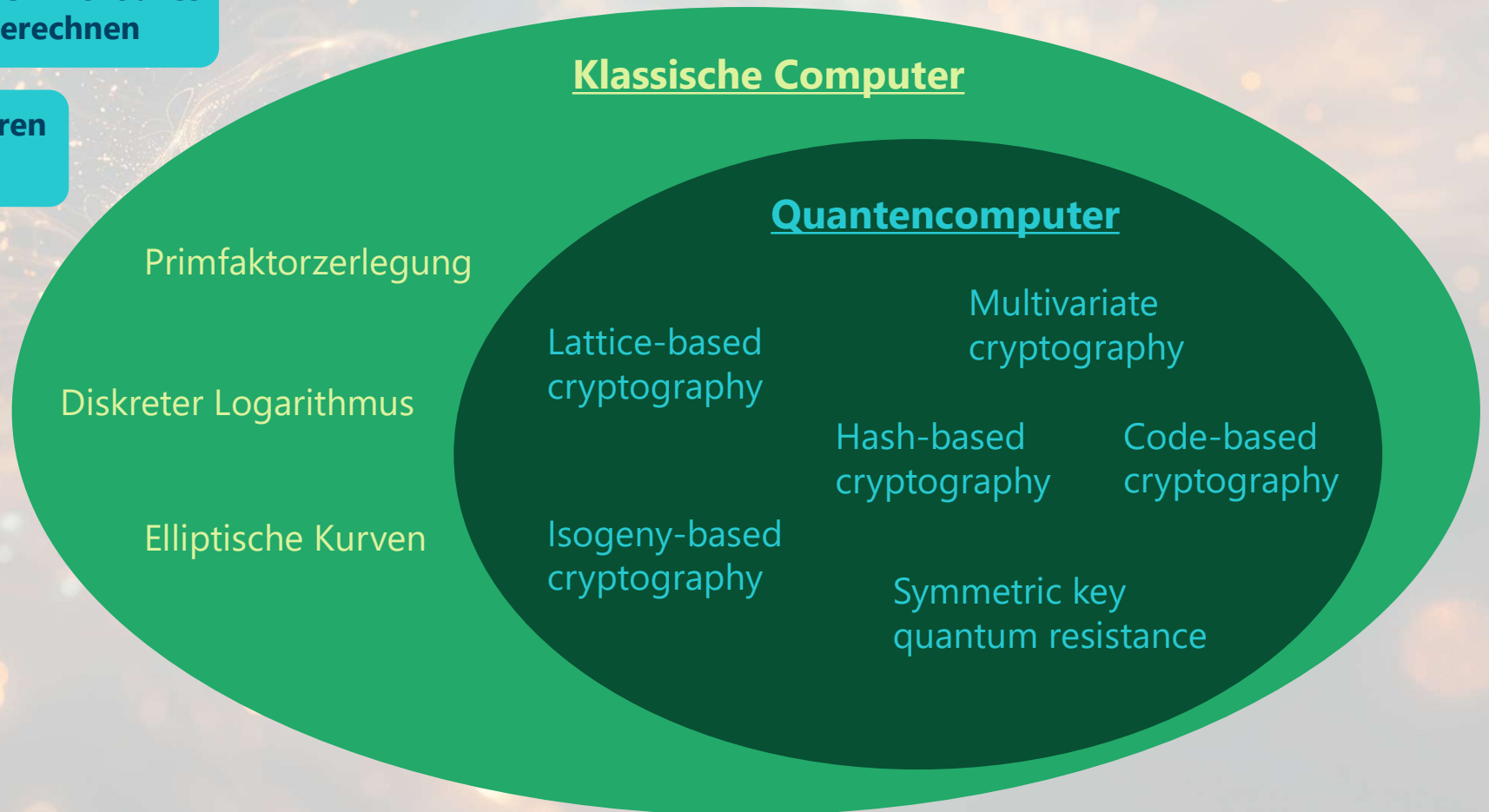


100k ~ 10M Qubit-Operationen

Quantum-Safe IT

Quantencomputer können nicht alles
(besser/schneller) berechnen

Quantensichere Verfahren
können schützen

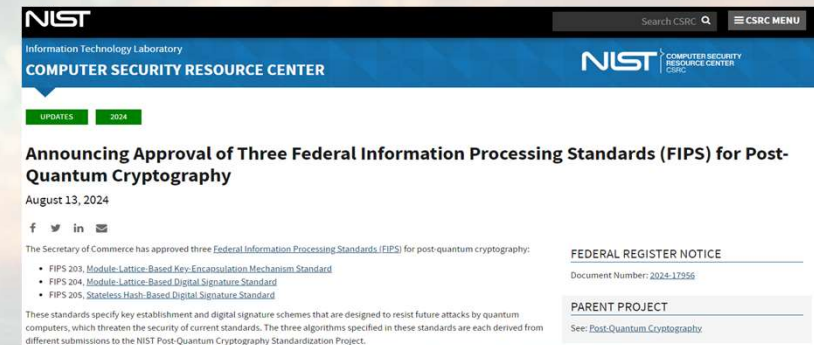


Standards für quantensichere Kryptografie

National Institute of Standards and Technology, August 2024:
Zulassung von 3 Verfahren, die gegen zukünftige Bedrohungen
durch Quantencomputer schützen sollen

**Empfehlung: Migration hin zu quantensicheren
Algorithmen jetzt starten/umzusetzen und die
Sicherheit sensibler Daten in Zukunft gewährleisten.**

Post-Quantum Cryptography Project (NIST 2016):
Suche nach quantensicheren Algorithmen & Prüfung – Ziel:
Standardisierung von Verfahren, deren Sicherheit auf
verschiedenen komplexen mathematischen Problemen basiert



- ◆ **ML-KEM (CRYSTALS-Kyber):**
Schlüsselkapselungsverfahren, das für die
allgemeine Verschlüsselung ausgewählt wurde,
etwa für den Zugriff auf gesicherte Websites
- ◆ **ML-DSA (CRYSTALS-Dilithium):**
gitterbasierter Algorithmus, der für allgemeine
digitale Signaturprotokolle ausgewählt wurde
- ◆ **SLH-DSA (SPHINCS+):**
hashbasiertes digitales Signaturverfahren

State of the Art

	KEMs	Signaturen
NIST 2024	CRYSTALS-Kyber	CRYSTALS-Dilithium SPHINCS+ Falcon
Botan 3.4.0	Kyber/ML-KEM FrodoKEM	Dilithium/ML-DSA SPHINCS+ XMSS
Erste BSI Erweiterung	Classic McEliece	HSS/LMS
Kommende BSI Erweiterung	BIKE oder HQC	Falcon

Quanten-robuste Methoden

Klasse	Eigenschaften & Beispiele
Hash-basiert / Symmetrisch	Für digitale Signaturen, keine Public-Key-Encryption; z. B. Merkle-Signaturen, SPHINCS+, Picnic
Code-basiert	Seit vielen Jahren gut studiert; z. B. McEliece, Niederreiter
Multivariate	Z. B. Oil-and-Vinegar-Methode
Gitter-basiert	Zeigen gute Eigenschaften für digitale Signaturen, Schlüsselaustausch & Key Encryption, relativ kurze Schlüssel & Ciphertexte; z. B. NTRU, LWE, Ring LWE, Learning with Rounding, CRYSTALS-Kyber, CRYSTALS-Dilithium
Isogenies	Relativ langsame Verfahren; z. B. Supersingular Elliptic Curve Isogenies

Eintauchen.

bechtle

