

State of the Art bei Quantencomputer

Univ.-Prof. Dr. Wolfgang Lechner - ParityQC

Quantencomputer als disruptive Schlüsseltechnologie

Technologien



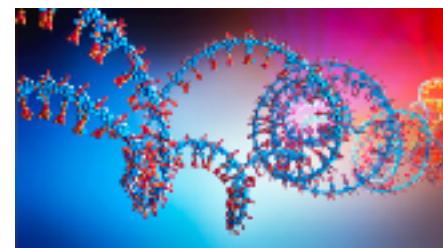
Anwendungen



Logistik/Transport



Kommunikation



Gesundheit

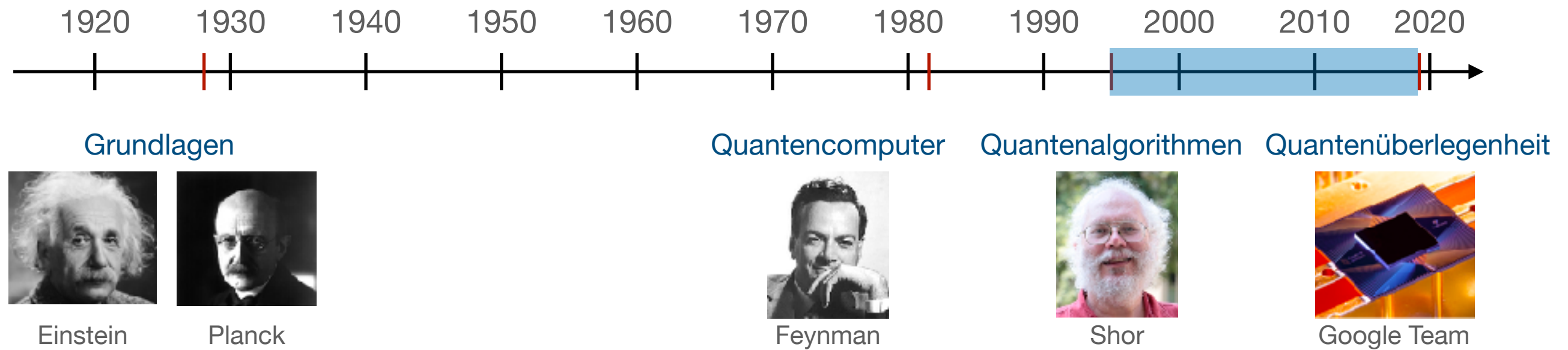


Finanz

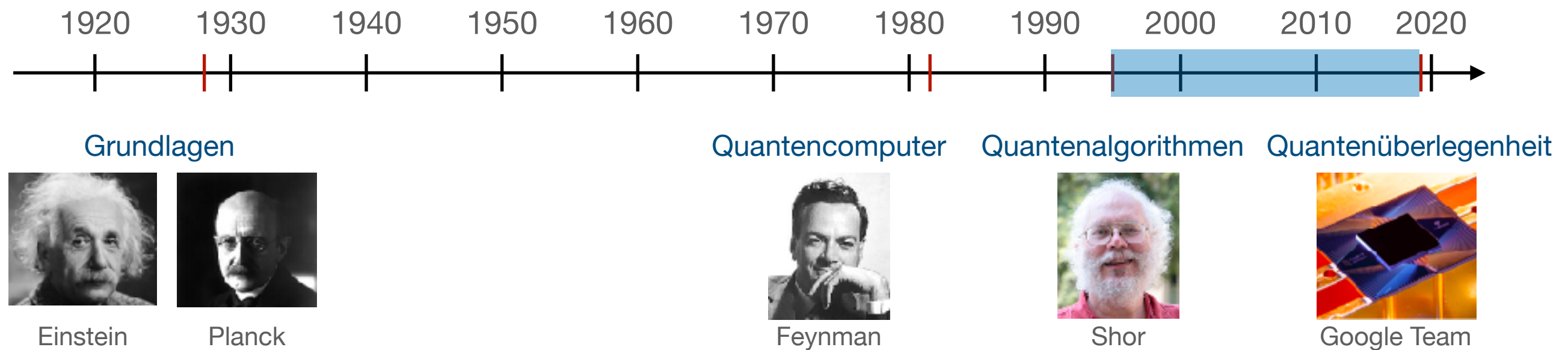
... und viele weitere **zentrale** Aspekte unserer Gesellschaft.

Bereits eine kleine Verbesserung der etablierten Systeme hat enorme Auswirkungen auf die Wirtschaft.

Quantencomputer als disruptive Schlüsseltechnologie



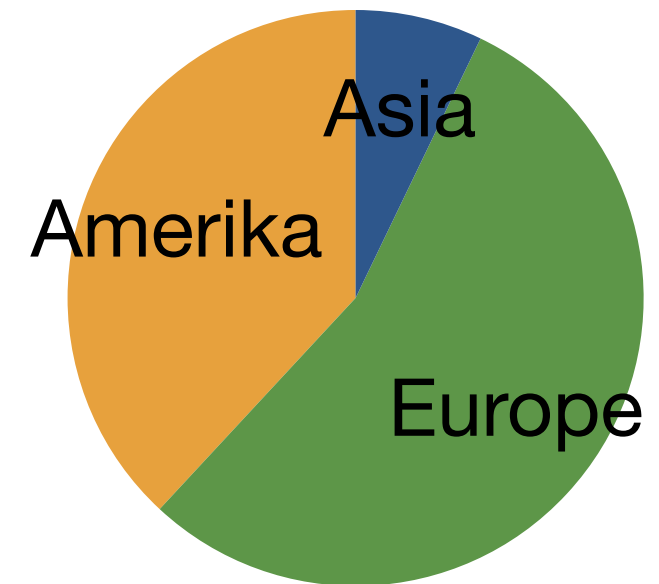
Quantencomputer als disruptive Schlüsseltechnologie



Seit 2019 ist es keine Frage mehr,
ob der Quantencomputer kommt,
sondern nur mehr
wann und **wo** er kommen wird.

Der Quantencomputer ist eine **Europäische** Erfolgsgeschichte

Meilensteine des Quantencomputers



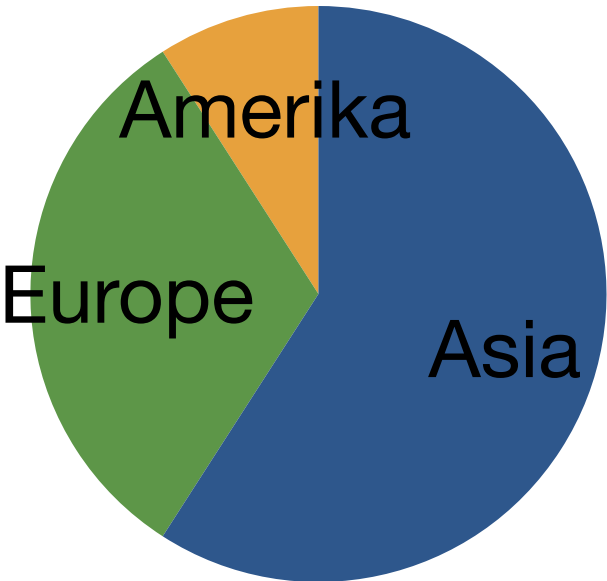
Quelle:

Forbes

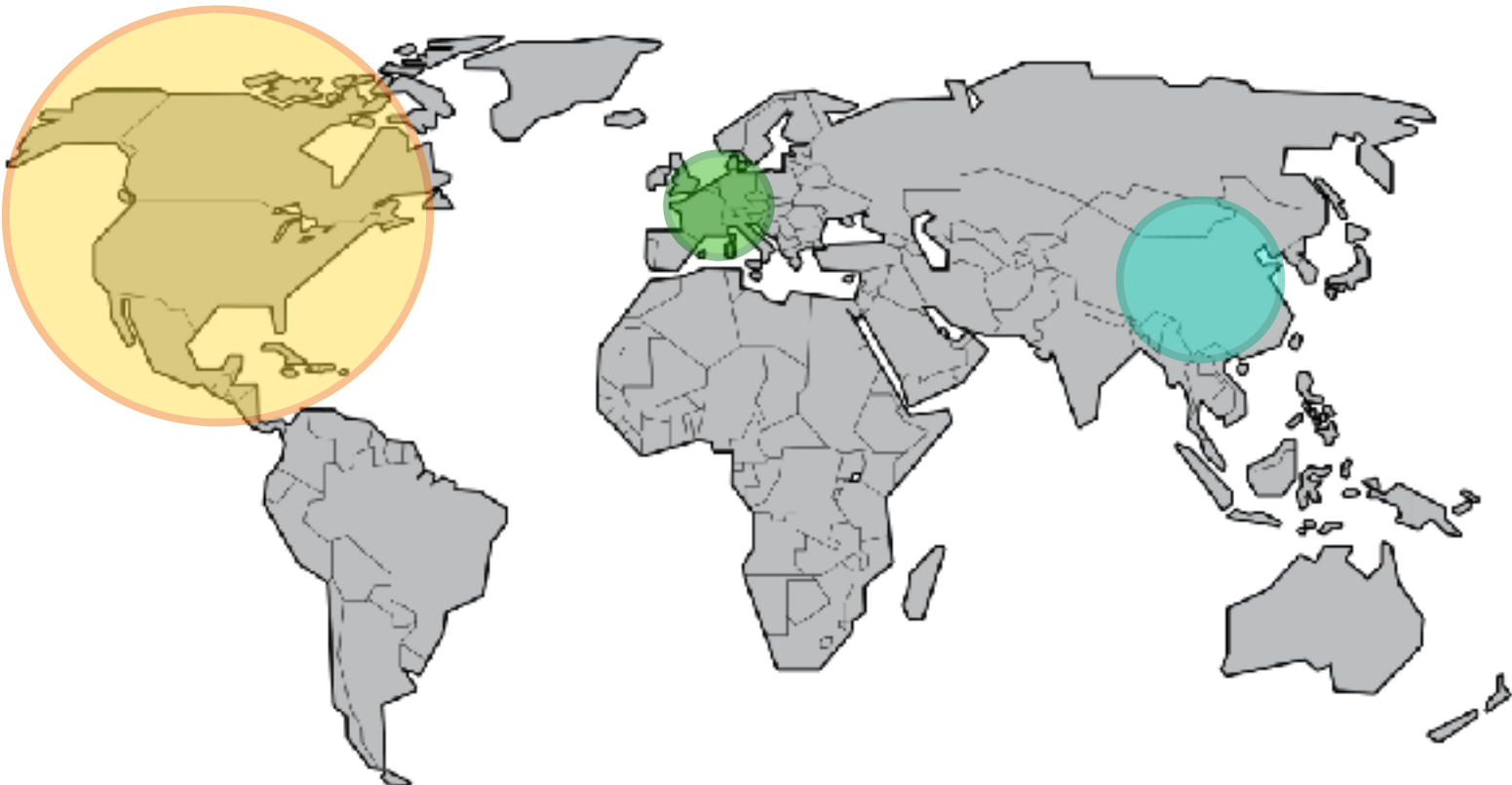
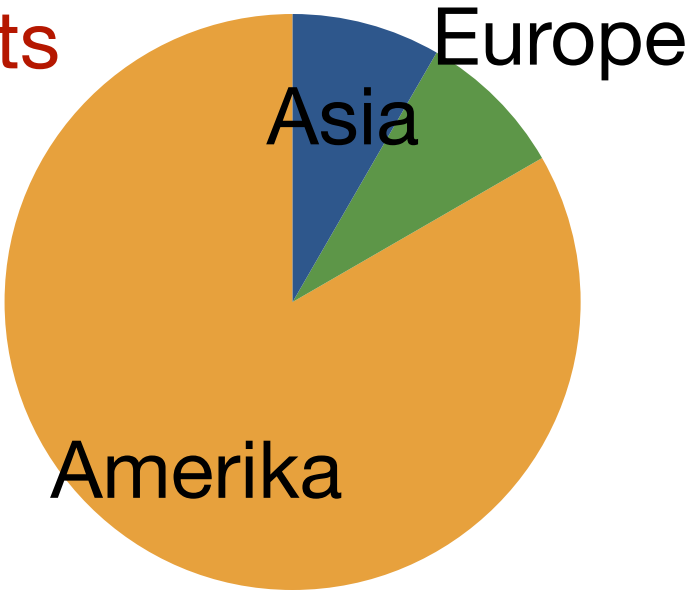


Der Quantencomputer war(?) eine **Europäische** Erfolgsgeschichte

Staatliche
Programme
2020-2025: ~22bn\$

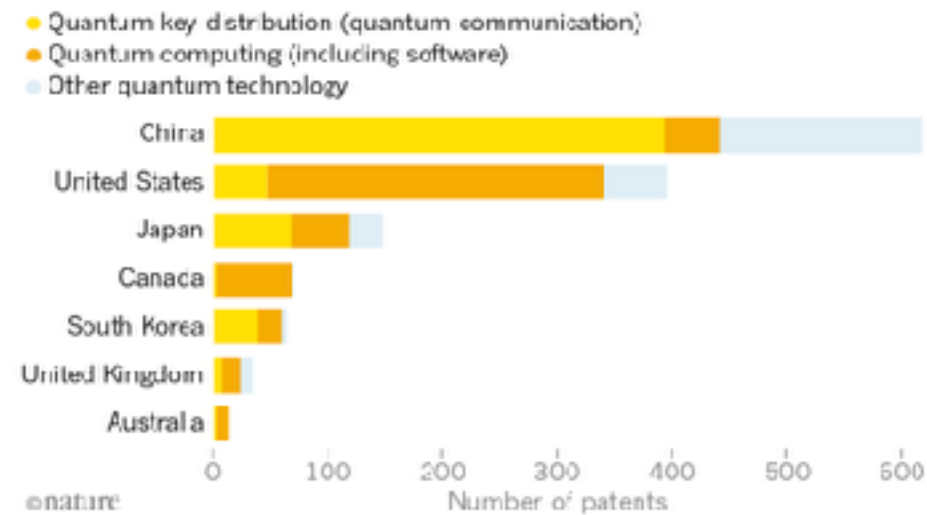


Investments
2020: ~0.5bn\$

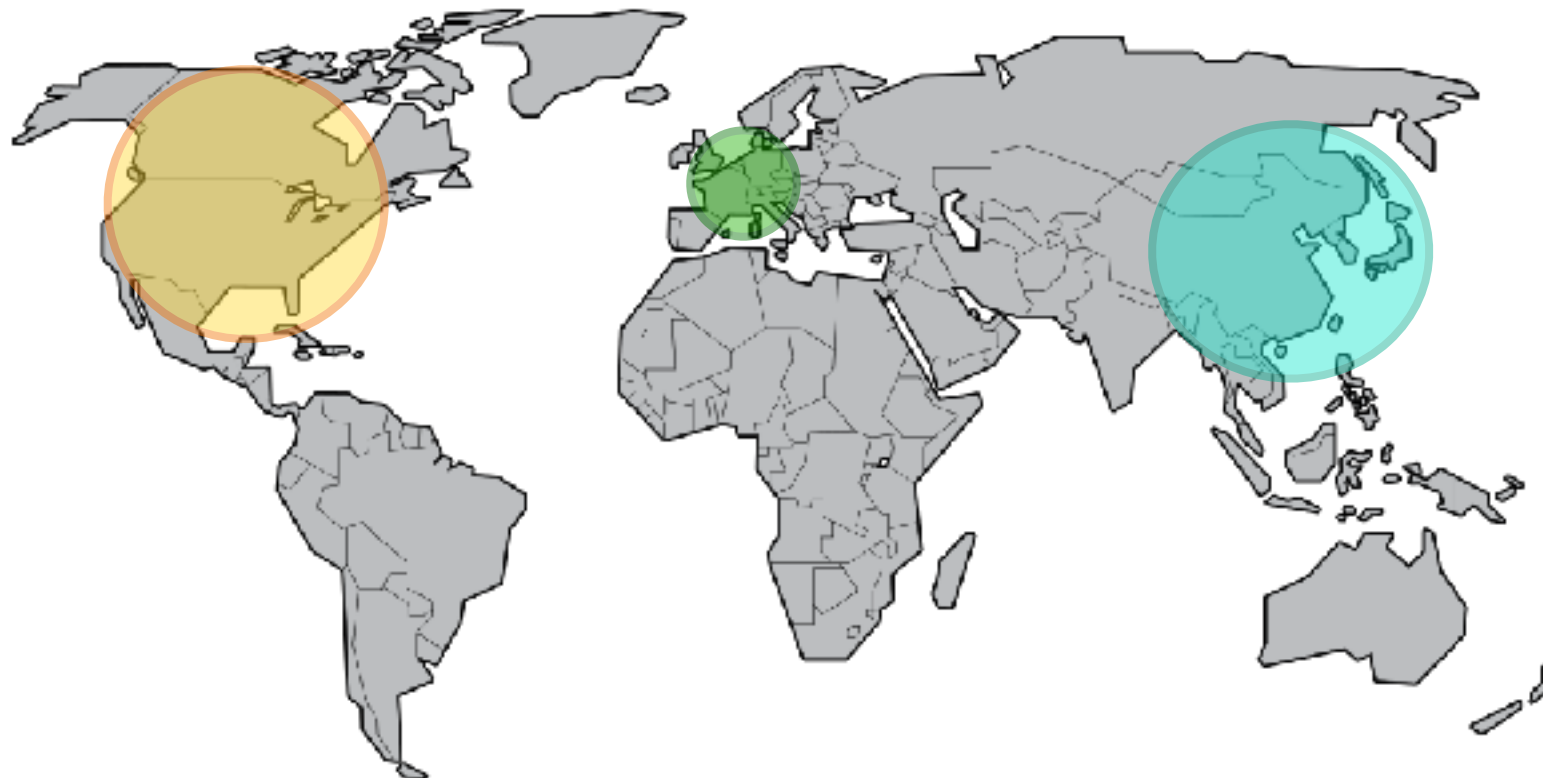


Der Quantencomputer war(?) eine **Europäische** Erfolgsgeschichte

Patente für Quantencomputer

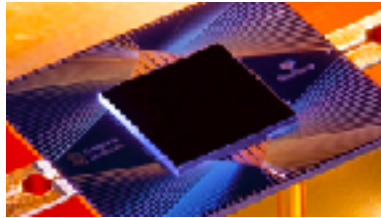


Source: Martino Travagnin/EC Joint Research Centre

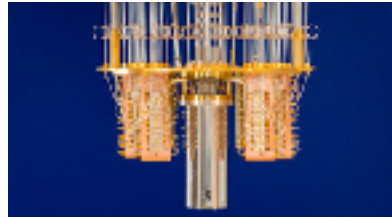


Der Quantencomputer war(?) eine **Europäische** Erfolgsgeschichte

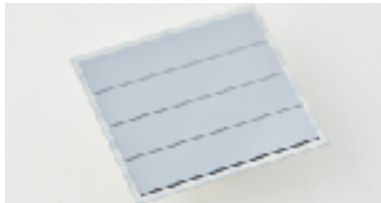
Hardware Rennen



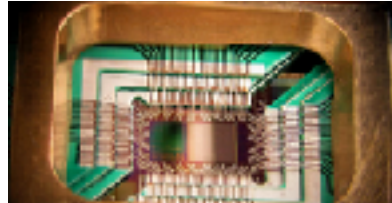
Google* - 53qubits



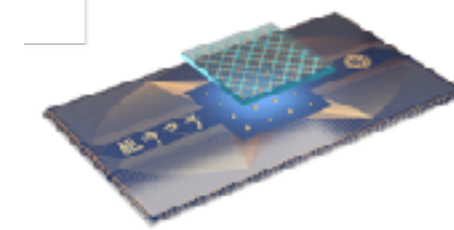
IBM - 150 qubits



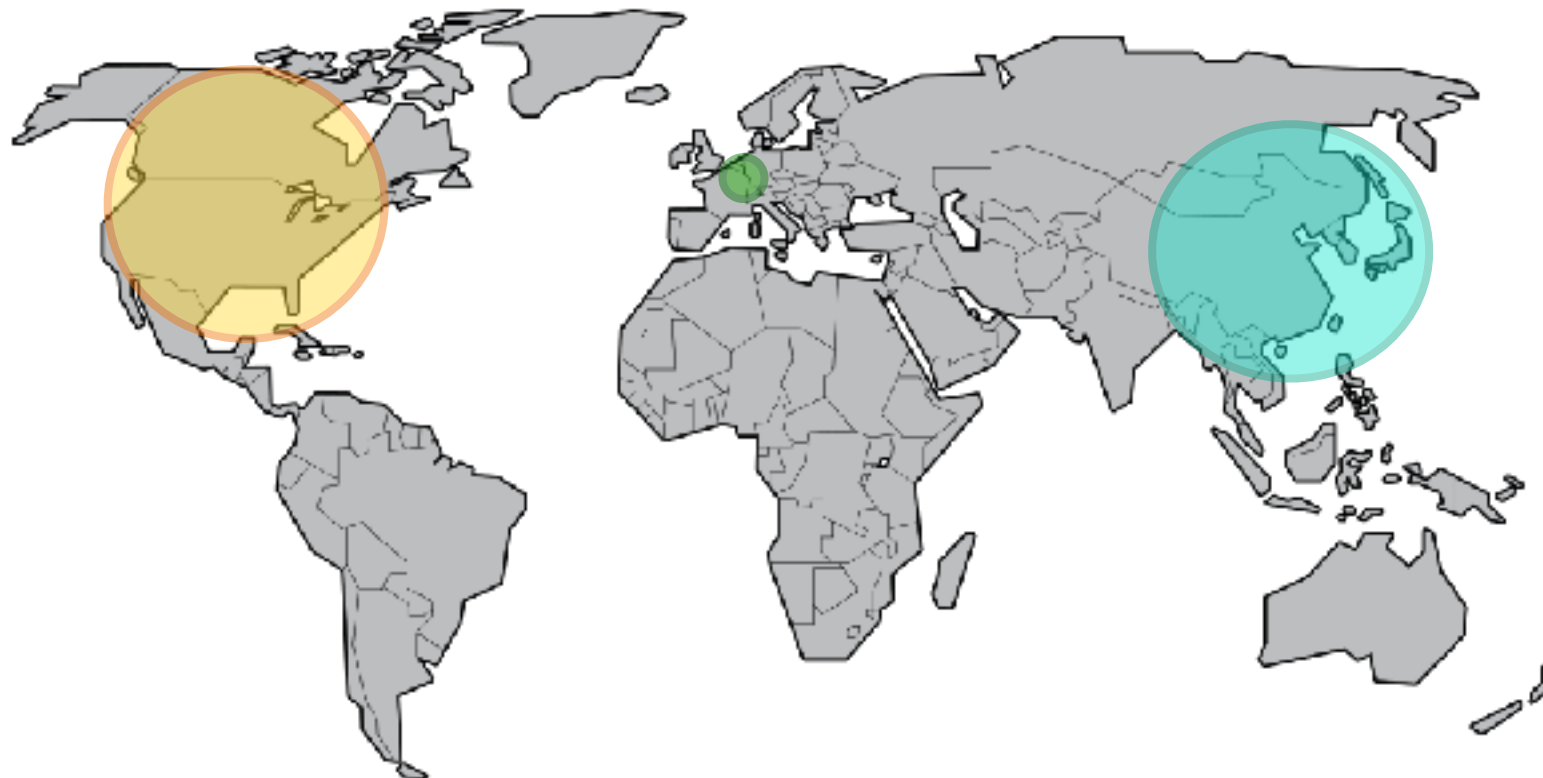
Rigetti - 30 qubits



D-Wave - 1000 qubits



Hefei* - 66 qubits

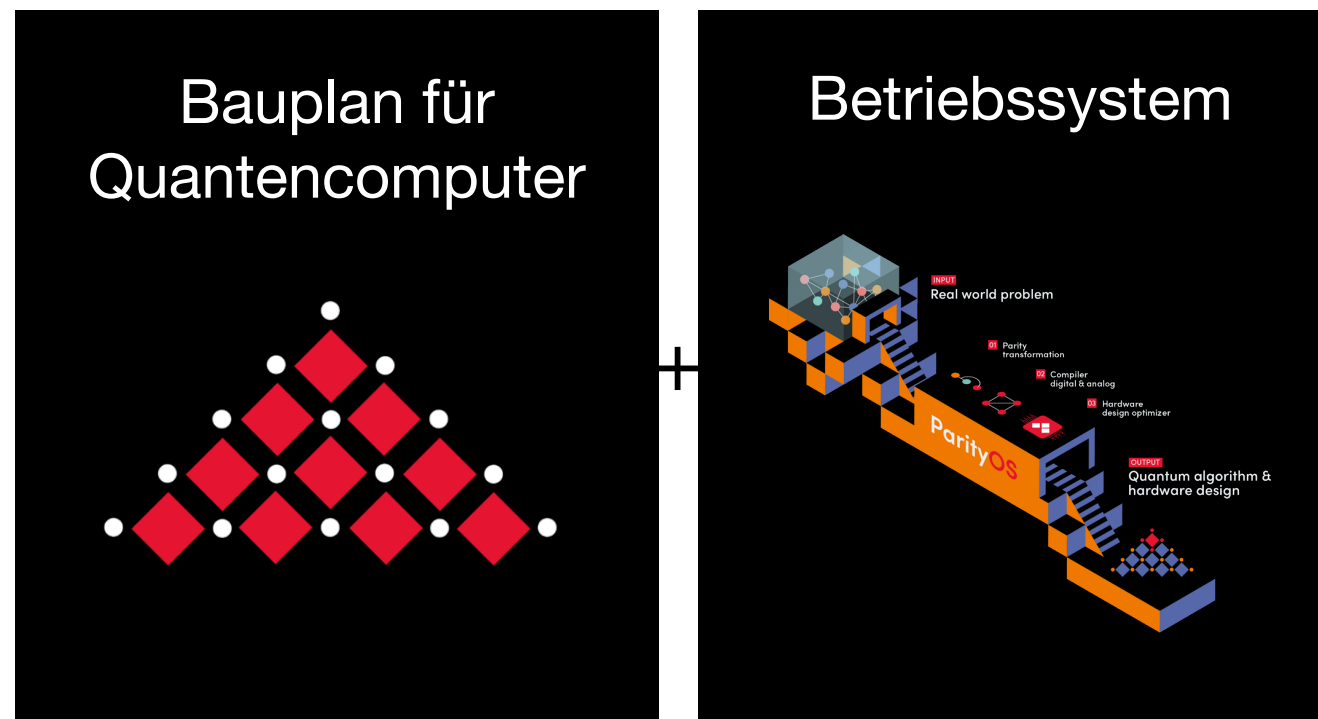


* - Quantum Supremacy Demonstrated



Architektur für Quantencomputer als weltweiter Standard

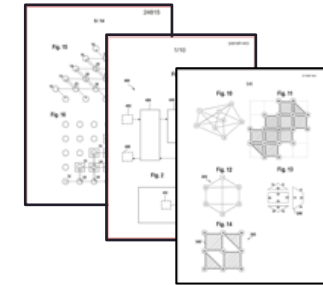
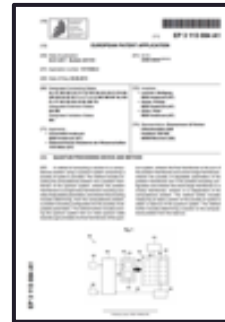
Technologie



Architektur



- Patente in Europäischer Hand



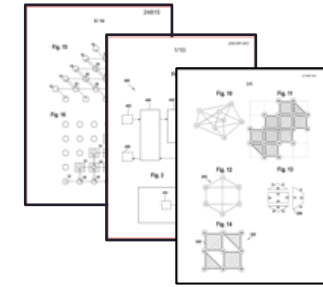
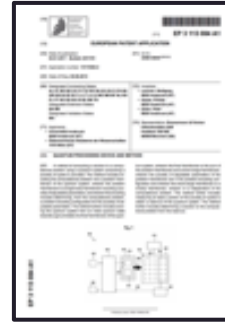
Architektur Patent 2015 20 weitere fundamentale Patentfamilien

Kaufangebot bereits 2015 aus USA ausgeschlagen um
Technologie in Europa zu halten.

Architektur



- Patente in Europäischer Hand



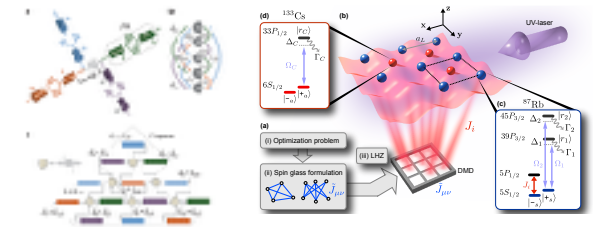
Architektur Patent 2015 20 weitere fundamentale Patentfamilien

Kaufangebot bereits 2015 aus USA ausgeschlagen um Technologie in Europa zu halten.

- Globales Rennen

RESEARCH ARTICLE
QUANTUM TECHNOLOGY
A quantum annealing architecture with all-to-all connectivity from local interactions
Sheng Gong^{1,2,3,4}, Michael J. Heuley^{1,2,3,4}, Peter J. Hogg^{1,2,3,4}

Science



Publikation 2015 in Science

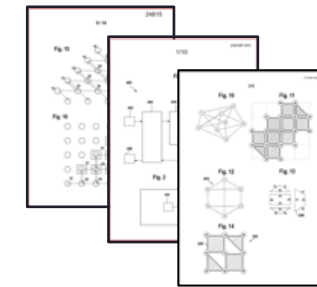
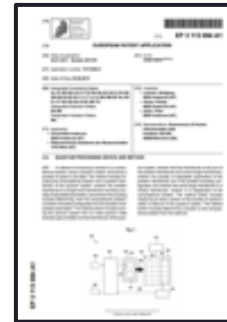
400 Publikationen
zu Weiterentwicklungen

Forschungsgruppe an der Universität Innsbruck mit globaler Reputation.

Architektur



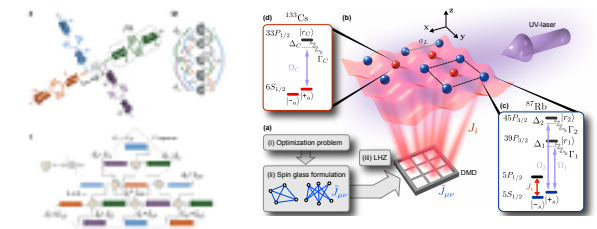
- Patente in Europäischer Hand



Schlüsselpatent 2015 20 weitere fundamentale Patentfamilien

Kaufangebot bereits 2015 aus USA ausgeschlagen um Technologie in Europa zu halten.

- Globales Rennen



Publikation 2015 in Science

400 Publikationen
zu Weiterentwicklungen

Forschungsgruppe an der Universität Innsbruck mit globaler Reputation.

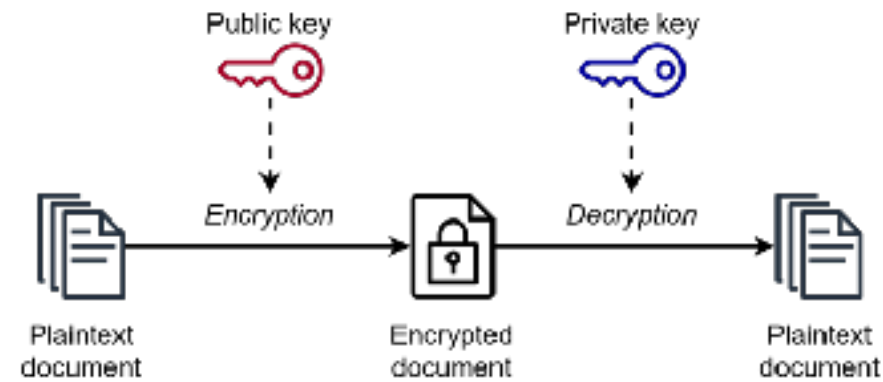
- Weltweit gebaut



Hardware-Hersteller in Japan, USA, Europa bauen unsere Architektur.

Shor's Algorithmus

Annahme von z.B. RSA ist: Primfaktorenzerlegung ist computationally hard.

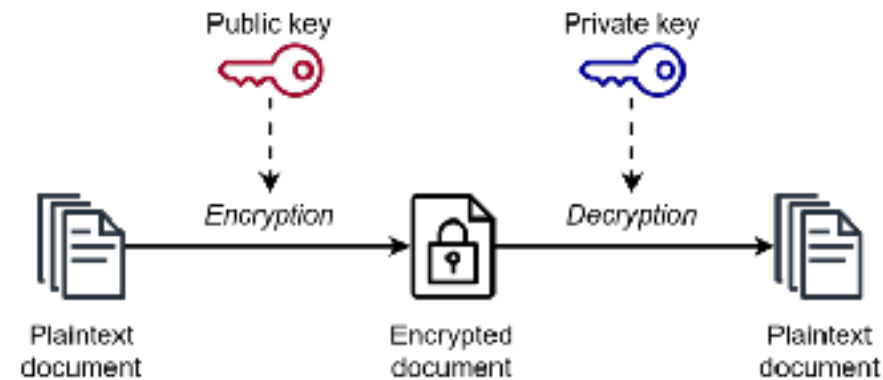


Computer: $O\left(e^{1.9(\log N)^{1/3}(\log \log N)^{2/3}}\right)$

Quantencomputer: $O\left((\log N)^2(\log \log N)\right)$ exponentiell schneller

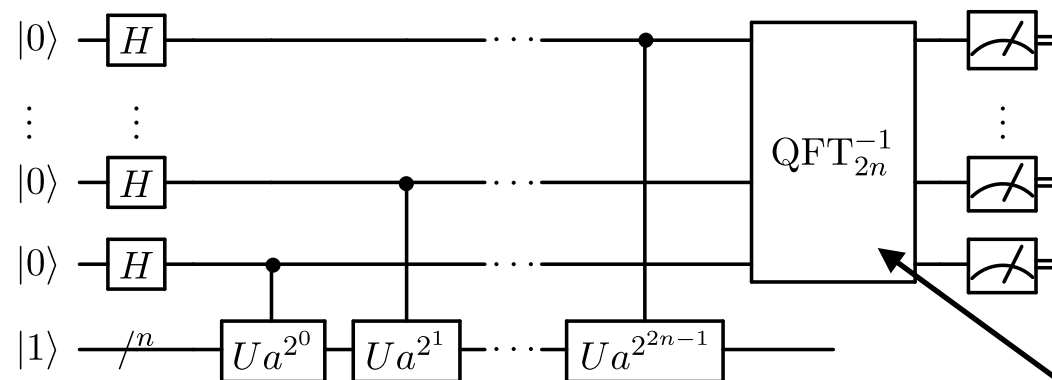
Shor's Algorithmus

Annahme von z.B. RSA ist: Primfaktorenzerlegung ist computationally hard.



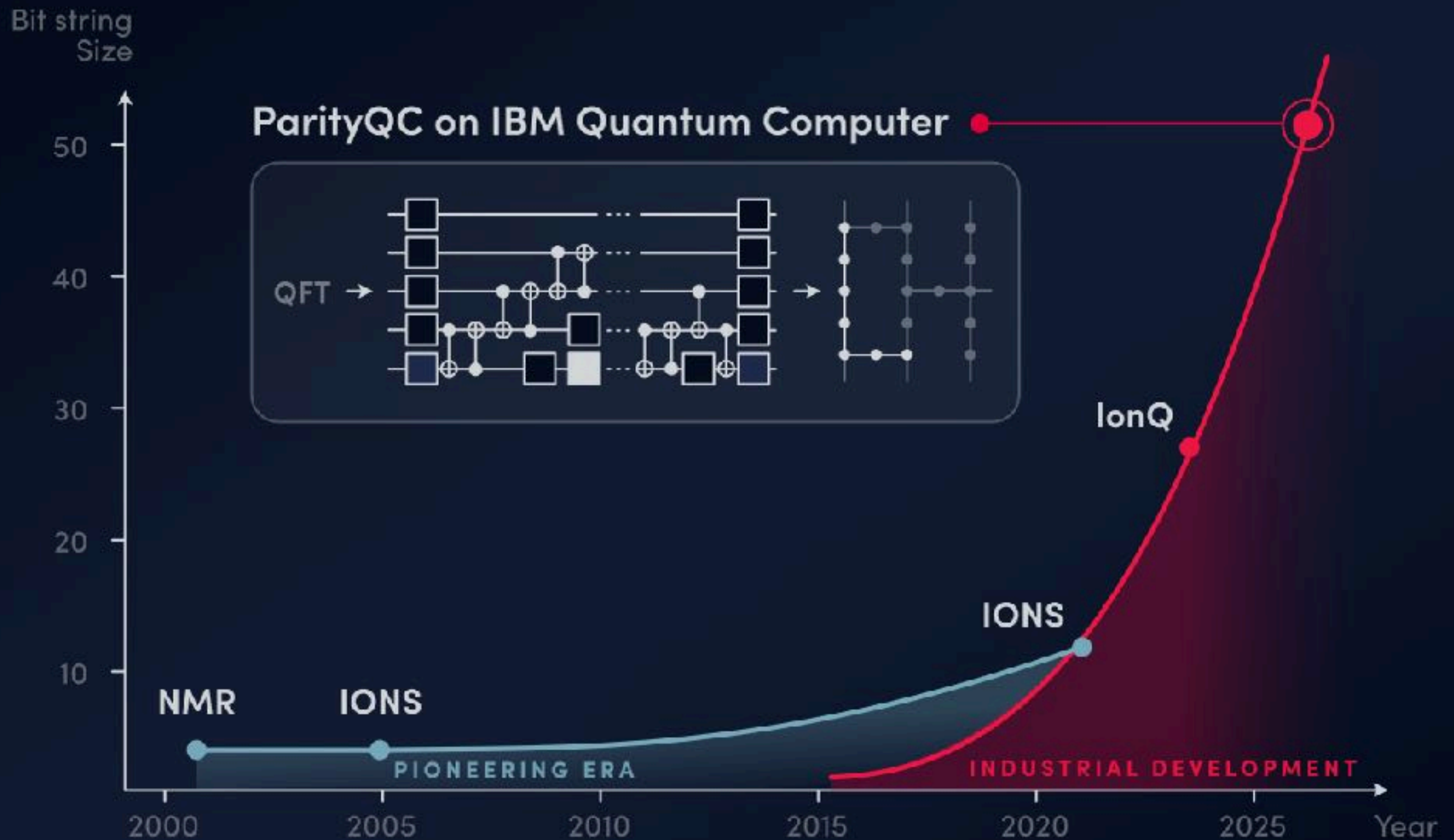
Computer: $O\left(e^{1.9(\log N)^{1/3}(\log \log N)^{2/3}}\right)$

Quantencomputer: $O((\log N)^2(\log \log N))$ exponentiell schneller



wichtigster Baustein: Fourier Transformation

Weltrekord hält ParityQC



Post-Quantum

Executive Order 14412 (22 Juni 2026) :
alle US Institute müssen bis 2030 auf Post-Quantum Cryptographie umgestellt sein



Post-Quantum

Executive Order 14412 (22 Juni 2026) :
alle US Institute müssen bis 2030 auf Post-Quantum Cryptographie umgestellt sein

Umgesetzt von NIST:





 Menu

UPDATES

Nine Candidates Advance to the Third Round of the Additional Digital Signatures for the PQC Standardization Process

NIST Internal Report (IR) 8610 announces nine candidates advancing to the third round of the Additional Digital Signatures for the Post-Quantum Cryptography (PQC) Standardization Process.

May 14, 2026



After 18 months of evaluation, NIST has selected nine candidates for the third round of the Additional Digital Signatures for the [Post-Quantum Cryptography \(PQC\) Standardization Process](#). The advancing digital signature algorithms are:

• FAEST • HAWK* • MAYO	• MQOM • QR-UOV • SDitH	• SNOVA • SQIsign • UOV
--	---	---

NIST IN YOUR INBOX

Stay up to date with the latest news from NIST.

Sign Up >

 ORGANIZATIONS

Information Technology Laboratory

Ein Weg für Europa



Kopf schlägt Kapital

Weltweites Hardware Rennen - sehr kostenintensiv!

Wir liefern wir Know-How, Bauplan und Betriebssystem
IP und Wertschöpfung bleibt in Europa.

Know-How nach Europa holen



Durch unsere **Schlüsselpatente** holen wir jetzt schon Know-How nach Europa.

Know-How nach Europa holen



Durch unsere **Schlüsselpatente** holen wir jetzt schon Know-How nach Europa.

Quantum Silicon Valley in **Österreich** möglich!