

Quanten-Computer

Workshop

marcus, katharina, patrik, antonius



22. Januar 2019: *Lasst uns was hacken 2018/19*



Quelle: IBM

Übersicht

1. Möglichkeiten und Grenzen von Quantencomputern
2. Rechnen mit Quantencomputern
3. Anwendungen für frühe Quantencomputer
4. Quantencomputer Programmieren

Übersicht

Möglichkeiten und Grenzen von Quantencomputern

1. Was können Quantencomputer?
2. Was können Quantencomputer nicht?
3. Real existierende Quantencomputer

Was können Quantencomputer?

Was können klassische Computer?

- Speicher besteht aus Bits (b_0, b_1, b_2, \dots)
- Bits sind entweder 0 oder 1.
- Programm besteht aus Befehlen
- Ein Befehl kann eine begrenzte Anzahl Bits lesen und abhängig davon eine begrenzte Anzahl anderer Bits schreiben.
- Die Adressierung kann direkt oder indirekt sein.
- Church-Turing-These

Die Klasse der Turing-berechenbaren Funktionen stimmt mit der Klasse der intuitiv berechenbaren Funktionen überein.

Was können Quantencomputer?

- Speicher besteht aus Quanten-Bits (qbits) (q_1, q_2, q_3, \dots)
- qbits sind 0 oder 1 oder eine Wahrscheinlichkeitsverteilung über 0 und 1.
- qbits können miteinander verschränkt werden.
 - Jede Kombination von verschränkten qbits hat eine eigene Wahrscheinlichkeit.
- Ein Programm besteht aus einer Reihe von Matrix-Operation, welche die Wahrscheinlichkeiten in eine gewünschte Richtung verschieben.
- Am Ende findet eine Messung statt, bei der eine der Möglichkeiten gemäß der Verteilung zufällig ausgewählt wird.
- Wiederholung des Experiments (z.B. 1000x)

Algorithmen für Quantencomputer

- Auch in Kombination mit klassischen Computern
- Auswahl des Anfangszustand und des Quantenalgorithmus klassisch.
- Optimierte Ausführung auf dem Quantencomputer.
- Auswertung des Ergebnisses, eventuell neue Iteration bis zum gewünschten Ergebnis.

Algorithmen für Quantencomputer

- Quantum Fourier Transformation
 - Shor's Algorithmus (RSA, DSA, ECC in polynomieller Zeit)
- Amplitude Amplification
 - Grover's Algorithmus: Datenbanksuche in $O(\sqrt{N})$ (SHA-512)
- Quantum Walk
 - Doppelte Elemente in Liste finden: $O(N^{\frac{2}{3}})$
- Simulation von Quantensystemen
 - s. Patrik's Vortrag

siehe auch: https://en.wikipedia.org/wiki/Quantum_algorithm

Post-Quanten-Kryptografie

Shor's Algorithmus ist nicht das Ende der Kryptografie.

Quanten-Computer-Resistente Algorithmen werden bereits entwickelt.

NIST-Wettbewerb mit mehreren Dutzend Einreichungen.

NP-Vollständige Probleme, für die kein Quanten-Algorithmus bekannt ist. Dann repräsentatives Teilproblem auswählen, um die Schlüsselgrösse zu begrenzen.

Quanten-Computer in der Praxis

Quantum Threshold Theorem

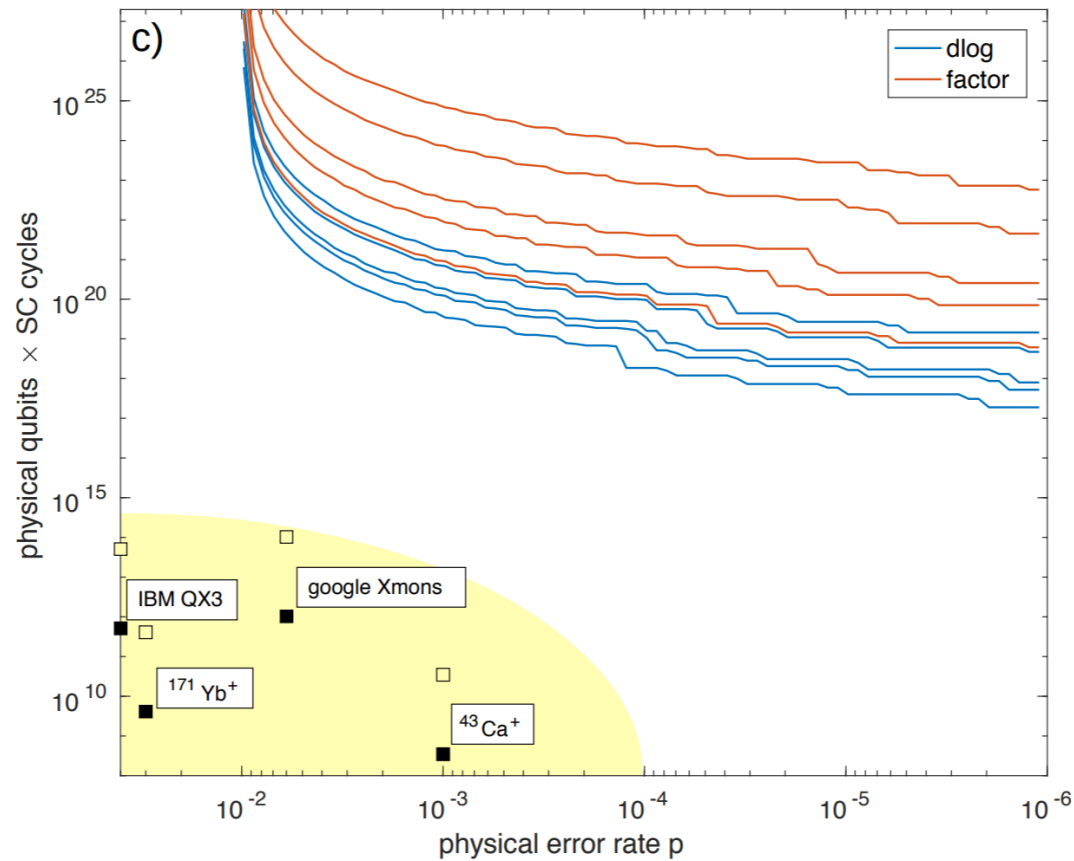
Es gibt eine Fehlergrenze ϵ , unter der ein idealer Quanten-Computer effizient durch einen fehlerbehafteten simuliert werden kann. (Ben-Or, Aharonov, 1997).

"The entire content of the Threshold Theorem is that you're correcting errors faster than they're created. That's the whole point, and the whole non-trivial thing that the theorem shows. That's the problem it solves."

$\epsilon = 0.001$ würde bedeuten: 1000 – 10,000 physische qbit pro logisches qbit.

Beispiel RSA-2048: $\epsilon = 0.0001$, 100 Tage, 1 Million qbits (BSI)

Quanten-Fehler-Korrektur



Published online 31 May 2011 | *Nature* **474**, 18 (2011) |
doi:10.1038/474018a

News

First sale for quantum computing

But critics say that D-Wave's system is still something of a black box.

Zeeya Merali

It could turn out to be a milestone for quantum computing. Last week, D-Wave Systems of Burnaby in British Columbia, Canada, announced the first sale of a commercial quantum computer, to global security firm Lockheed Martin, based in Bethesda, Maryland.



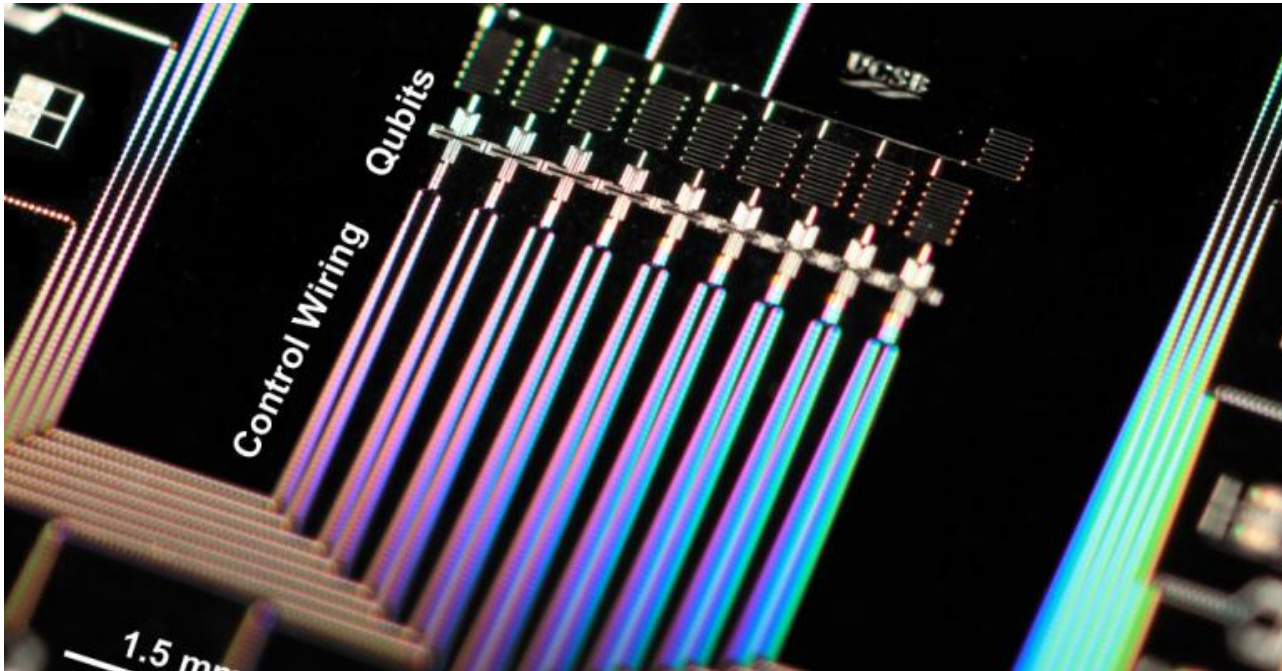
D-Wave co-founder Geordie Rose with his black monolith.

Dominic Schaefer Photography

D-Wave One

Google

Josephson Junction Quantum Computing at University of California, Santa Barbara (UCSB)

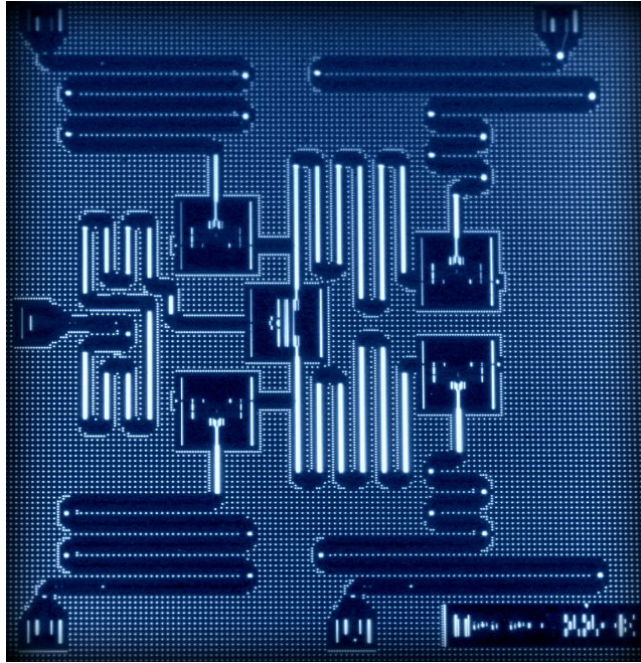


Google, UCSB

72 qubits im März 2018 angekündigt.

Quanten-Computer in der Praxis

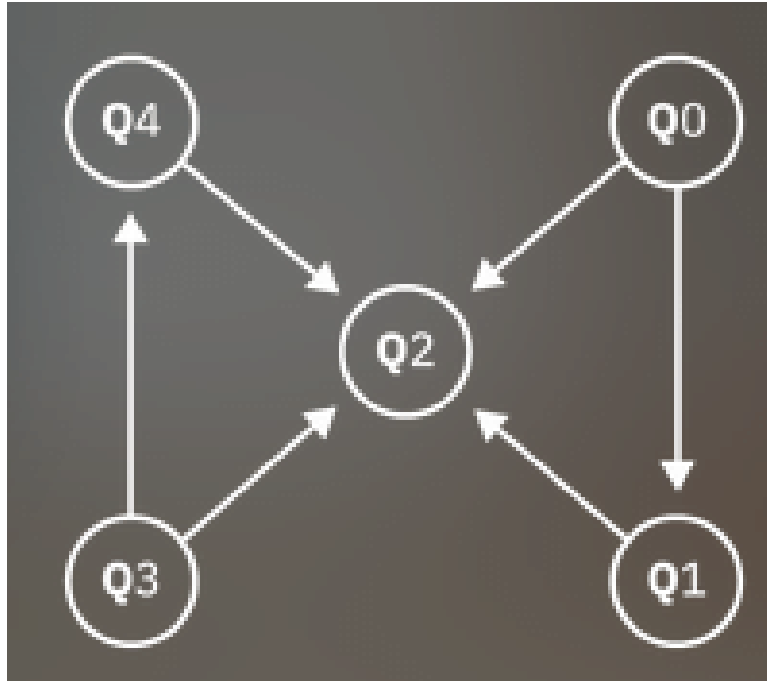
IBM Q



IBM Q - ibmqx2

Quanten-Computer in der Praxis

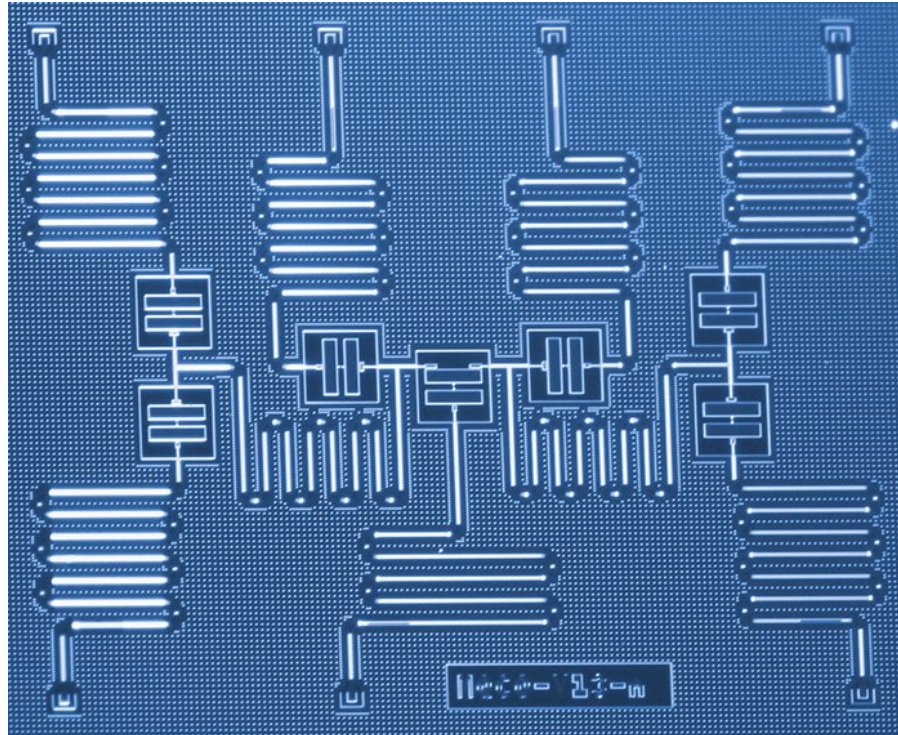
IBM Q



IBM Q - ibmqx2 (CNOT-Konfiguration)

Quanten-Computer in der Praxis

IBM Q



Vielen Dank!

Fragen?