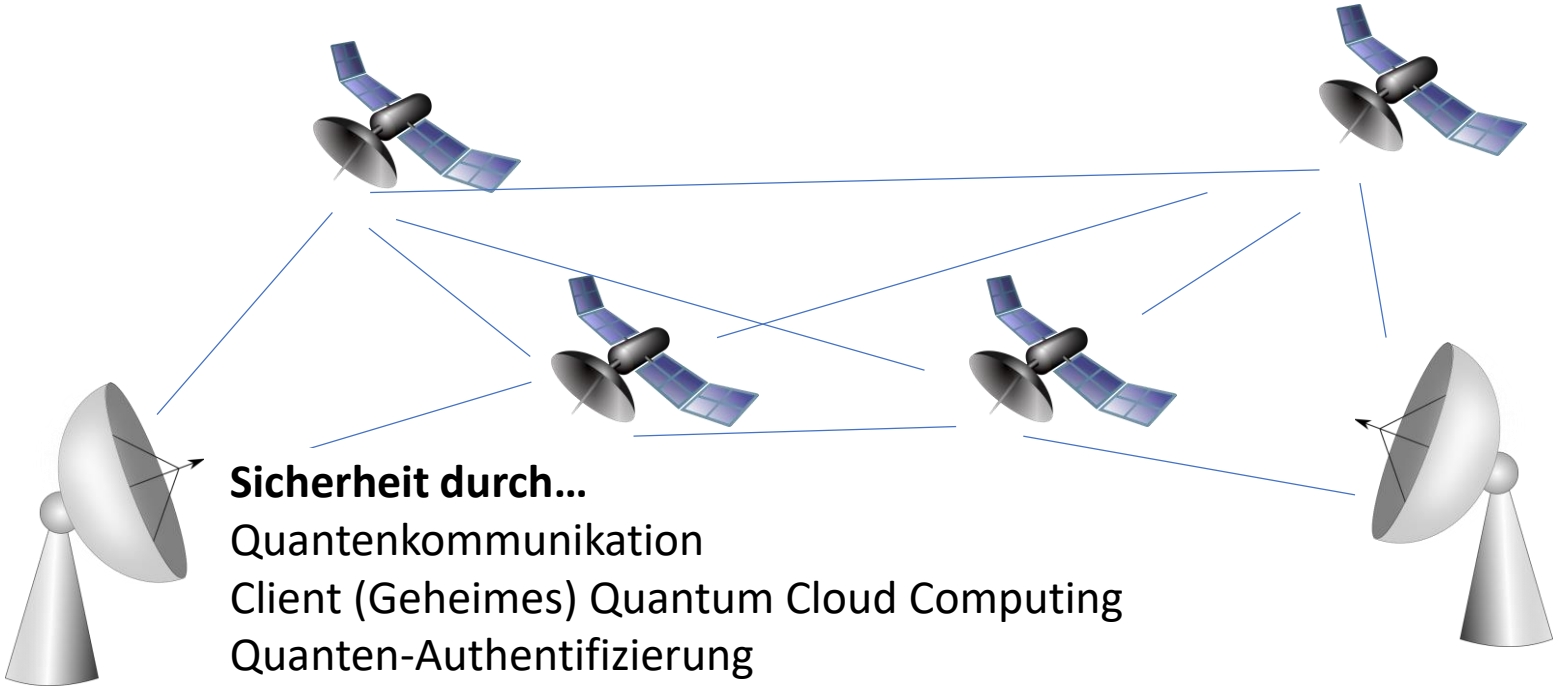
QUANTENCOMPUTING: RISIKO UND POTENTIAL

PD. Dr. Sabine Wölk

DLR Institut für Quantentechnologien, Ulm

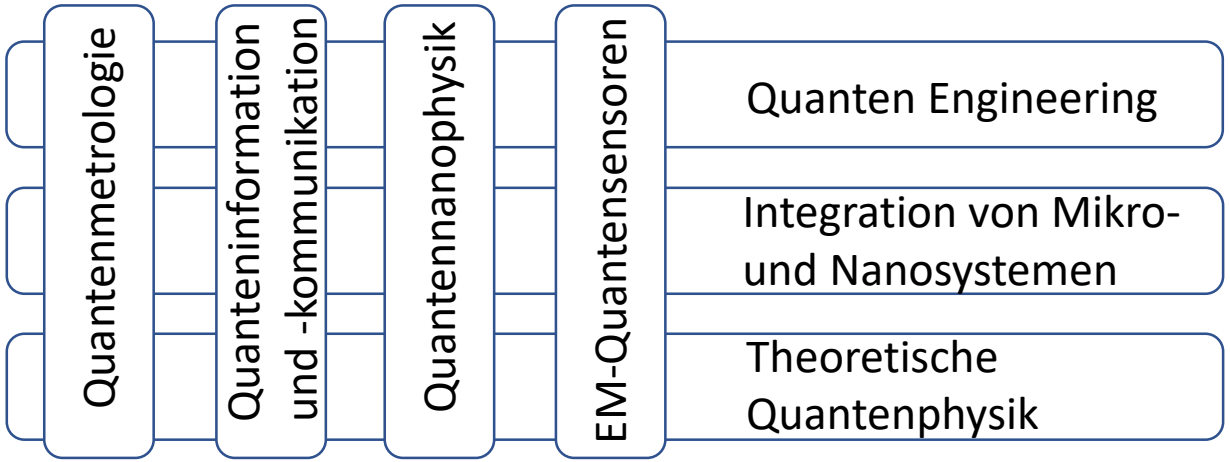
DLR QT: Quantentechnologie für die Digitalisierung



Sicherheit durch…
Quantenkommunikation
Client (Geheimes) Quantum Cloud Computing
Quanten-Authentifizierung

Sensoren und Uhren für…
Navigation
Luftraumüberwachung
Space Debris Mapping
Klimaschutz

Determinismus durch…
Zeitreferenzen
Positionsbestimmung
Orbitkontrolle



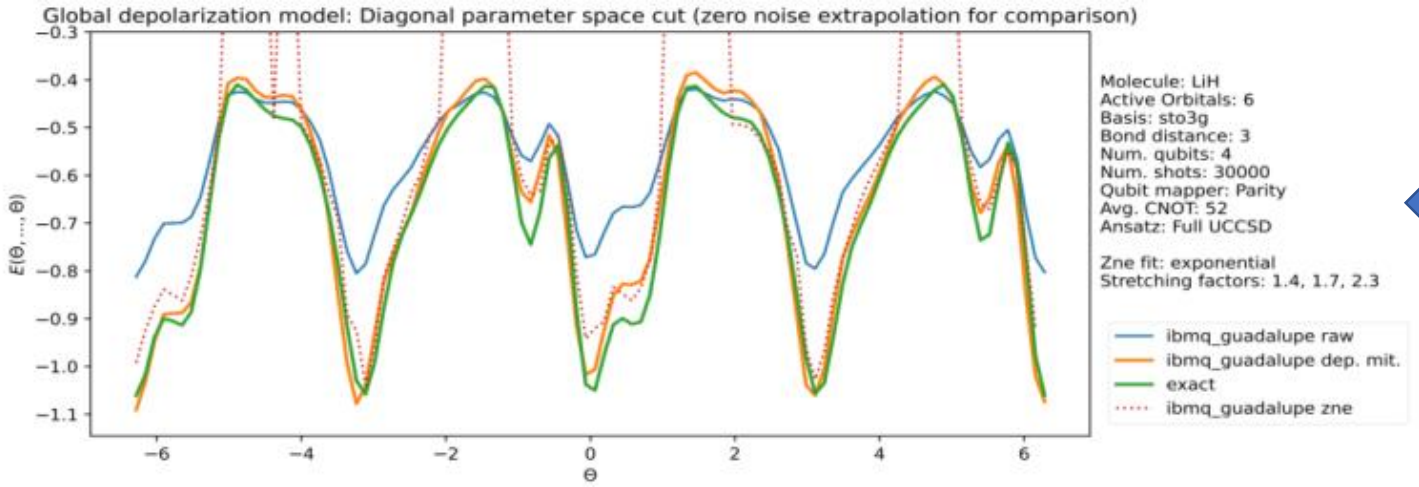
Wie gefährlich sind derzeitige Quantencomputer?

- Um einen 2048bit RSA-Code zu brechen braucht man ca. 4100 fehlerfreie Qubits bzw. 10-100mio fehlerbehaftete Qubits

Quantum. 5, 433 (2019) oder arxiv:1905.09749

- Die Anzahl an benötigten Quantengatter für Shor‘s Algorithmus skaliert quadratisch mit der Anzahl der Qubits
- Die derzeit besten Quantencomputer schaffen mit 20 Qubits 20 Operationen

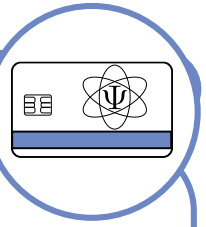
https://en.wikipedia.org/wiki/Quantum_volume



Beispiel: Rechenergebnis eines Quantencomputers mit 4 Qubits

Ausgewählte QC-Projekte am DLR QT:

Quantenkomm. und -verarbeitung

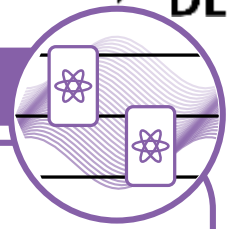


- **Quantennetzwerke**
- **Quantenauthentifizierung und Quantenidentifizierung**
- **Quanten-Maschinelles Lernen**

bdr. BUNDESDRUCKEREI

CURANDO · UNIVERSITÄT ULM · SCIENDO · DOCENDO

Quanten Maschinelles Lernen



- Quantenalgorithmen für das Maschinelle Lernen
- Kollaboration mit Quantenhardwareherstellern

QUIX QUANTUM

XEED

eleQtron

QCi

Quantenanwendungen

QC Mobility

Untersuchung des Potentials von Quanten-computern für Transportanwendungen

Luftverkehr

Straßen-verkehr

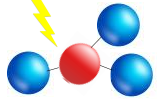
Schienen-verkehr

Maritimer-verkehr

Intermodaler-verkehr

QCi

Quantenfehlerkorrektur



Untersuchung und Implementierung von einfachen Quantenfehlercodes auf echter Quantenhardware

eleQtron

parityqc

QCi

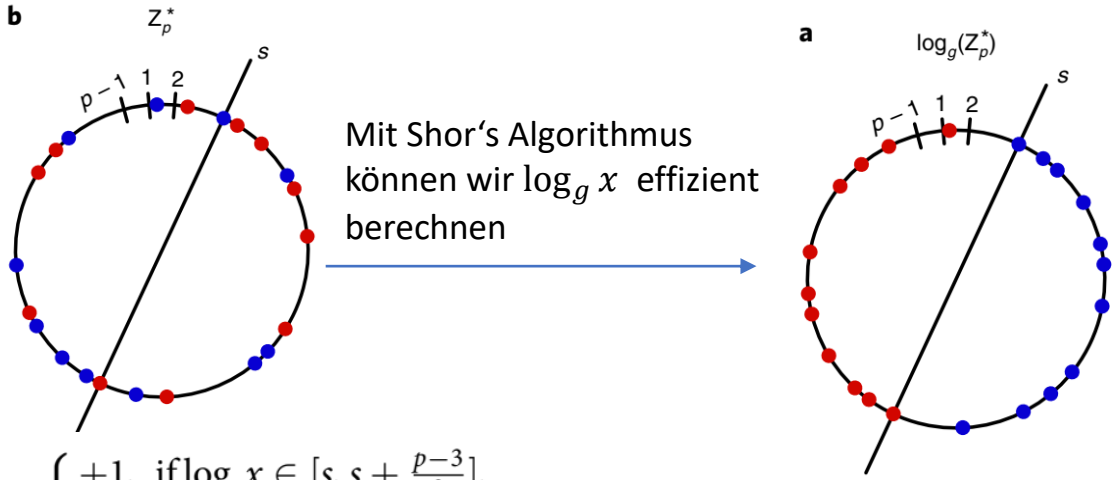
Maschinelles Lernen mit Quantencomputern

- Es existieren Quantenalgorithmen welche (exponentiell) schneller sind als alle bekannten klassischen Algorithmen ⟶ Subroutinen für ML
- Lernen basiert auf Korrelationen und Quantenkorrelationen (Verschränkung) gehen weiter als klassische Korrelationen ⟶ Quantenkernel bringen erhebliche Vorteile für bestimmte Lernprobleme

Biamonte et al., Nature **549**, 195 (2017), arXiv.org: 1611.09347; Dunjko & Briegel, Rep. Prog. Phys. **81**, 074001 (2018), arXiv.org: 1709.02779; Alchieri et al., Qu. Mach. Intell. **3**, 28 (2021)

- In wie weit Quantenkernels Vorteile für klassische Lernprobleme bergen ist derzeitiger Forschungsgegenstand

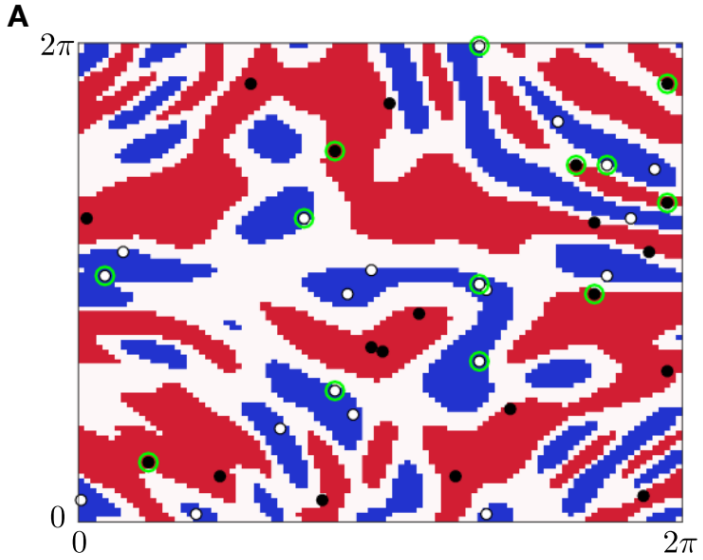
Gyurik & Dunjko: On establishing learning separations between classical and quantum machine learning with classical data (arXiv.org: 2208.06339)



Mit Shor's Algorithmus können wir $\log_g x$ effizient berechnen

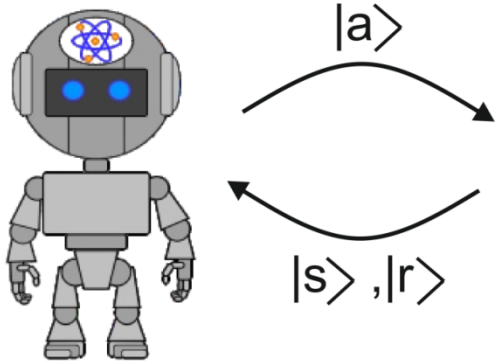
$$f_s(x) = \begin{cases} +1, & \text{if} \log_g x \in [s, s + \frac{p-3}{2}], \\ -1, & \text{else.} \end{cases}$$

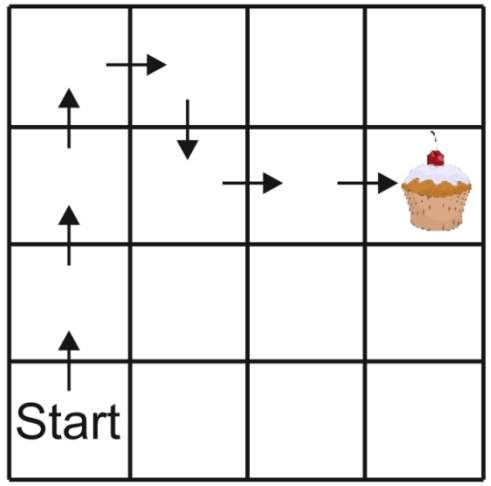
Liu et al., Nature Phys. 17, 1013 (2021), arXiv 2010.02174



Havlicek et al., Nature 567, 209 (2019),arXiv: 1804.11326

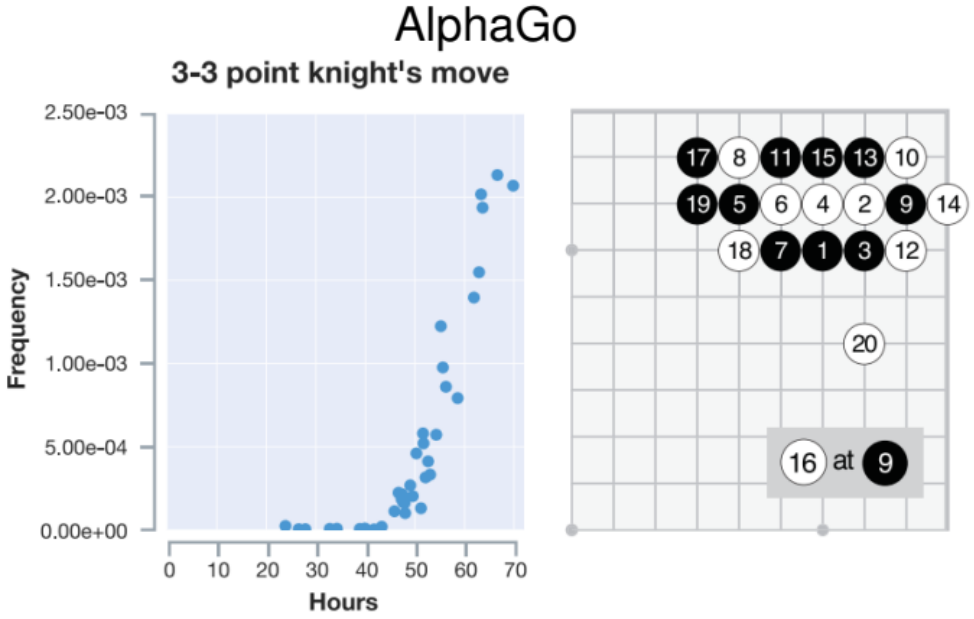
Bestärkendes Lernen



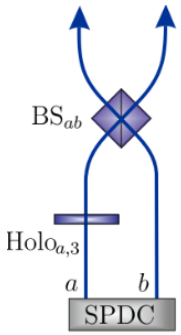


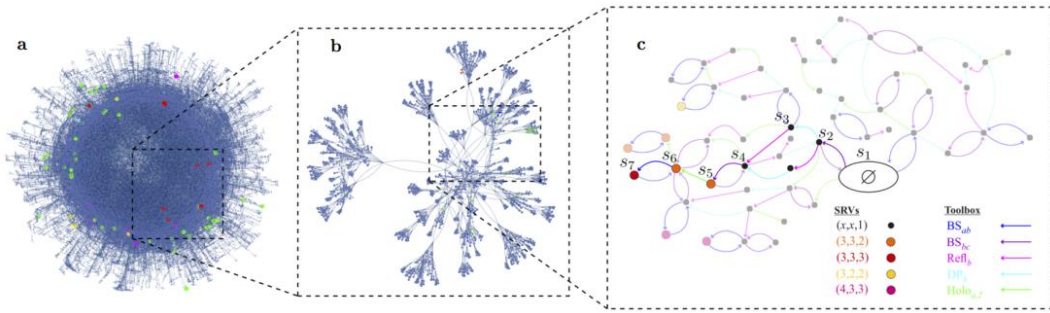
- Wenn Perzept s gegeben führe Aktion a mit Wahrscheinlichkeit π(a|s) aus.
- Update π(a|s) abhängig von der Belohnung r um die erwartete Langzeitbelohnung zu maximieren

$$R_j = \left\langle \sum_{k=0}^{\infty} \gamma^k r_{j+k} \right\rangle \qquad \gamma : \text{discount rate}$$



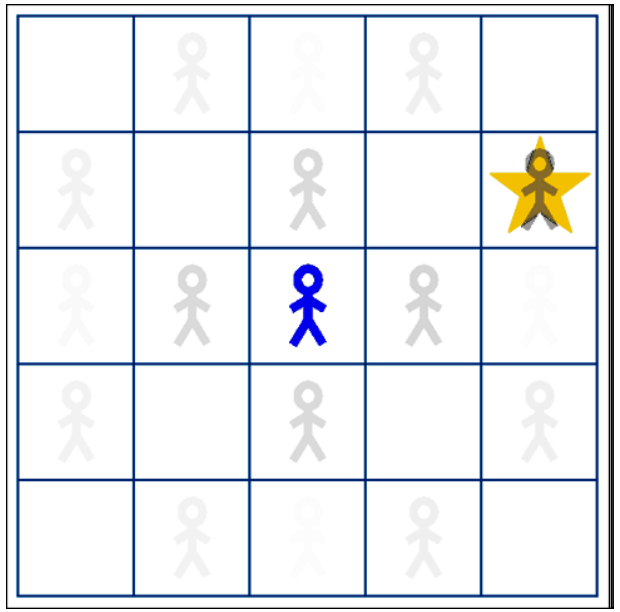
Nature **550**, 354 (2017)





PNAS **115**, 1221 (2018)

Belohnungen mit QC schneller finden



- QC erstellt eine Superposition aller N möglichen Aktionssequenzen: $N=4^3=64$
- Nur log(N)= 6 Qubits sind dafür notwendig

$$|\psi\rangle_A = \frac{1}{\sqrt{N}}(|\uparrow\uparrow\uparrow\rangle + |\uparrow\uparrow\downarrow\rangle + |\uparrow\uparrow\rightarrow\rangle + \cdots)$$

- Die Problemumgebung berechnet die Perzepts s und die Belohnung mittels der Unitären U_E : $|\Phi\rangle_{ASR} = U_E|\psi\rangle_A\,|\emptyset\rangle_S\,|\emptyset\rangle_R = \frac{1}{\sqrt{N}}\sum_{\{\vec{a}\}}|\vec{a}\rangle_A|\vec{s}(\vec{a})\rangle_S|r(\vec{a})\rangle_R$
- Die Gewinnwahrscheinlichkeit beträgt: p_C =3/64 ≈ 5%
- Die “Weginformation s” muss gelöscht werden um Interferenz zu ermöglichen. Mittels Groveriteration erhalten wir so eine Gewinnwahrscheinlichkeit von

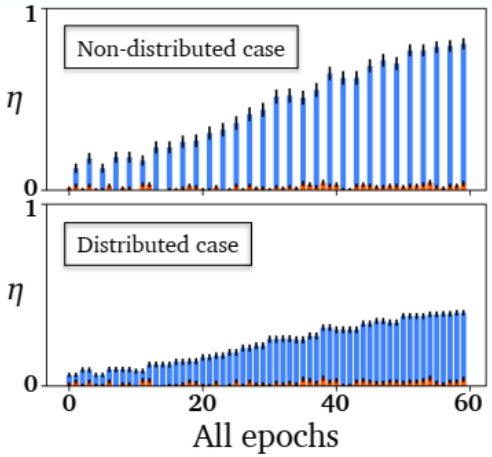
$$p_Q \approx 37{,}5\%$$

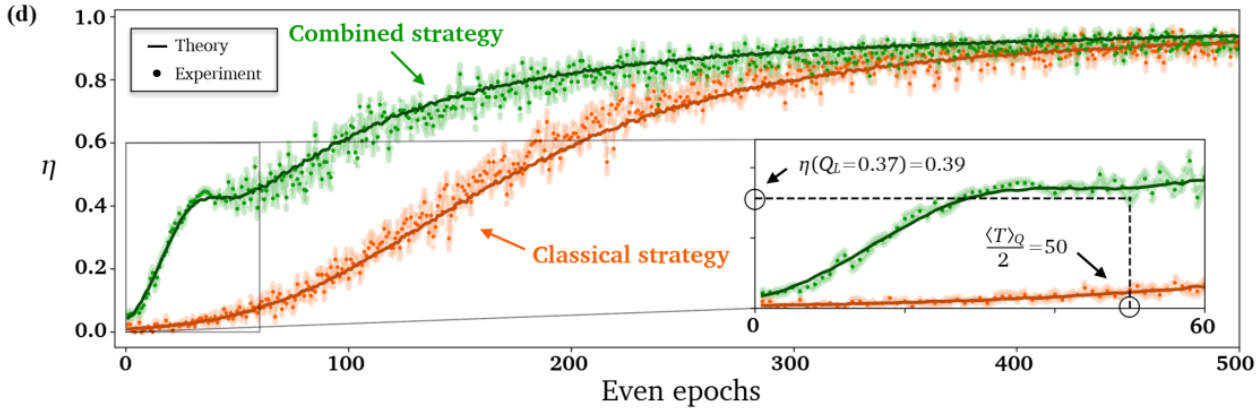
- K Groveriterationen führen zu einer Gewinnwahrscheinlichkeit von

$$p_Q(k) \approx sin^2[(2k+1)\sqrt{p_C}]$$

- Wir können Gewinne quadratisch schneller finden

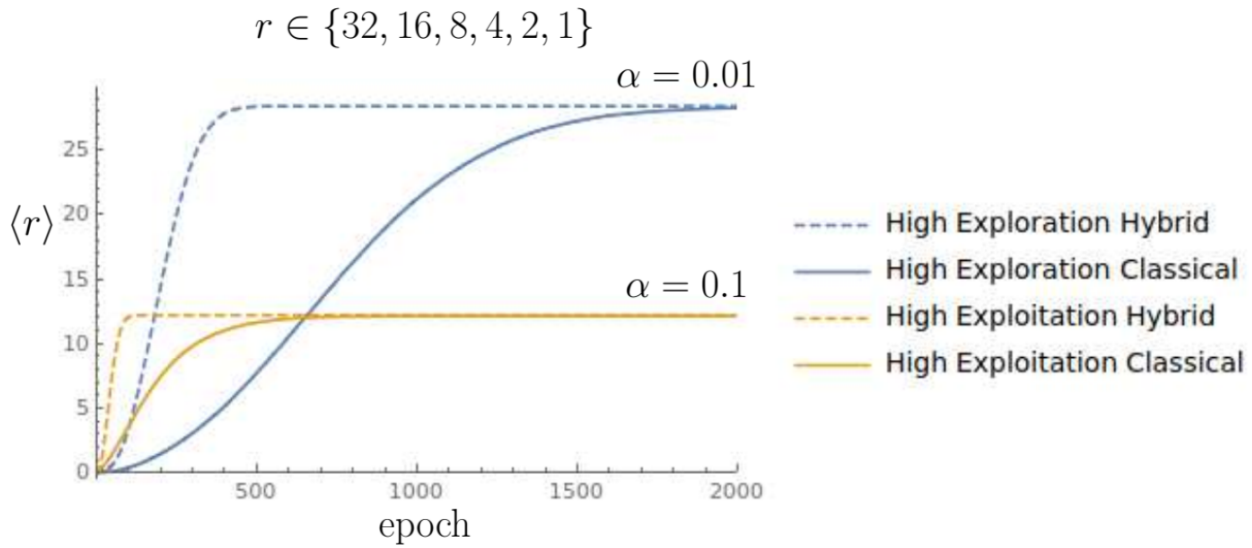
Ergebnisse





T_C= 266
T_Q= 100

V.Saggio et al.,Nature 591, 229 (2021)



A. Hamann and S. Wölk, New J. Phys. 24, 033044 (2022)