THE UNBEARABLE DIFFICULTY

OF FINDING NEAR-TERM QUANTUM ADVANTAGES

JENS EISERT, FU BERLIN

MUNICH 2025

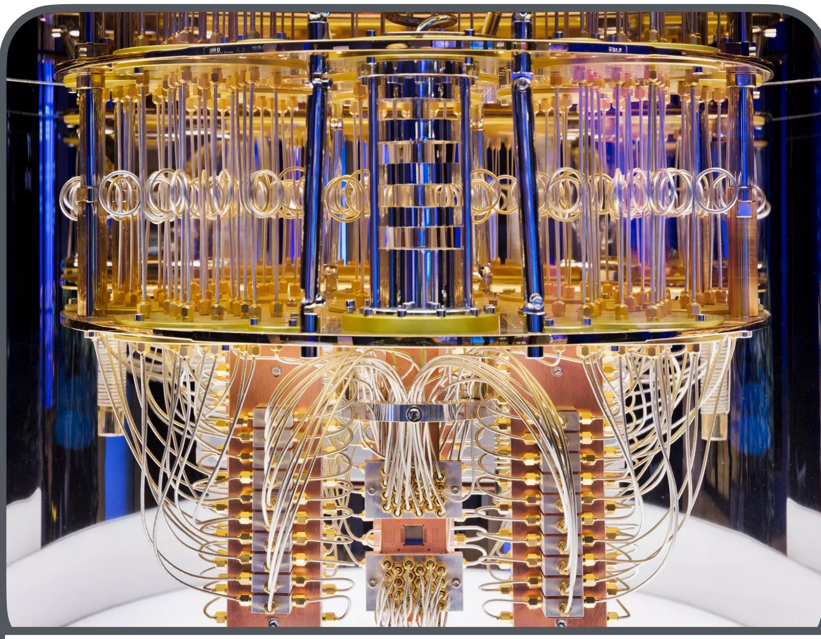
- Quantum computing was a purely conceptual idea

Feynman

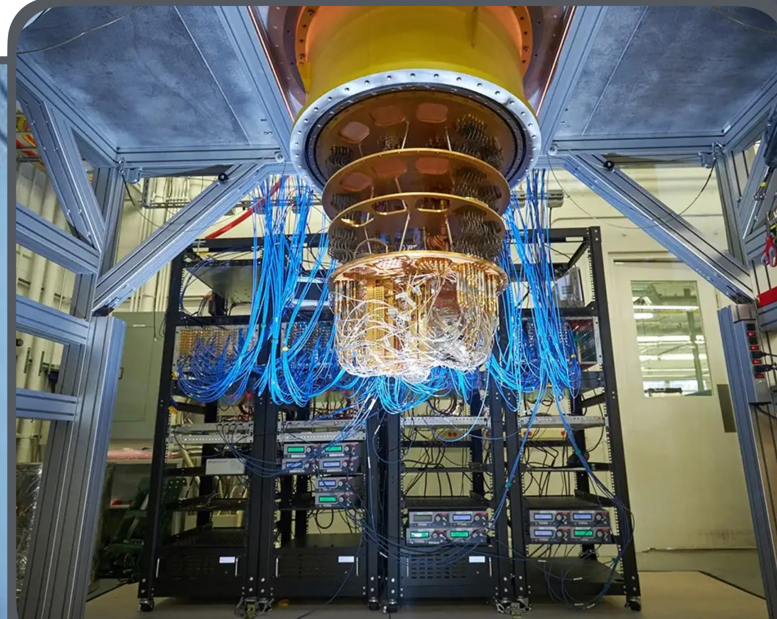
Benioff, Deutsch

Shor

- Seems to be moving closer to reality

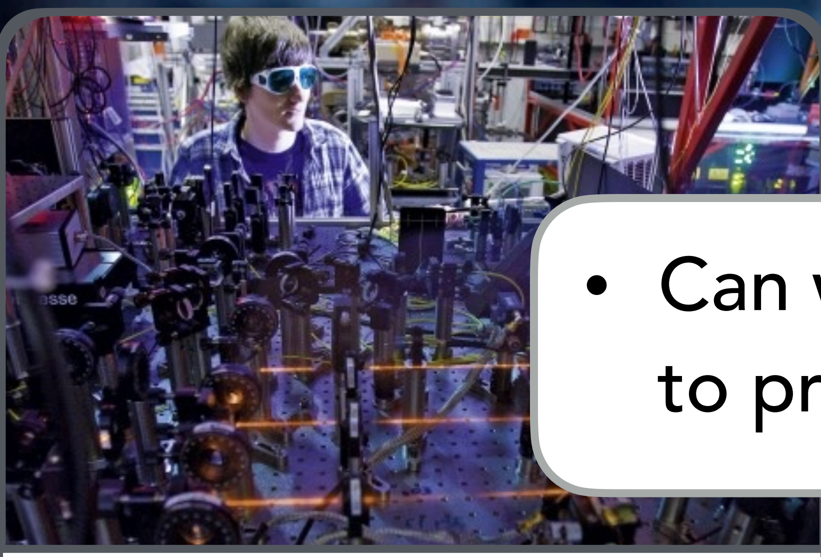


IBM



Google

QuERA



European efforts, MQV, planqc, Pasqal, etc

Chinese efforts

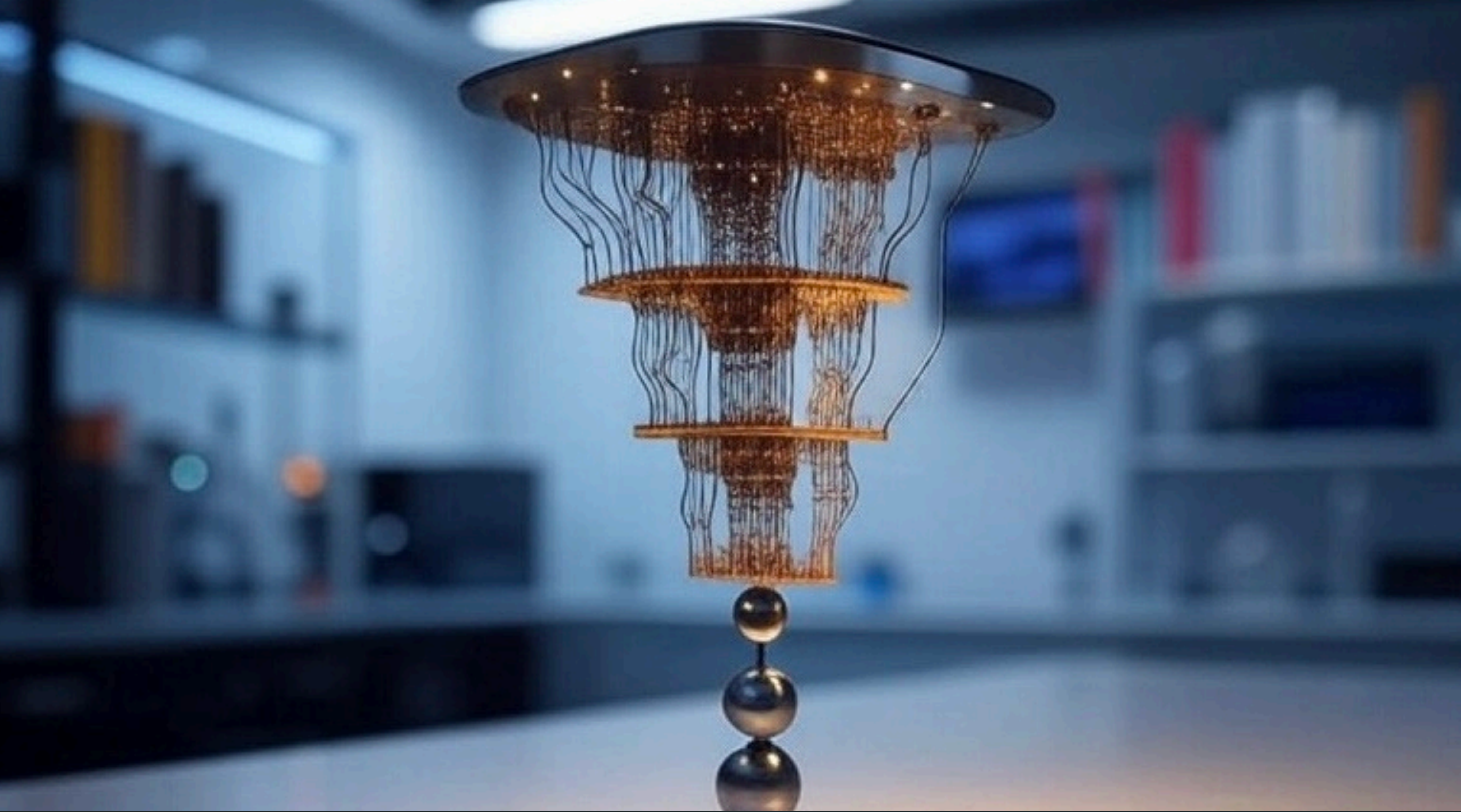
- Can we reasonably hope realistic quantum devices to provide a speedup over classical computers?

- ## Quantum algorithms

Problem	Group	Complexity	Cryptosystem
Factorisation	$\mathbb{Z}$	Polynomial [89]	RSA
Discrete log	$\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$	Polynomial [89]	Diffie-Hellman, DSA, ...
Elliptic curve discrete log	Elliptic curve	Polynomial [76]	ECDH, ECDSA, ...
Principal ideal	$\mathbb{R}$	Polynomial [46]	Buchmann-Williams
Shortest lattice vector	Dihedral group	Subexponential [58, 80]	NTRU, Ajtai-Dwork, ...
Graph isomorphism	Symmetric group	Exponential	–

Montanaro, arXiv:1511.04206 (2015)

- **Potentially controversial:** We do not know as much about **practically minded** problems and **near-term** algorithms as we would like to

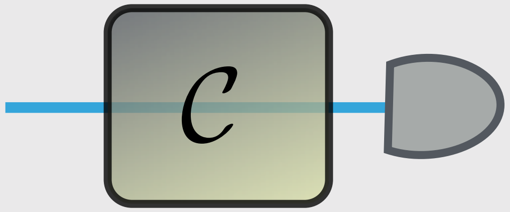


OBSTRUCTIONS FOR NOISY QUANTUM CIRCUITS

arXiv:2502.14252 (2025)
arXiv:2403.13927 (2024)
Nature Communications 15, 434 (2024)

NOISY QUANTUM CIRCUITS

- Actual circuits are **noisy**



Expectation values or samples

Quantum circuit

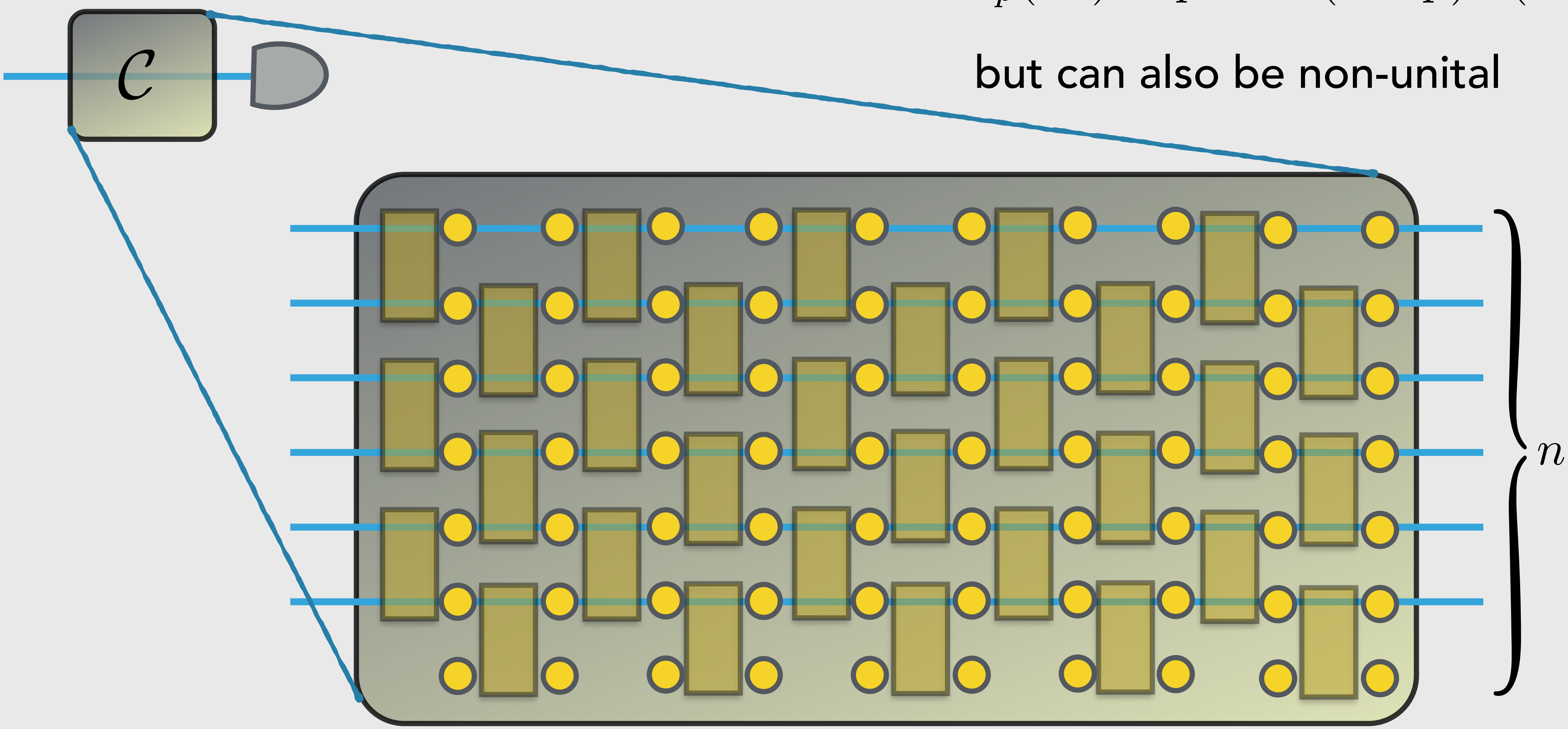
NOISY QUANTUM CIRCUITS

- Actual circuits are **noisy**

- Noise and decoherence, e.g., **depolarizing**

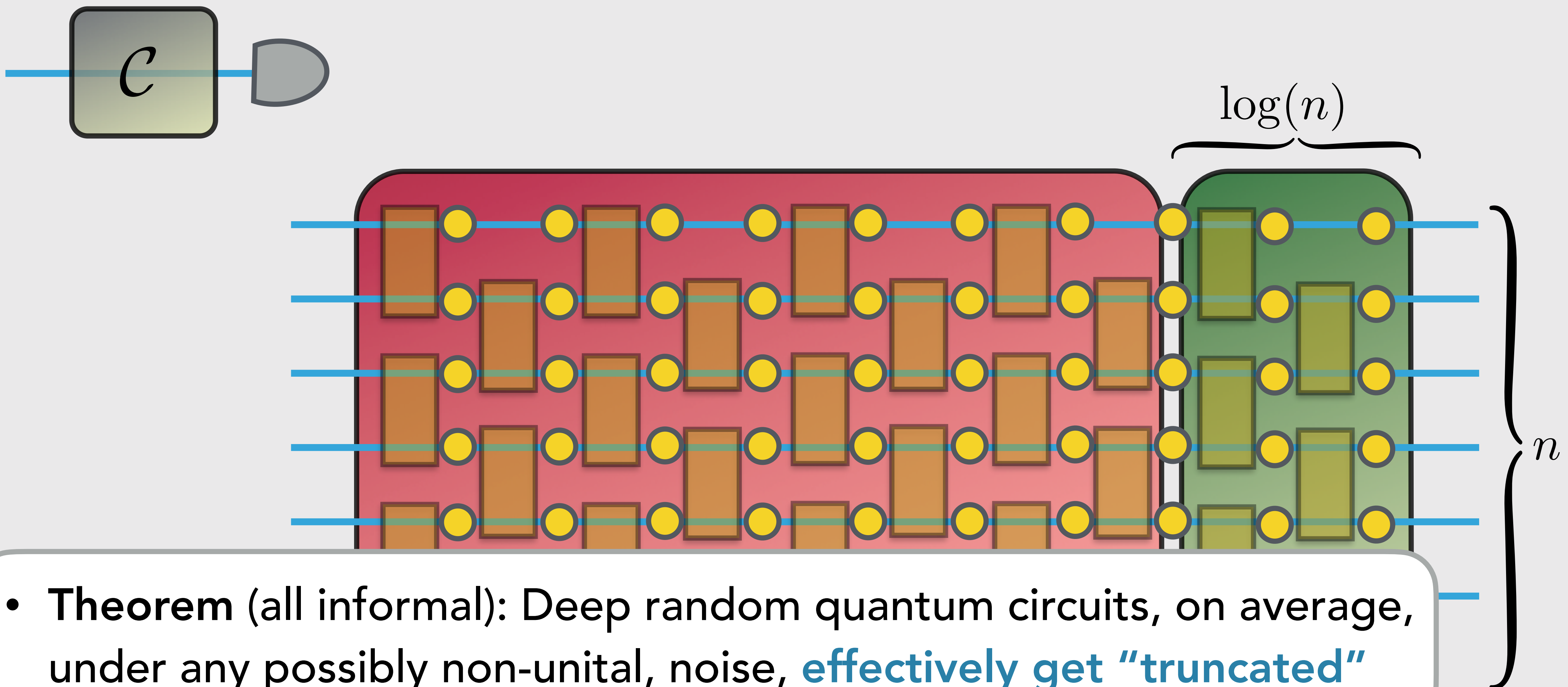
$$\mathcal{D}_p(M) = pM + (1-p)\mathrm{tr}(M)\frac{\mathbb{I}}{2}$$

but can also be non-unital



EFFECTIVE LOGARITHMIC DEPTH

- **Logarithmic depth** is all we have



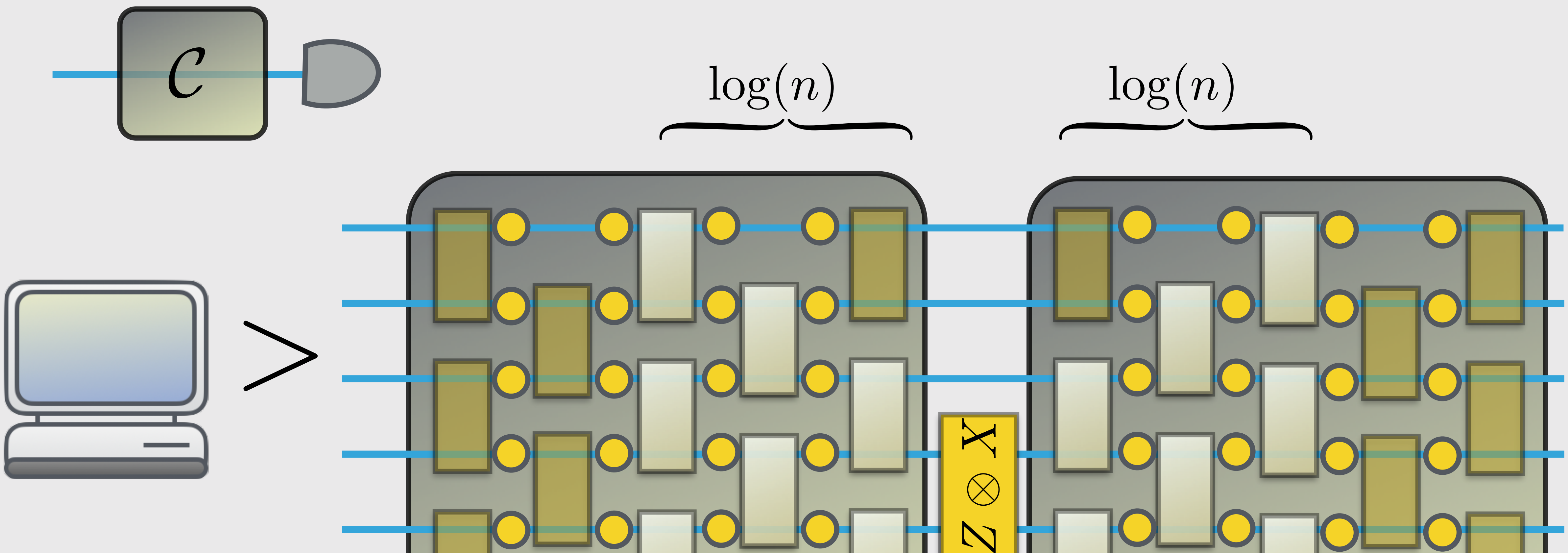
- **Theorem** (all informal): Deep random quantum circuits, on average, under any possibly non-unital, noise, **effectively get "truncated"**

- Influence of gates on Pauli expectation values decreases exponentially

Mele, Angrisani, Ghosh, Khatri, Eisert, Stilck França, Quek, arXiv:2403.13927 (2024)
Compare also Fawzi, Mueller-Herles, Shayeghi, ITCS (2022)

EFFICIENT CLASSICAL SIMULATION

- Can often **"dequantize"**



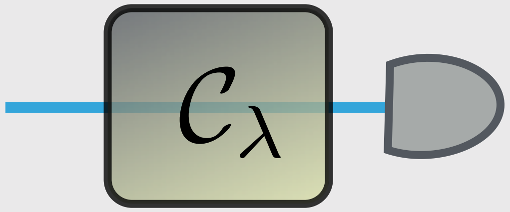
- **Theorem:** Can **classically simulate** on average expectation values observables to ε additive precision, with probability $1-\delta$, at any depth, with runtime of

$$O(\exp\left(\log^D(\delta^{-1}\varepsilon^{-2})\right))$$

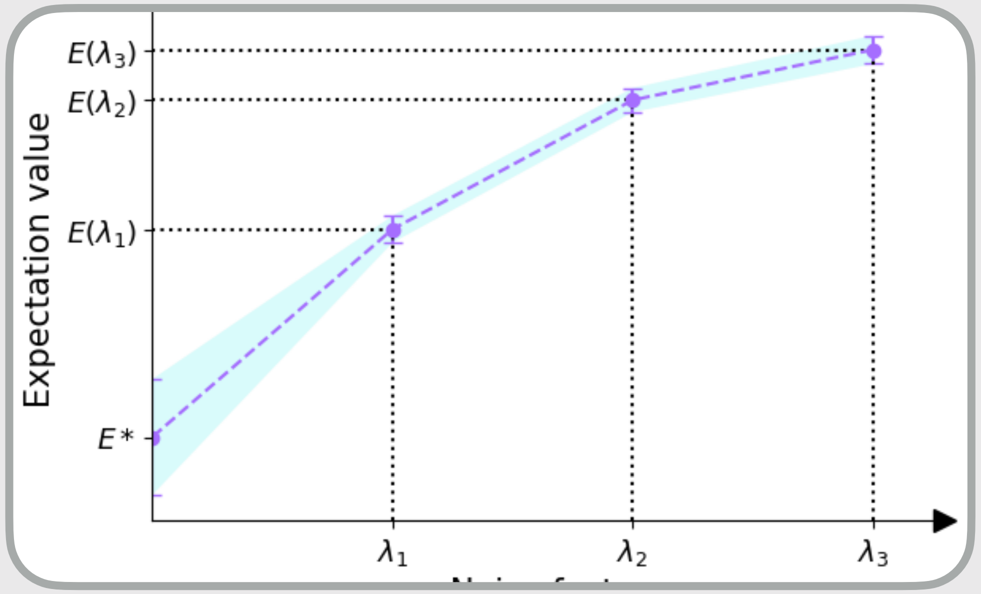
Mele, Angrisani, Ghosh, Khatri, Eisert, Stilck França, Quek, arXiv:2403.13927 (2024)

CAN QUANTUM ERROR MITIGATION HELP?

- **Zero-noise extrapolation**



- Add noise levels to $\mathcal{C}_\lambda$
- Measure $E(\lambda) = \mathrm{tr}(C_\lambda(\rho_{\mathrm{in}})O)$
- Extrapolate to $\lambda = 0$

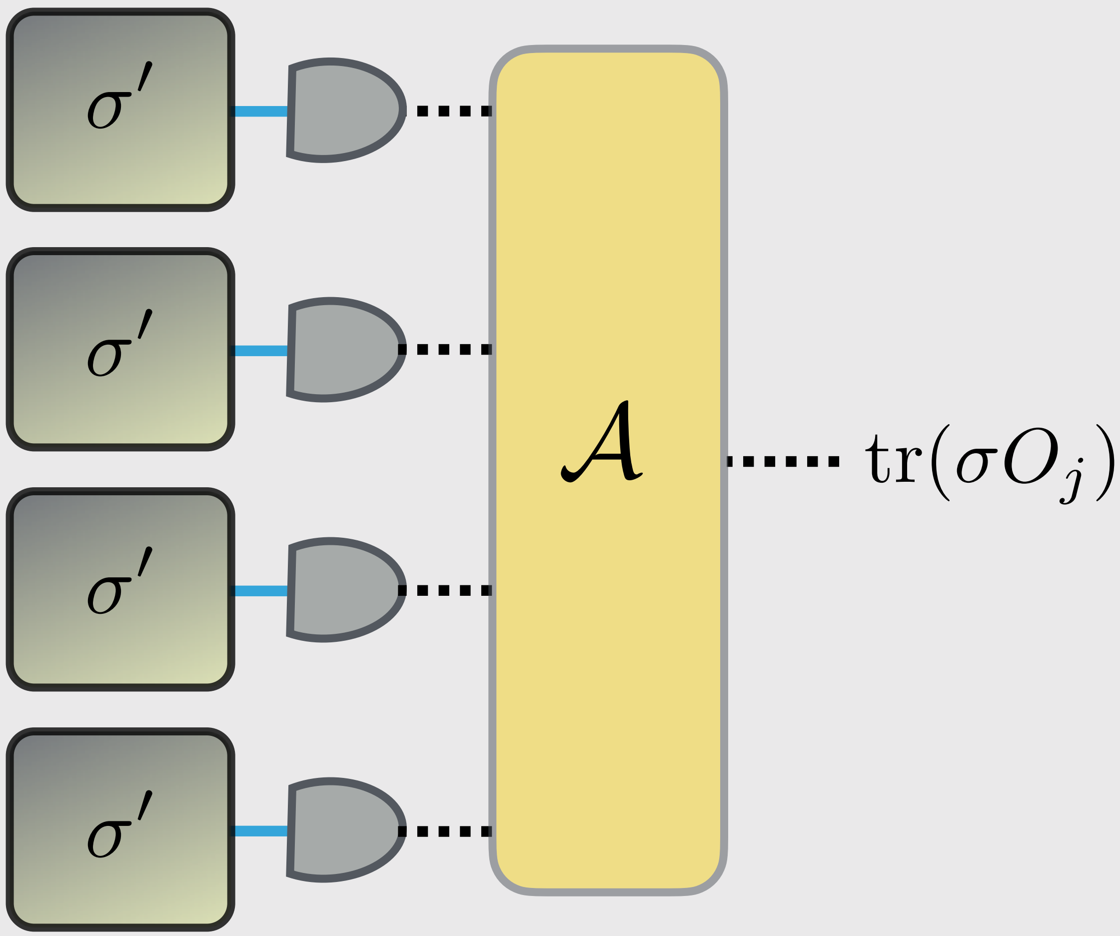


Majumdar, Rivero, Metz, Hasan, Wang, 2023 IEEE Int Conf Quant Comp Eng (2023)

Temme, Bravyi, Gambetta, Phys Rev Lett 119, 180509 (2017)
Cai, Babbush, Benjamin, Endo, Huggins, Li, McClean, O'Brien, arXiv:2210.00921 (2022)

OUR ABSTRACTION

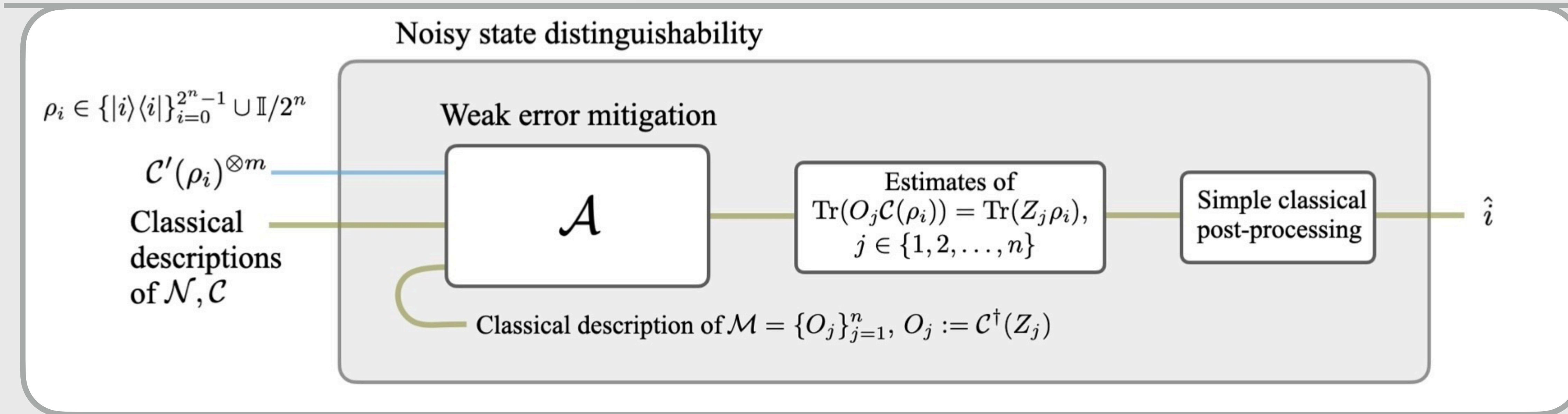
- How many copies of σ' are needed to estimate $\mathrm{tr}(\sigma O_j)$ for $O_j \in \mathcal{M}$ to precision ε and probability $1-\delta$?

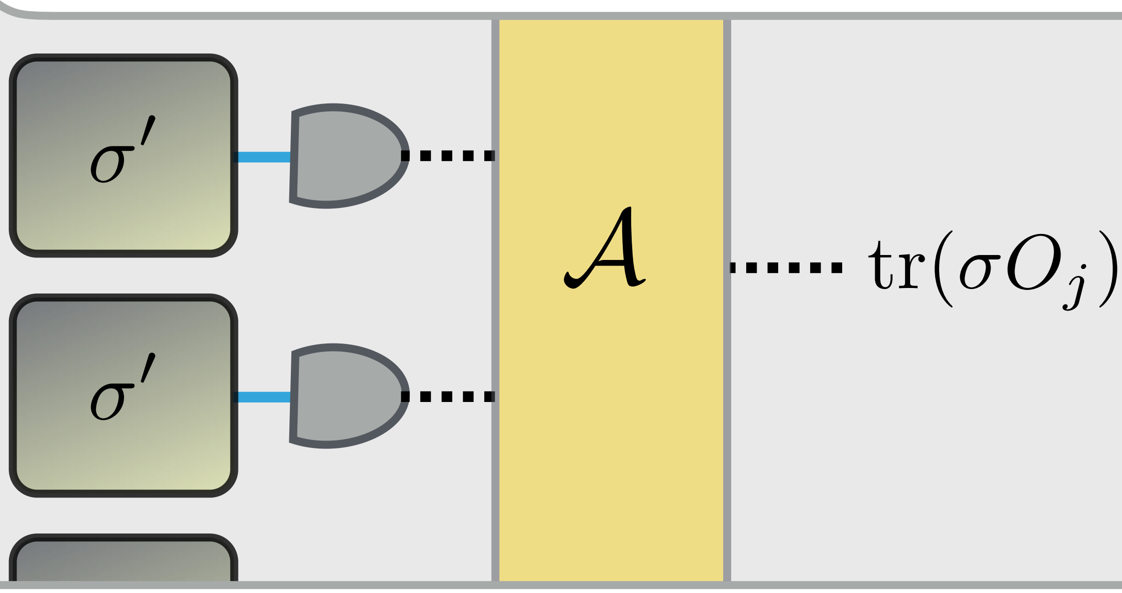


- **Statistical inference problem**
  - in terms of circuit depth d
  - circuit width n
  - depolarizing noise strength p

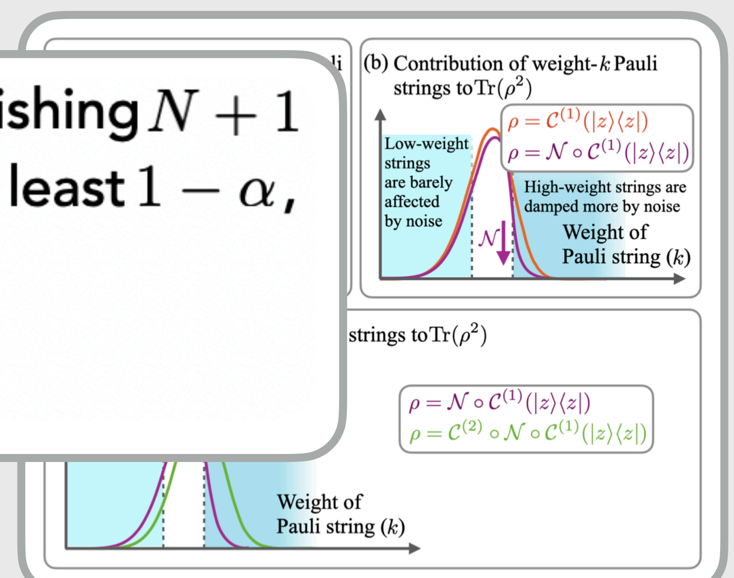
Quek, Stilck França, Khatri, Meyer, Eisert, Nature Physics 20, 1648 (2024)

PROOF TECHNIQUES





- **Proof techniques**
  - Multi-hypothesis testing
  - Fano's Lemma
  - Log-depth Clifford circuits approximate unitary 2-designs



- Use **Fano's Lemma**: Any single-sample test distinguishing $N+1$ distributions $P_1, \ldots, P_N$ must fail with probability at least $1-\alpha$,

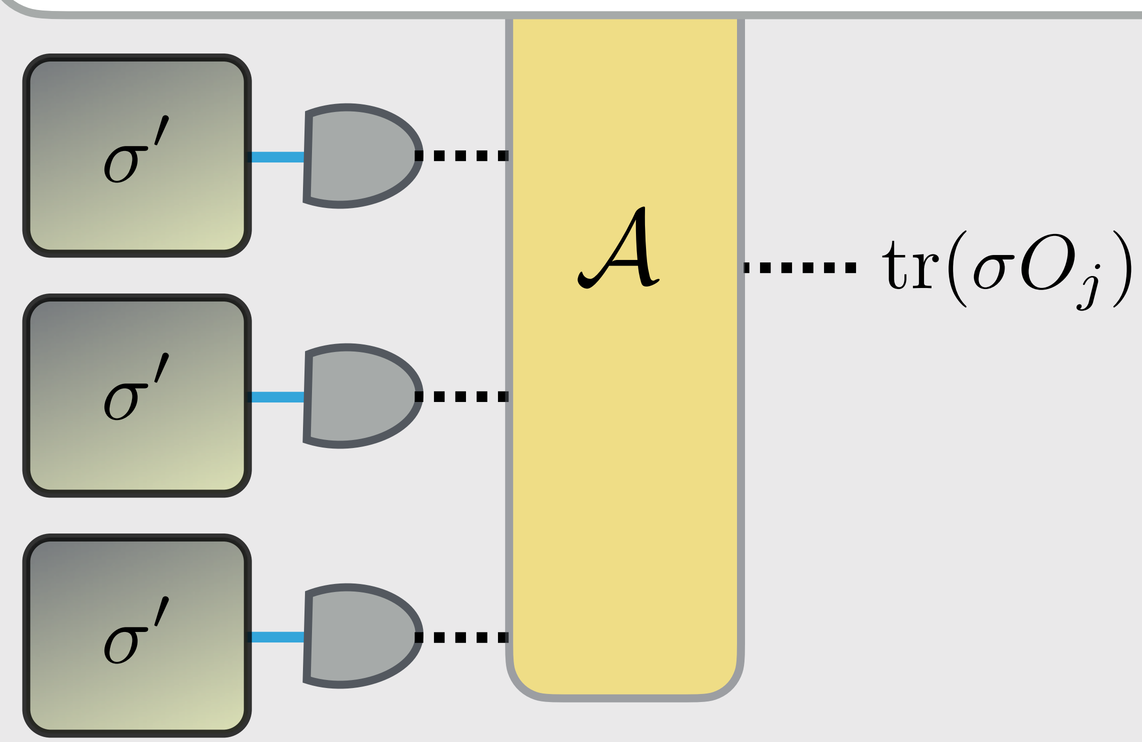
$$\frac{1}{\log(N)} \frac{1}{N+1} \sum_{k=0}^{N} D(P_k \| P_N) \leq \alpha$$

Quek, Stilck França, Khatri, Meyer, Eisert, Nature Physics 20, 1648 (2024)

OUR RESULTS

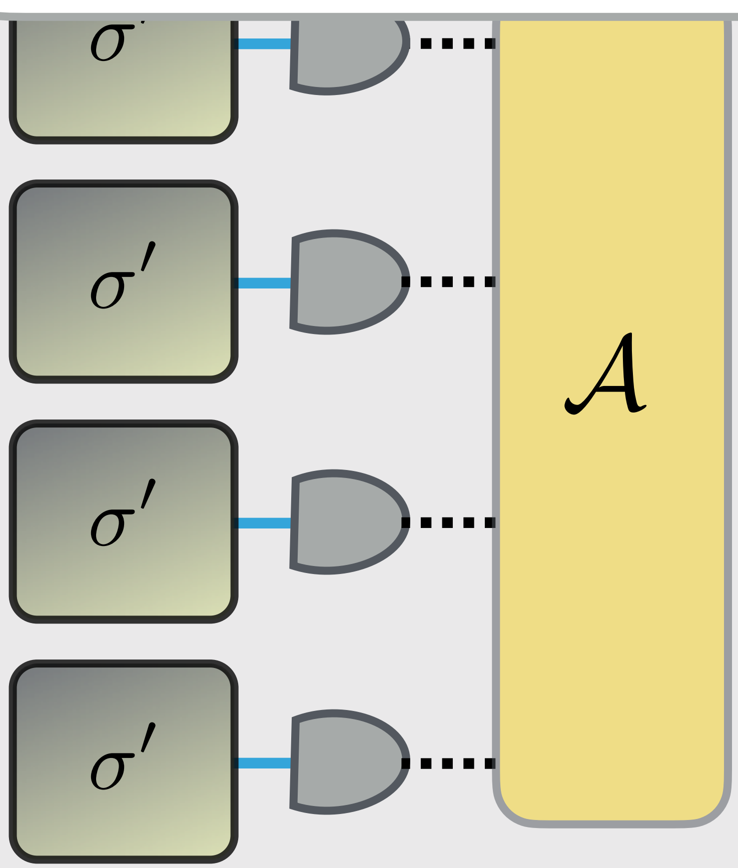
- **Theorem** (informal): One needs $\exp(\Omega(nd))$ **many samples**
- Previously thought: $\exp(\Omega(d))$, and since in NISQ regime $d = O(\log(n))$, our results are **exponentially** stronger

Takagi, Endo, Minagawa, Gu, npj Quant Inf 8, 114 (2022)
Takagi, Tajima, Gu, arXiv:2208.09178 (2022)



Quek, Stilck França, Khatri, Meyer, Eisert, Nature Physics 20, 1648 (2024)

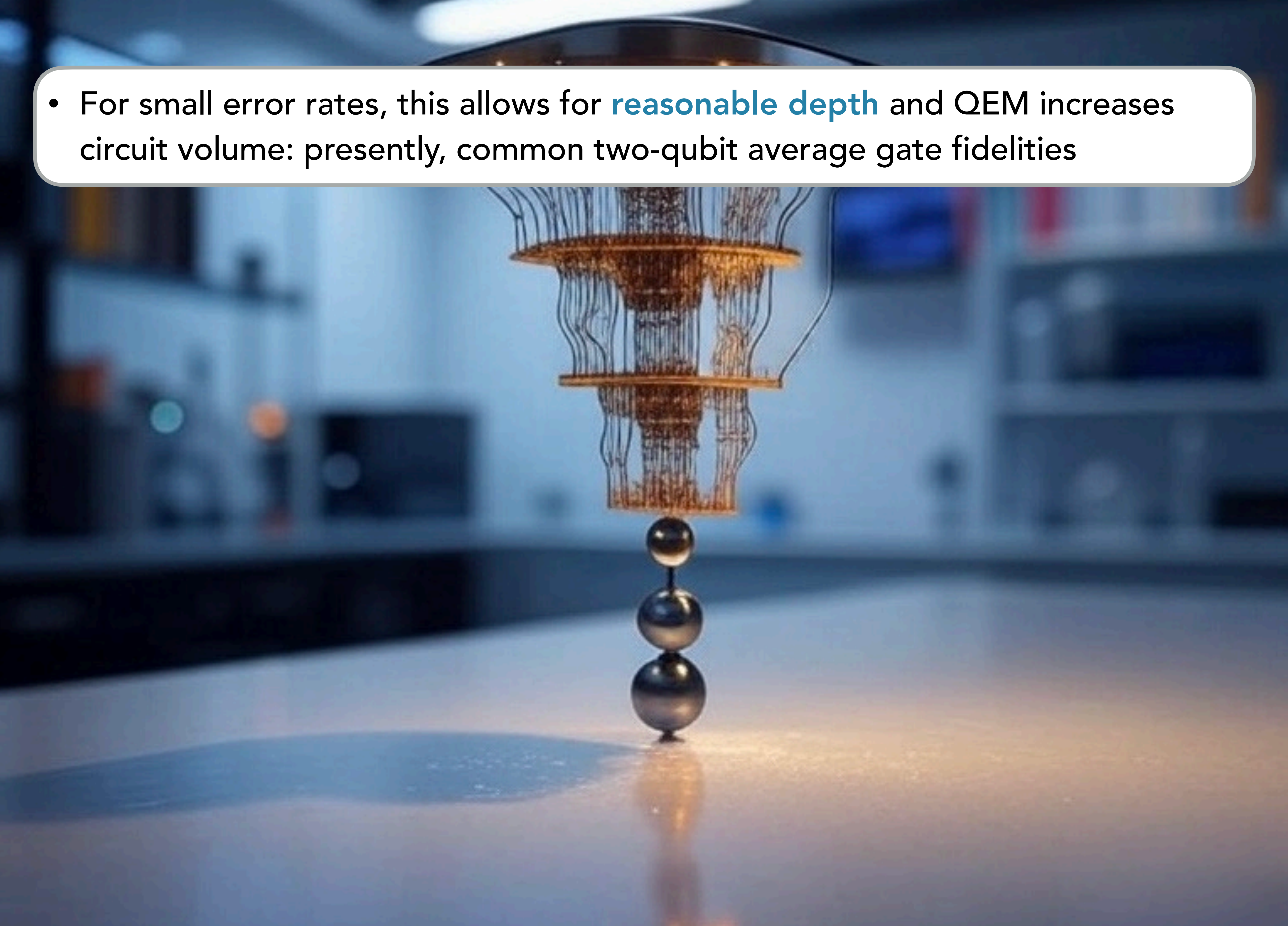
- There are **strong obstructions against error mitigation** already at log-log depth in worst case



- Does **not** mean it does not work: It does not **scale** and not work well **for all circuits**
  Compare also Gonzales-Garcia, Trivedi, Cirac, arXiv:2203.15632 (2022)
- Depolarizing noise catastrophic, non-unital noise allows **quantum refrigeration**
  Ben-Or, Gottesman, Hassidim, arXiv:1301.1995 (2013)

Quek, Stilck França, Khatri, Meyer, Eisert, Nature Physics 20, 1648 (2024)

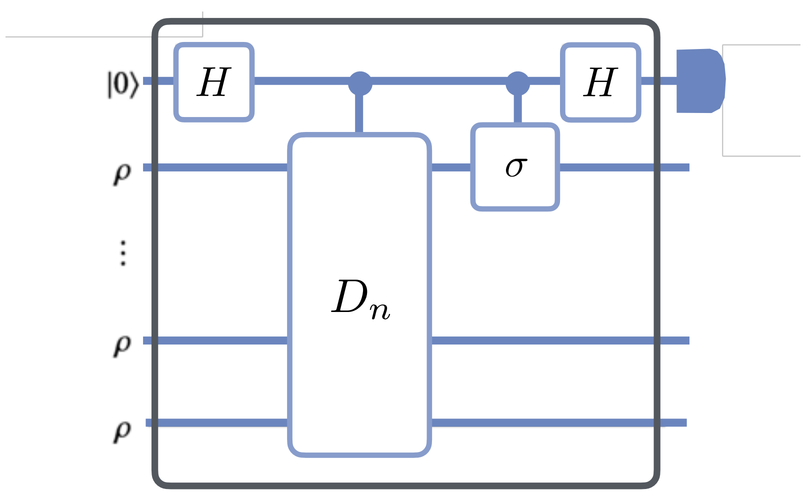
- For small error rates, this allows for **reasonable depth** and QEM increases circuit volume: presently, common two-qubit average gate fidelities

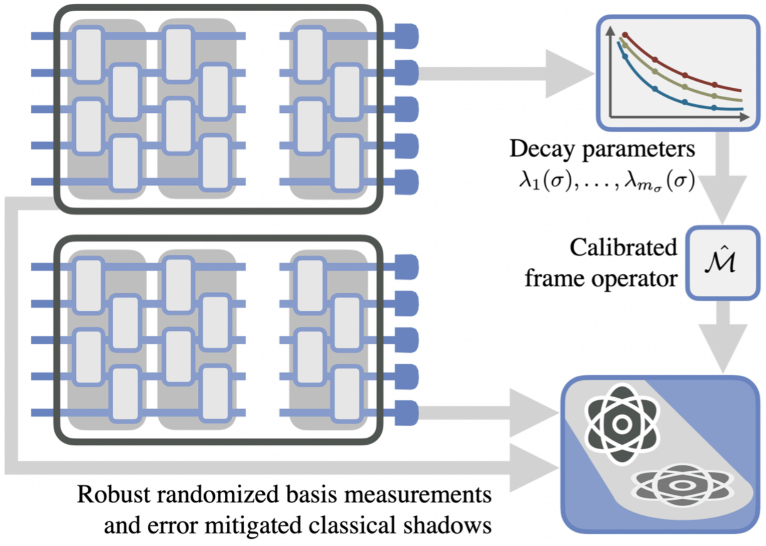


https://www.physik.fu-berlin.de/en/einrichtungen/ag/ag-eisert

- For small error rates, this allows for **reasonable depth** and QEM increases circuit volume: presently, common two-qubit average gate fidelities

- More intermediate steps: **coherent** quantum error mitigation



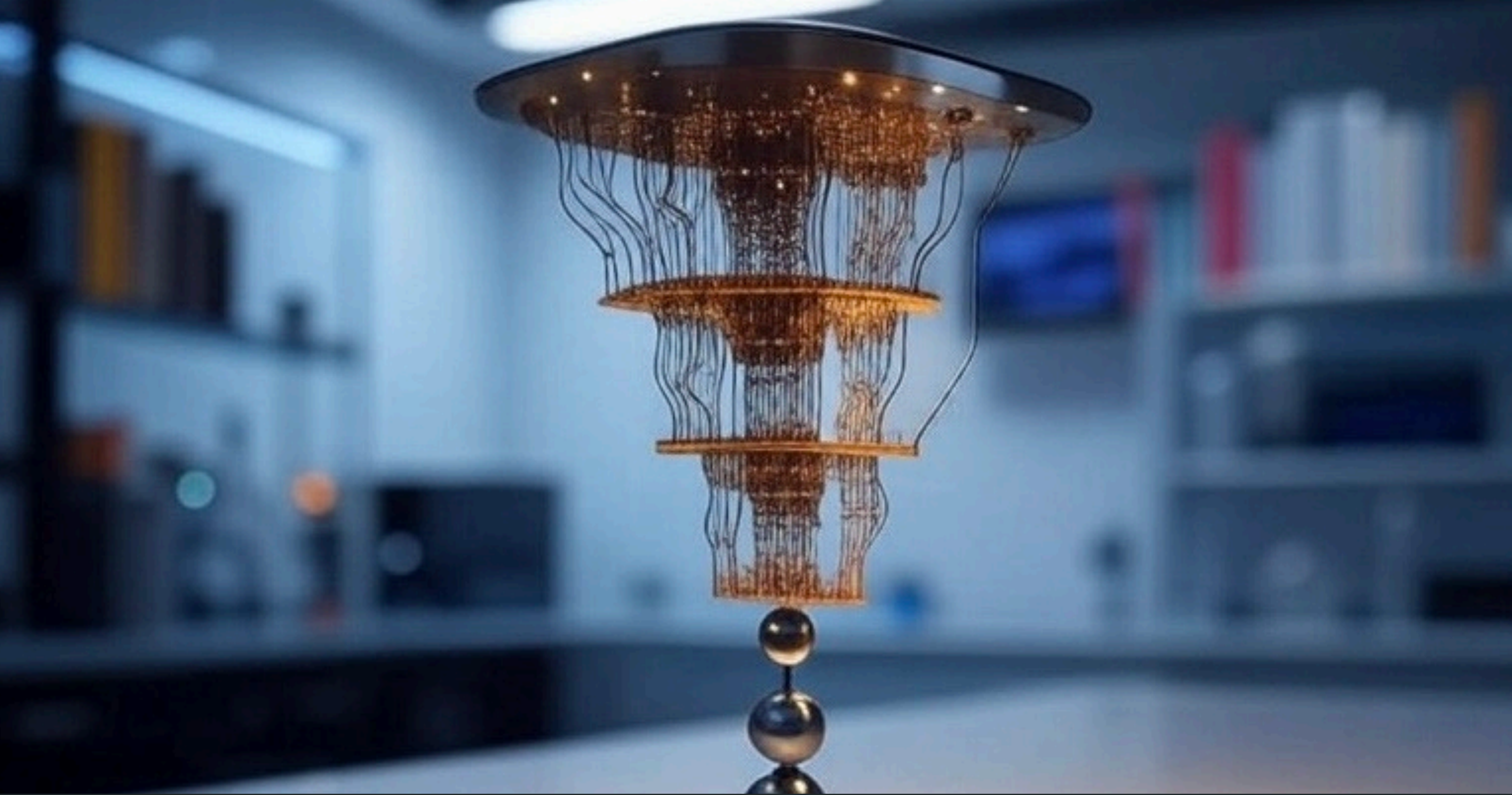


Onorati, Kitzinger, Helsen, Ioannou, Werner, Roth, Eisert, arXiv:2403.04751 (2024)
Seif, Cian, Zhou, Chen, Jiang, arXiv:2203.07309 (2022)
Koczor, Phys Rev X 11, 031057 (2021)
Huggins et al Phys Rev X 11, 041036 (2021)

- Steps **between** mitigation and fault tolerance, or virtual quantum channel purification - and will remain

Suzuki, Endo, Fujii Tokunaga, PRX Quantum 3, 010345 (2022)
Liu, Zhang, Fei, Cai, arXiv:2402.07866 (2024)

D_n



IS THERE HOPE FOR USEFUL NEAR-TERM ALGORITHMS?

arXiv:2502.14252 (2025)
arXiv:2505.04705 (2025)
arXiv:2505.15913, Phys Rev Lett, in press (2025)
arXiv:2411.15548 (2024)
Nature Comm 15, 9595 (2024)

CONSTANT DEPTH ADVANTAGES?

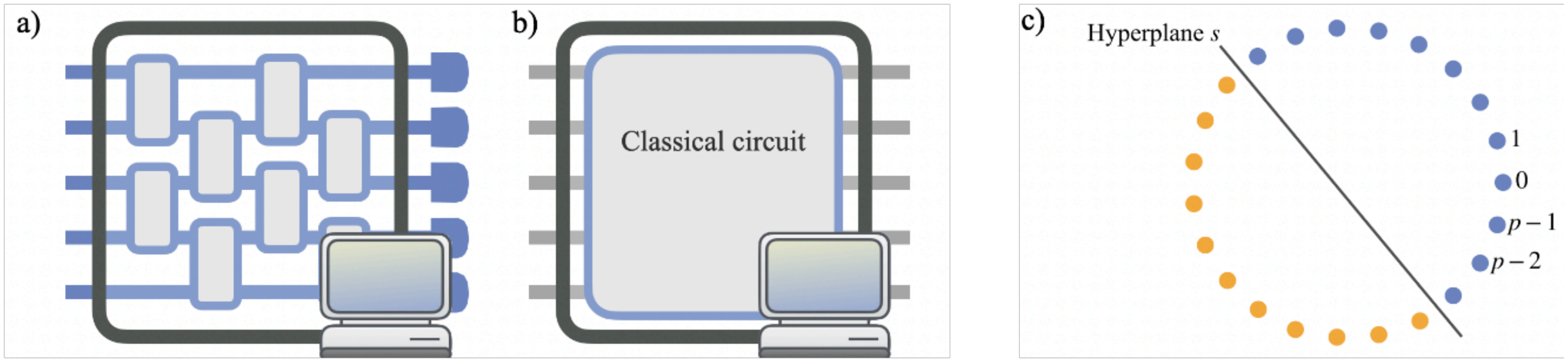
- Are there **constant depth** quantum advantages with a “practical feel”?

Pirnay, Jerbi, Seifert, Eisert, arXiv:2411.15548 (2024)

Compare Huang, Liu, Broughton, Kim, Anshu, Landau, McClean, arXiv:2401.10095 (2024)

CONSTANT DEPTH ADVANTAGES?

- **Theorem:** There is a PAC learning advantage for shallow quantum circuits



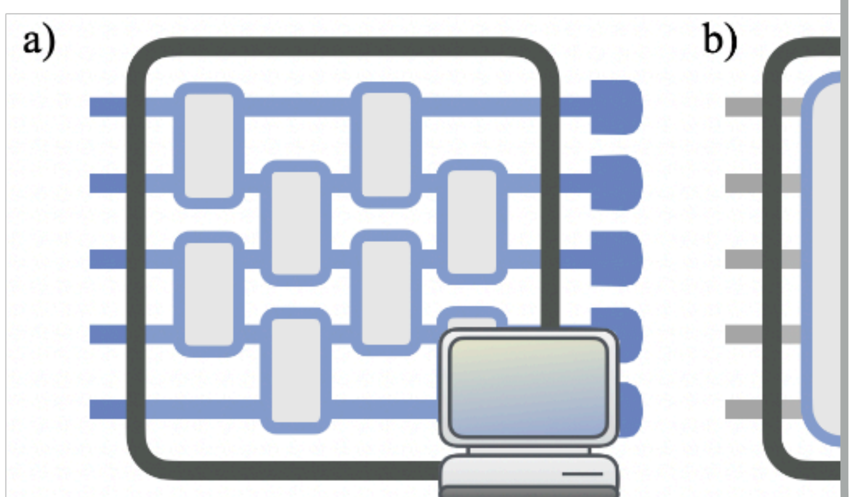
- **Proof techniques**
  - Construct concept classes from quantum advantages from shallow circuits

- **Features**
  - Constant-depth quantum vs $\omega(\log\log(n))$ (NC^0) circuits
  - Classical and artificial data
  - Near-term quantum computer

Pirnay, Jerbi, Seifert, Eisert, arXiv:2411.15548 (2024)
Compare Huang, Liu, Broughton, Kim, Anshu, Landau, McClean, arXiv:2401.10095 (2024)
Building on Bene Watts, Parham, arXiv:2301.00995 (2013)
Bravyi, Gosset, König, Science 362, 308 (2018)

CONSTANT DEPTH ADVANTAGES?

- **Theorem:** There is a PAC learning advantage for shallow quantum circu



- **"Probably approximately correct" learning of distribution classes**
  - A distribution class $\mathcal{C}$ is efficiently PAC learnable w.r.t. distance d if there is an algorithm $\mathcal{A}$ which for every $D \in \mathcal{C}$ and every $\epsilon, \delta > 0$ given access to an oracle $O(D)$, outputs in time $\mathrm{poly}(|D|, 1/\epsilon, 1/\delta)$
  - with probability at least $1 - \delta$ ("probably") a generator $\mathrm{GEN}_{D'}$
  - of a distribution D' such that

$$d(D, D') < \epsilon$$

("approximately correct")

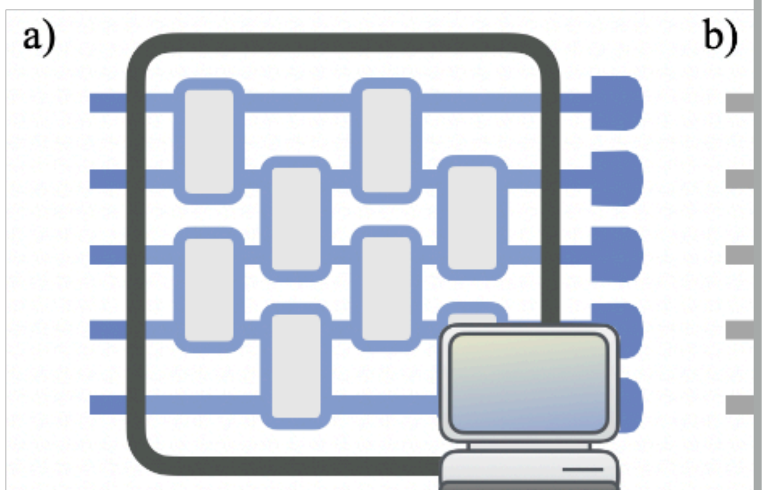
- **Proof techniques**
  - Construct concept classes from quantum advantages from shallow circuits

- **Features**
  - Constant-depth quantum vs $\omega(\log\log(n))$ (NC^0) circuits
  - Classical and artificial data
  - Near-term quantum computer

Pirnay, Jerbi, Seifert, Eisert, arXiv:2411.15548 (2024)
Compare Huang, Liu, Broughton, Kim, Anshu, Landau, McClean, arXiv:2401.10095 (2024)
Building on Bene Watts, Parham, arXiv:2301.00995 (2013)
Bravyi, Gosset, König, Science 362, 308 (2018)

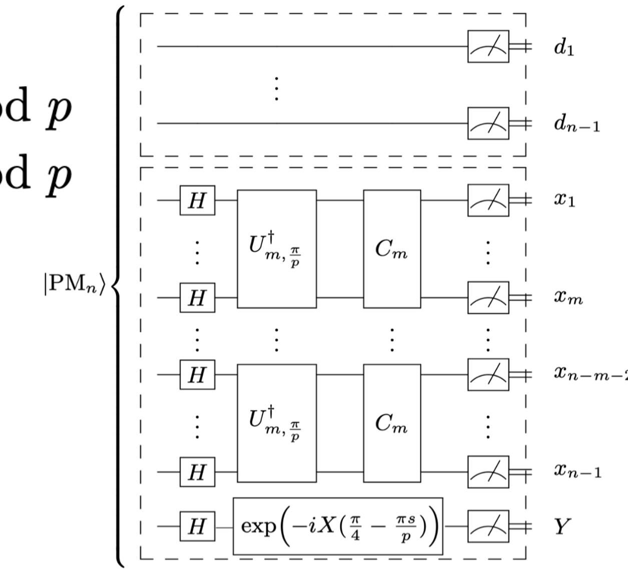
CONSTANT DEPTH ADVANTAGES?

- **Theorem:** There is a PA
  for shallow quantum ci



- Core idea: Devise a PAC generator learning advantage from an unconditional sampling advantage of QNC⁰ over NC⁰
- Encode hyperplane learning problem into the "majority mod p"

$$\text{majmod}_{p,s}(x) = \begin{cases} 0, \text{ if } |x| + s < p/2 & \text{mod } p \\ 1, \text{ if } |x| + s > p/2 & \text{mod } p \end{cases}$$



Building on Bene Watts, Parham, arXiv:2301.00995 (2013)
Bravyi, Gosset, König, Science 362, 308 (2018)

- ## Proof techniques
  - Construct concept classes from quantum advantages from shallow circuits
  - Constant-depth quantum vs $\omega(\log\log(n))$ (NC⁰) circuits
  - Classical and artificial data
  - Near-term quantum computer

- **Lesson:** Think of first applications beyond sampling

Jerbi, Seifert, Eisert, arXiv:2411.15548 (2024)
Compare Huang, Liu, Broughton, Kim, Anshu, Landau, McClean, arXiv:2401.10095 (2024)
Building on Bene Watts, Parham, arXiv:2301.00995 (2013)
Bravyi, Gosset, König, Science 362, 308 (2018)

STATE HIDDEN SUBGROUP PROBLEM

- Are there **simple learning algorithms**?

- Identifying the **symmetry properties** of quantum states

- **Definition** [State hidden subgroup problem] Let G be a finite group with a unitary representation $R : G \to \mathcal{H}$ acting on the Hilbert space $\mathcal{H}$ and let $H \leq G$ be a subgroup of G. Assume you have access to copies of an unknown state vector $|\psi\rangle \in \mathcal{H}$ that is promised to have the properties

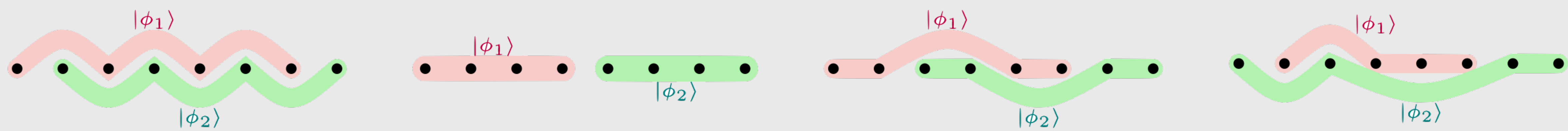
  1. $\forall\, h \in H, \quad R(h)\,|\psi\rangle = |\psi\rangle$
  2. $\forall g \notin H, \quad |\langle\psi|R(g)|\psi\rangle| \leq 1 - \epsilon$

  The problem is to identify H

Bouland, Giurgica-Tiron, Wright, arXiv:2410.12706 (2024)

STATE HIDDEN SUBGROUP PROBLEM

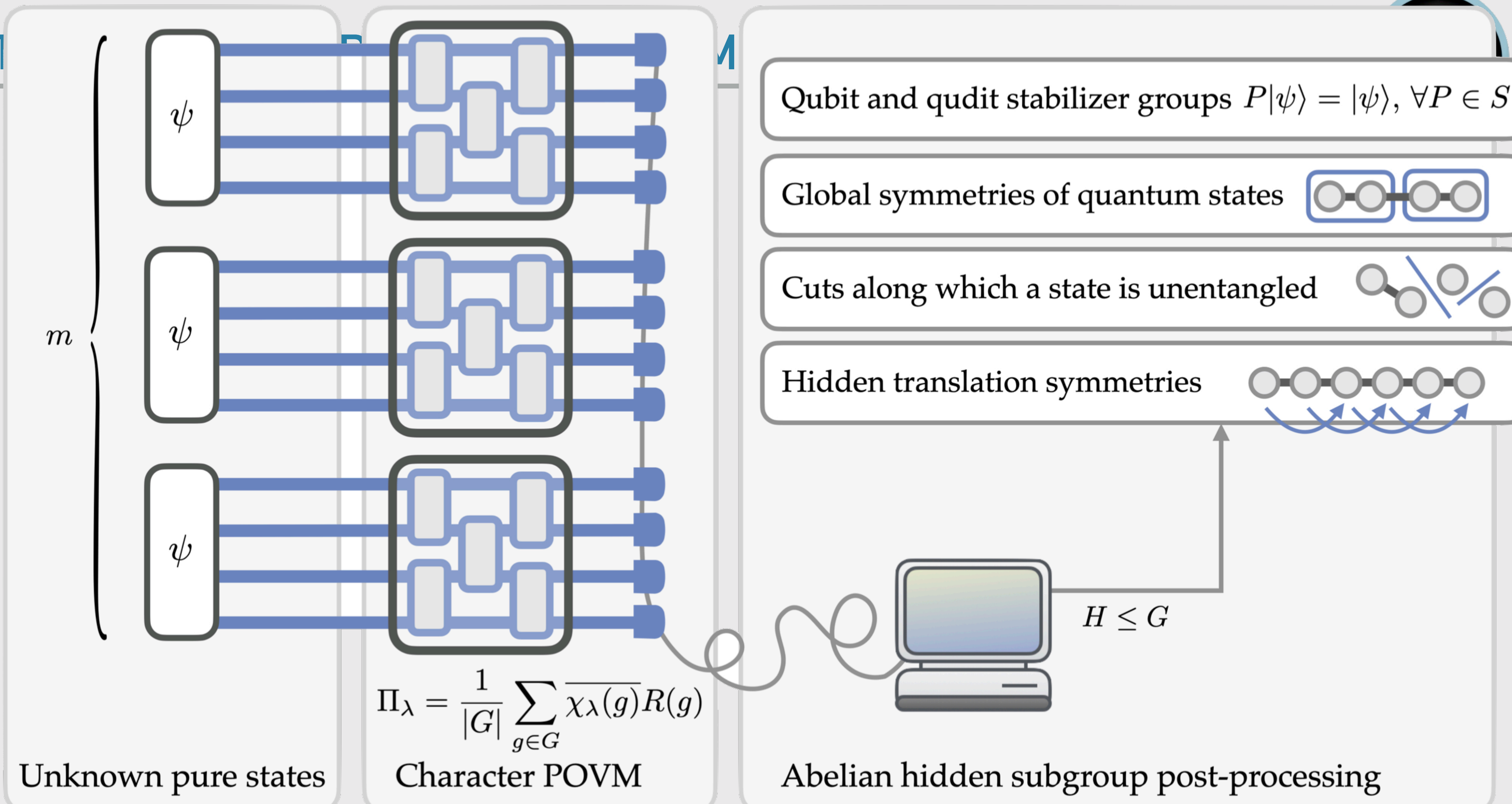
- Their application: Find "hidden cuts" along which pure states are unentangled



- **Our contribution:** Understand representation theory of problem and define "character POVM"

$$\Pi_\lambda = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_\lambda(g)} R(g)$$

Hinsche, Eisert, Carrasco, arXiv:2505.15770 (2025)
Perez-Salinas, Hinsche, Eisert, Carrasco, in preparation (2025)



- **Our contribution:** Understand representation theory of problem and define "character POVM"

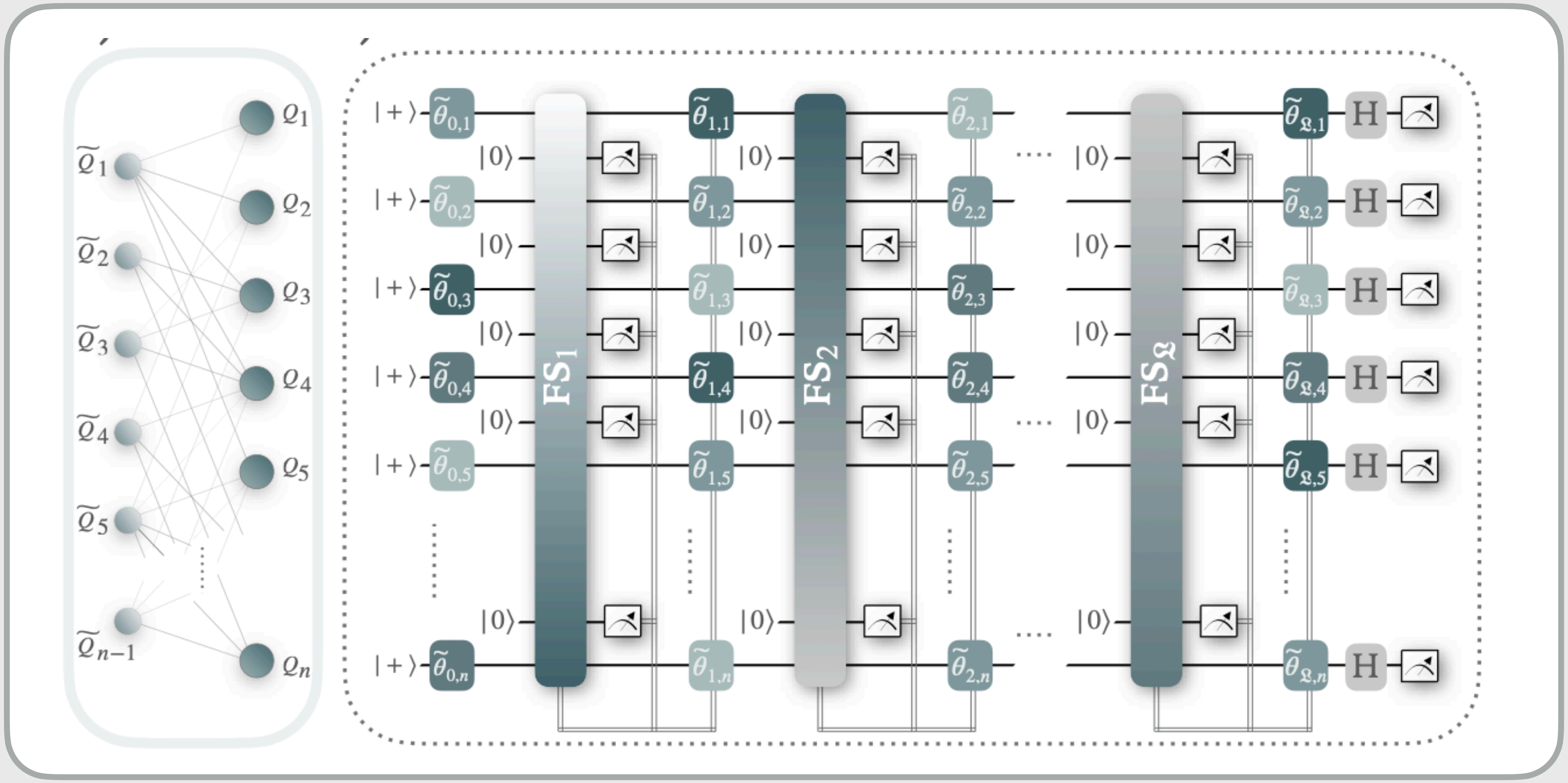
$$\Pi_\lambda = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_\lambda(g)}R(g)$$

- **Lesson:** Is relatively near-term

Hinsche, Eisert, Carrasco, arXiv:2505.15770 (2025)
Perez-Salinas, Hinsche, Eisert, Carrasco, in preparation (2025)

MID-CIRCUIT MEASUREMENTS

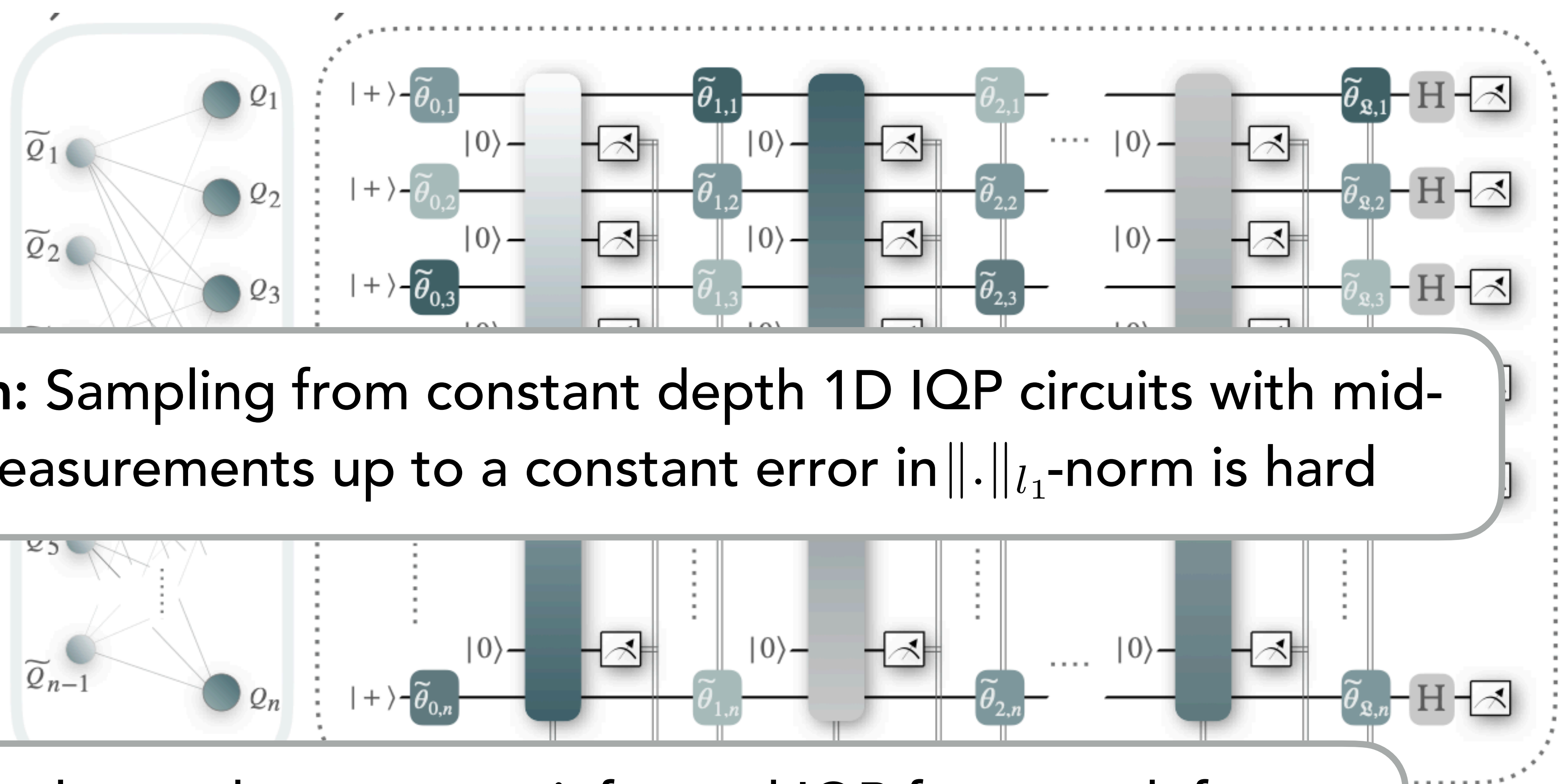
- Can **mid-circuit measurements** help?



Cao, Eisert, arXiv:2505.04705 (2025)
Cao, Eisert, in preparation (2025)

MID-CIRCUIT MEASUREMENTS

- Can mid-circuit measurements help?



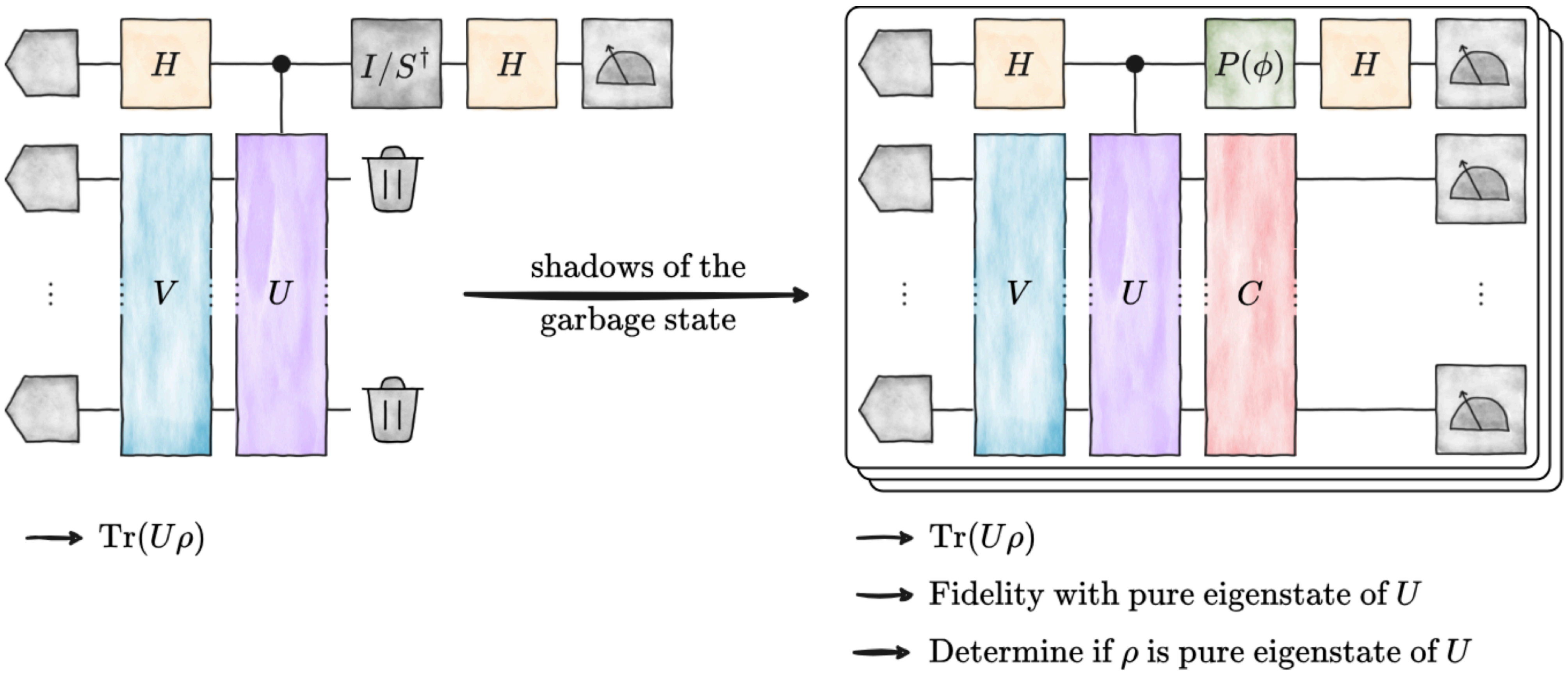
- **Theorem:** Sampling from constant depth 1D IQP circuits with mid-circuit measurements up to a constant error in $\|.\|_{l_1}$-norm is hard

- **Lesson:** Can be made geometry-informed IQP framework for learning ground states - mid-circuit measurements seem to help

Cao, Eisert, arXiv:2505.04705 (2025)
Cao, Eisert, in preparation (2025)

HADAMARD TEST

- Can we improve quantum algorithmic **primitives**?



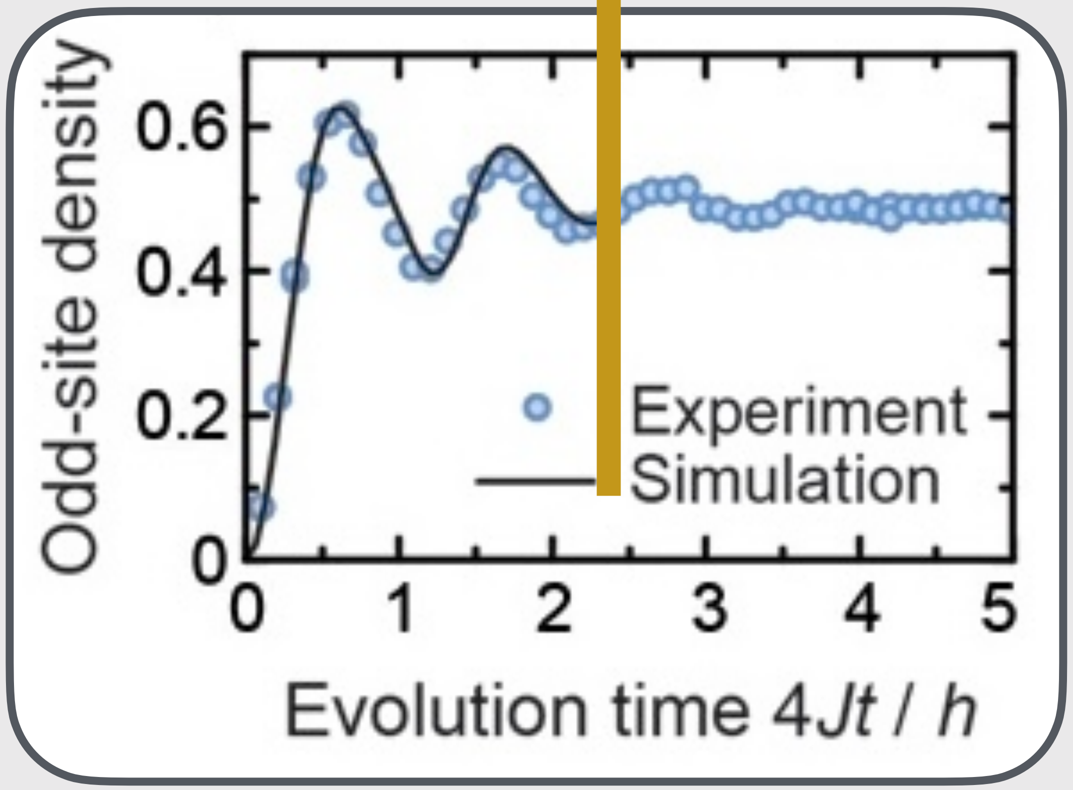
- **Lesson:** Hadamard test on a single auxiliary readout qubit with classical shadows on the remaining n-qubit work register improves primitive

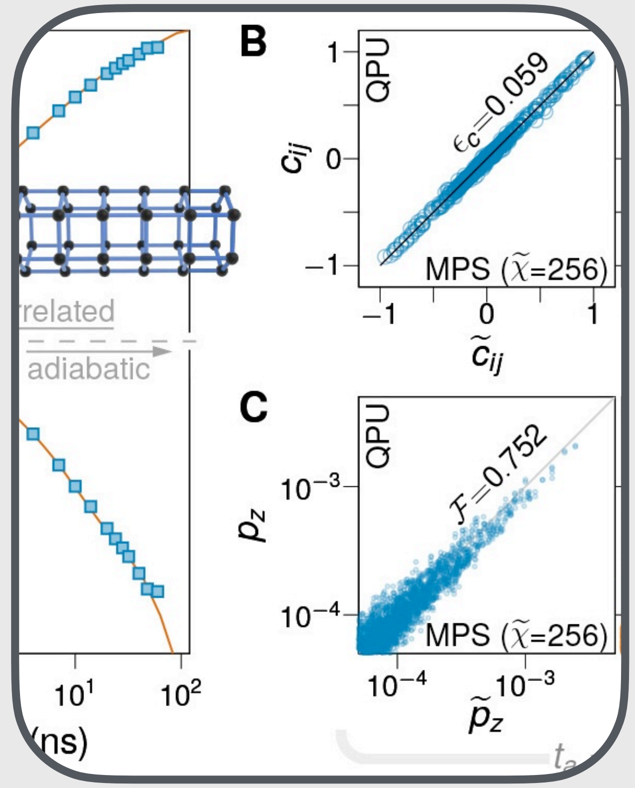
Faehrmann, Eisert, Kueng, arXiv:2505.15913, Phys Rev Lett, in press (2025)

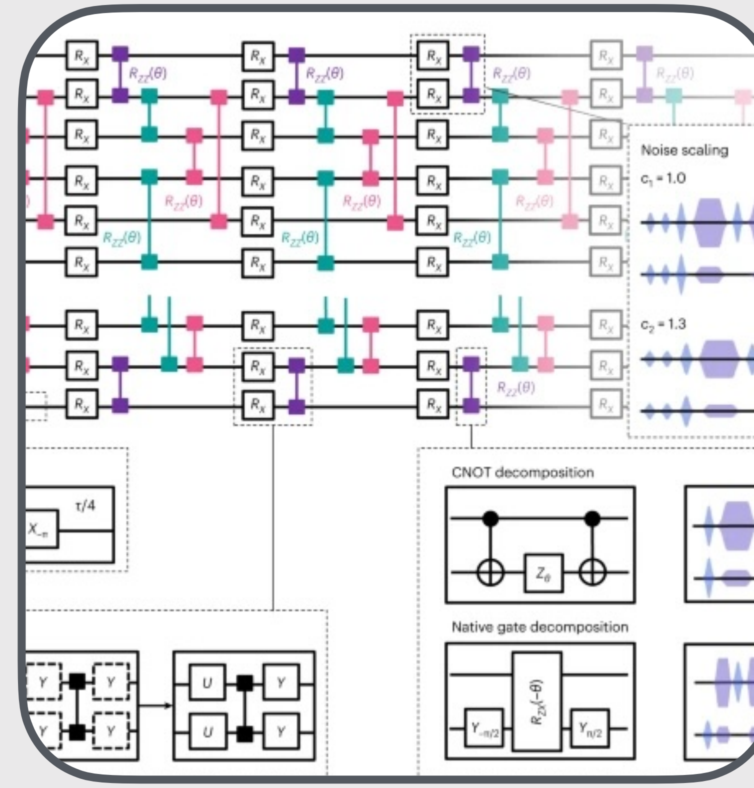
QUANTUM UTILITY IN QUANTUM SIMULATION?

- Can quantum simulation provide first **quantum utility**?

- Quenched ultra-cold atoms
- Annealers
- Superconducting circuits







vs matrix product states

Trotzky, Chen, Flesch, McCulloch, Schollwoeck, Eisert, Bloch, Nature Phys 8, 325 (2012)

vs tensor networks, belief prop, neural network states

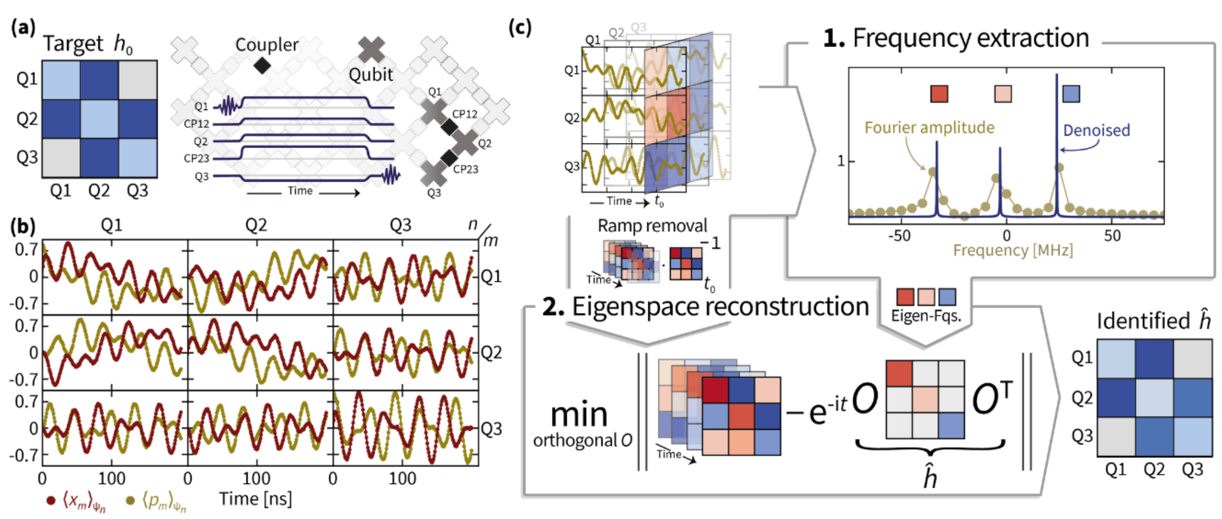
King et al, Science (2025)
Tindall, Mello, Fishman, Stoudenmire, Sels, arXiv:2503.05693 (2025)

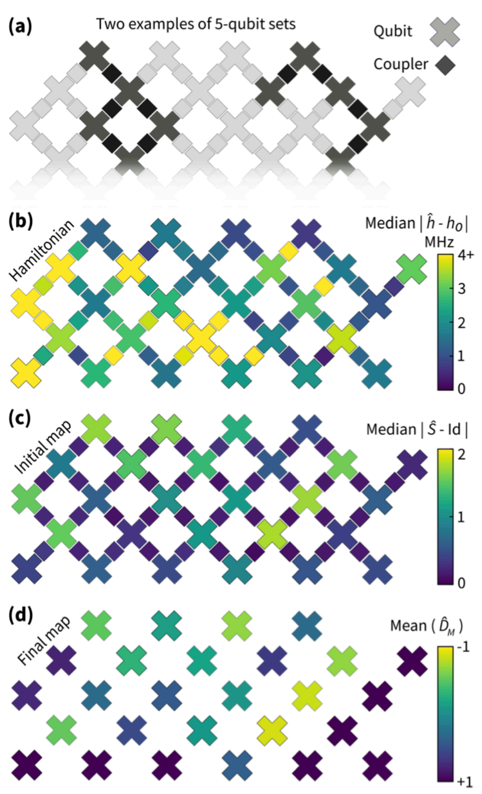
Kim et al, Nature, 618, 500–5 (2023)
Tindall, Fishman, Stoudenmire, Sels, PRX Quantum 5, 010308 (2024)

- **Sweet spot** provided by **two-dimensional systems** in **non-equilibrium**

QUANTUM UTILITY IN QUANTUM SIMULATION?

- **Hamiltonian** and Liovillian **learning**





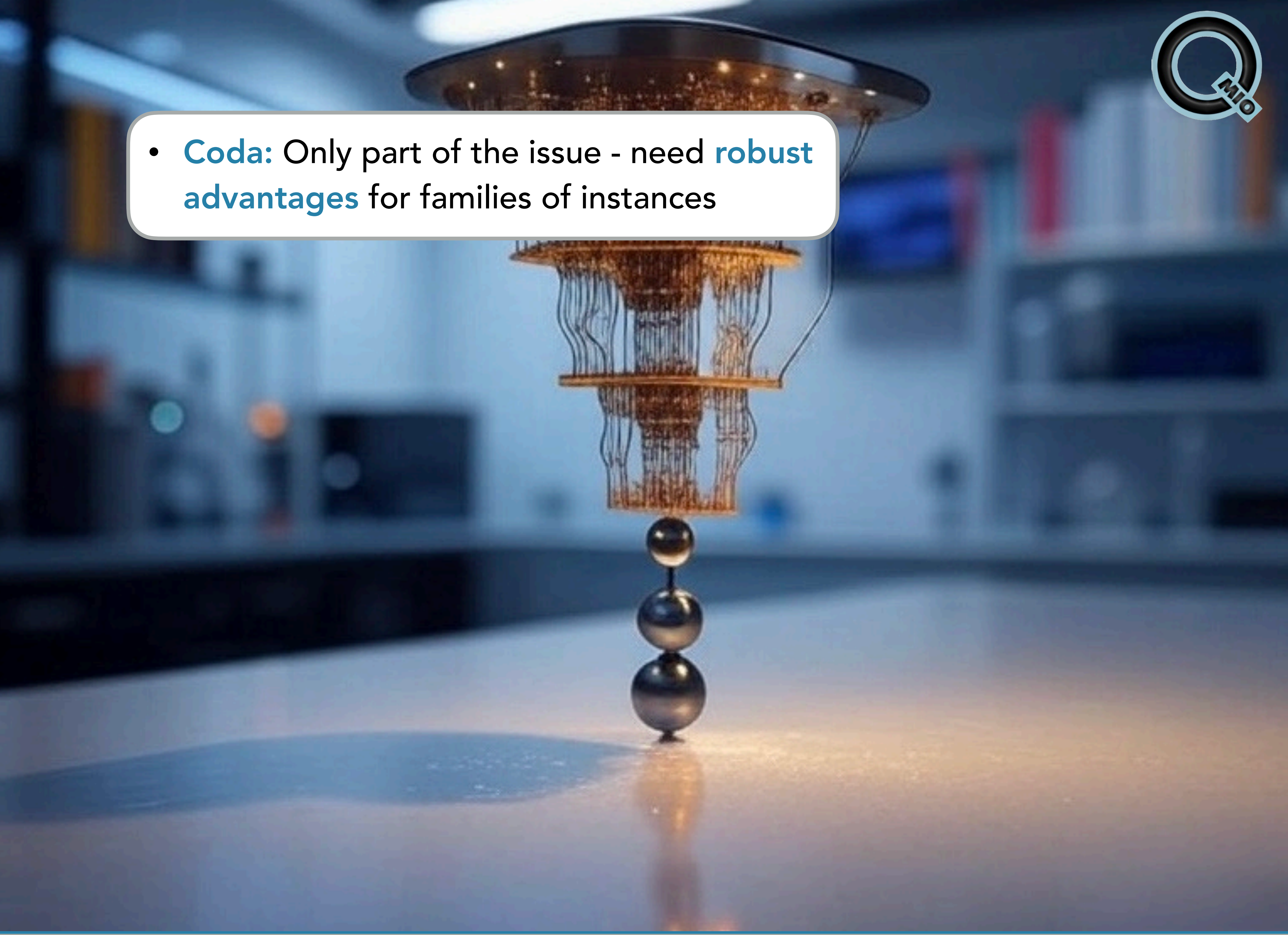
- **Lesson:** Such techniques can increase predictive power

Hangleiter, Roth, Fuksa, Eisert, Roushan, Nature Comm 15, 9595 (2024)
Wilde, Kshetrimayum, Roth, Hangleiter, Sweke, Eisert, arXiv:2209.14328 (2022)

CODA

arXiv:2502.14252 (2025)
Science Advances 10, eadj5170 (2024)
Nature Cimmunications 15, 434 (2024)
arXiv:2411.15548 (2024)
Quantum 5, 417 (2021)

- **Coda: Near-term** quantum advantages are not easy - constant factors matter



- **Coda:** Only part of the issue - need **robust advantages** for families of instances

- **Coda:** Only part of the issue - need **robust advantages** for families of instances

- **Our results on optimization:**
  - Approximate classically hard instances of integer programming

Pirnay, Ulitzsch, Wilde, Eisert, Seifert, arXiv:2212.08678, Science Advances 10, eadj5170 (2024)

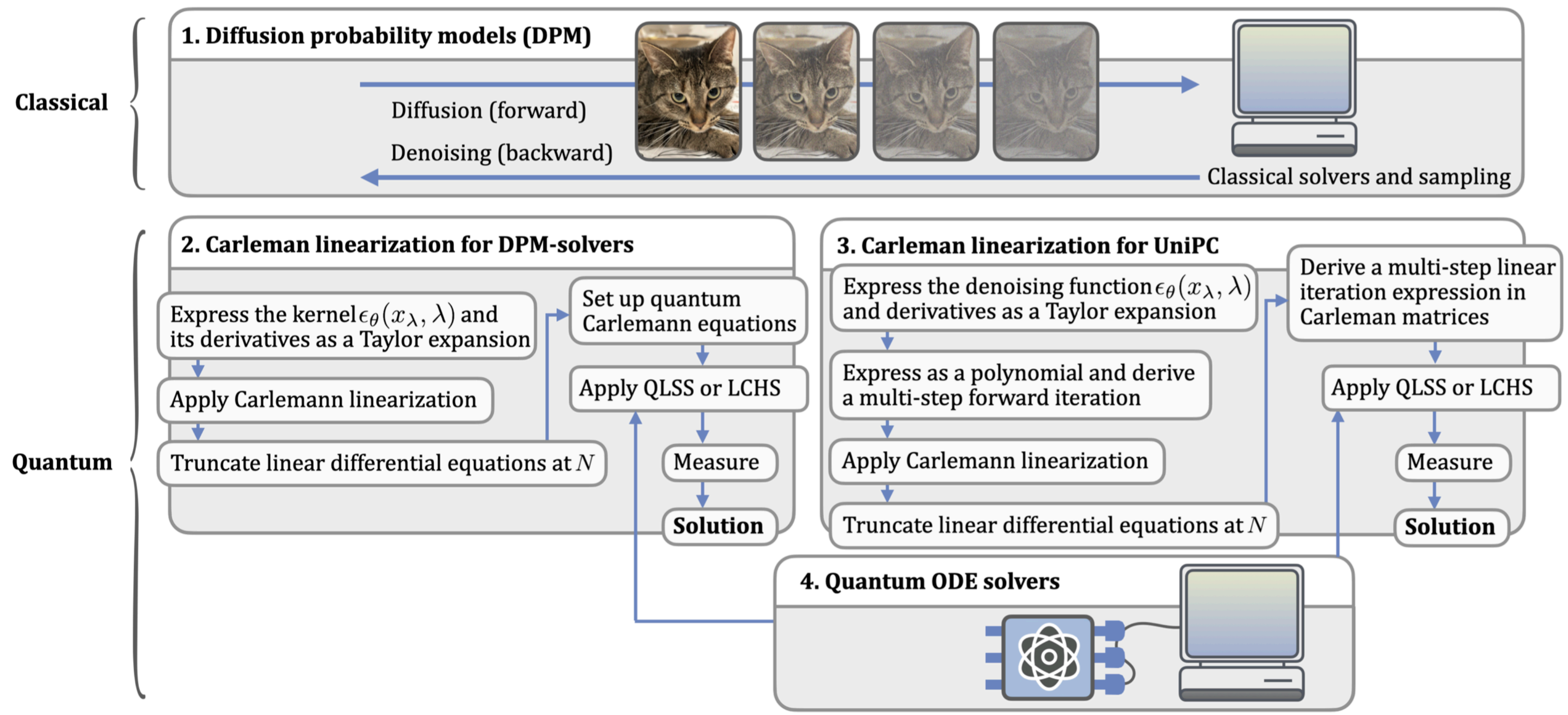
- **Result by Google AI: Decoded quantum interferometry**
  - Find $\mathbf{x} \in \mathbb{F}_2^n$ satisfying as many as possible among the m linear mod-2 equations $B\mathbf{x} = \mathbf{v}$, with $B \in \mathbb{F}_2^{m\times n}$, $\mathbf{v} \in \mathbb{F}_2^m$
  - Approximate solutions of optimization by reduction to decoding of classical codes
  - Max-k-XORSAT

Jordan, Shutty, Wootters, Zalcman, Schmiedhuber, King, Isokov, Babbush, arXiv:2408.08292 (2024)

- Question to audience

- **Coda:** Only part of the issue - need **robust advantages** for families of instances

- Quantum **probability diffusion models**



Wang, Jiang, Fan, Jia, Eisert, Liu, Liu, arXiv:2502.14252 (2025)
Liu, Liu, Liu, Ye, Wang, Alexeev, Eisert, Jiang, Nature Communications 15, 434 (2024)

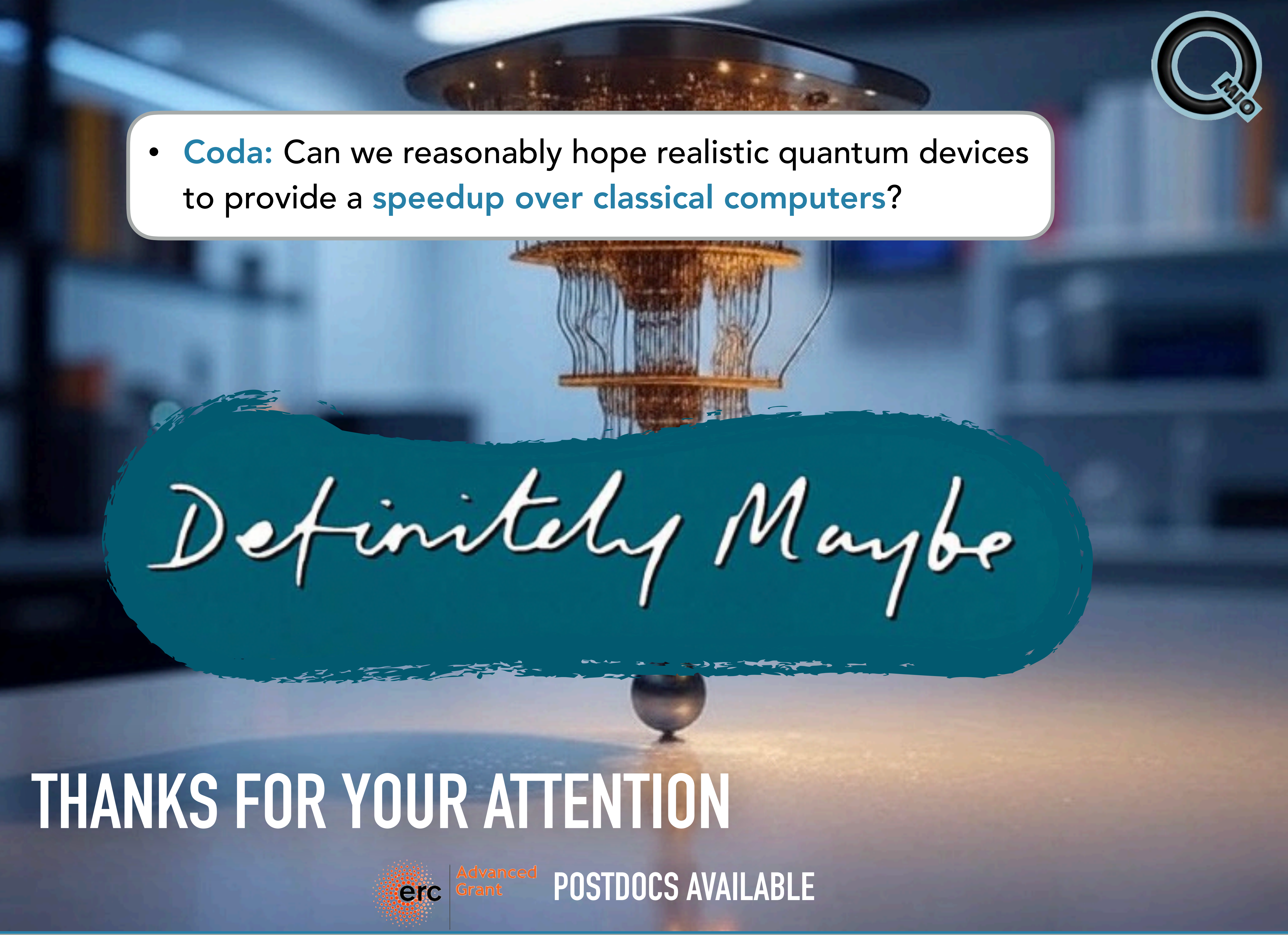
- **Coda:** As long as we stay away from the hype and take step by step, all will be well

Mind the gap: The fraught road to quantum advantage

Jens Eisert,[1,2,3] Steven T. Flammia,[4,5] and John Preskill[6,7]

[1]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, G*
[2]*Helmholtz-Zentrum Berlin für Materialien und Energie, 14109 Berlin, Germany*
[3]*Fraunhofer Heinrich Hertz Institute, 10587 Berlin, Germany*
[4]*Department of Computer Science, Virginia Tech, Alexandria, VA 22314, USA*
[5]*Phasecraft Inc., Washington, DC 20001, USA*
[6]*Institute for Quantum Information and Matter, California Institute of Technology, CA 91*
[7]*AWS Center for Quantum Computing, Pasadena, CA 91125, USA*

https://www.phy



• Coda: Can we reasonably hope realistic quantum devices to provide a speedup over classical computers?
Definitely Maybe
THANKS FOR YOUR ATTENTION
erc Advanced Grant
POSTDOCS AVAILABLE