

NEAR-TERM QUANTUM COMPUTING AND QUANTUM ADVANTAGES

JENS EISERT, FU BERLIN

SUMMER SCHOOL ON QUANTUM COMPUTING, AUG-SEP 2020



NEAR-TERM QUANTUM COMPUTING AND QUANTUM ADVANTAGES

JENS EISERT, FU BERLIN

SUMMER SCHOOL ON QUANTUM COMPUTING, AUG-SEP 2020



NEAR-TERM QUANTUM COMPUTING AND QUANTUM ADVANTAGES

JENS EISERT, FU BERLIN

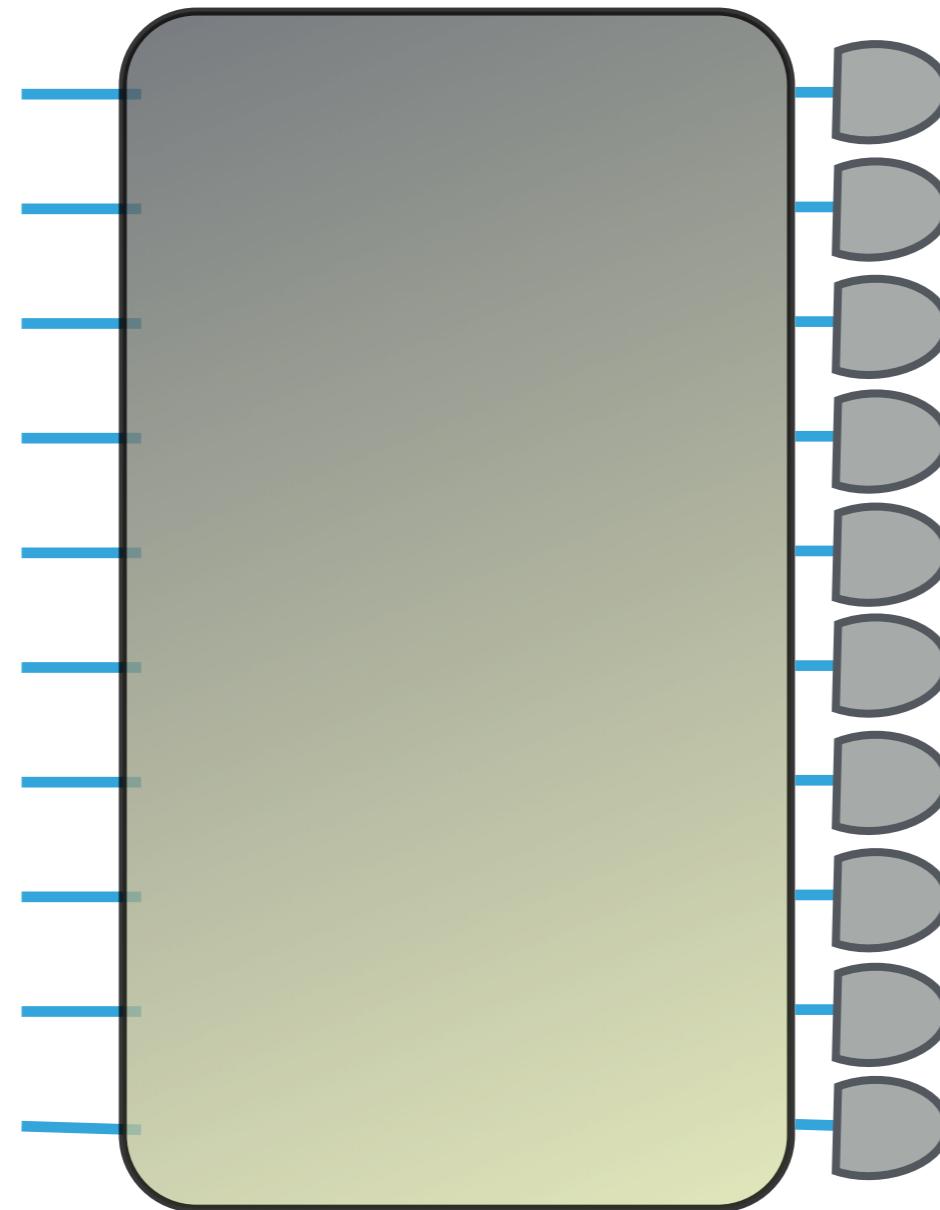
SUMMER SCHOOL ON QUANTUM COMPUTING, AUG-SEP 2020

NEAR-TERM QUANTUM COMPUTING AND QUANTUM ADVANTAGES

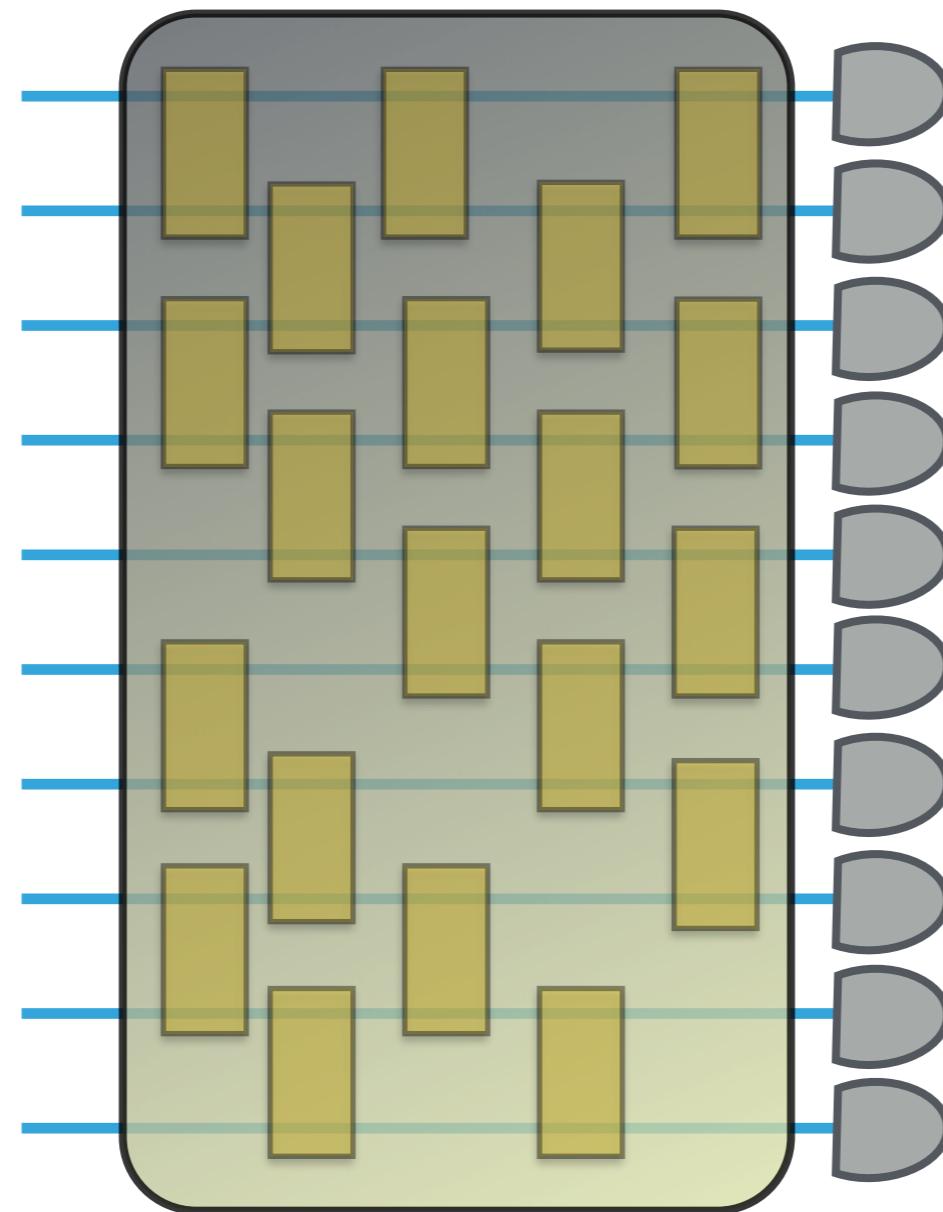
JENS EISERT, FU BERLIN

SUMMER SCHOOL ON QUANTUM COMPUTING, AUG-SEP 2020

QUANTUM COMPUTERS AS FICTIONAL DEVICES

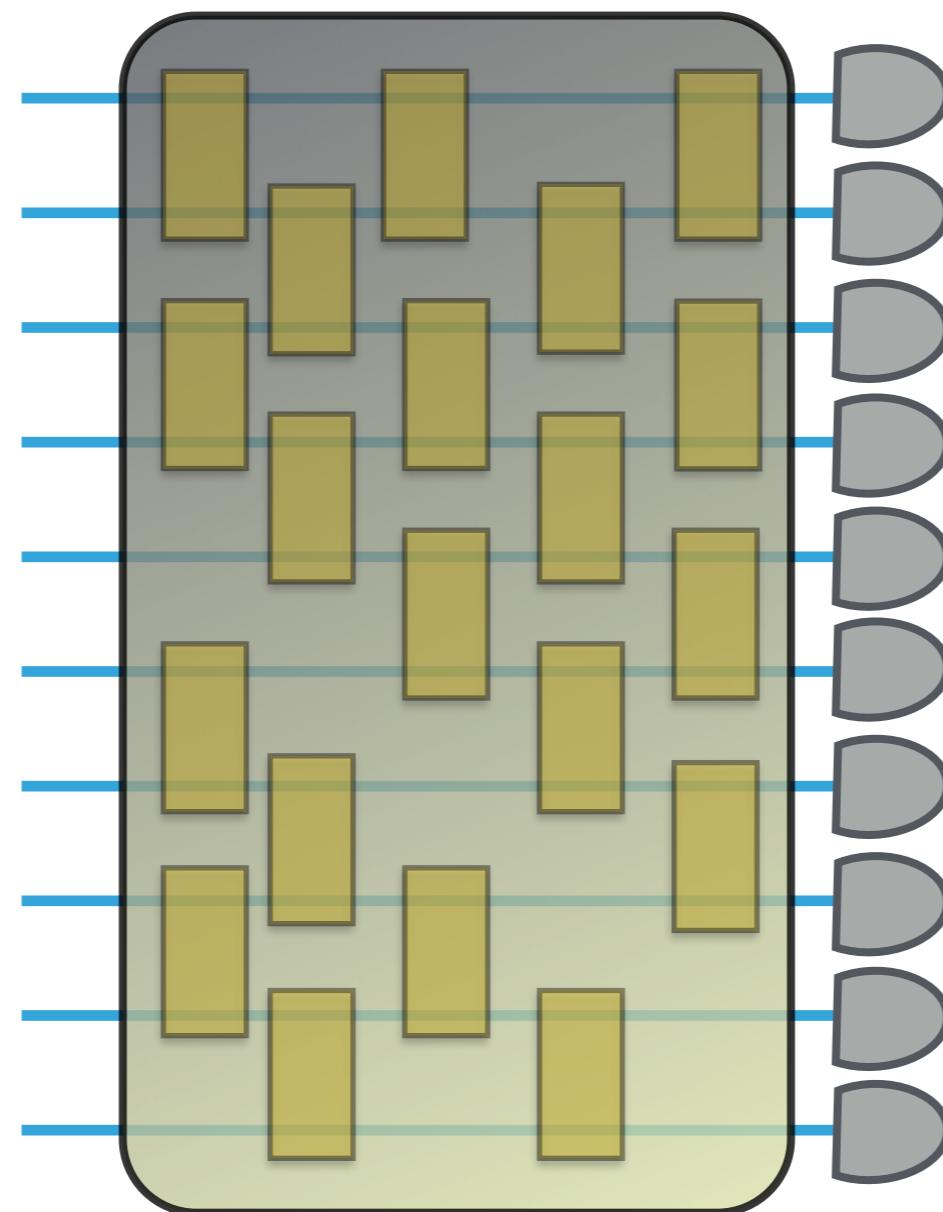


QUANTUM COMPUTERS AS FICTIONAL DEVICES



QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time



QUANTUM COMPUTERS AS FICTIONAL DEVICES

► **Quantum computers** solve some problems in NP in polynomial time

► **NP** (non-deterministic polynomial time)

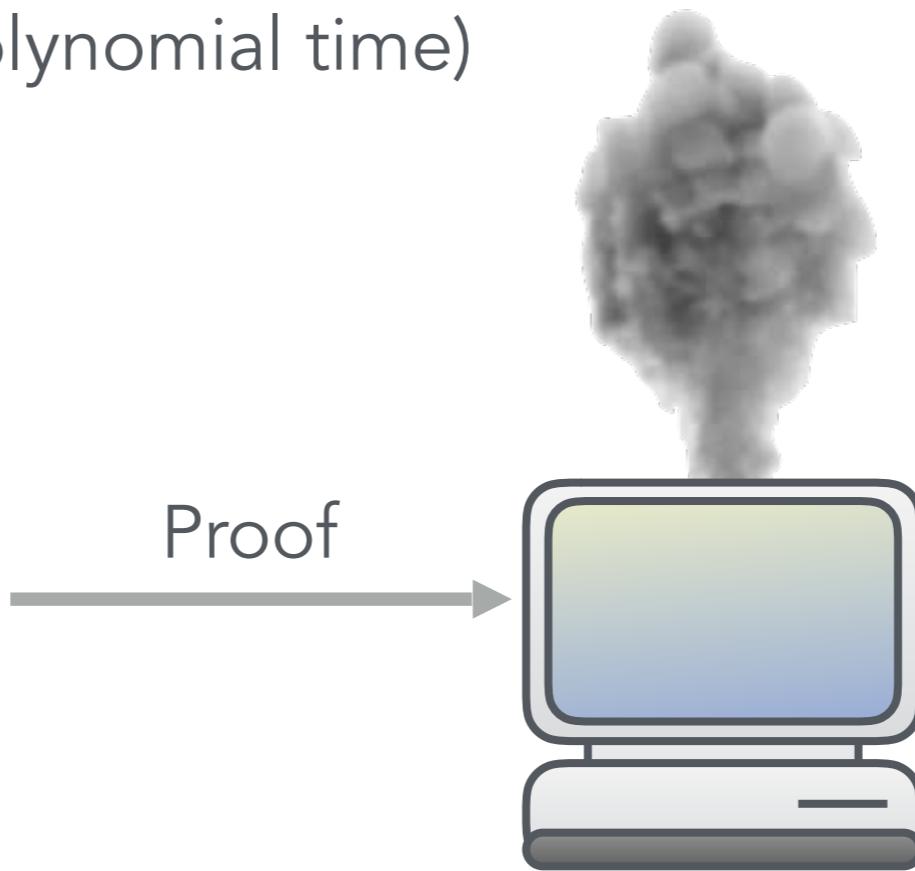


Is $x \in L?$

QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time

- ▶ NP (non-deterministic polynomial time)

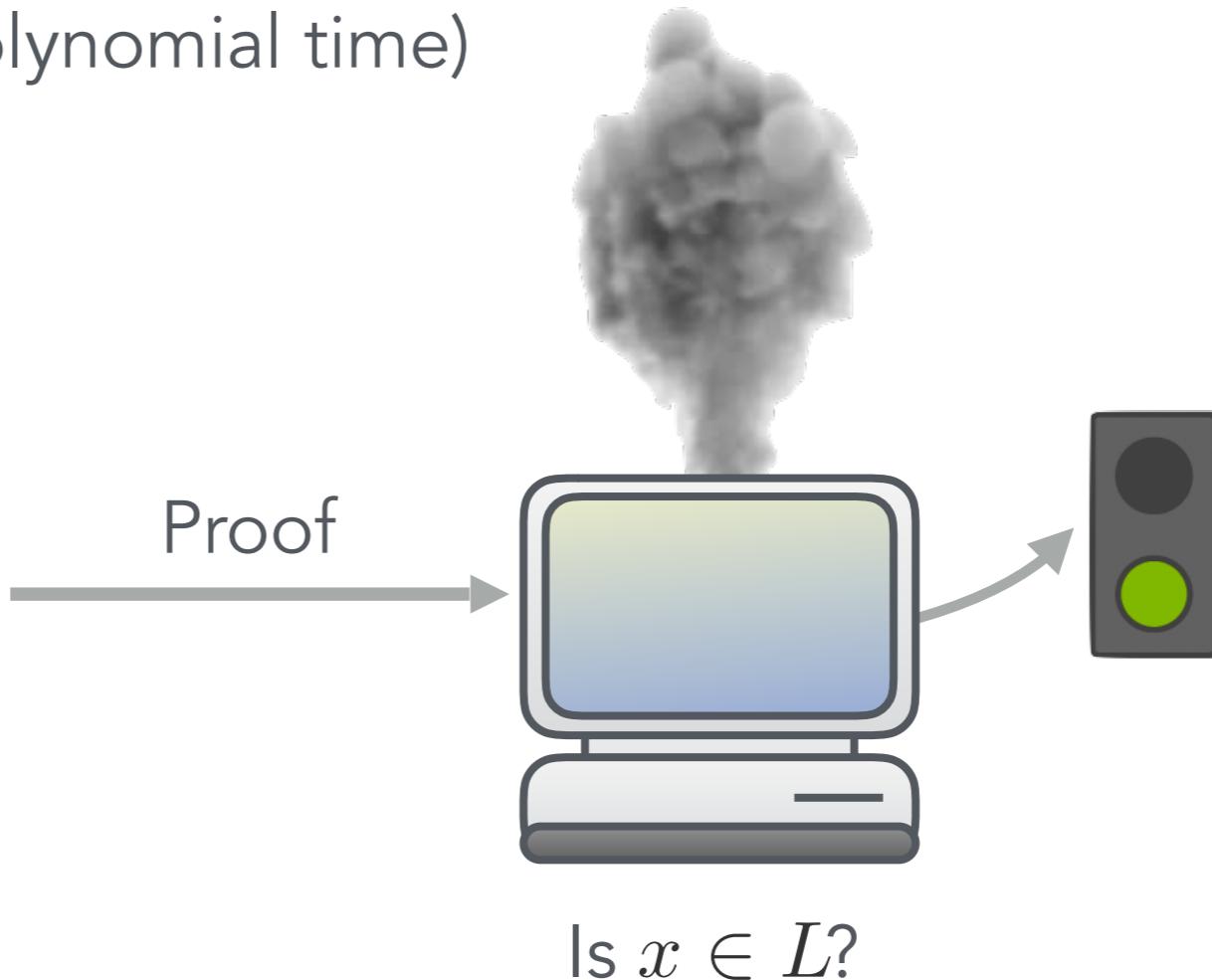


Is $x \in L?$

QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time

- ▶ NP (non-deterministic polynomial time)

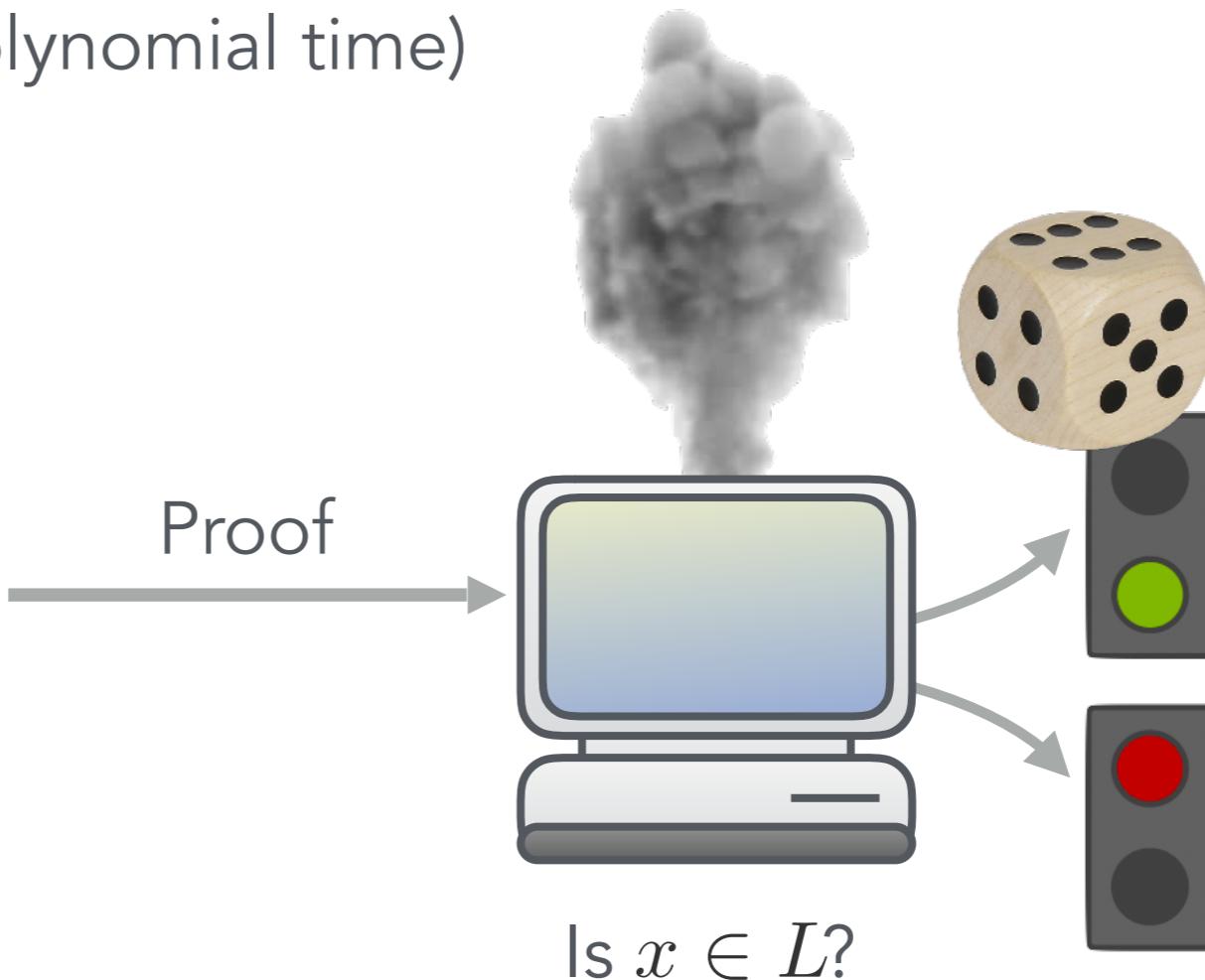


- ▶ **Completeness:** If $x \in L$, there is proof that is accepted in polynomial time

QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time

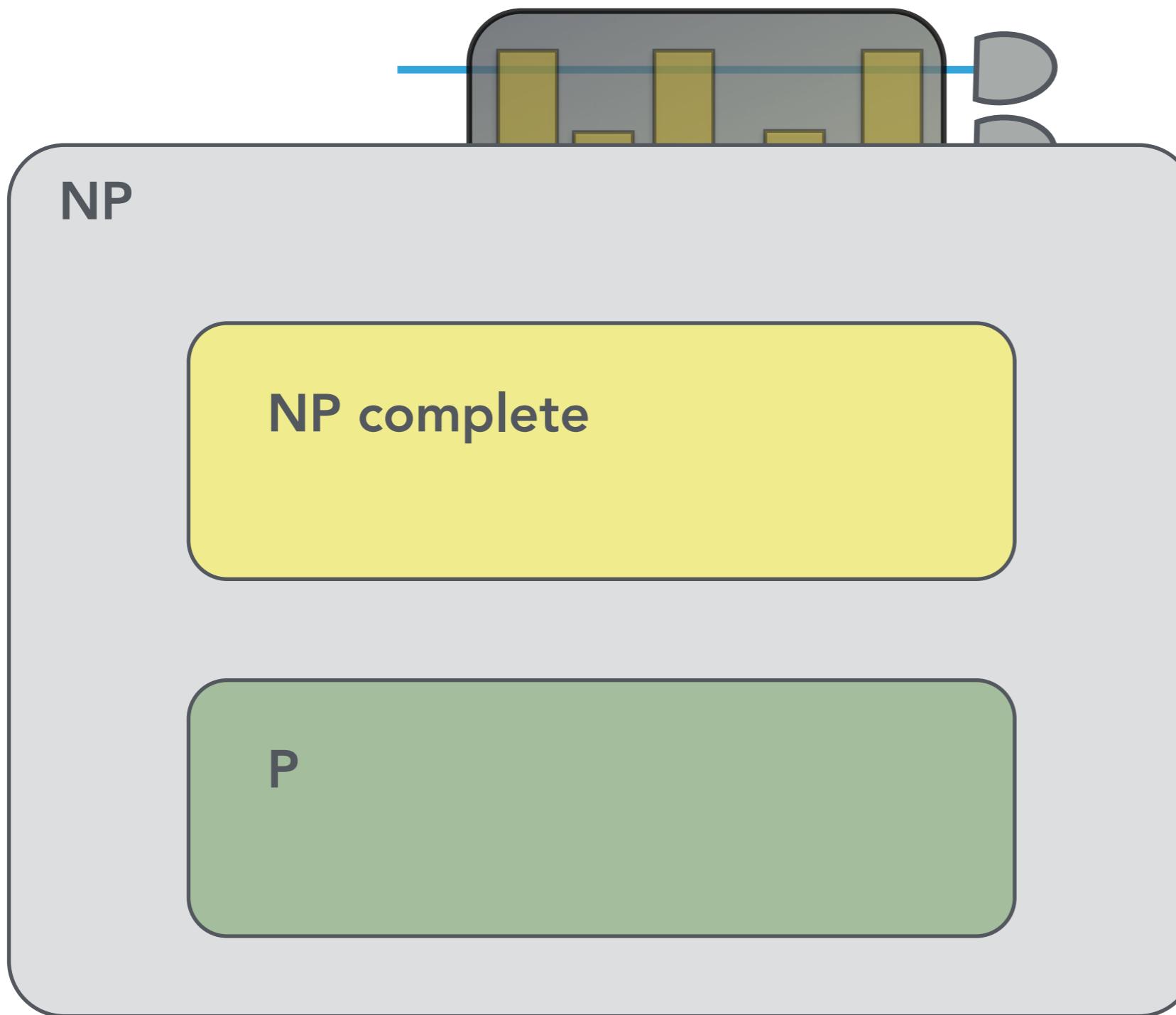
- ▶ NP (non-deterministic polynomial time)



- ▶ **Completeness:** If $x \in L$, there is proof that is accepted in polynomial time
- ▶ **Soundness:** If $x \notin L$, no proof is accepted

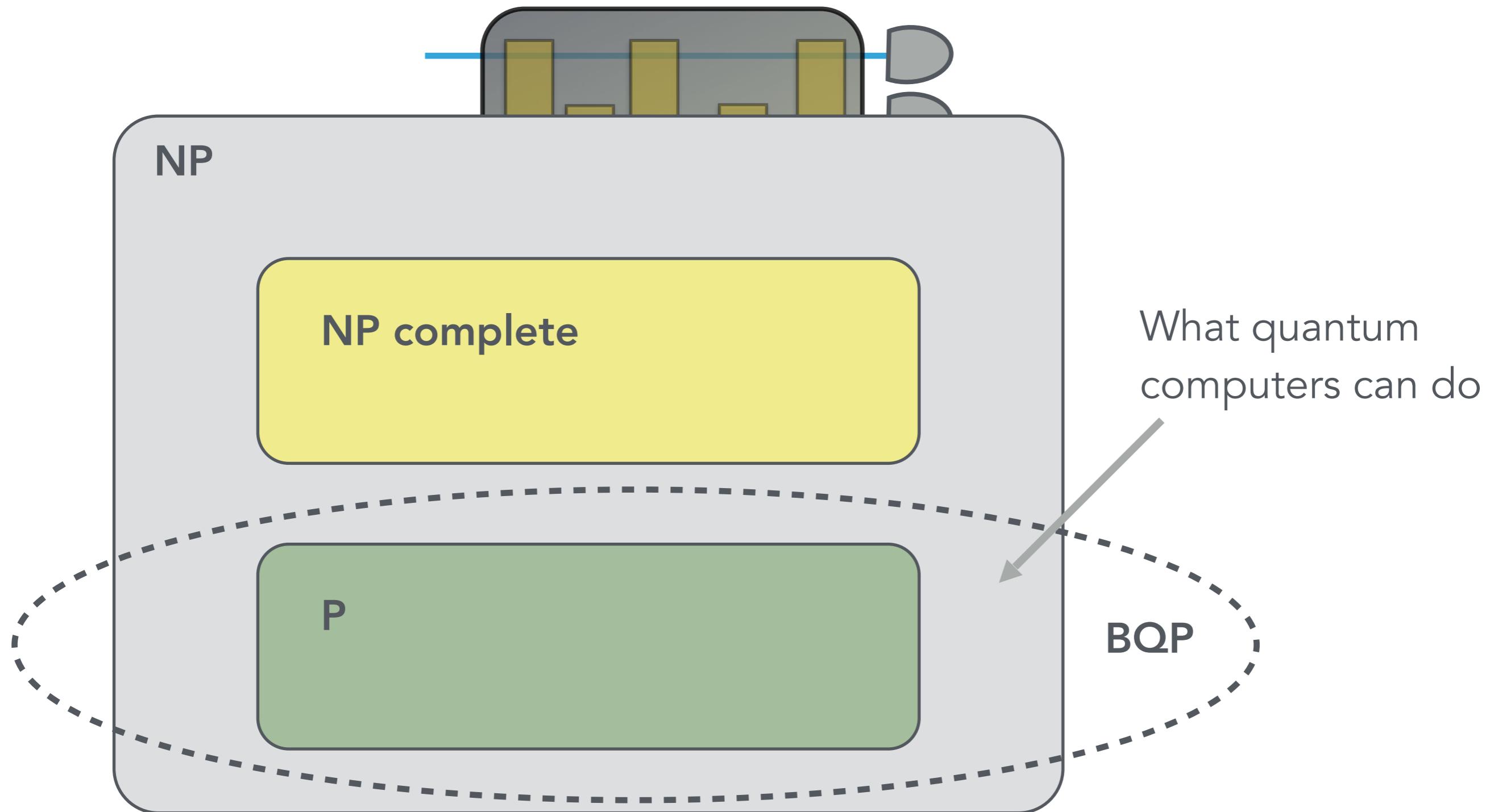
QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time



QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time



- ▶ Quantum computers solve some problems in NP in polynomial time



- ▶ Get factor of a large number N from the **period** p of the function

$$f(x) = a^x \bmod N$$

- ▶ Periods can be found using the **quantum Fourier transform**

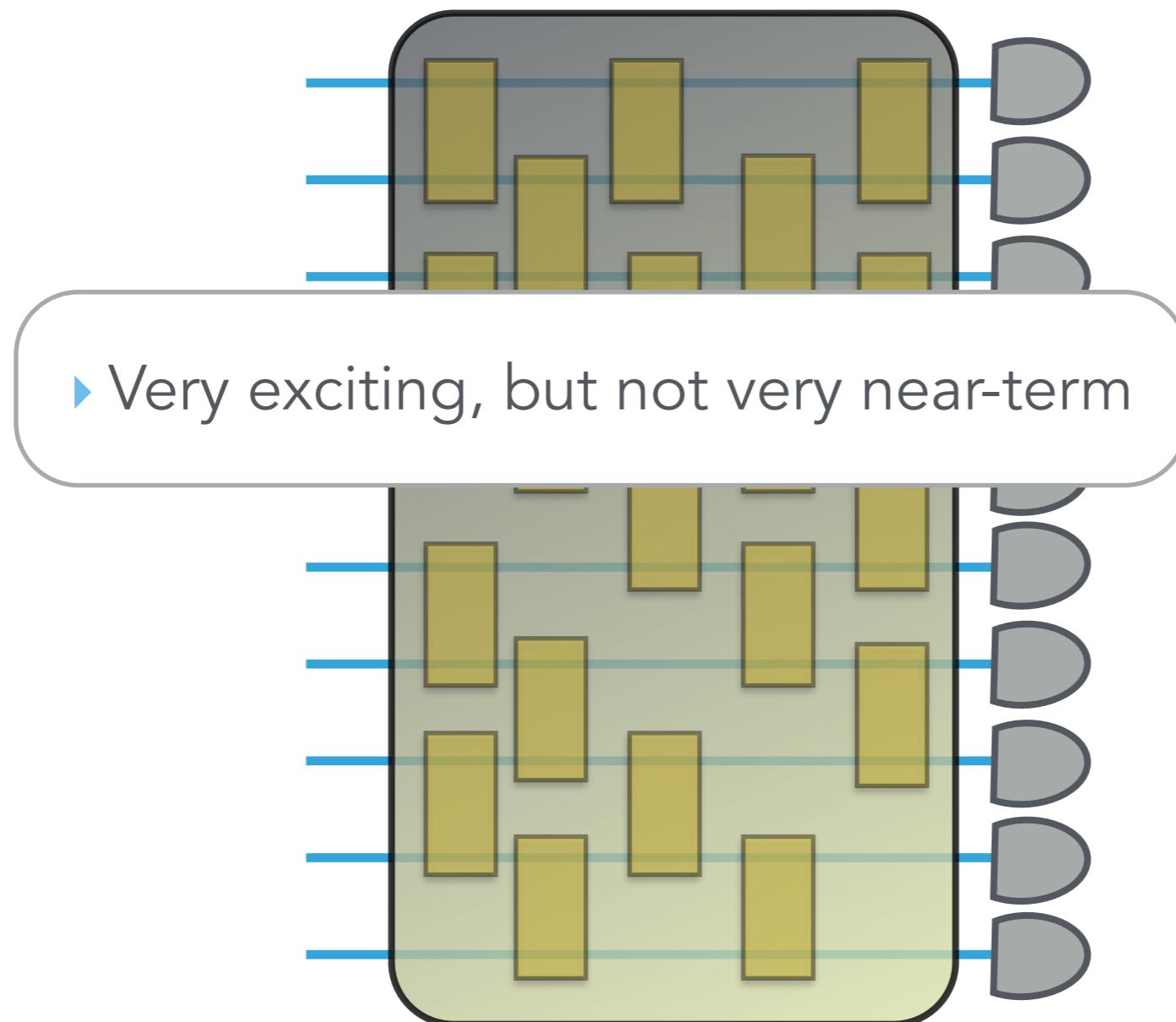
$$\sum_{i=0}^{n-1} x_i |i\rangle \mapsto \sum_{i=0}^{n-1} y_i |i\rangle \text{ with } y_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} x_j e^{2\pi i j k / n}$$

- ▶ Solves NP problem in poly time: Runtime $O((\log N)^3)$
- ▶ Best known classical algorithm $\exp(O((\log N)^{1/3}(\log \log N)^{2/3}))$



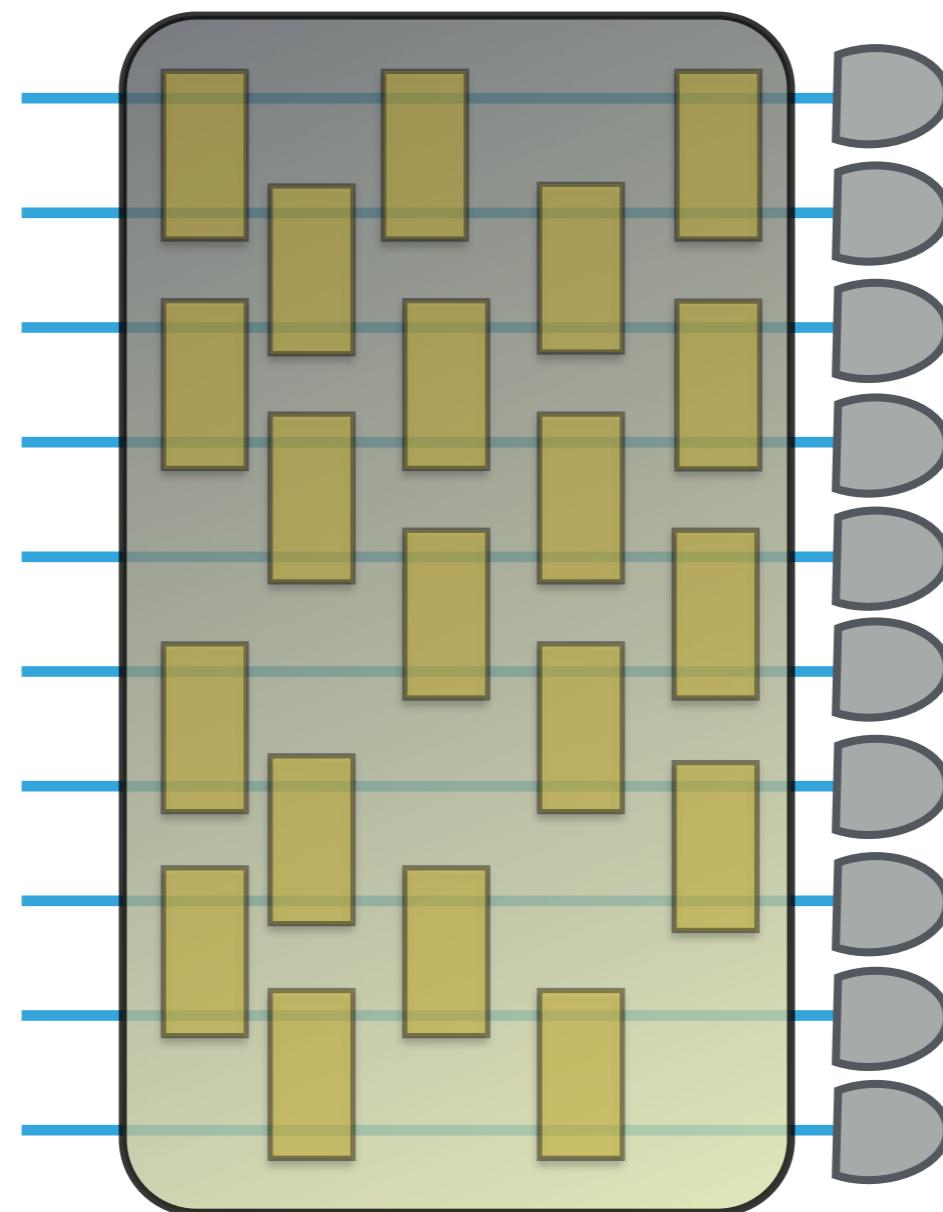
QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time



QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time



QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time

- ▶ Principal component analysis

Lloyd, Mohseni, Rebentrost, Nature Phys 10, 631 (2014)

- ▶ Matrix inversion and linear systems

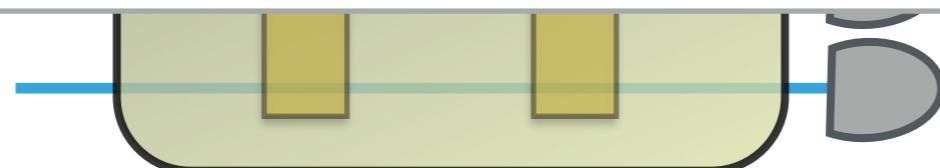
Harrow, Hassidim, Lloyd, Phys Rev Lett 103, 150502 (2008)

- ▶ Spectral analysis

Steffens, Rebentrost, Marvian, Eisert, Lloyd, New J Phys 19, 033005 (2017)

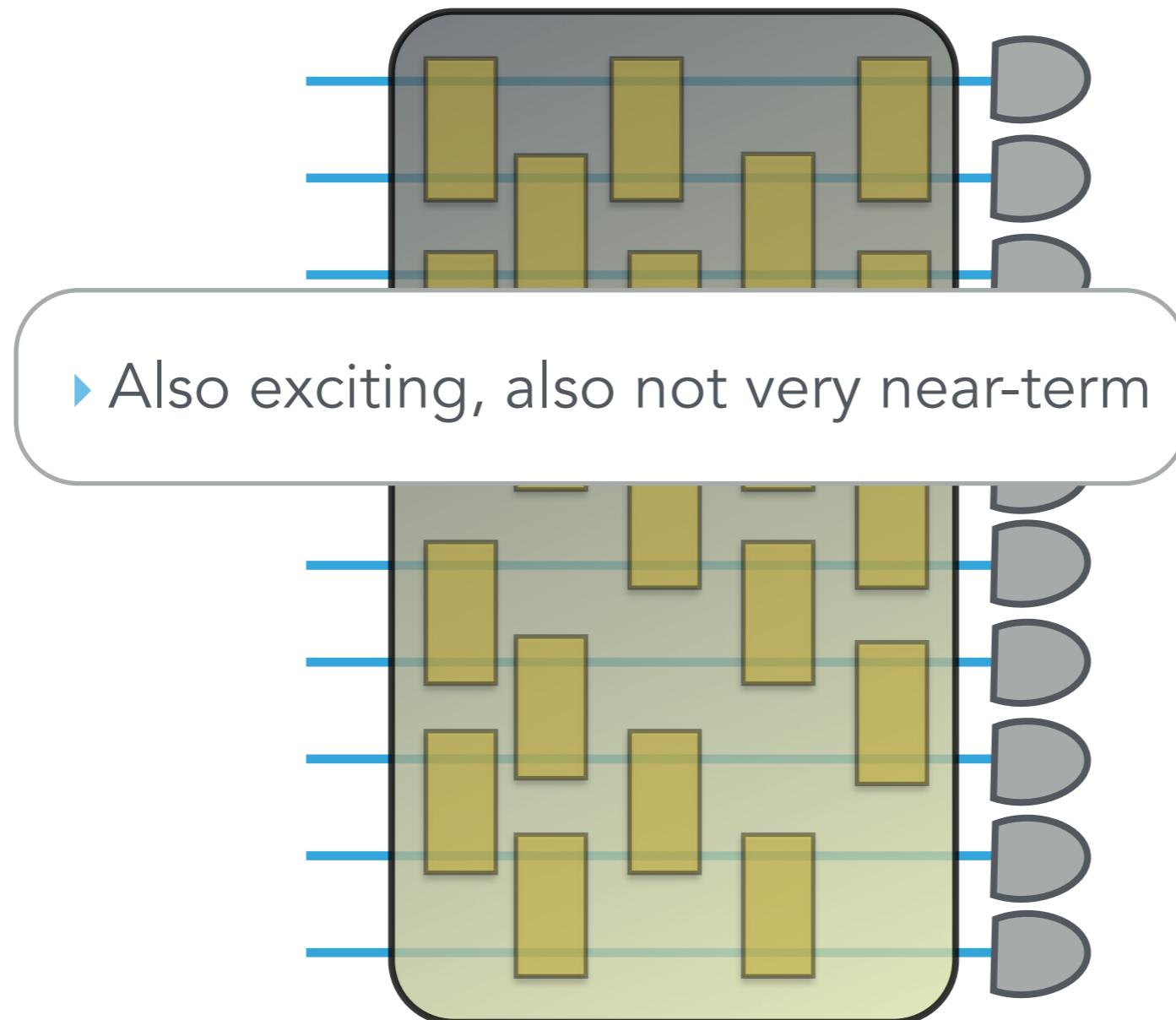
- ▶ Semi-definite programming

Brandão, Kalev, Li, Lin, Svore, Wu, arXiv:1710.02581

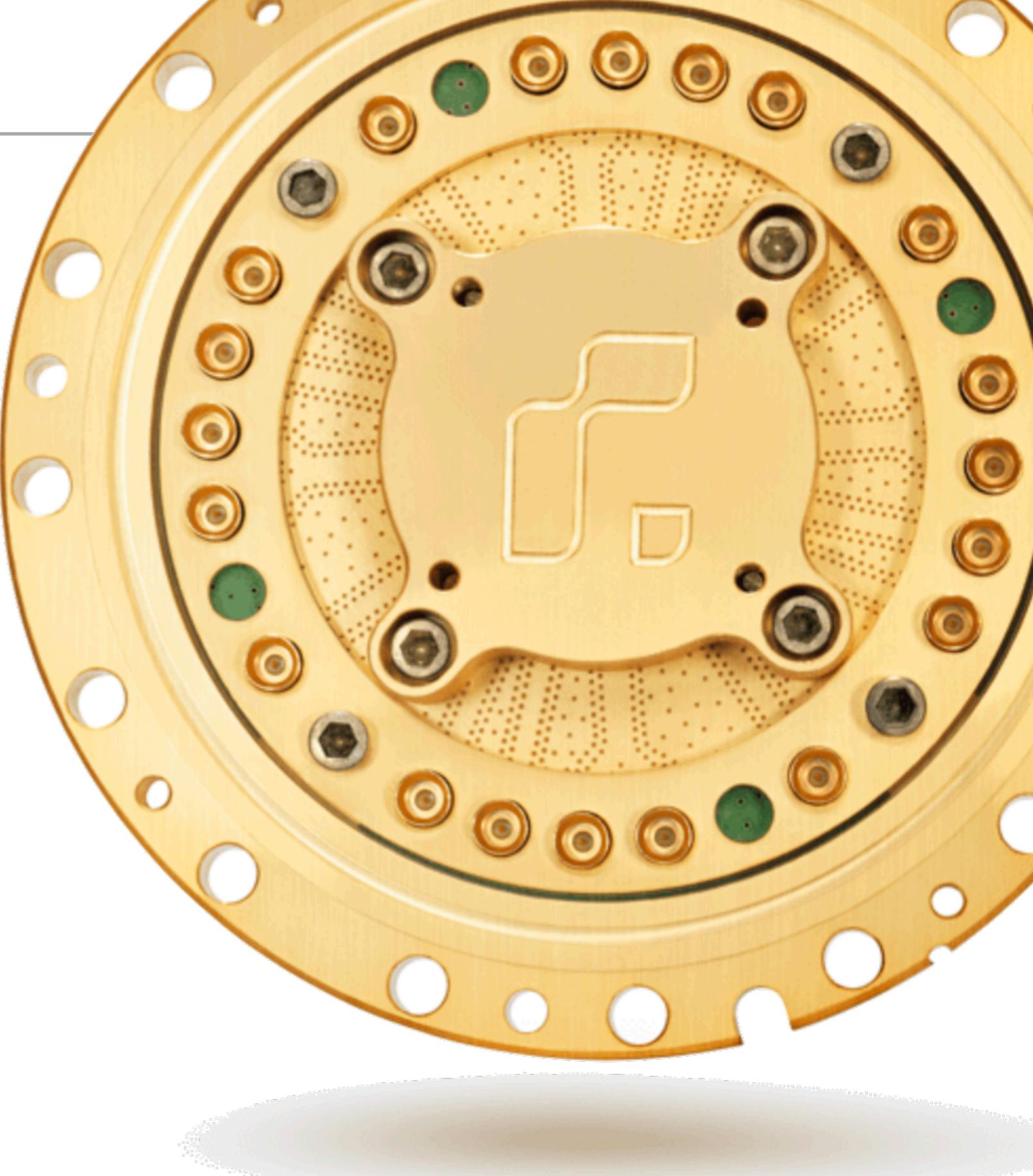


QUANTUM COMPUTERS AS FICTIONAL DEVICES

- ▶ Quantum computers solve some problems in NP in polynomial time

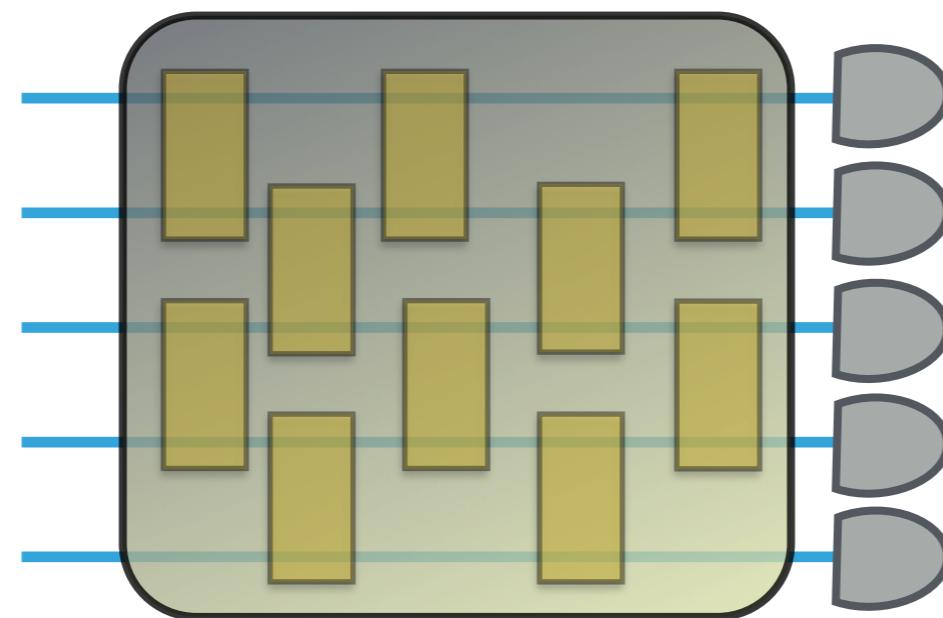


NEAR-TERM QUANTUM COMPUTERS



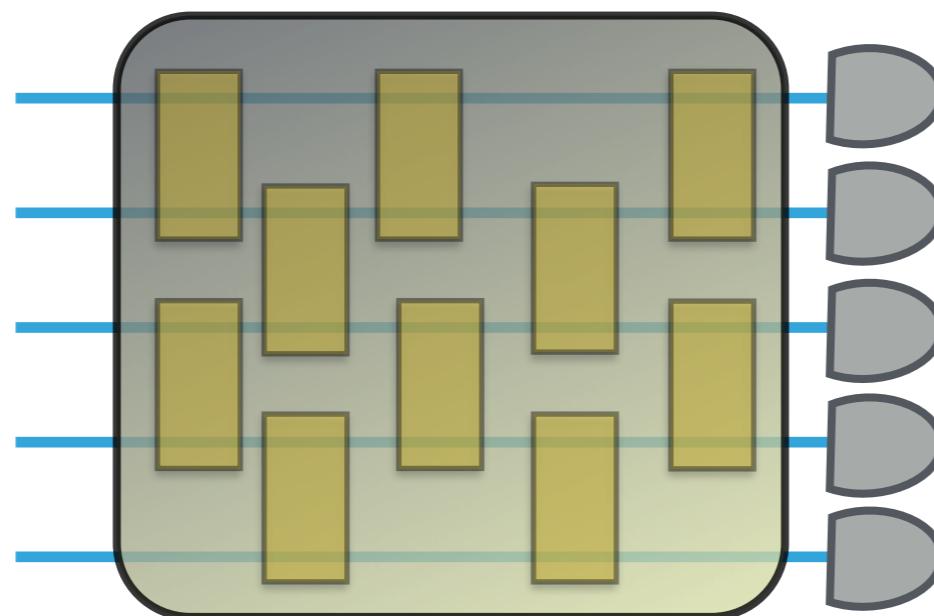
NOISY INTERMEDIATE SCALE QUANTUM DEVICES

- We presently have **small and noisy quantum computers**



NOISY INTERMEDIATE SCALE QUANTUM DEVICES

- We presently **have** small and noisy quantum computers

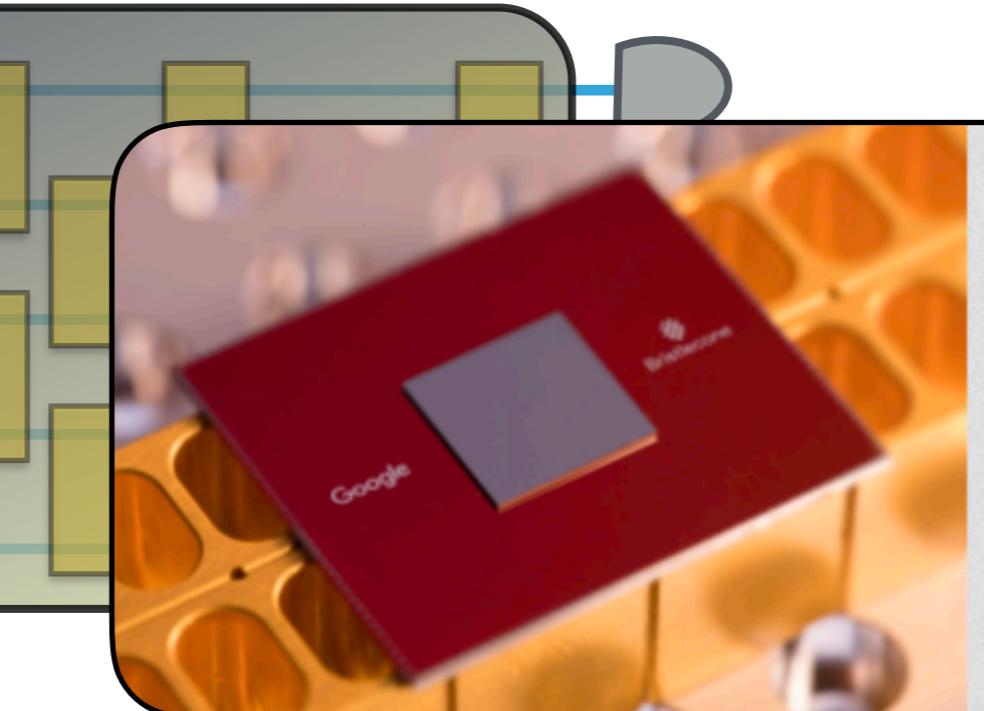


NOISY INTERMEDIATE SCALE QUANTUM DEVICES

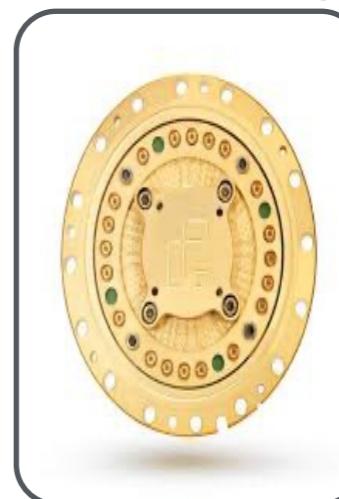
- We presently **have** small and noisy quantum computers



IBM's 53 qubit superconducting device



Google's 53/72 (Brizzecone) qubits devices



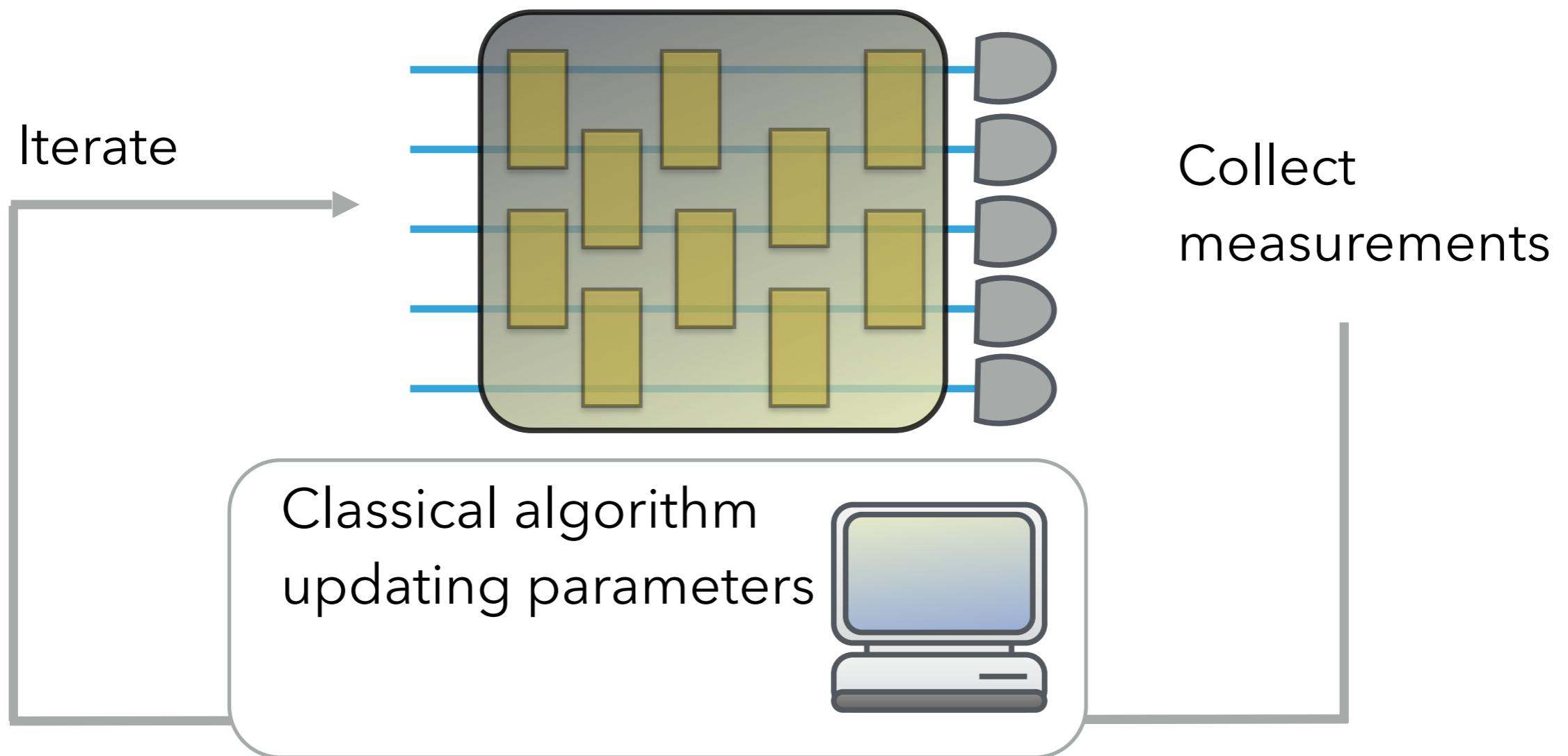
Rigetti



PsiQuantum

CLASSICAL-QUANTUM HYBRID ALGORITHMS

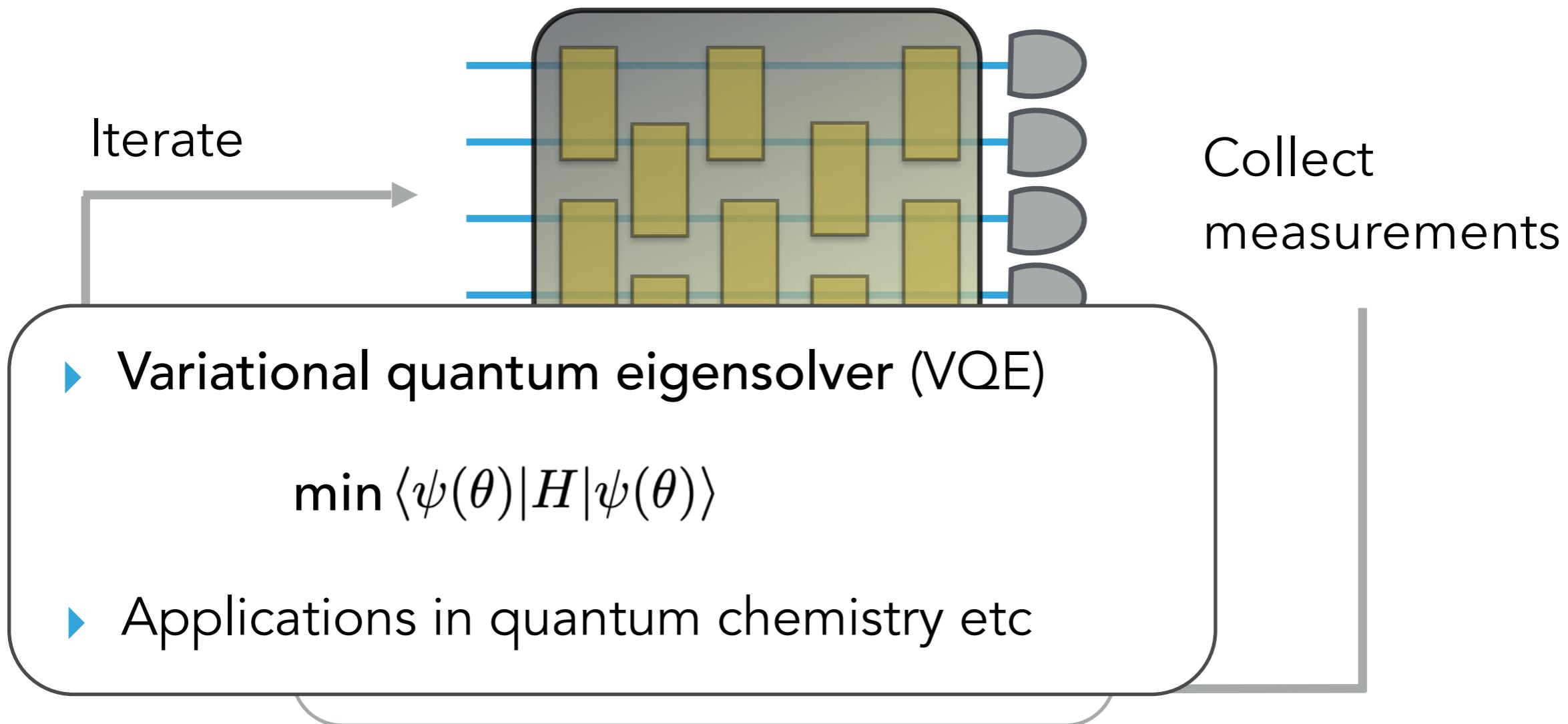
- We presently **have** small and noisy quantum computers



- Heuristically encouraging performance

CLASSICAL-QUANTUM HYBRID ALGORITHMS

- We presently **have** small and noisy quantum computers

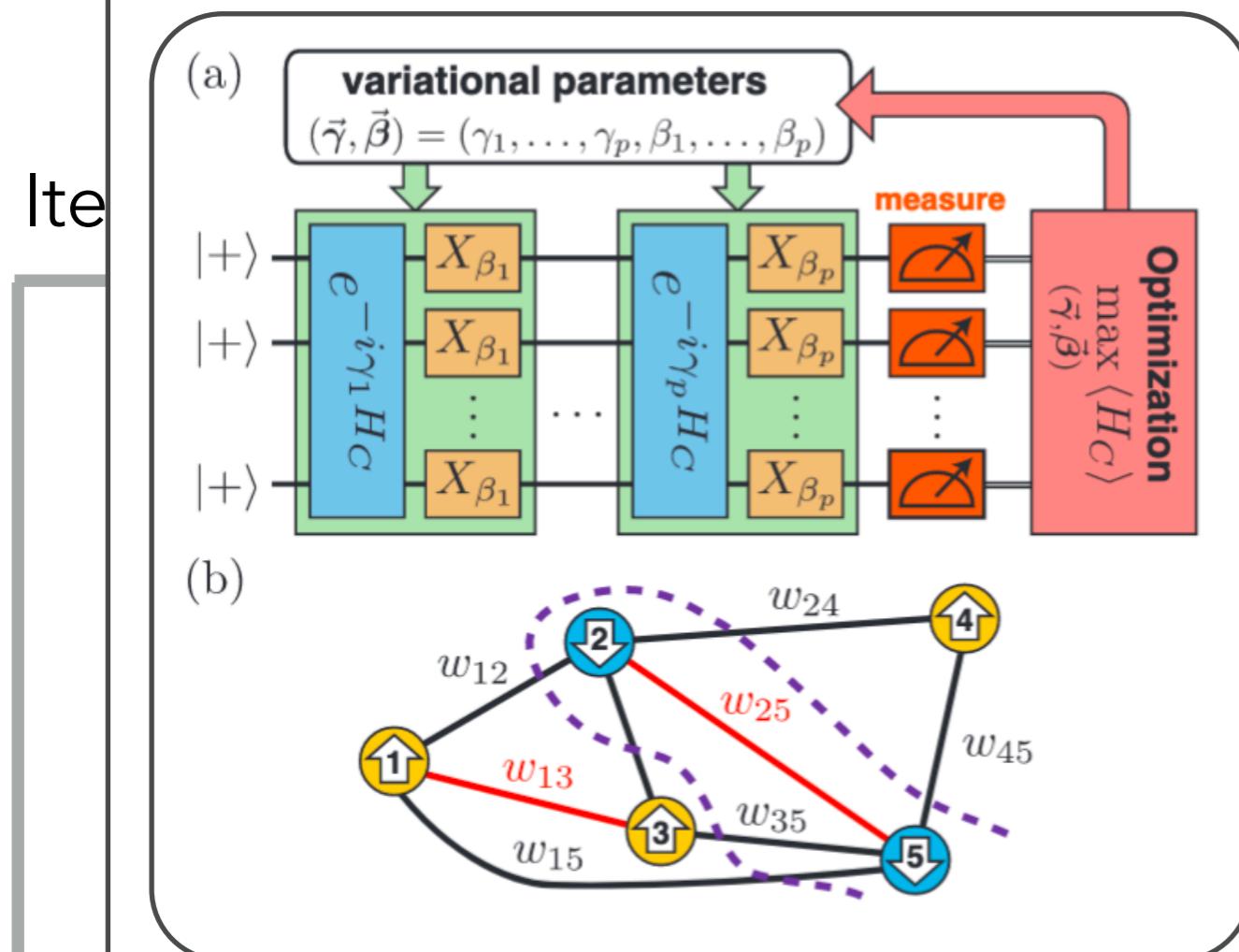


- Heuristically encouraging performance

CLASSICAL-QUANTUM HYBRID ALGORITHMS

► We pr

► Quantum approximate optimization algorithm (QAOA)



- Combinatorial optimization problems (e.g., MaxCUT)
- Goal: determine binary string maximizing a given classical objective function
- $C : \{-1, 1\}^n \rightarrow \mathbb{R}_{\geq 0}$
- Aims to find a string achieving a desired approximation ratio

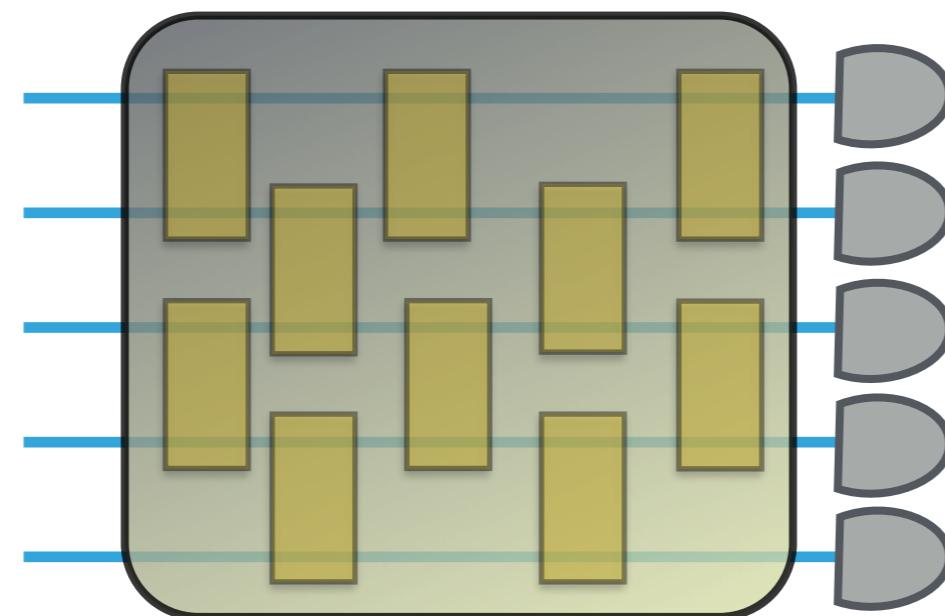
$$\frac{C(z)}{C_{\max}} \geq r$$

► Heur

- Not yet so well understood beyond single layer

CLASSICAL-QUANTUM HYBRID ALGORITHMS

- In variational algorithms, loss function $\mathcal{L} : \mathbb{R}^d \rightarrow \mathbb{R}$ needs to be optimized



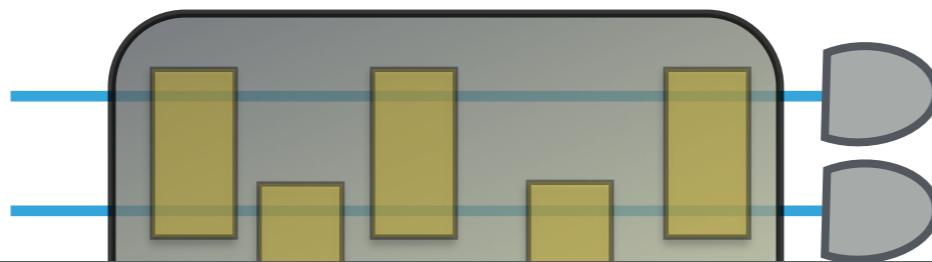
Parameters $\theta \in \mathbb{R}^d$

- Estimate the gradient for update

$$\partial \mathcal{L}(\boldsymbol{\theta}) / \partial \theta_i$$

- $\frac{C(z)}{C_{\text{max}}} \geq r^*$
- Estimate expectation values
- $$\langle O_i \rangle_{\boldsymbol{\theta}} = \langle \mathbf{0} | U^\dagger(\boldsymbol{\theta}) O_i U(\boldsymbol{\theta}) | \mathbf{0} \rangle$$

- In variational algorithms, loss function $\mathcal{L} : \mathbb{R}^d \rightarrow \mathbb{R}$ needs to be optimized



- Parameter shift rule:** A quantum circuit $U(\theta), \theta \in \mathbb{R}^d$, satisfies a K -term shift rule, if [...]

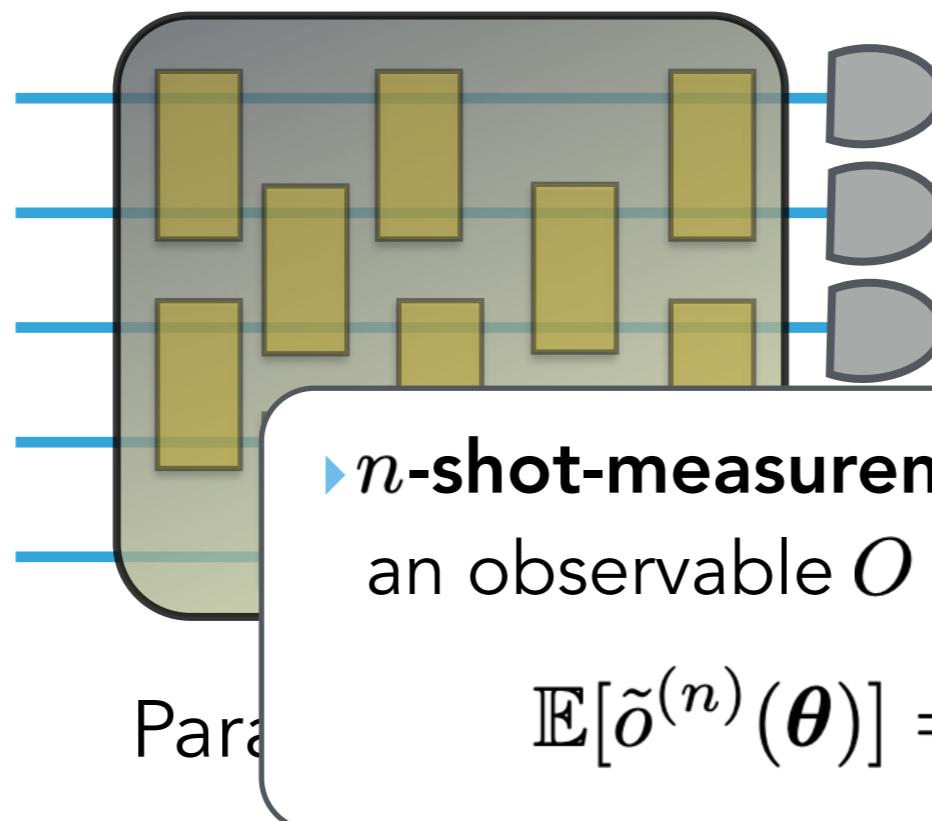
$$\frac{\partial}{\partial \theta_i} \langle O \rangle_{\theta} = \sum_{k=1}^K \gamma_{k,i} \langle O \rangle_{\theta_{k,i}}$$

- Estimate the gradient for update

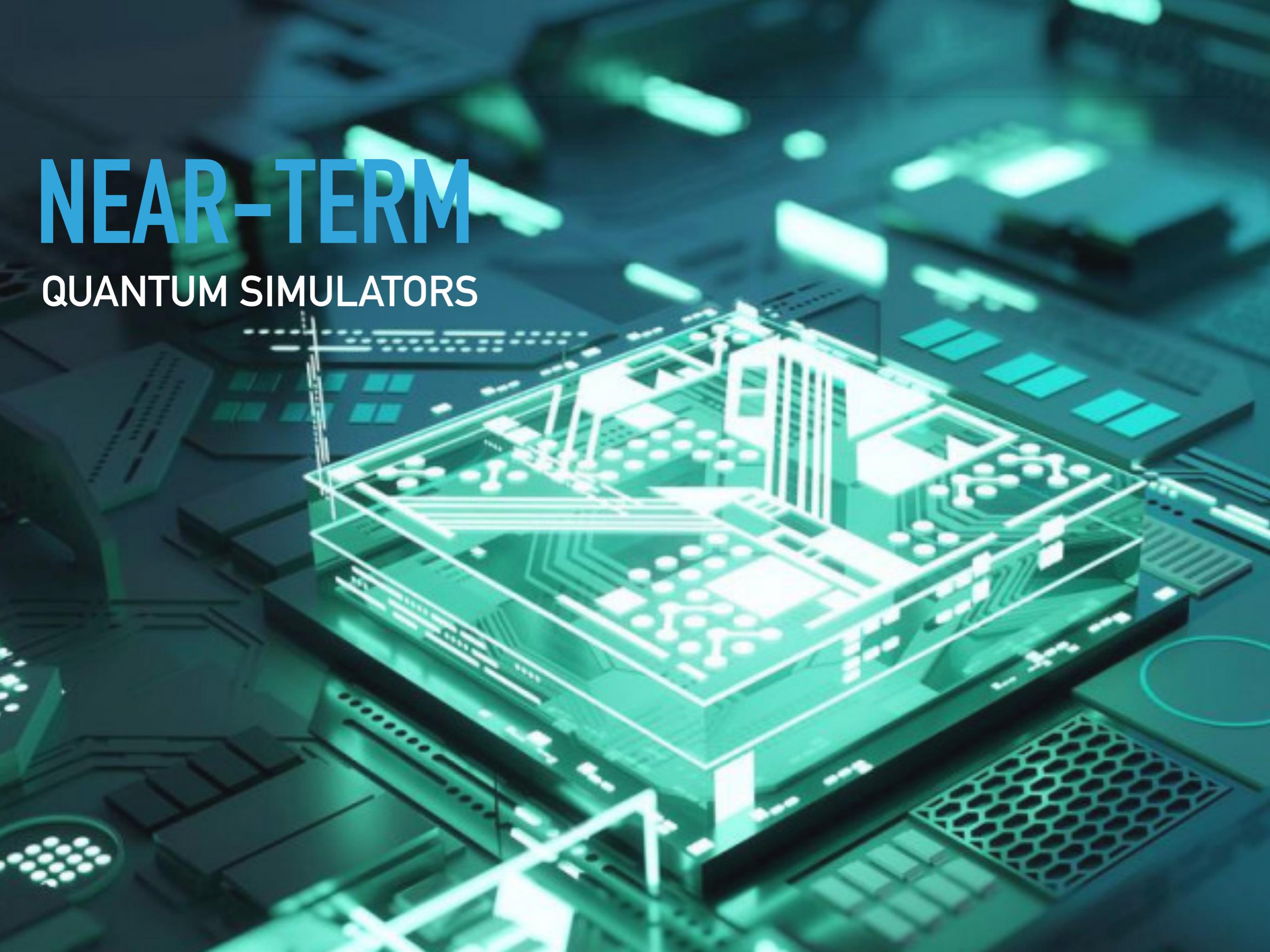
$$\partial \mathcal{L}(\theta) / \partial \theta_i$$

- $\frac{C(z)}{C_{\text{max}}} \geq r^*$
- Estimate expectation values
- $$\langle O_i \rangle_{\theta} = \langle \mathbf{0} | U^\dagger(\theta) O_i U(\theta) | \mathbf{0} \rangle$$

- Can be improved by stochastic gradient methods

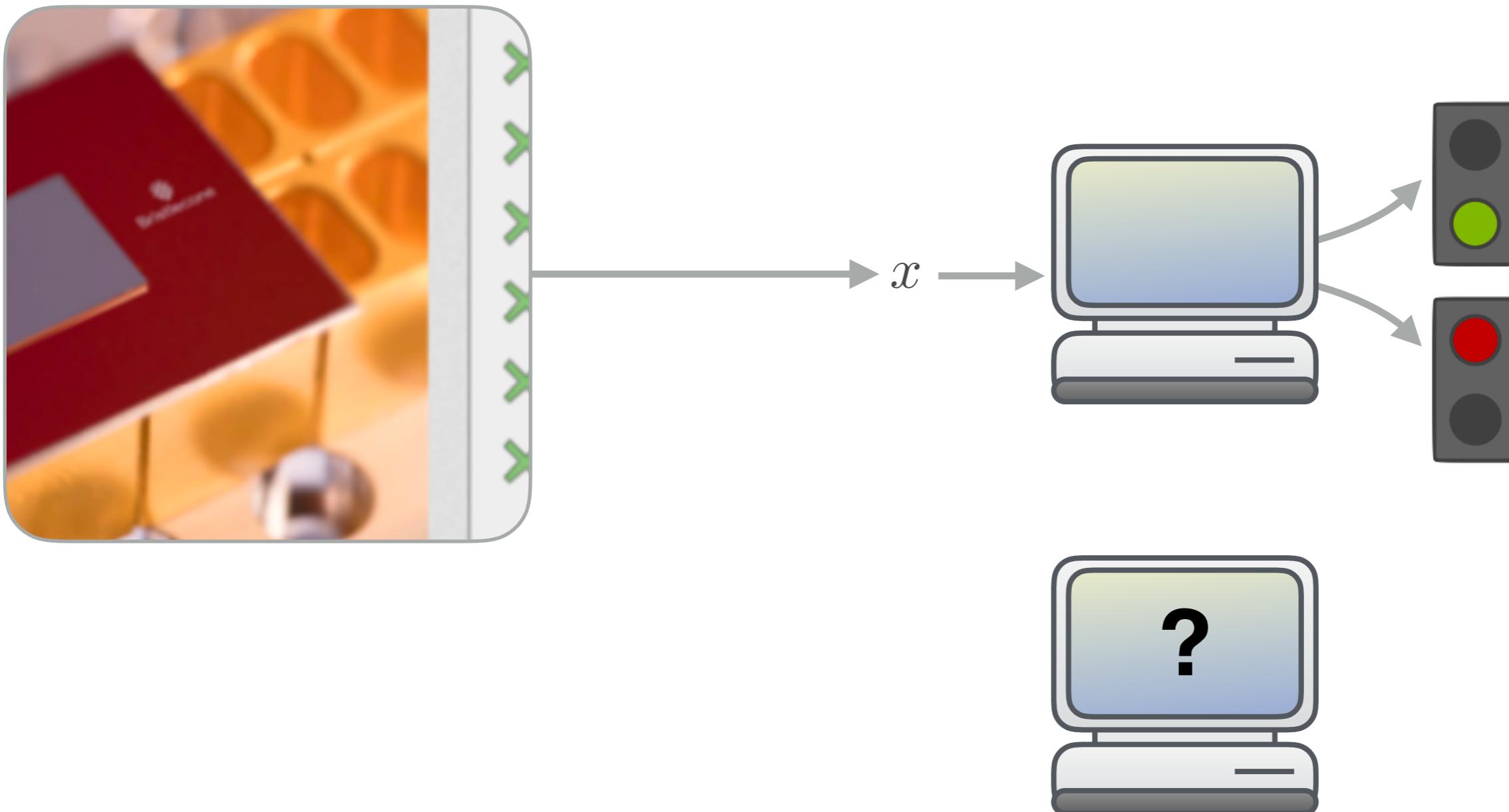


NEAR-TERM QUANTUM SIMULATORS



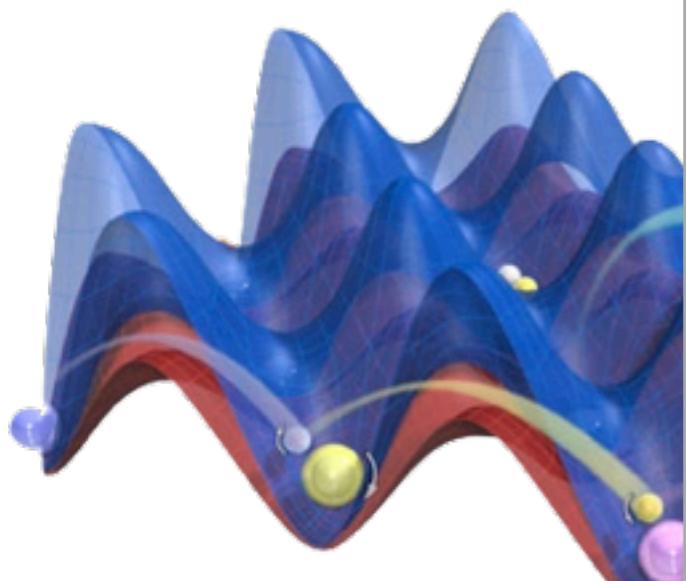
QUANTUM SIMULATORS

- ▶ Can we hope noisy, realistic quantum devices to provide a speedup over classical computers?



QUANTUM SIMULATORS

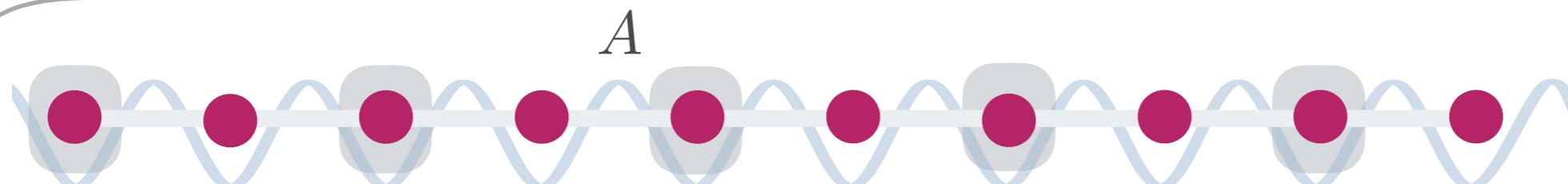
- ▶ Can we hope noisy, realistic quantum devices to provide a speedup over classical computers?



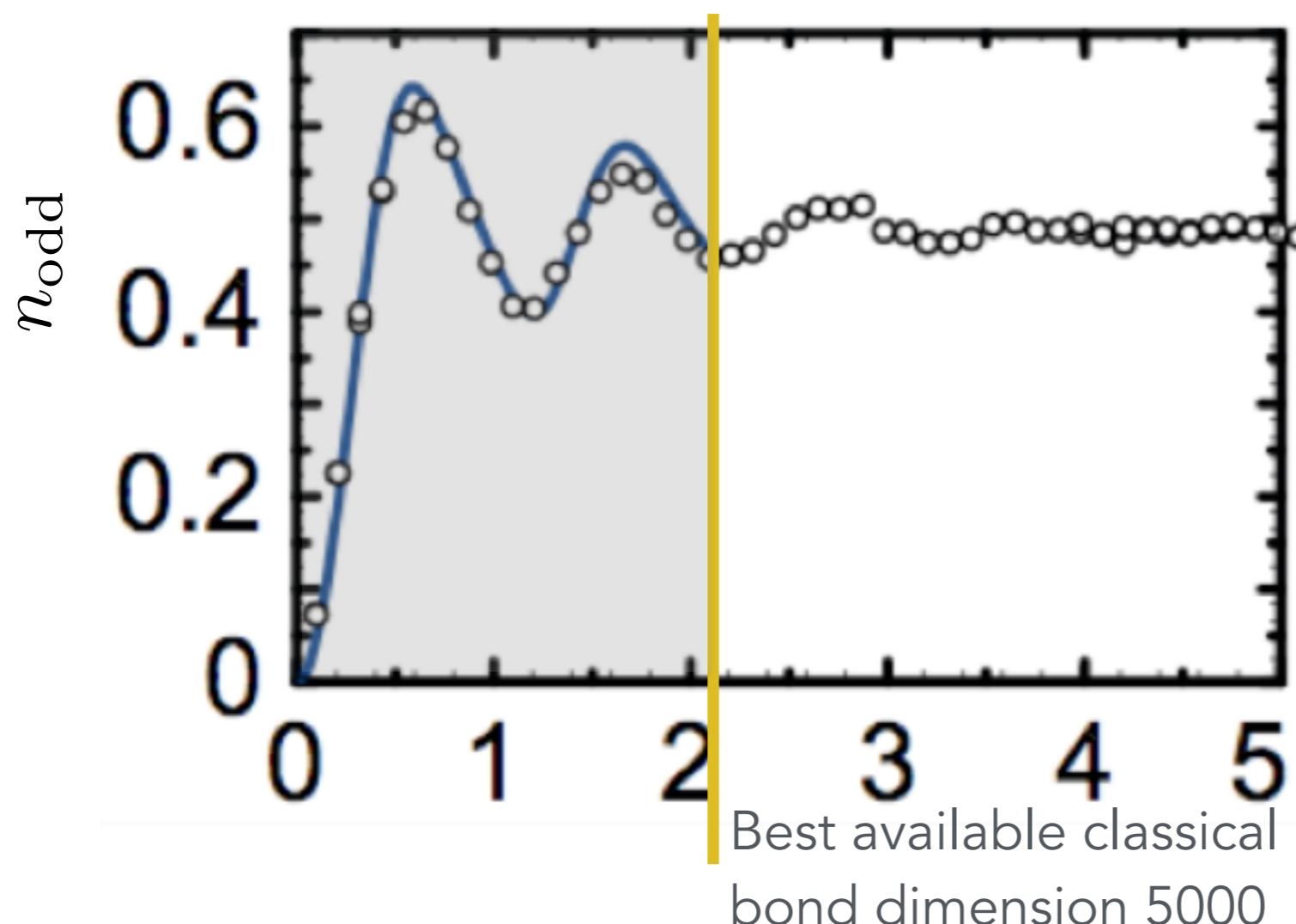
Quantum

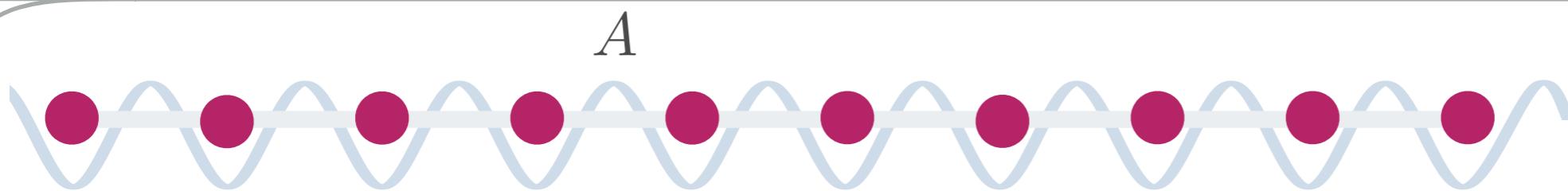
- ▶ Ground state problems
- ▶ “Quenches” $\rho(t) = e^{-itH} \rho e^{itH}$ (time evolution)
- ▶ Slow evolutions, reminiscent of adiabatic quantum computing

QUANTUM SIMULATORS

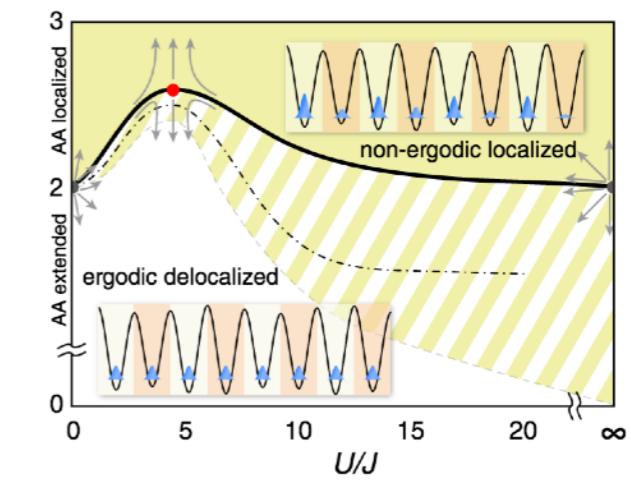
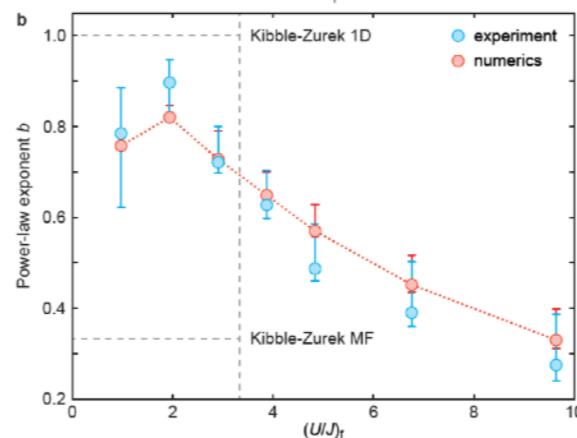


- ▶ Equilibration and thermalisation of atoms in optical super-lattices (MPQ)
- ▶ Imbalance as function of time for $|\psi(0)\rangle = |0, 1, \dots, 0, 1\rangle$ under Bose-Hubbard Hamiltonian





Kibble-Zurek mechanism Many-body localization



1D systems can be efficiently simulated,
2D systems not

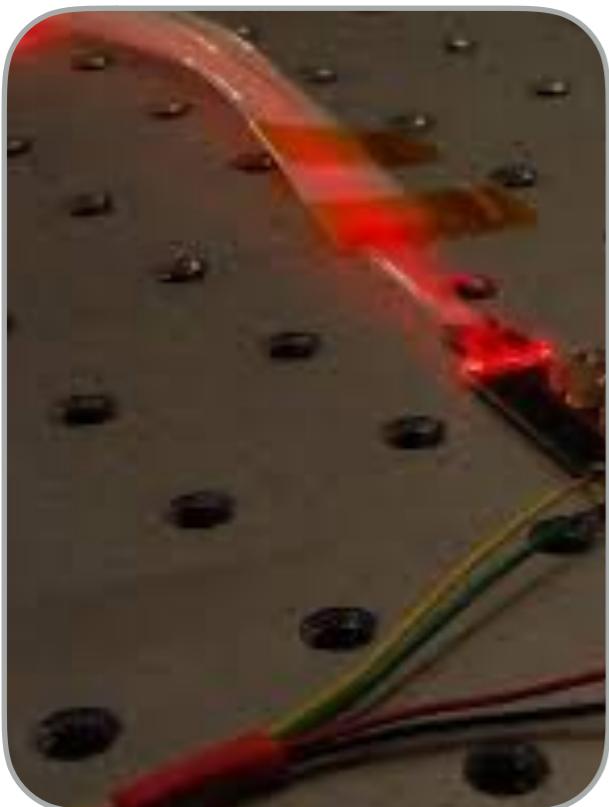
Schreiber, Hodgman, Bordia, Lüschen, Fischer, Vosk, Altman, Schneider, Bloch, Science 349, 842 (2015)

Braun, Friesdorf, Hodgman, Schreiber, Ronzheimer, Riera, del Rey, Bloch, Eisert, Schneider, Proc Natl Acad Sci 112 3641 (2015)

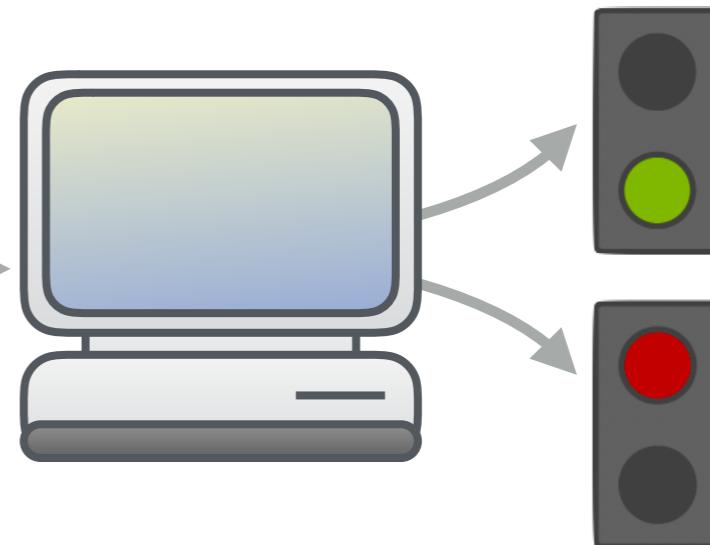
- ▶ To be safe against “lack of imagination”, must prove the hardness of the task in a complexity-theoretic sense

QUANTUM SUPREMACY

- ▶ Can we hope noisy, realistic quantum devices to provide a speedup over classical computers?



→ x



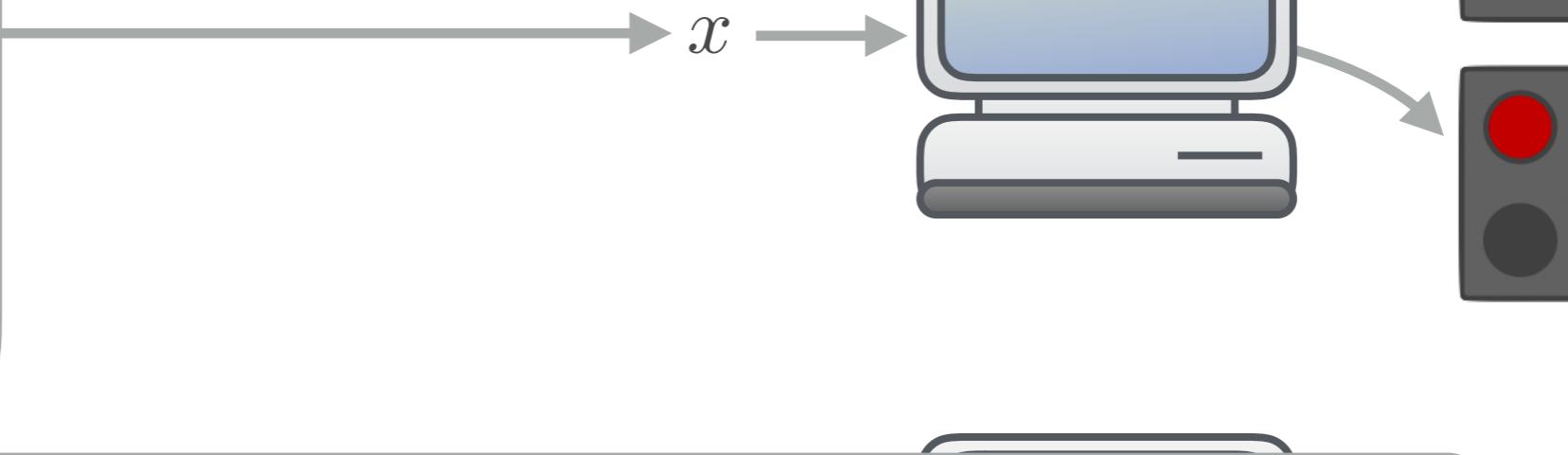
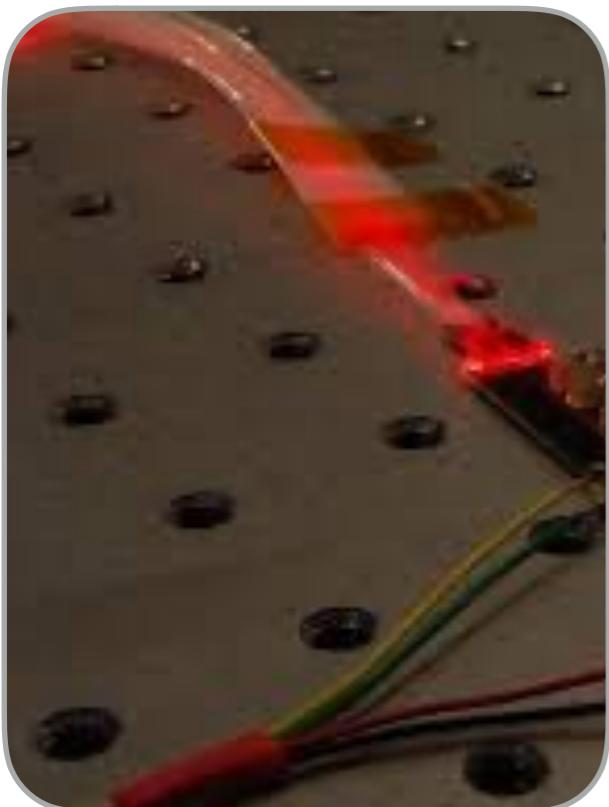
- ▶ To be safe against “lack of imagination”, must prove the hardness of the task in a complexity-theoretic sense

THE QUEST FOR QUANTUM ADANTAGES



QUANTUM ADVANTAGES OR “SUPREMACY”

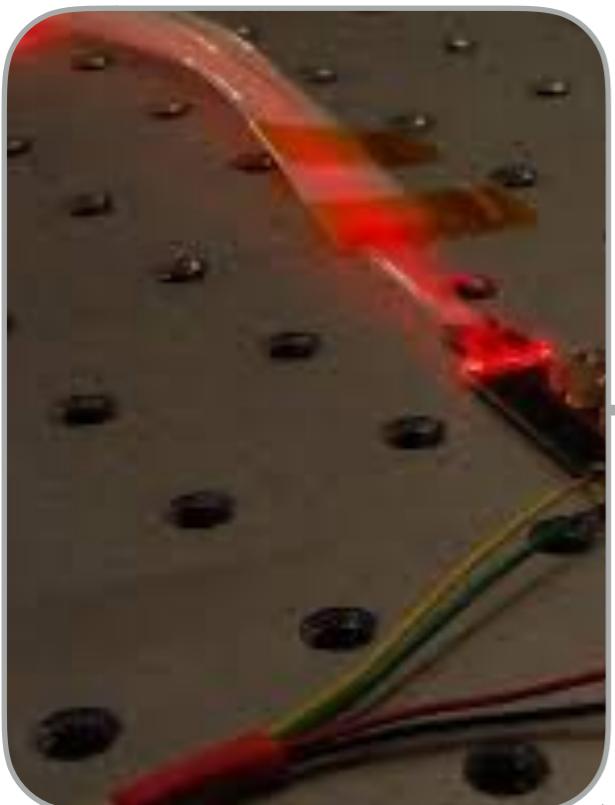
- ▶ Can we hope noisy, realistic quantum devices to provide a speedup over classical computers?



- ▶ To be safe against “lack of imagination”, must prove the hardness of the task in a complexity-theoretic sense

QUANTUM ADVANTAGES OR “SUPREMACY”

- ▶ Can we hope noisy, realistic quantum devices to provide a speedup over classical computers?



NP

NP complete

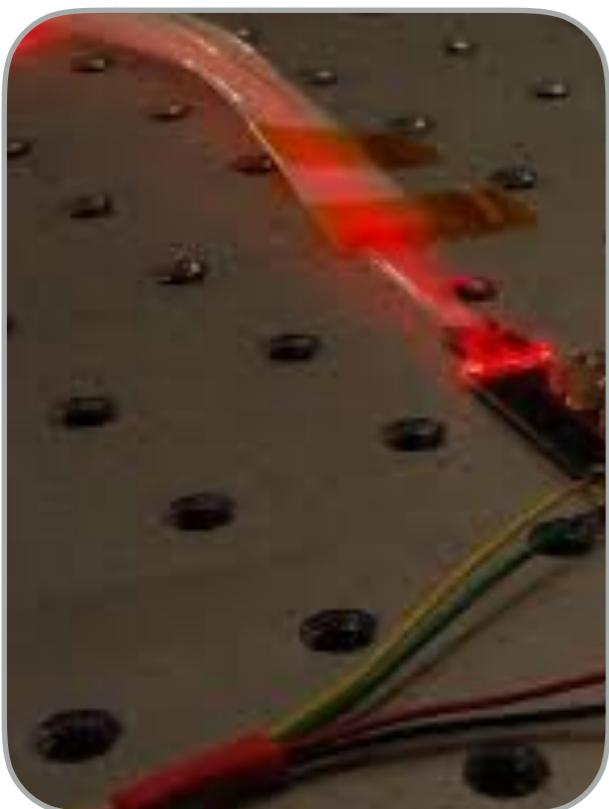
P

▶ To be safe about hardness of

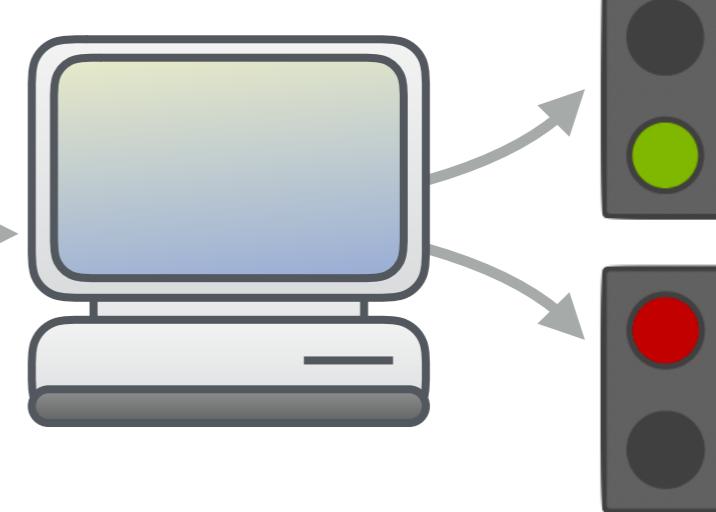
BQP

QUANTUM ADVANTAGES OR “SUPREMACY”

- ▶ Can we hope noisy, realistic quantum devices to provide a speedup over classical computers?

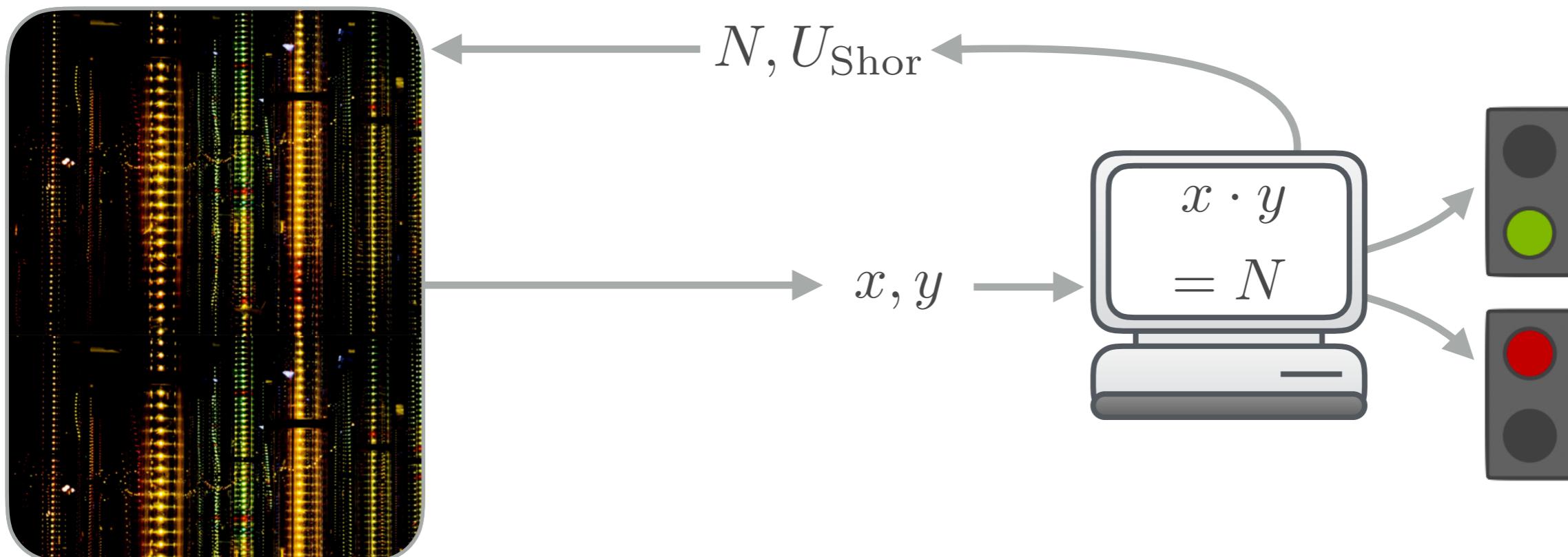


→ x →



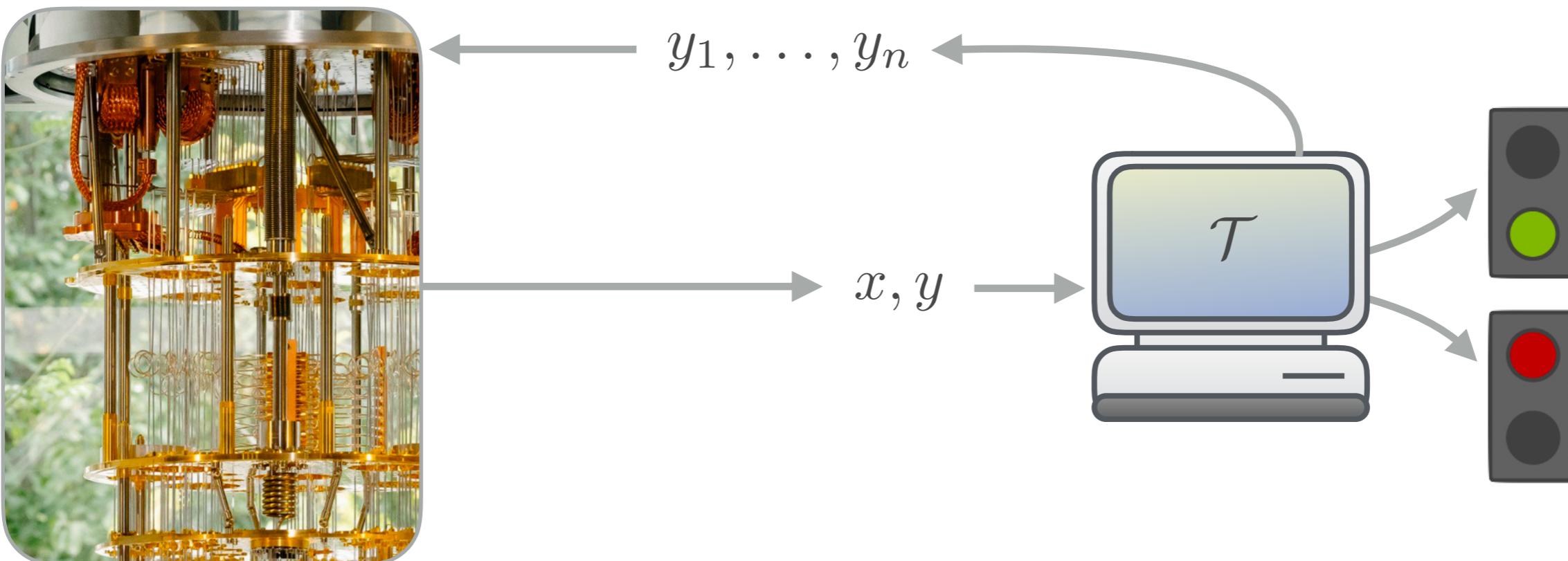
QUANTUM ADVANTAGES OR “SUPREMACY”

► **Computational Bell tests:** Does nature permit computations that are (exponentially) faster than probabilistic Turing machines?



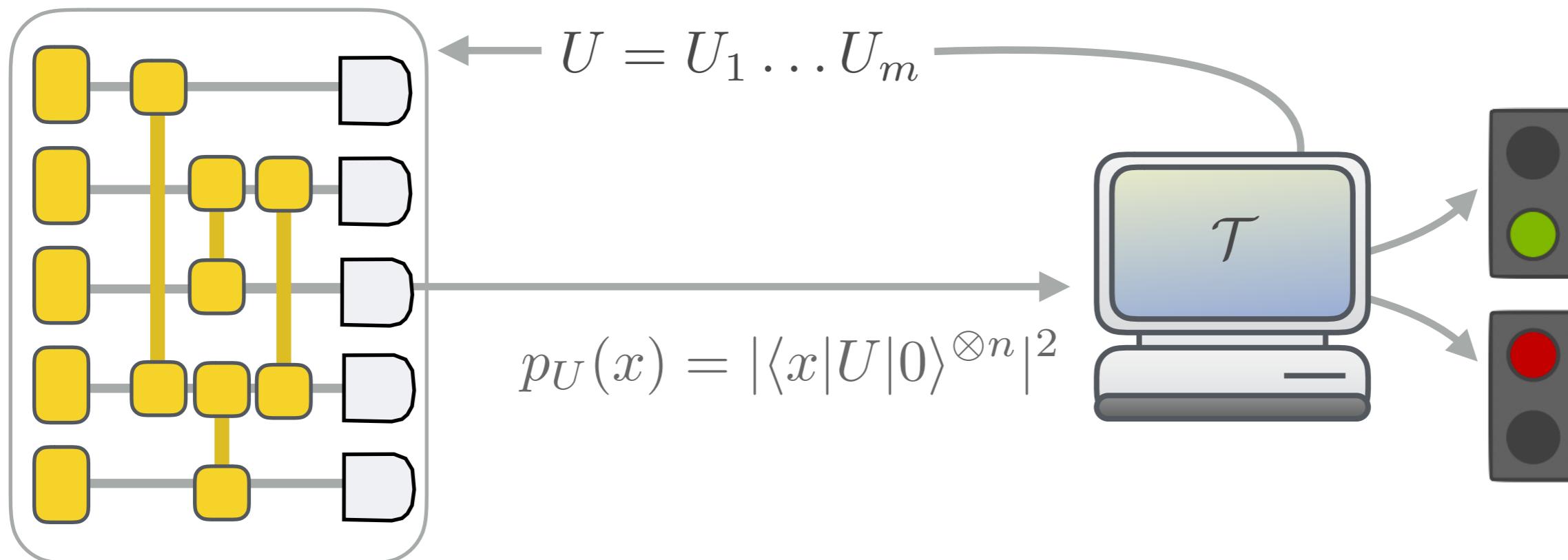
QUANTUM ADVANTAGES OR “SUPREMACY”

- ▶ Single round, classical data, “small” quantum device



RANDOM CIRCUITS

► Sampling tasks natural for QC, but hard on classical computers

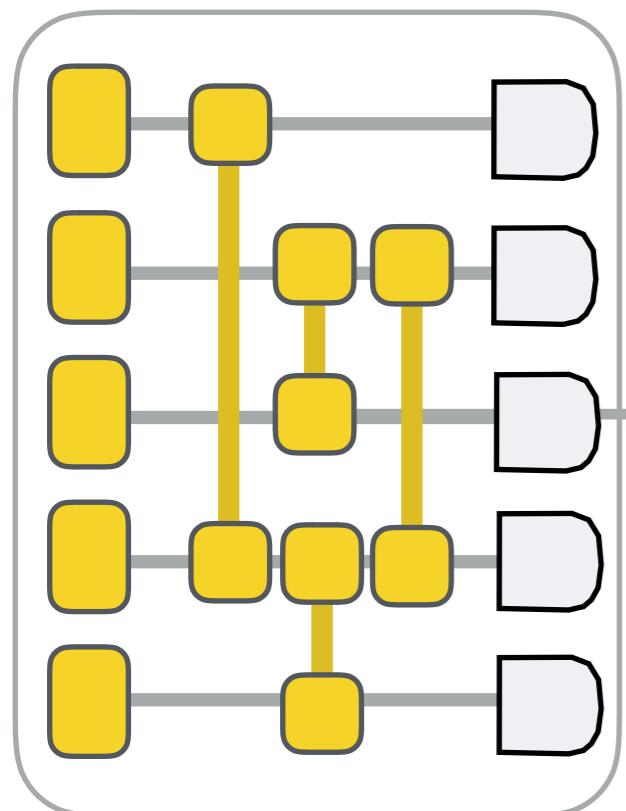


► Random circuits

Boixo, Isakov, Smelzanski, Babbush, Ding, Jiang, Bremner, Martinis, Neven, Nature Physics 14, 595-600 (2018)

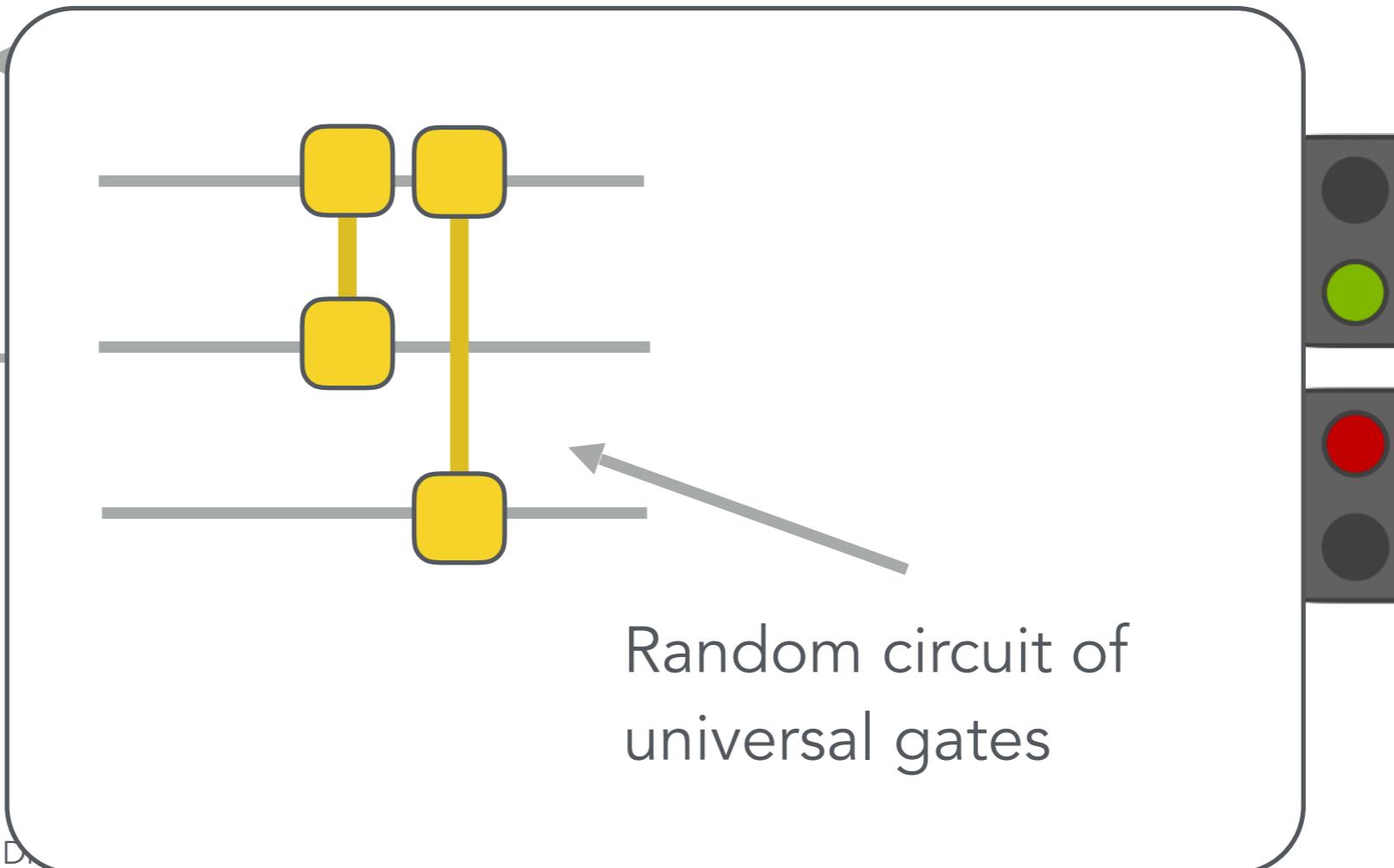
RANDOM CIRCUITS

▶ Sampling tasks natural for QC, but hard on classical computers

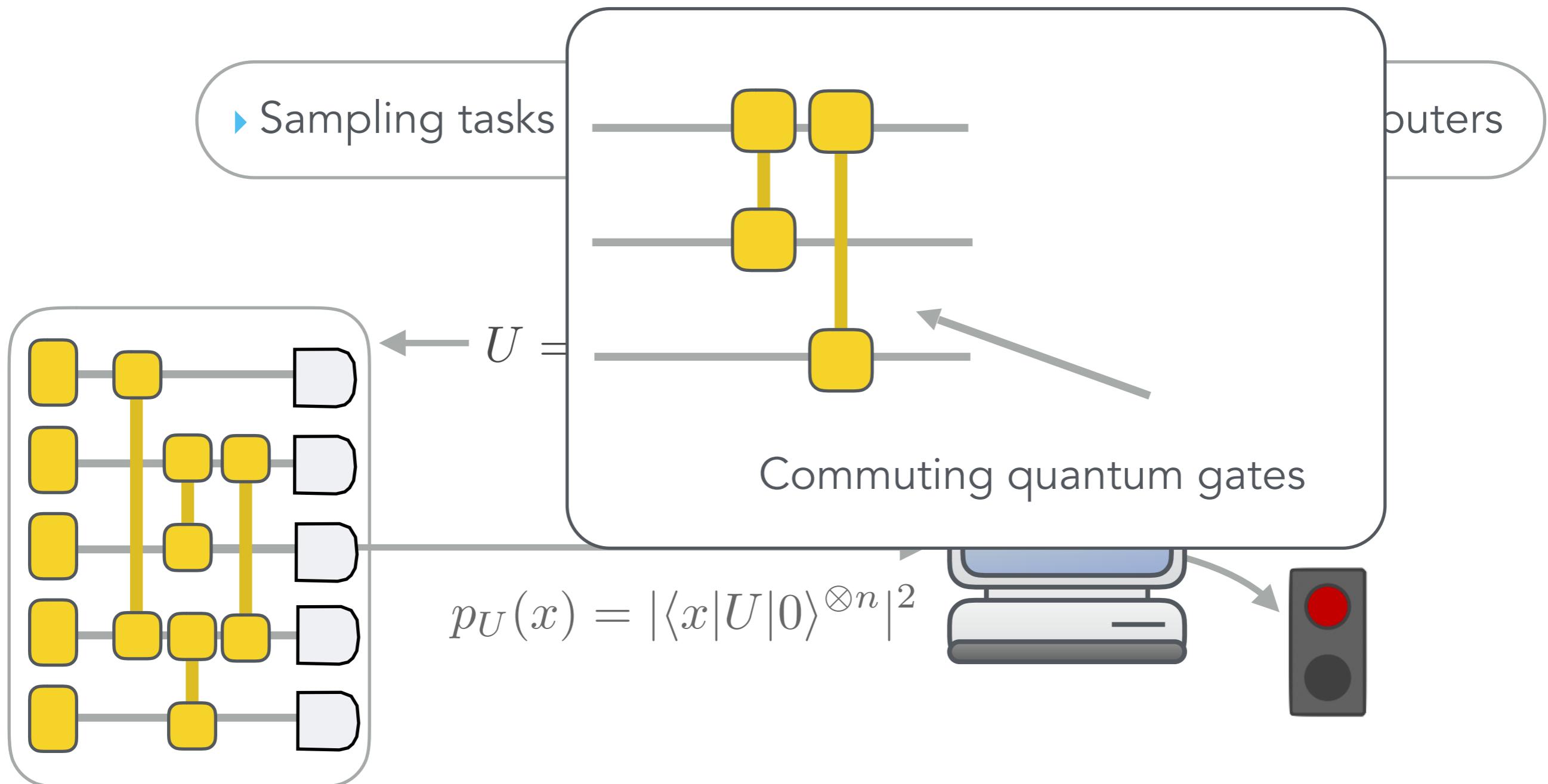


▶ Random circuits

Boixo, Isakov, Smelzanski, Babbush, D.



IQP CIRCUITS

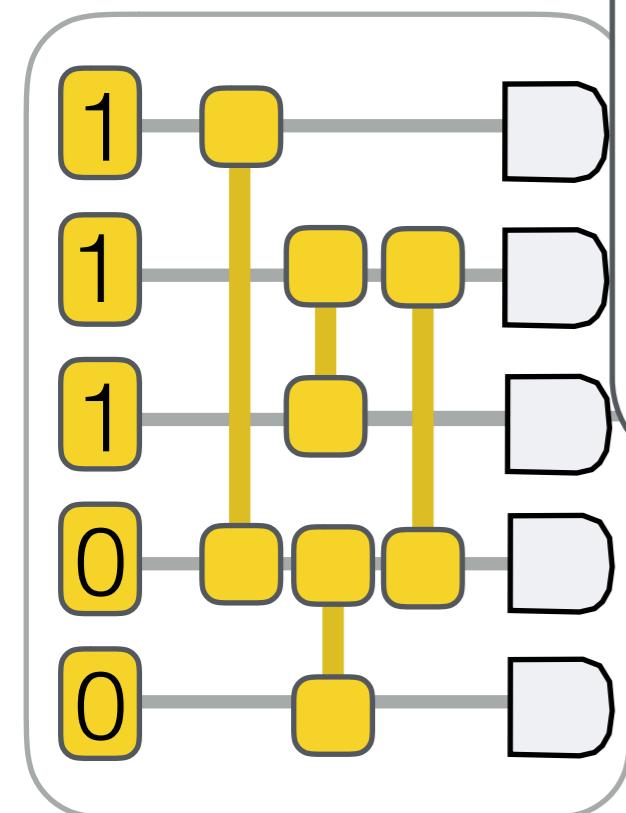


▶ Instantaneous quantum polynomial (IQP) circuits

Bremner, Montanaro, Shepherd: Phys Rev Lett 117, 080501 (2016)

Bremner, Jozsa, Shepherd, arXiv:1005.1407

BOSON SAMPLING

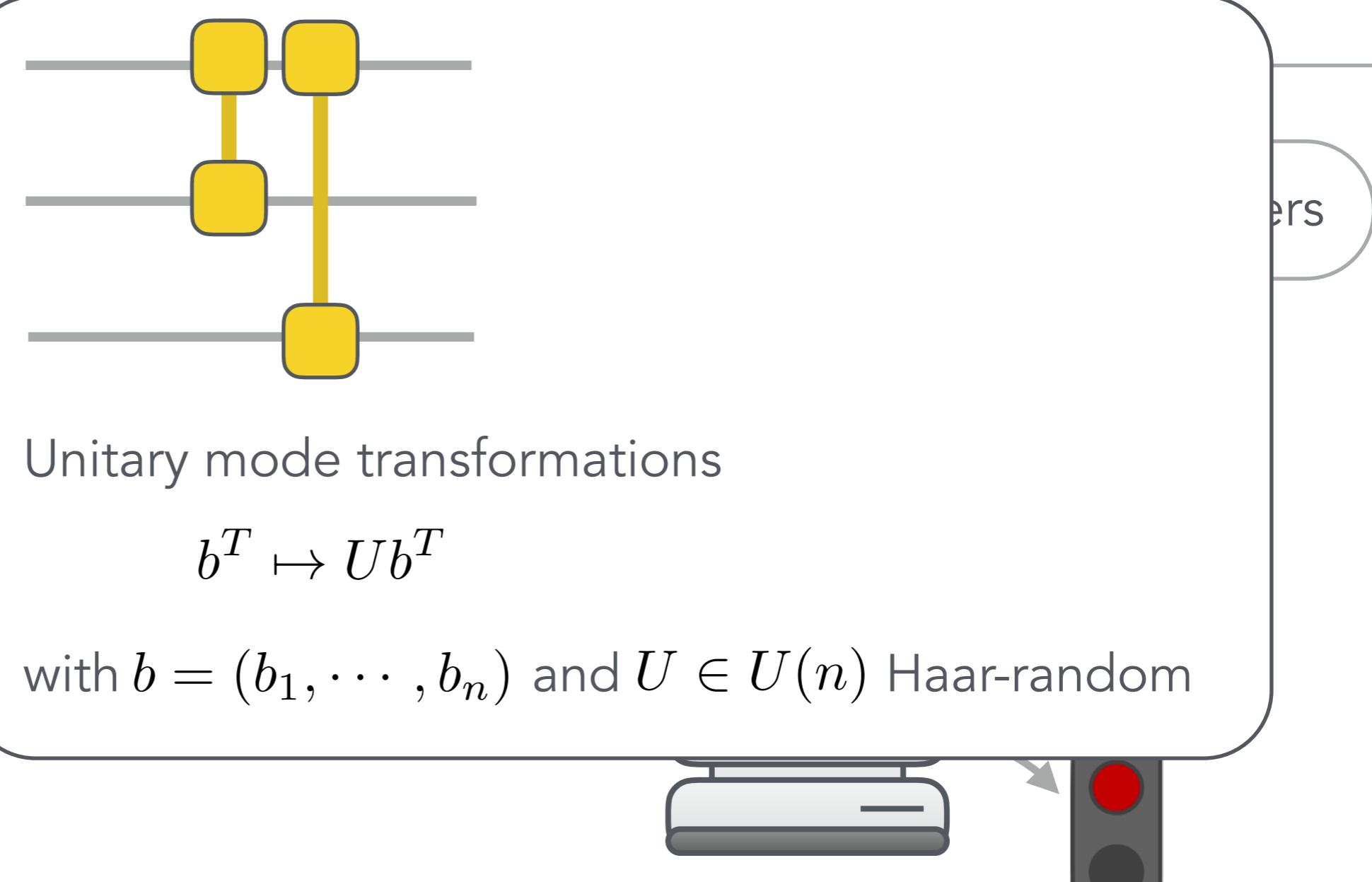


▶ Samp

Unitary mode transformations

$$b^T \mapsto Ub^T$$

with $b = (b_1, \dots, b_n)$ and $U \in U(n)$ Haar-random

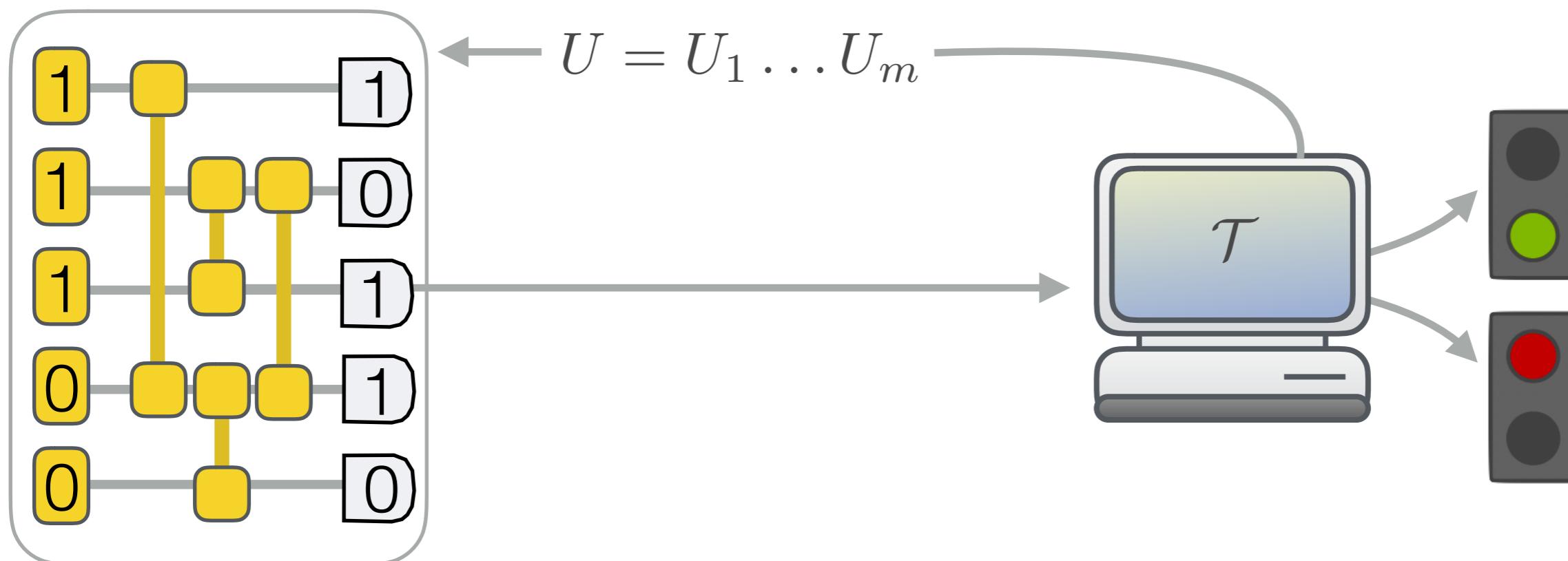


▶ Boson sampling

Aaronson, Arkhipov, Th Comp 9, 143 (2013)

BOSON SAMPLING

► Sampling tasks natural for QC, but hard on classical computers

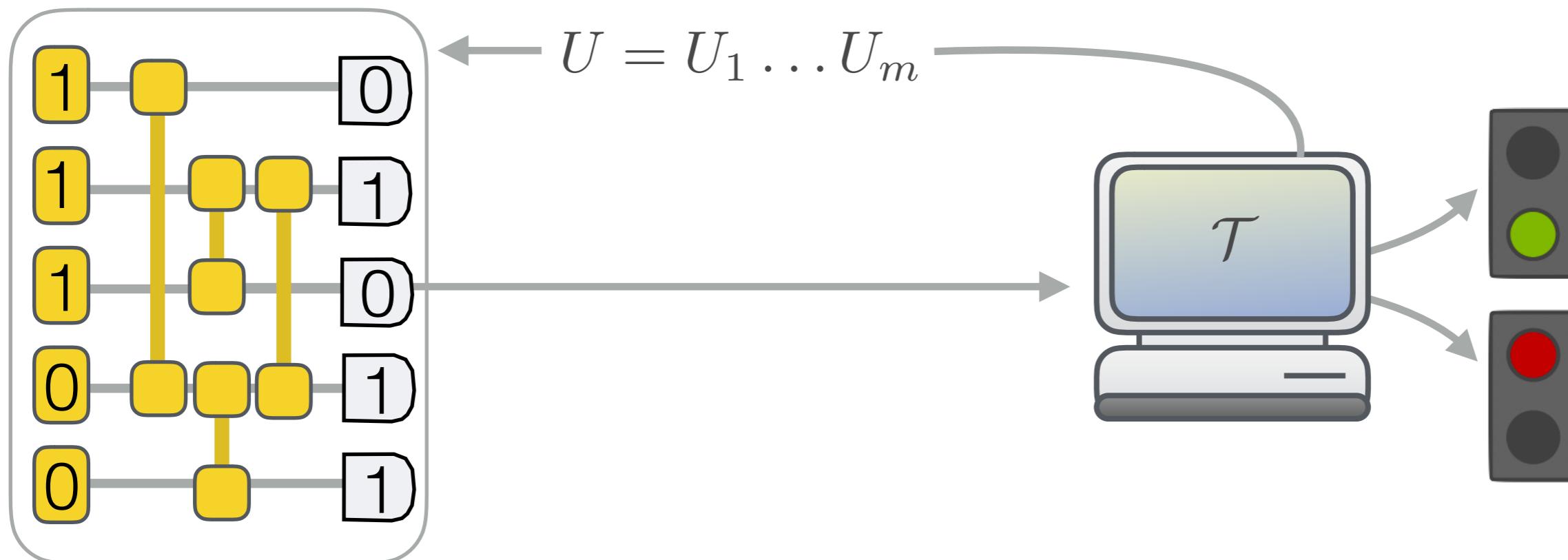


► **Boson sampling**

Aaronson, Arkhipov, Th Comp 9, 143 (2013)

BOSON SAMPLING

► Sampling tasks natural for QC, but hard on classical computers

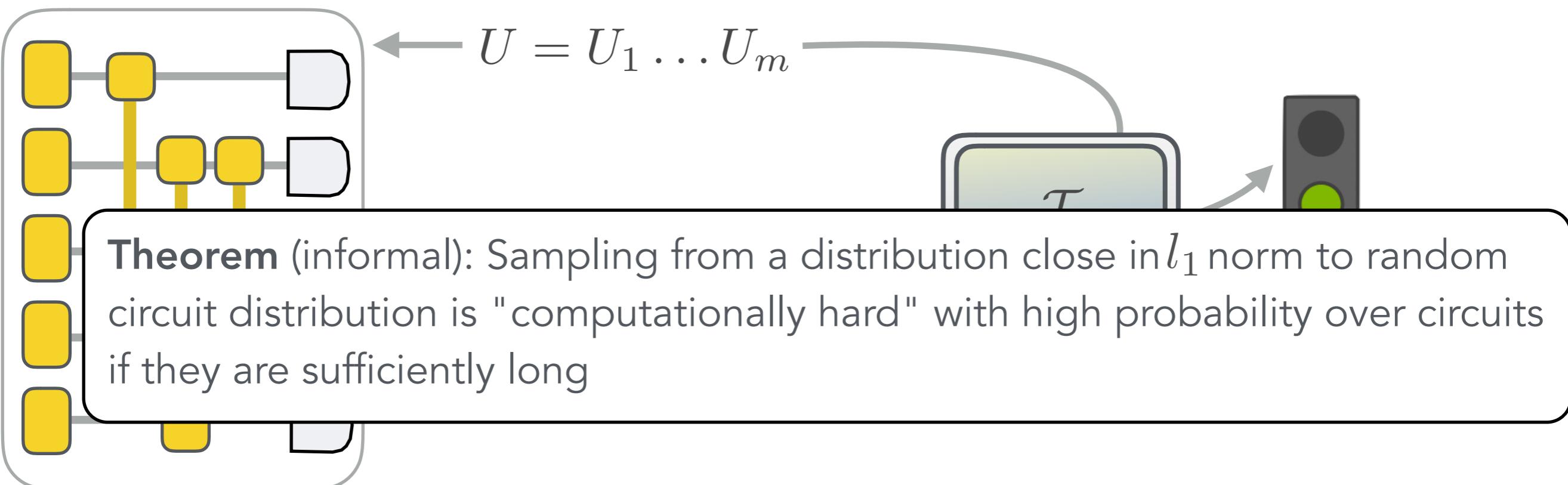


► **Boson sampling**

Aaronson, Arkhipov, Th Comp 9, 143 (2013)

HARDNESS OF RANDOM CIRCUITS

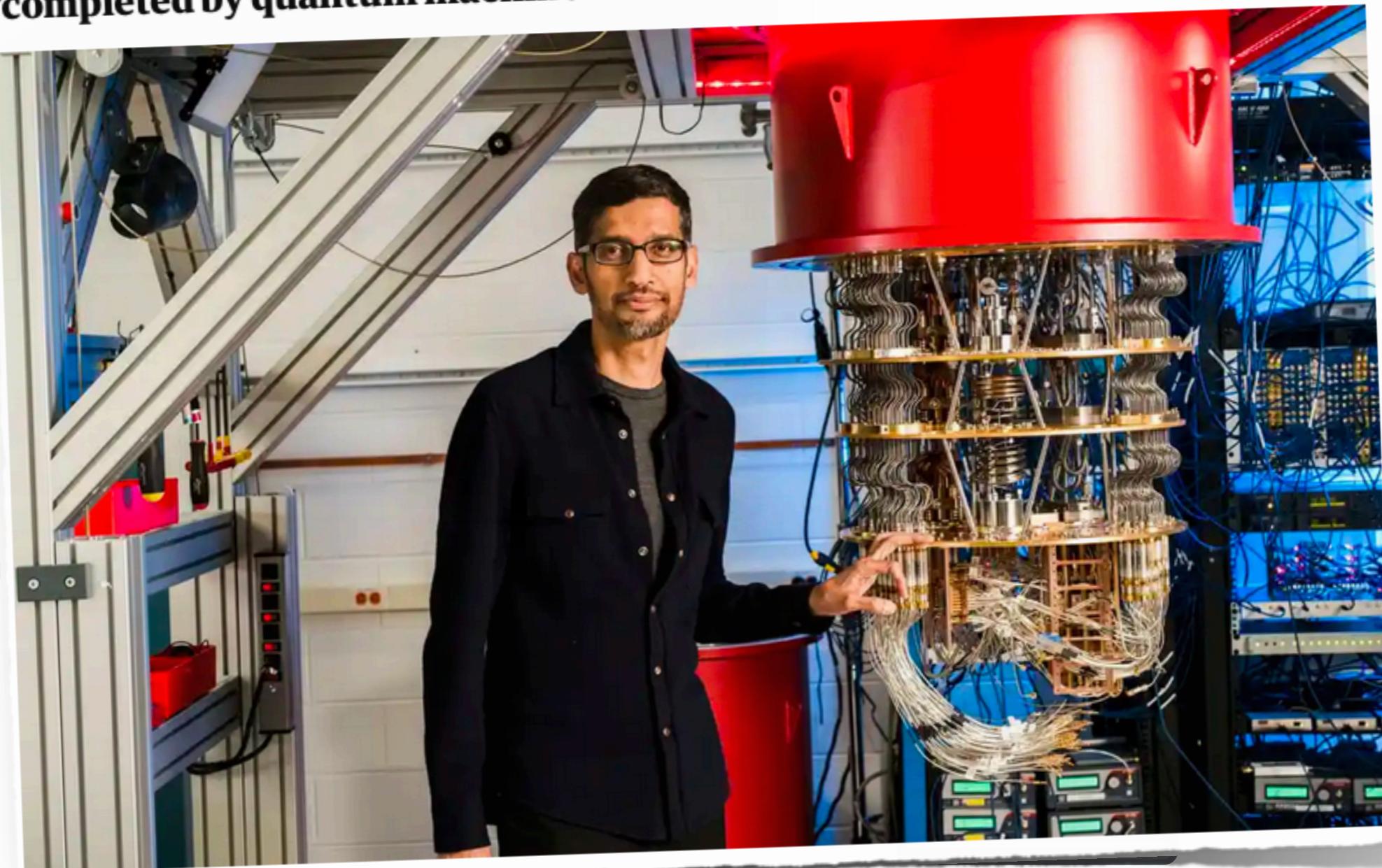
- Sampling tasks natural for QC, but hard on classical computers



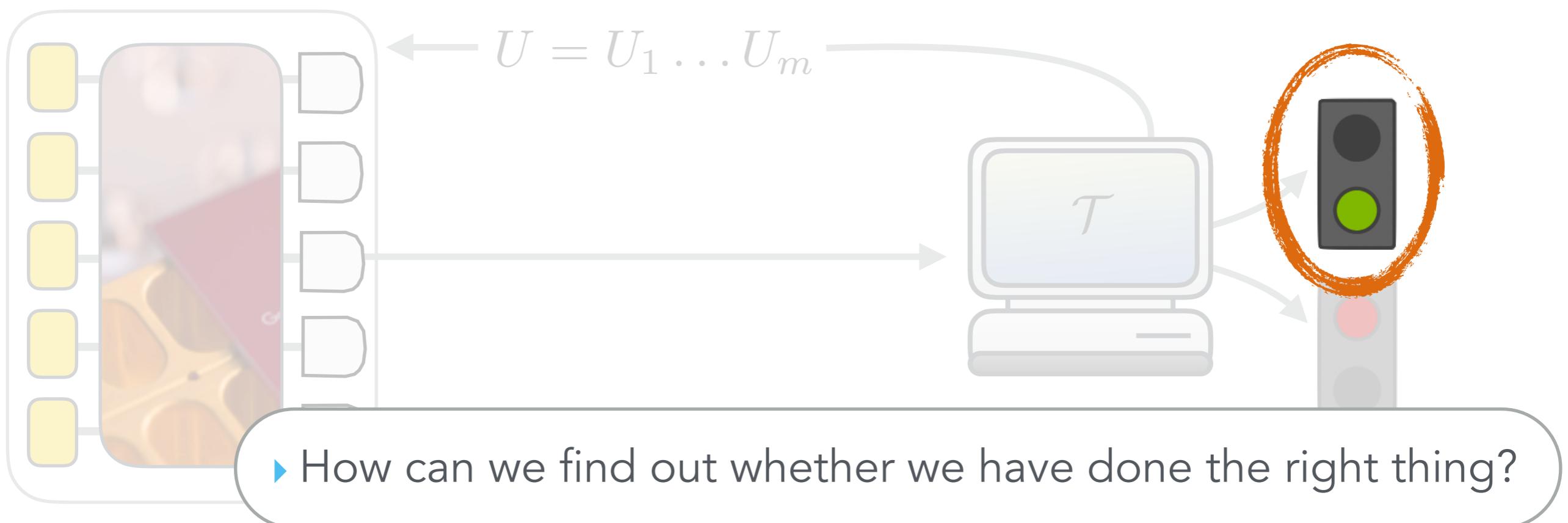
Google
breakthrough

Google claims it has achieved 'quantum supremacy' - but IBM disagrees

**Task that would take most powerful supercomputer 10,000 years
'completed by quantum machine in minutes'**



VERIFICATION?

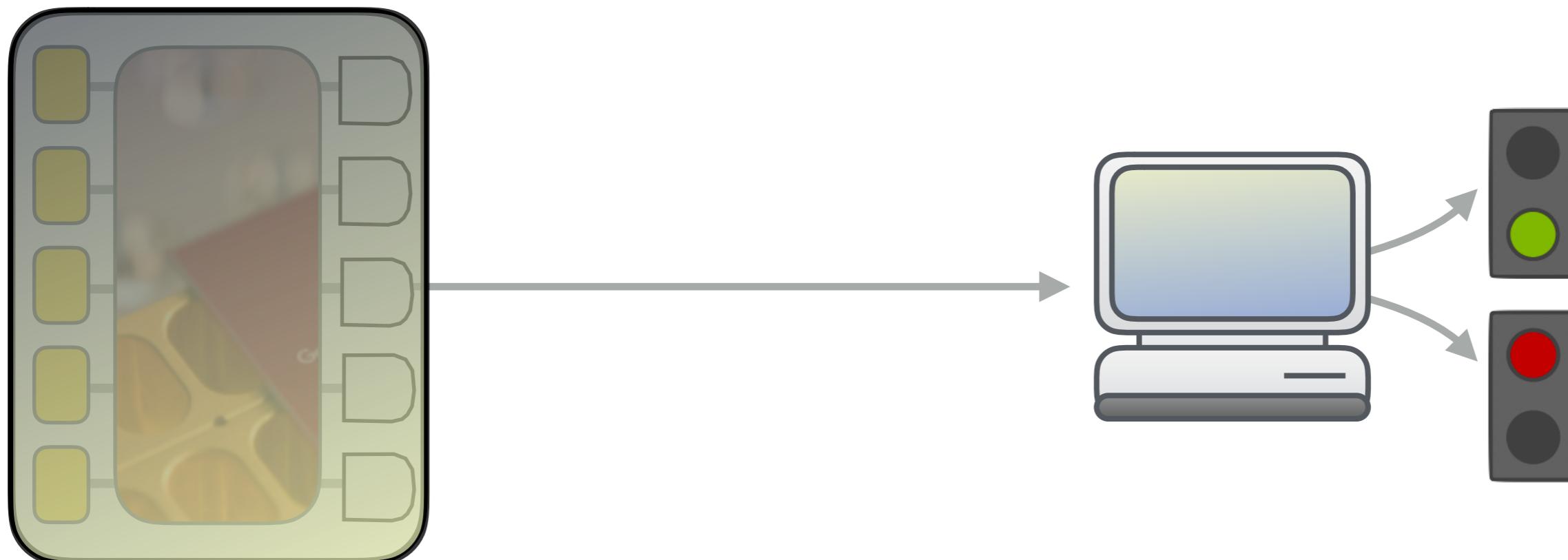


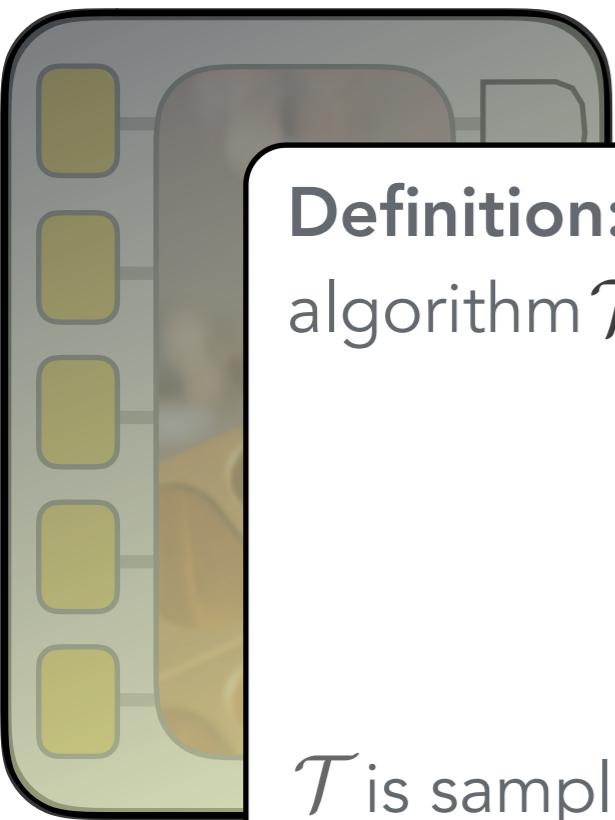


BLACK BOX CERTIFICATION

LOOKING AT DATA FROM QUANTUM DEVICES

VERIFICATION?





Definition: A black-box certification test with sample complexity m is an algorithm $\mathcal{T} : (\{0, 1\}^n)^m \rightarrow \{0, 1\}$

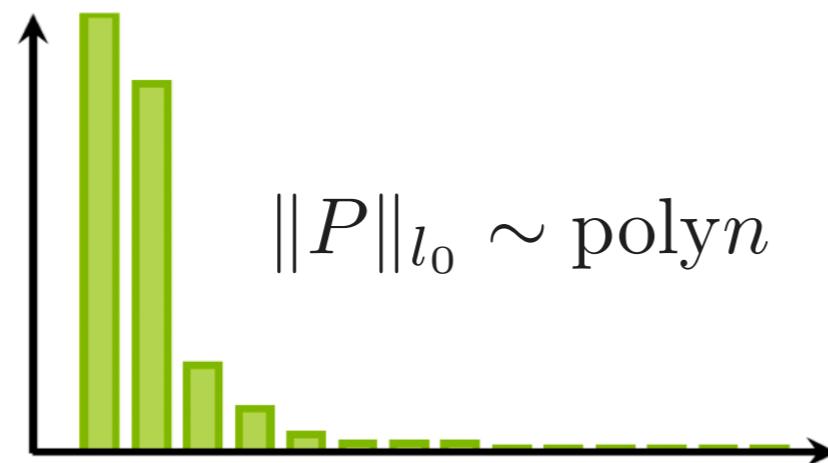
$$Q = P \Rightarrow \Pr_{X \sim Q}(\mathcal{T}(X) = 1) \geq \frac{2}{3}$$

$$\|Q - P\|_{l_1} > \epsilon \Rightarrow \Pr_{X \sim Q}(\mathcal{T}(X) = 1) < \frac{1}{3}.$$

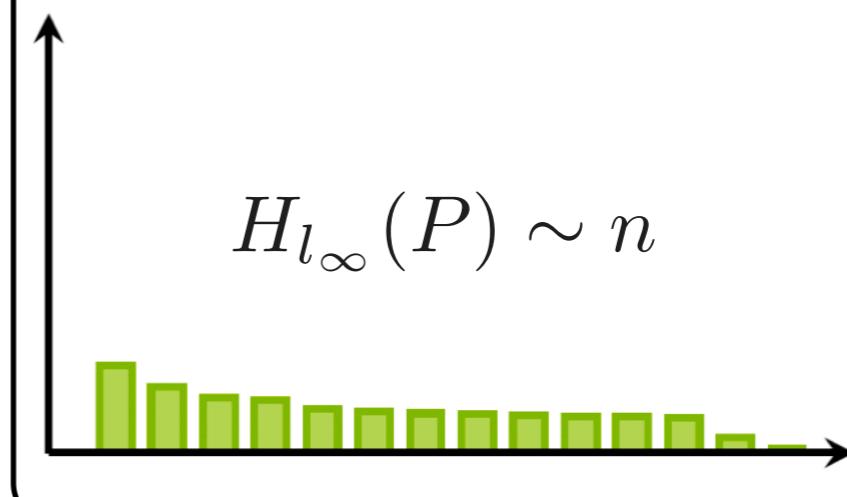
\mathcal{T} is sample-efficient if $m \sim \text{poly } n$

VERIFICATION

► Concentration



► Anti-concentration



► Black box certifiable
from $O(\text{poly}(n))$ many
samples

► Every black-box test
requires at least $O(\sqrt{2^n})$
many samples

VERIFICATION?

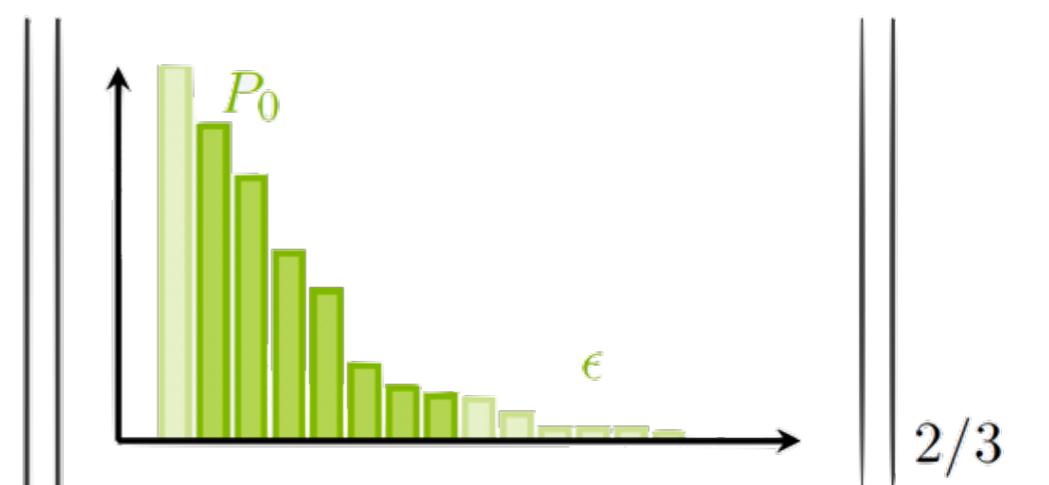
► **Theorem** (informal): Boson sampling, IQP circuits, random circuits cannot be black-box certified from polynomially many samples



► One needs further assumptions



► Proof tool: $\|P_{-\epsilon}^{\max}\|_{2/3} =$

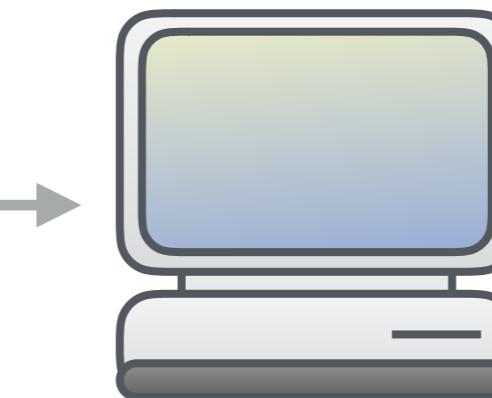
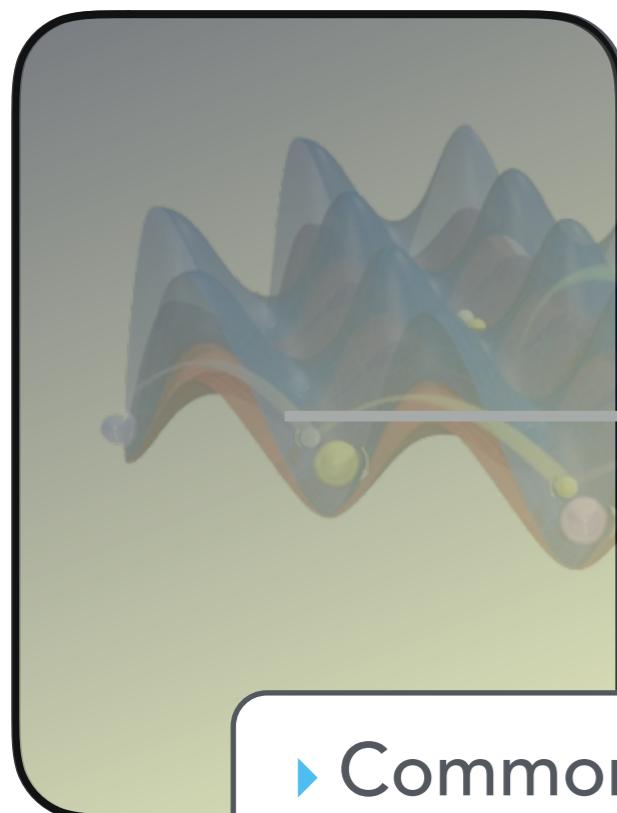


Valiant, Valiant, ECCC 111 (2013)

Hangleiter, Kliesch, Eisert, Gogolin, arXiv:1812.01023

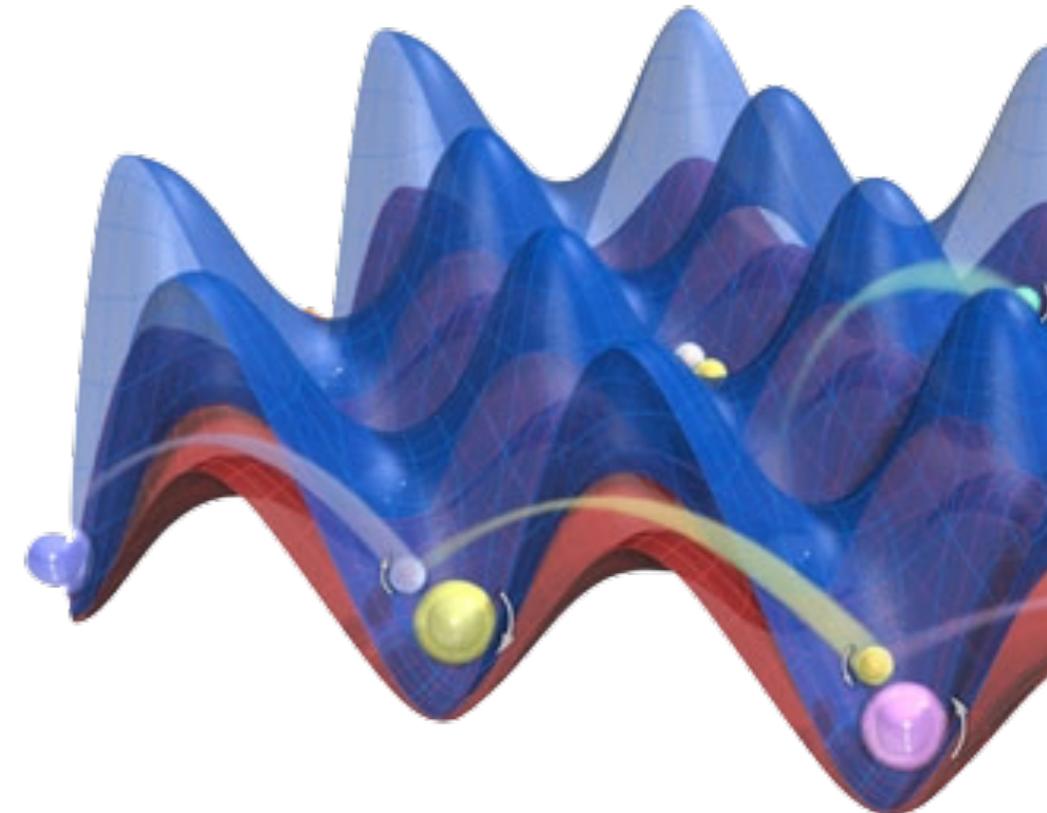
Harrow at al, in preparation

VERIFICATION?



?

- ▶ **Common prejudice:** In order to be able to verify a quantum simulation, one needs to be able to efficiently simulate it



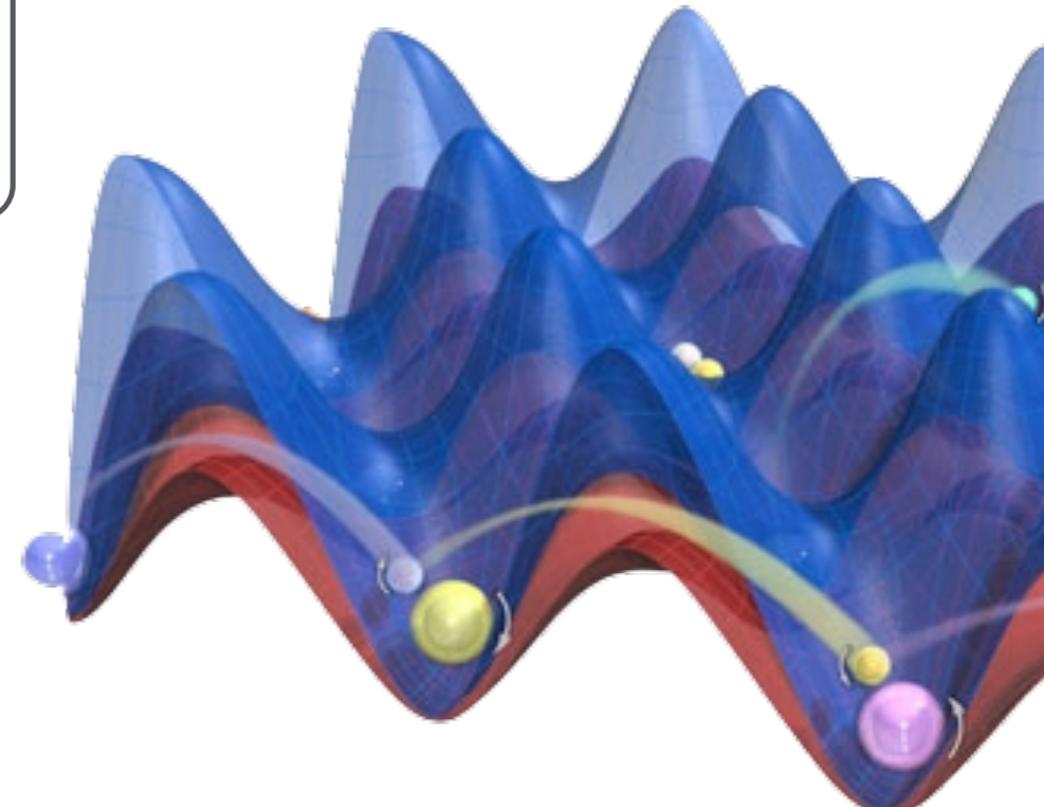
BEYOND BLACK BOXES

A SIMPLE NEAR-TERM QUANTUM ADVANTAGE SCHEME

A FEASIBLE SCHEME

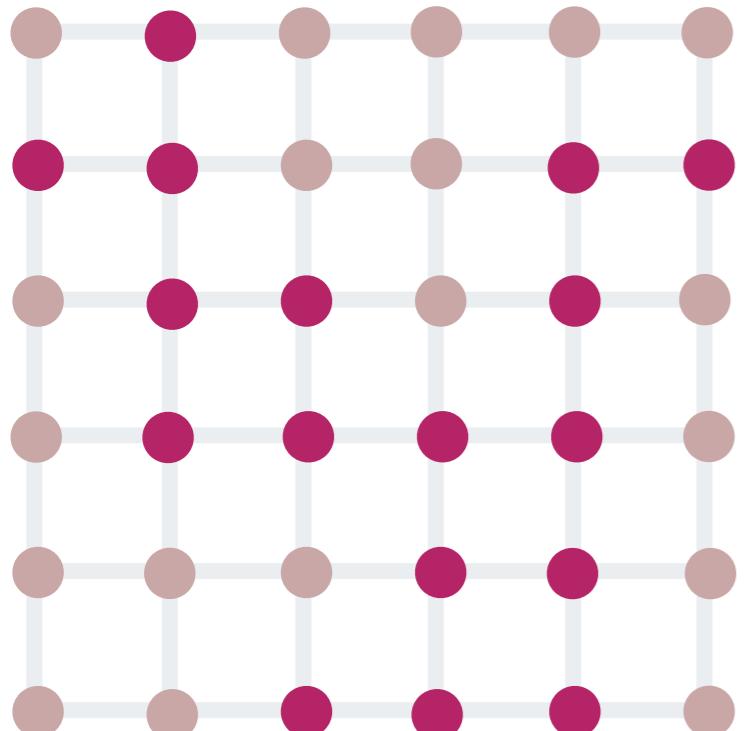
► What is the **simplest conceivable scheme** that can show quantum supremacy?

- Simple **Hamiltonian** quantum simulation
- **Hardness proofs** with l_1 -norm error

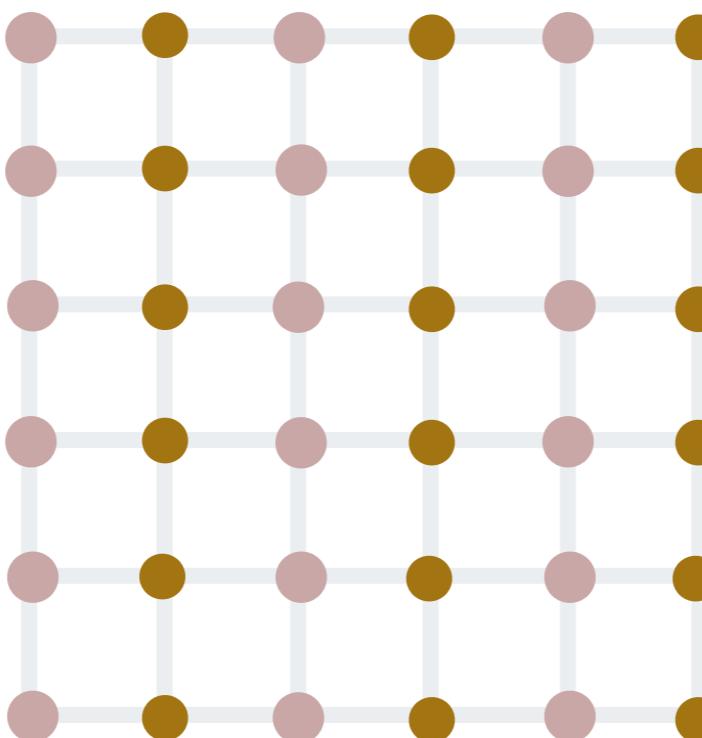


SIMPLE ISING MODELS

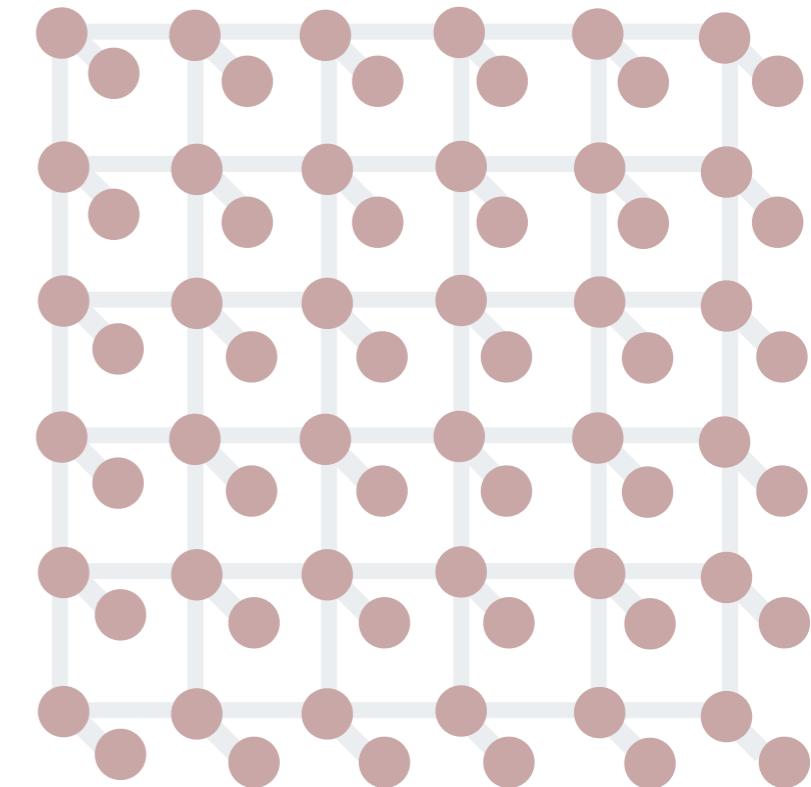
► What is the **simplest conceivable scheme** that can show quantum supremacy?



Random



Quasi-periodic



Translationally invariant

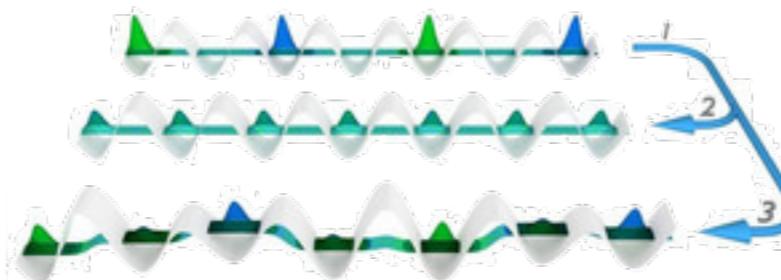
SIMPLE ISING MODELS

- ▶ Prepare N qubits in $n \times m$ square lattice in product

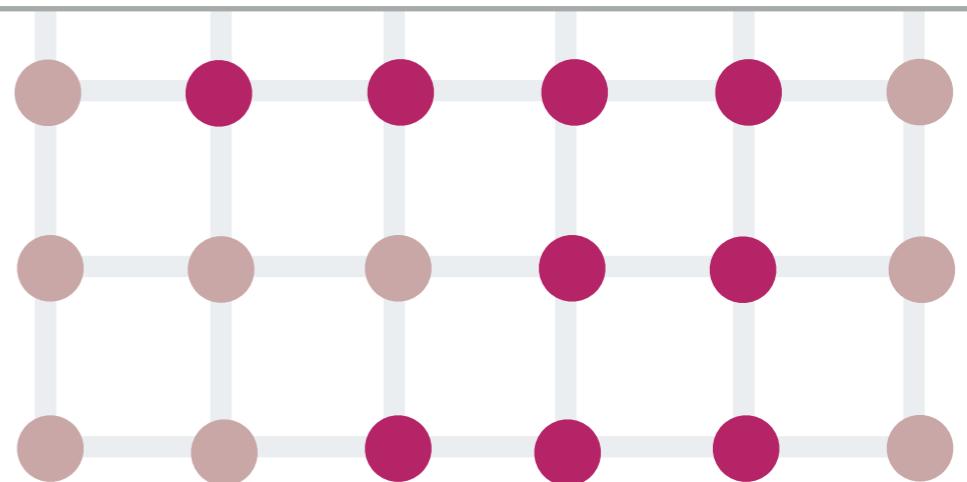
$$|\psi_\beta\rangle = \otimes_{i,j=1}^{n,m} (|0\rangle + e^{i\beta_{i,j}} |1\rangle)$$

with $\beta_{i,j} \in \{0, \pi/4\}$, {●, ●} i.i.d. randomly

- ▶ Reminscient of disordered optical lattices



Schreiber, Hodgman, Bordia, Lüschen, Fischer, Vosk, Altman, Schneider, Bloch, Science 349, 842 (2015)



SIMPLE ISING MODELS

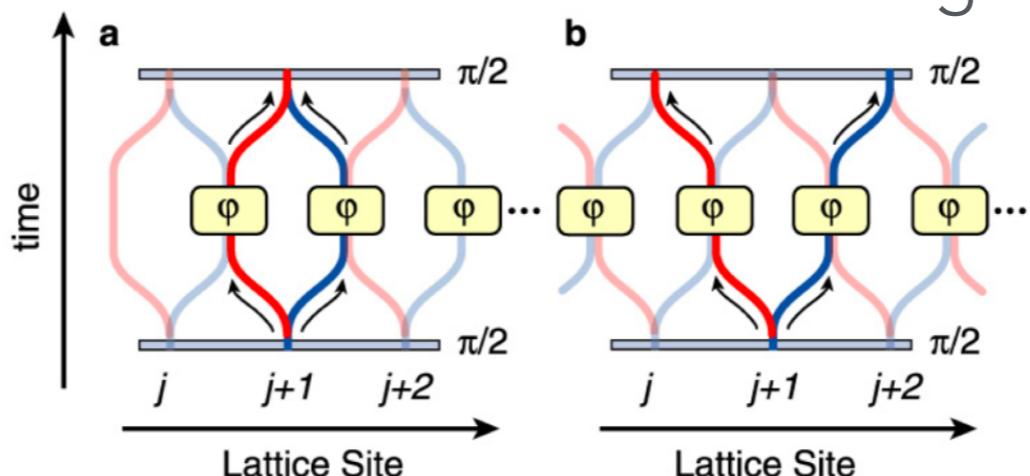
- ▶ Prepare N qubits in $n \times m$ square lattice in product

$$|\psi_\beta\rangle = \otimes_{i,j=1}^{n,m} (|0\rangle + e^{i\beta_{i,j}} |1\rangle)$$

with $\beta_{i,j} \in \{0, \pi/4\}$, i.i.d. randomly

- ▶ Quench to $H = \sum_{(i,j) \in E} Z_i Z_j + \frac{\pi}{4} \sum_{i \in V} Z_i$ and evolve under $U = e^{iH}$

- ▶ Controlled coherent collisions long realized



Mandel, Greiner, Widera, Rom, Hänsch, Bloch, Nature, 425, 937 (2003)

SIMPLE ISING MODELS

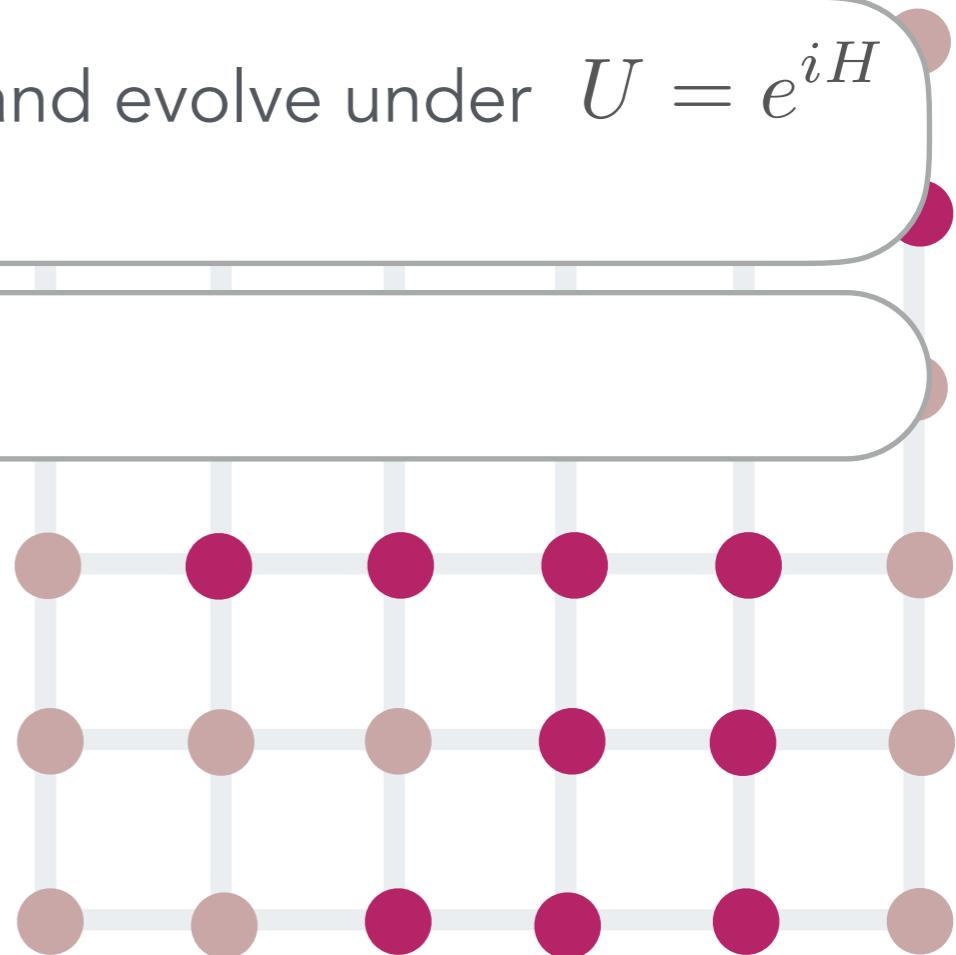
- ▶ Prepare N qubits in $n \times m$ square lattice in product

$$|\psi_\beta\rangle = \otimes_{i,j=1}^{n,m} (|0\rangle + e^{i\beta_{i,j}}|1\rangle)$$

with $\beta_{i,j} \in \{0, \pi/4\}$, {●, ●} i.i.d. randomly

- ▶ Quench to $H = \sum_{(i,j) \in E} Z_i Z_j + \frac{\pi}{4} \sum_{i \in V} Z_i$ and evolve under $U = e^{iH}$

- ▶ Measure all qubits in X -basis



SIMPLE ISING MODELS

- ▶ Prepare N qubits in $n \times m$ square lattice in product

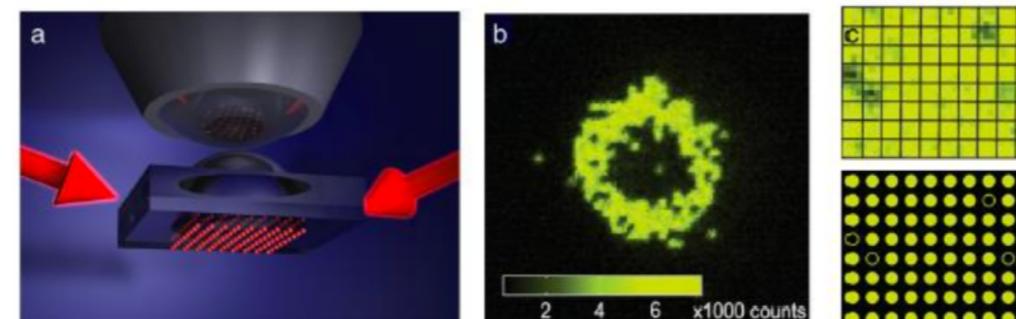
$$|\psi_\beta\rangle = \otimes_{i,j=1}^{n,m} (|0\rangle + e^{i\beta_{i,j}} |1\rangle)$$

with $\beta_{i,j} \in \{0, \pi/4\}$, {●, ●} i.i.d. randomly

- ▶ Quench to $H = \sum_{(i,j) \in E} Z_i Z_j + \frac{\pi}{4} \sum_{i \in V} Z_i$ and evolve under $U = e^{iH}$

- ▶ Measure all qubits in X -basis

- ▶ Single-site addressing possible (within limits)

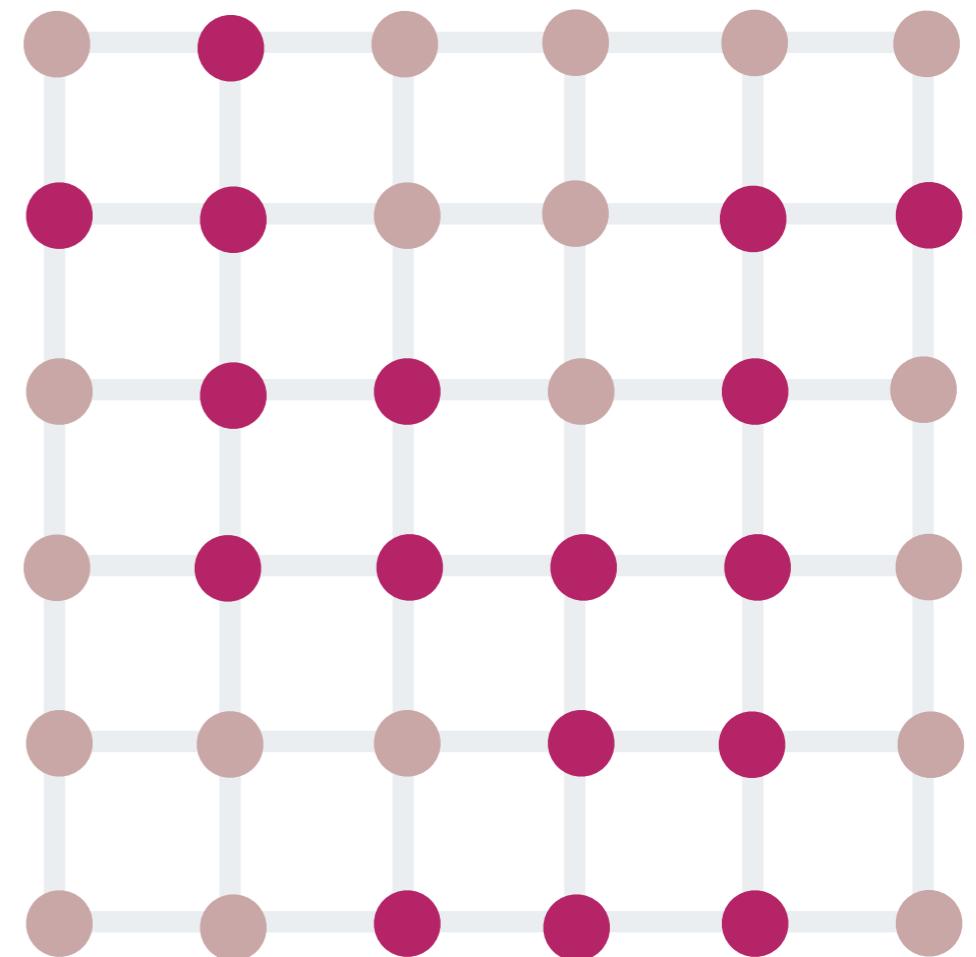


Bakr, Gillen, Peng, Foelling, Greiner, Nature 462, 74–77 (2009)

Weitenberg, Endres, Sherson, Cheneau, Schauß, Fukuhara, Bloch, Kuhr, Nature 471, 319 (2011)

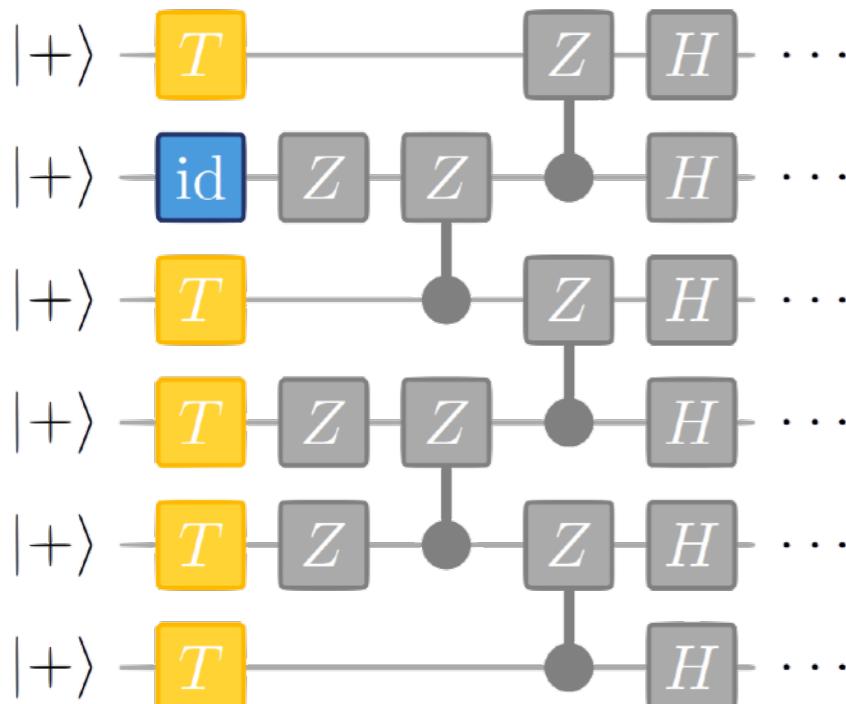
► **Theorem** (Hardness of classical sampling):

Assuming three highly plausible conjectures are true a classical computer cannot efficiently sample from the outcome distribution of our scheme up to constant error in l_1 distance



- Relate quench architecture to post-selected measurement-based quantum computing

- Universal quantum circuit for postBQP



- It is $\#P$ -hard to approximate the outcome distribution

- Polynomial hierarchy (similar $P \neq NP$)
- Average-case complexity

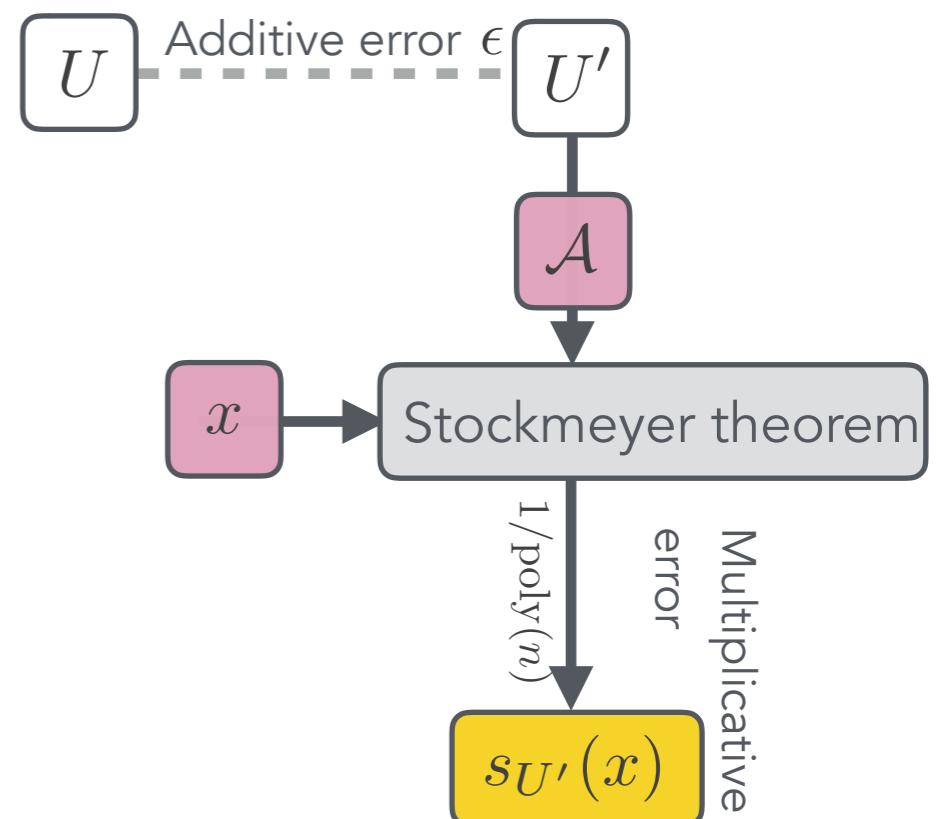
Bouland, Fefferman, Nirkhe, Vazirani, arXiv:1803.04402

- Anti-concentration

Hangleiter, Bermejo-Vega, Schwarz, Eisert, Quantum 2, 65 (2018)

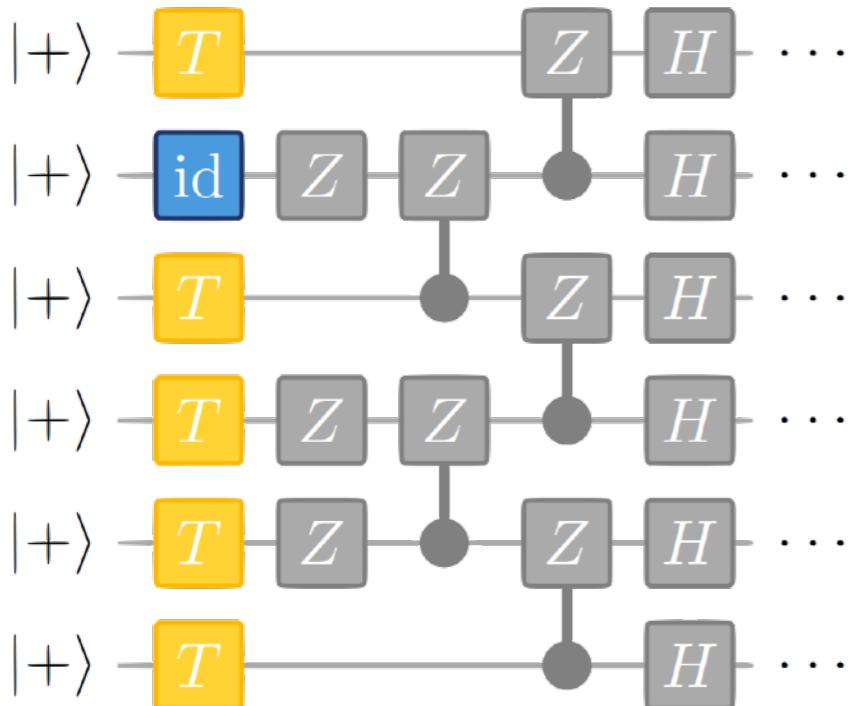
Mann, Bremner, arXiv:1711.00686

- Relate hardness of computing probabilities to hardness of sampling with additive errors



- Relate quench architecture to post-selected measurement-based quantum computing

- Universal quantum circuit for postBQP



- It is $\#P$ -hard to approximate the outcome distribution

- Polynomial hierarchy (similar $P \neq NP$)
- Average-case complexity

Bouland, Fefferman, Nirkhe, Vazirani, arXiv:1803.04402

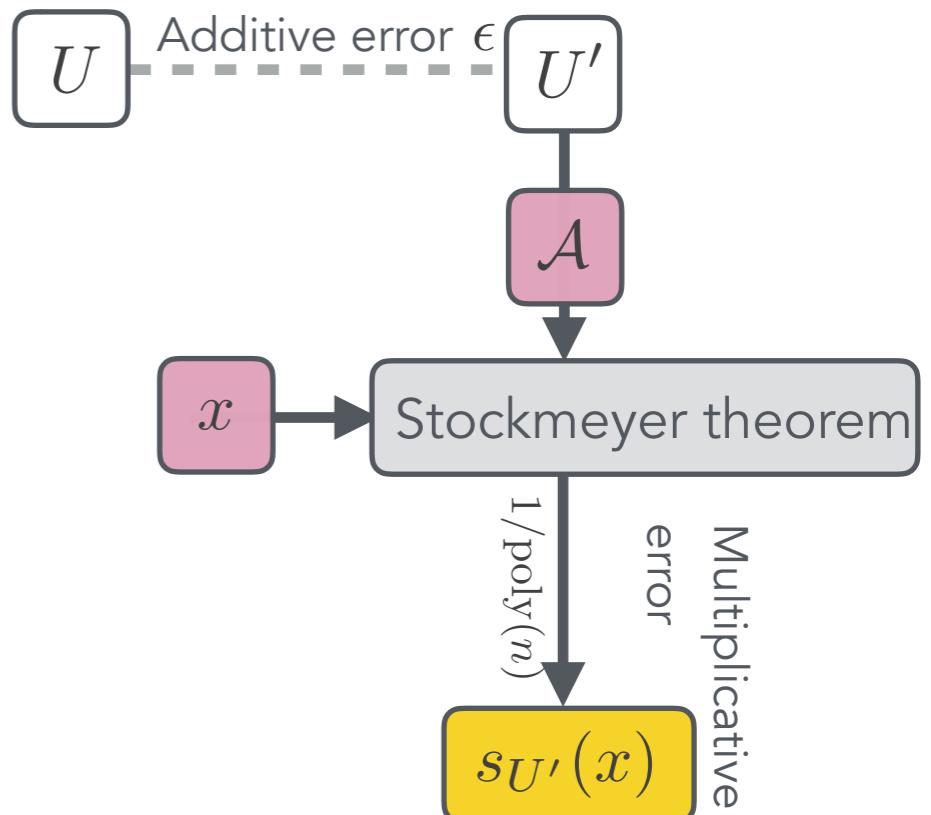
- Anti-concentration

Hangleiter, Bermejo-Vega, Schwarz, Eisert, Quantum 2, 65 (2018)

Mann, Bremner, arXiv:1711.00686

- Are true a classical computer able to sample the distribution of our scheme up to

- Relate hardness of computing probabilities to hardness of sampling with additive errors



► **Theorem** (Hardness of classical sampling):

Assuming a highly plausible conjecture is true a classical computer cannot efficiently sample from the outcome distribution of our scheme up to constant error in l_1 distance

► **Theorem** (Anti-concentration):

► The output probabilities of a family of unitaries \mathcal{U} anti-concentrates if there ex $\gamma > 0$ such that for all $x \in \{0, 1\}^n$

$$\Pr_{U \in \mathcal{U}} \left(P_U(x) \geq \frac{\alpha}{2^n} \right) \geq \gamma$$

Haferkamp, Hangleiter, Bermejo-Vega, Bouland, Fefferman, Eisert, arXiv:1908.08069

Hangleiter, Bermejo-Vega, Schwarz, Eisert, Quantum 2, 65 (2018)

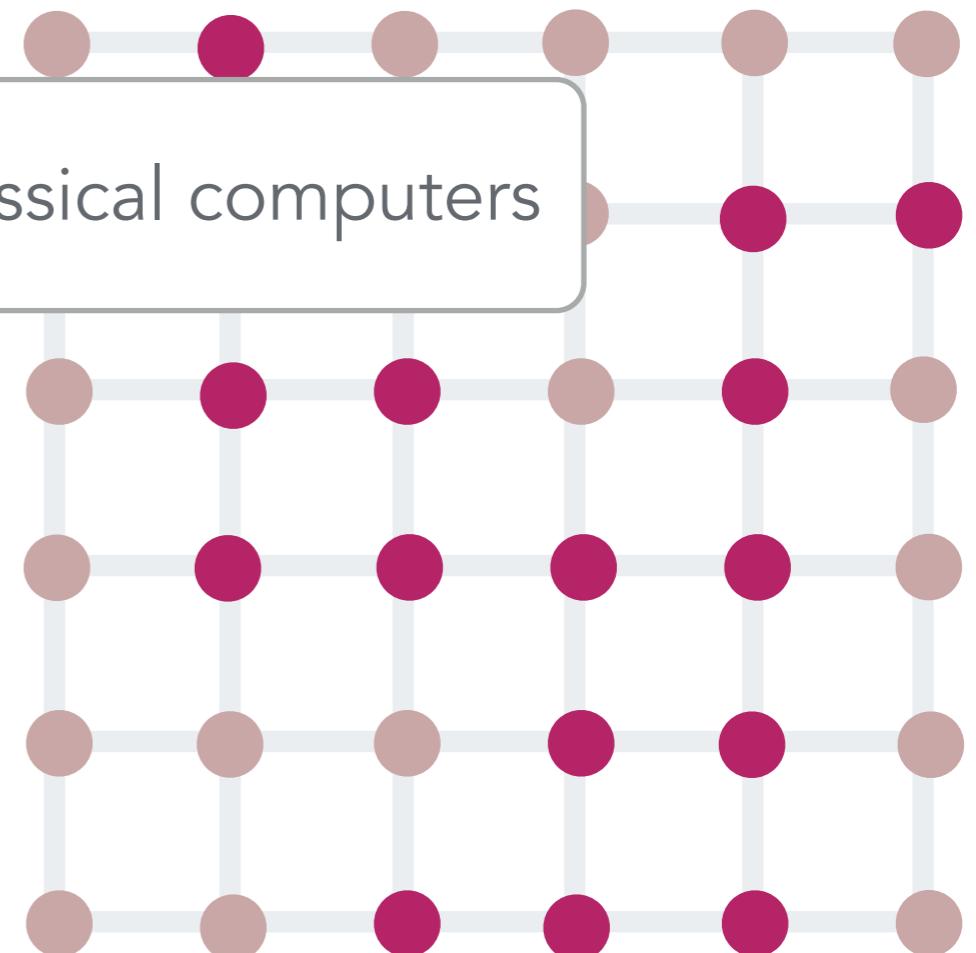
Mann, Bremner, arXiv:1711.00686

► **Theorem** (Average-case hardness): For multiplicative errors

Haferkamp, Hangleiter, Bermejo-Vega, Bouland, Fefferman, Eisert, arXiv:1908.08069

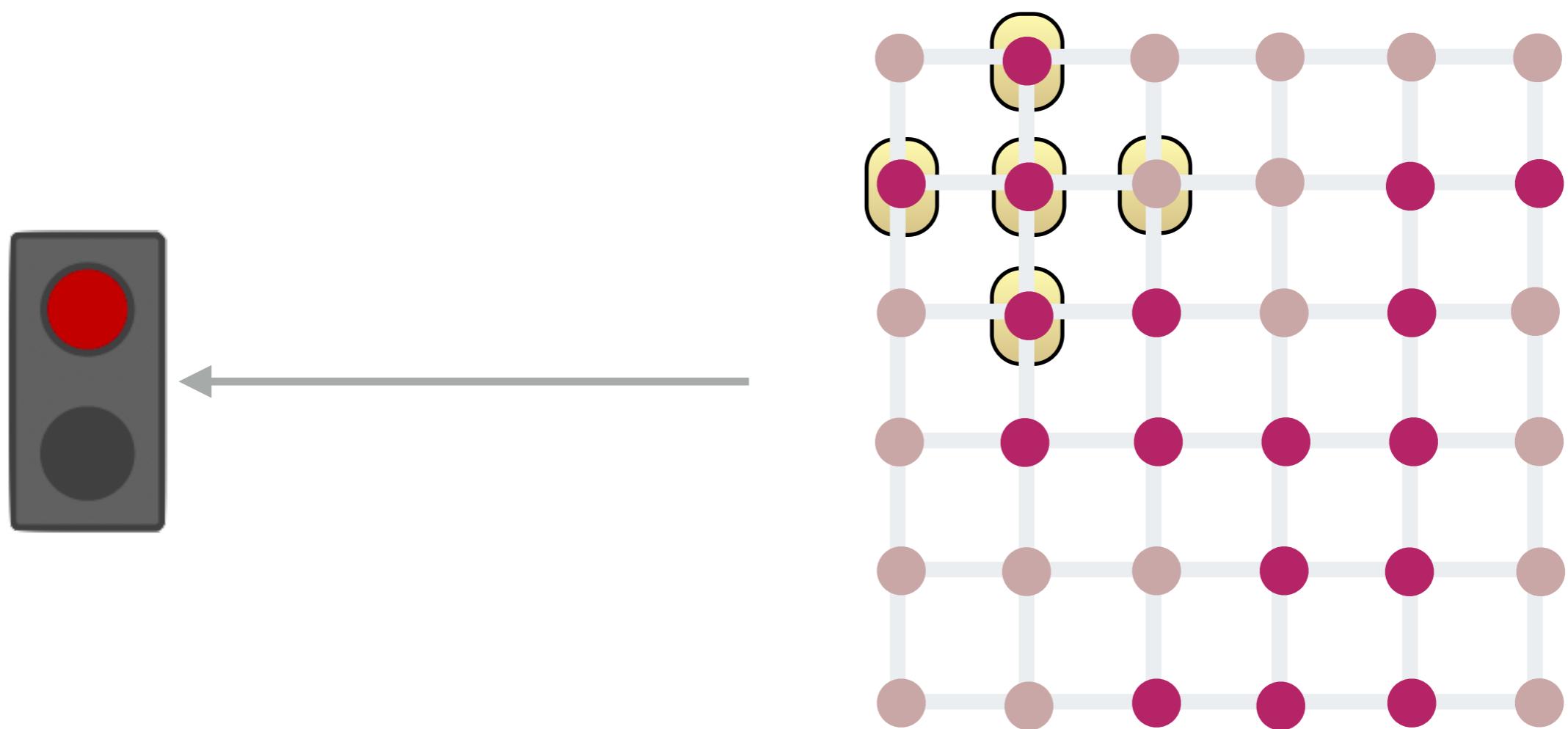
LESSON

► Near-term devices intractable for classical computers



VERIFIABLE QUANTUM ADVANTAGES

- ▶ One can with $\theta(N)$ many measurements detect closeness in l_1 -norm!
- ▶ Ground state of fictitious frustration-free Hamiltonian



- ▶ One can with $\theta(N)$ many measurements detect closeness in l_1 -norm!
- ▶ Ground state of fictitious frustration-free Hamiltonian

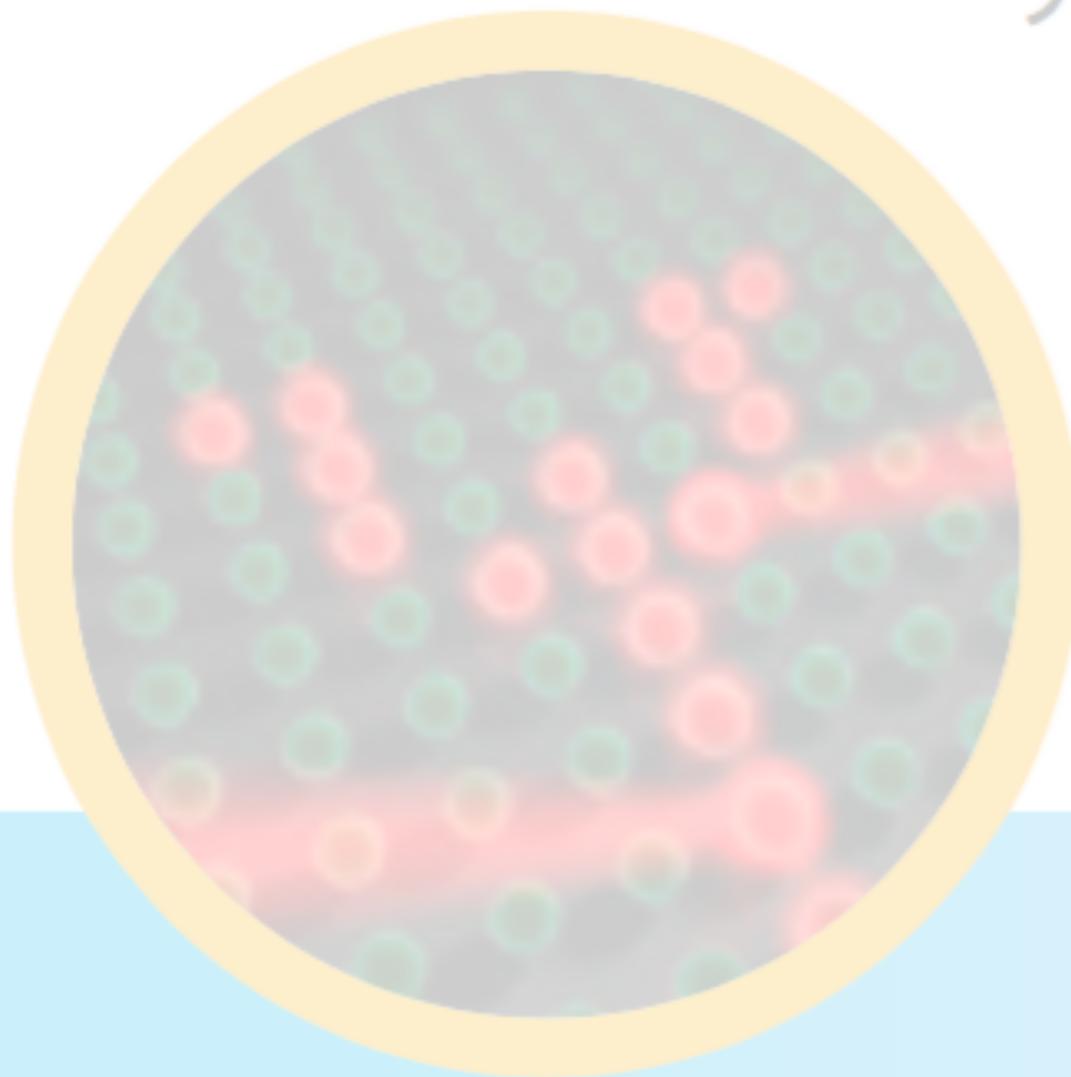


VERIFIABLE QUANTUM ADVANTAGES

- ▶ **Common prejudice:** In order to be able to verify a quantum device, one needs to be able to efficiently simulate it

SUMMARY, OUTLOOK AND OPEN QUESTIONS

- Analog quantum simulators already outperform good classical algorithms



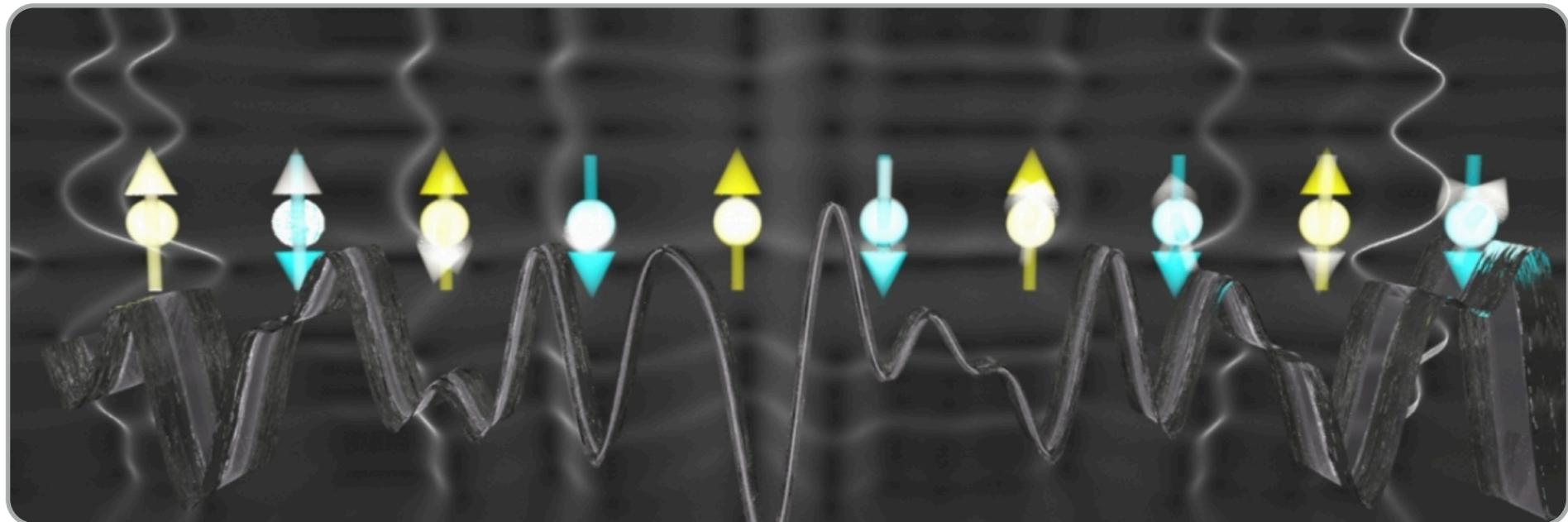
SUMMARY, OUTLOOK AND OPEN QUESTIONS

- ▶ Analog quantum simulators already outperform good classical algorithms
- ▶ Hope for feasible quantum devices with **superpolynomial speedup**



SUMMARY, OUTLOOK AND OPEN QUESTIONS

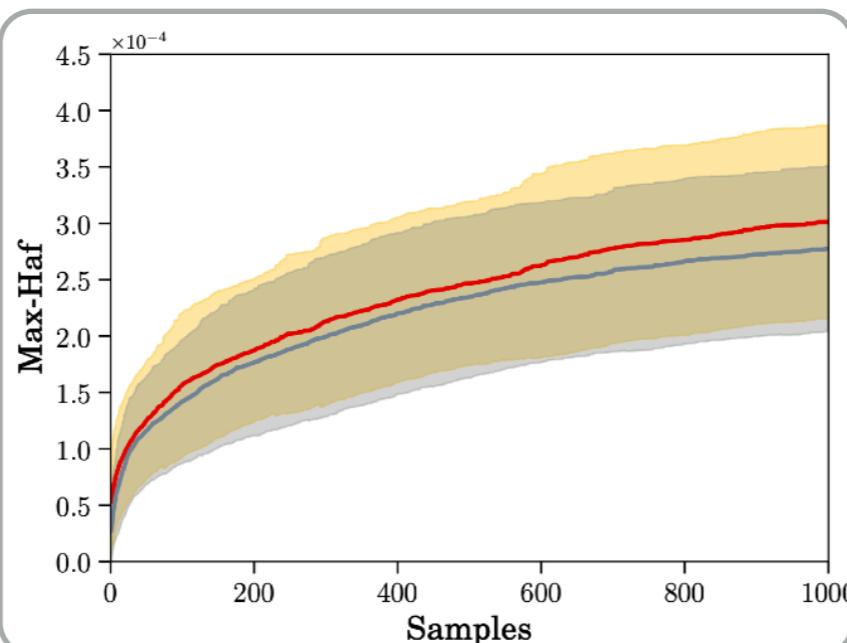
- ▶ Analog quantum simulators already outperform good classical algorithms
 - ▶ Hope for feasible quantum devices with **superpolynomial speedup**
 - ▶ Not fault tolerant, but can be certified: **Bell test for quantum computing**
 - even if simulators exhibit quantum computational speedup
- ▶ Closer to physically more interesting schemes?



SUMMARY, OUTLOOK AND OPEN QUESTIONS

- ▶ Analog quantum simulators already outperform good classical algorithms
- ▶ Hope for feasible quantum devices with **superpolynomial speedup**
- ▶ Not fault tolerant, but can be certified: **Bell test for quantum computing**
 - even if simulators exhibit quantum computational speedup

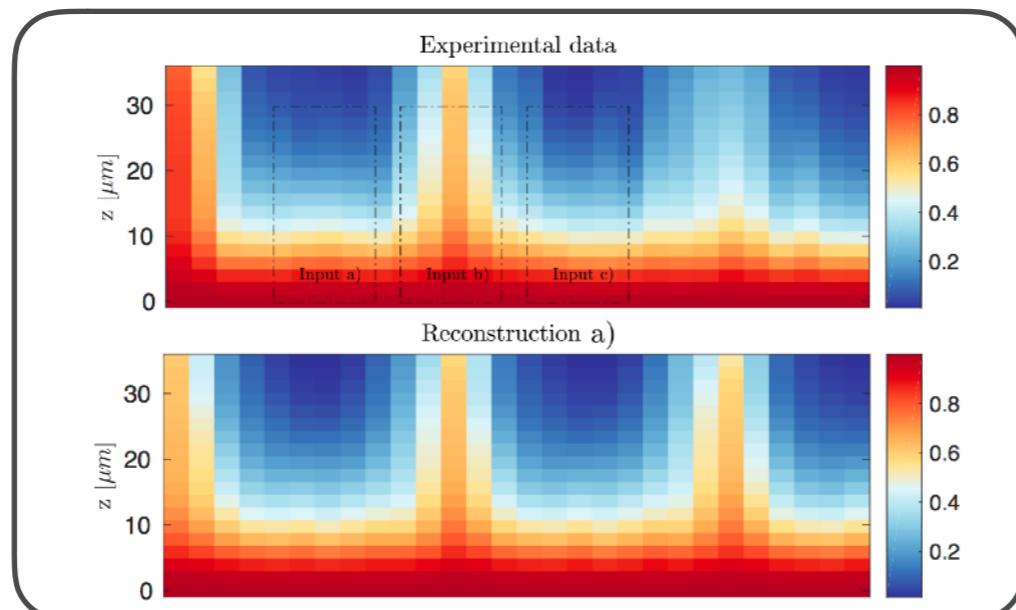
- ▶ Closer to physically more interesting schemes?
- ▶ More structured problems, optimization?



Arrazola, Bromley, Rebentrost, arXiv:1803.10731

SUMMARY, OUTLOOK AND OPEN QUESTIONS

- ▶ Analog quantum simulators already outperform good classical algorithms
 - ▶ Hope for feasible quantum devices with **superpolynomial speedup**
 - ▶ Not fault tolerant, but can be certified: **Bell test for quantum computing**
 - even if simulators exhibit quantum computational speedup
-
- ▶ Closer to physically more interesting schemes?
 - ▶ More structured problems, optimization?
 - ▶ Robustness of quantum devices? Readout?



SUMMARY, OUTLOOK AND OPEN QUESTIONS

- ▶ Analog quantum simulators already outperform good classical algorithms
- ▶ Hope for feasible quantum devices with superpolynomial speedup
- ▶ Not fault tolerant, but can be certified: Bell test for quantum computing
 - even if simulators exhibit quantum computational speedup

- ▶ Closer to physically more interesting schemes?
- ▶ More structured problems, optimization?
- ▶ Robustness of quantum devices? Readout?
- ▶ Space-time trade-offs

Thanks for your attention!
(Postdoc available)



(Mick Bremner)