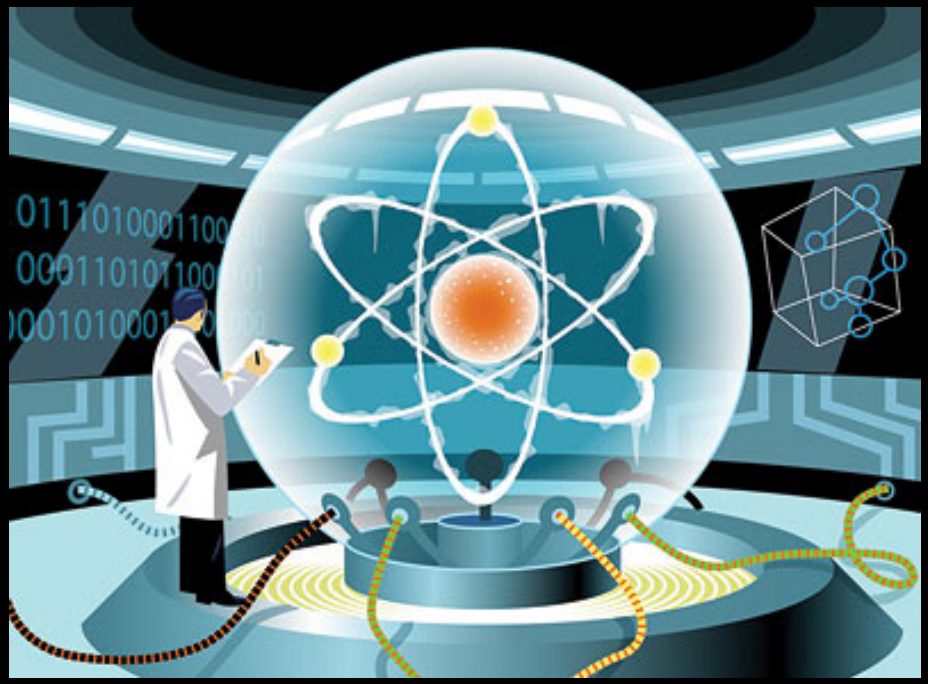
Quantum Computational Supremacy



Scott Aaronson (University of Texas at Austin)

Quantum Science Seminar

May 20, 2021

"Quantum Supremacy"

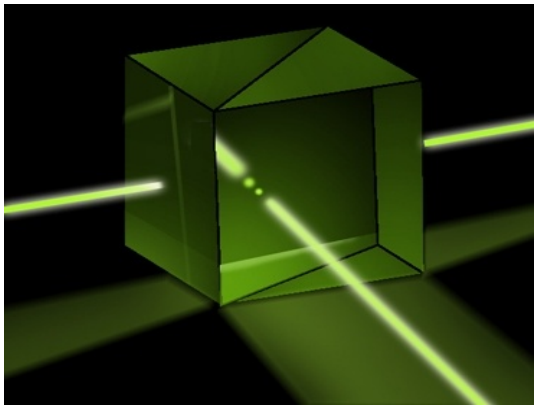
For me, the #1 application of qu
disprove the people who say it's not poss

Interesting

Wait, building a full scalable fault-tolerant QC is **how** hard?

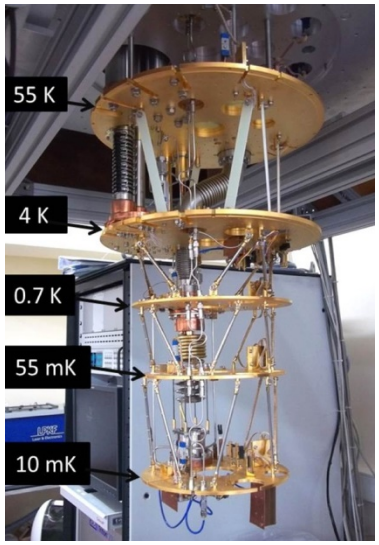
qu factor an
digit integer in only n^2 steps

A.-Arkhipov 2011, others: Look instead at **sampling** tasks



BosonSampling: Generate n photons, send through a network of beamsplitters, measure where they land. Under plausible assumptions, takes ~2^n time to simulate classically!

Google's Quantum Supremacy Demo Last Year

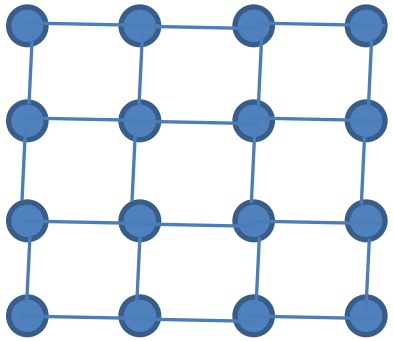


"Like BosonSampling, but with a random circuit applied to superconducting qubits"

They built a 53-qubit chip called Sycamore, and used it to sample from a probability distribution over 53-bit strings, in a way that *seems* to take ~ $2^{53} \approx 9$ quadrillion steps to simulate classically

~20 layers of gates in the circuit
~40 microseconds per sample
~3 mins for millions of samples
~0.2% measured circuit fidelity

The Random Circuit Proposal



Challenge the QC by sending it a randomly generated quantum circuit C on n qubits

Ask the QC to send back (quickly!) samples $s_1,\ldots,s_k$ from D_C, the distribution over n-bit strings obtained by applying C to 0…0

Then, using classical brute force, check if

$$\sum_{i=1}^{k} \left| \langle 0 \cdots 0 | C | s_i \rangle \right|^2 \geq \frac{bk}{2^n}$$

for some constant $b \in (1,2)$

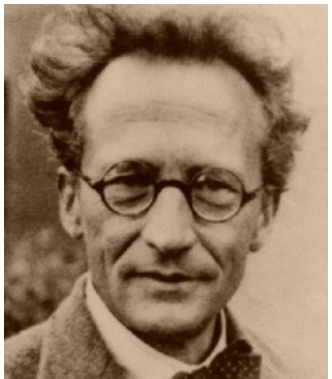
Google's "Linear Cross-Entropy Benchmark"

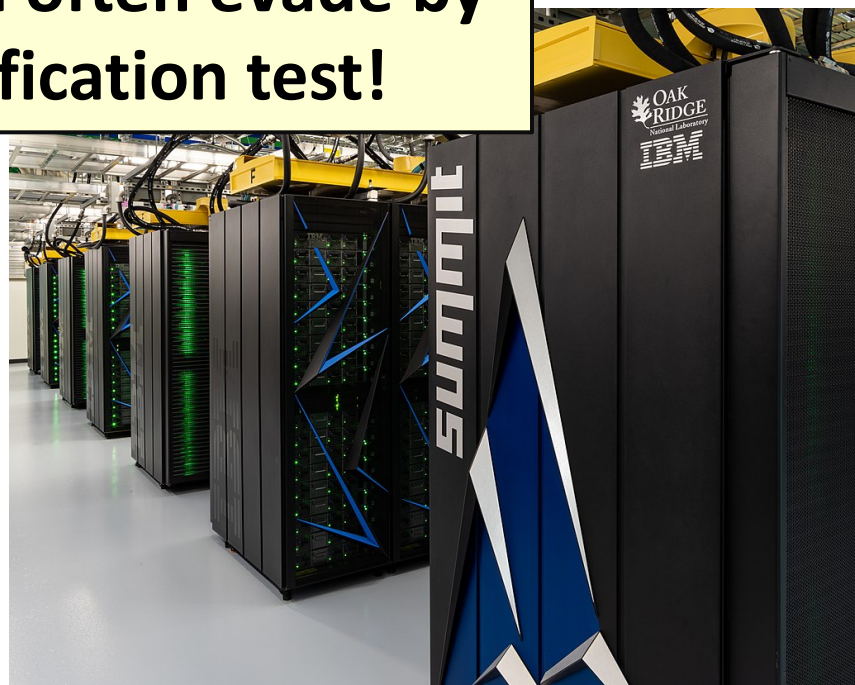
IBM's Response

Using Summit, the largest supercomputer currently on earth—which fills 2 basketball courts and has 250 petabytes of hard disk—it should be possible to simulate Google's 3-minute calculation in ~2.5 days, rather th

Very recently: Faster tensor network simulations. But can often evade by changing the verification test!

How? By
~ 9 quadr
amplitudes to disk and doing a "naïve Schrödinger simulation"





Is There A 2^n Barrier?

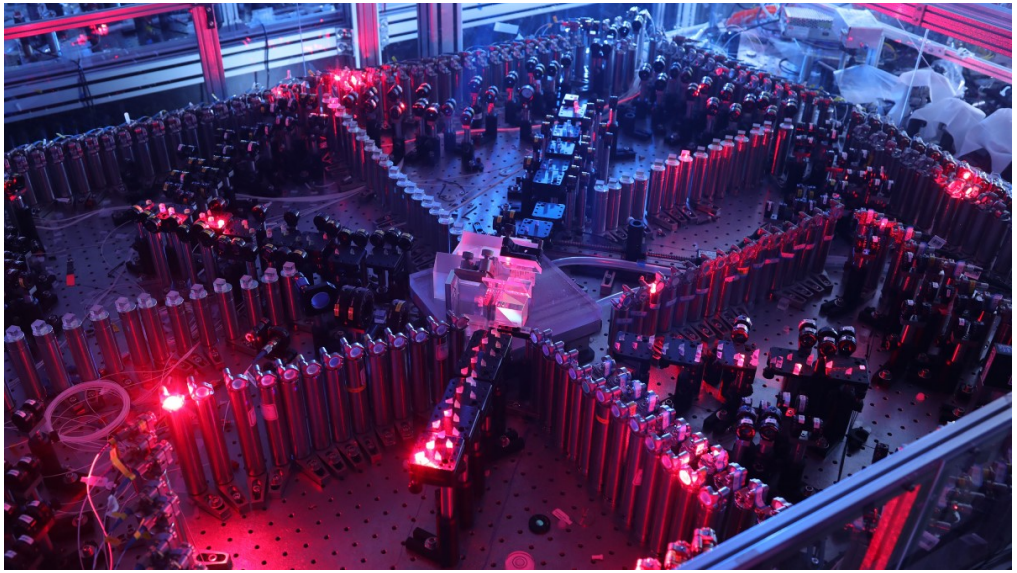
Classical Simulation Algorithm	Time	Memory
Schrödinger	~2^n (n=#qubits)	~2^n
Feynman	~2^m (m=#gates)	Linear
Schrödinger-Feynman (A.-Chen 2017)	~d^n (d=depth)	Linear

Theorem (A.-Chen 2017, A.-Gunn 2019): If there's a classical algorithm to spoof Linear XEB in $<<2^n$ time, then there's *also* a fast classical algorithm that estimates a *specific* output probability like $|\langle 0^n|C|0^n\rangle|^2$, with *slightly* better variance than always guessing 2^{-n}

Proof Idea: First hide which output z you care about. Then run the spoofing algorithm and see if it outputs z

New! ~50-photon BosonSampling

Announced in late 2020 by the group of Chaoyang Lu and Jianwei Pan at USTC, China

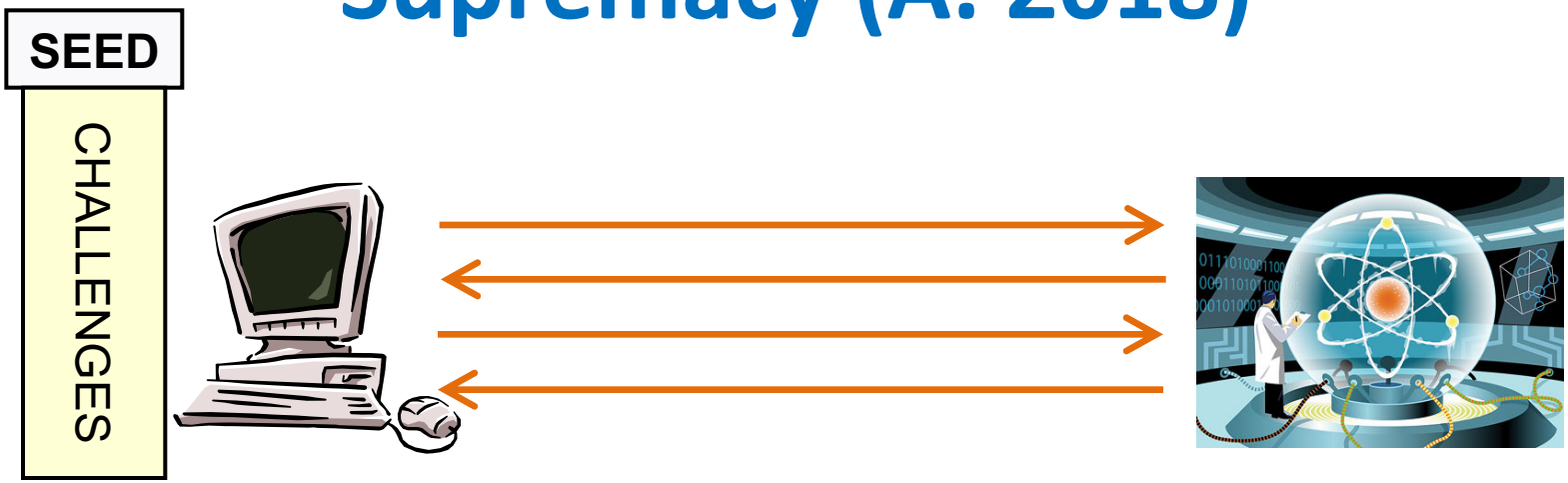


Would be the first quantum supremacy demo using photonics, and the second overall

Has ~10^{30} possible outputs, getting around some attacks

But is it hard to simulate classically? The jury is still out!

Certified Randomness from Quantum Supremacy (A. 2018)



If a quantum computer repeatedly and quickly passes the Linear XEB test, then under a suitable complexity assumption, we show that its responses must contain lots of entropy; they can't be deterministic

Leads to a scheme to produce public verifiably-random bits using existing QCs—useful for, e.g., proof-of-stake cryptocurrencies??

Where To Go Next?

Near-term quantum supremacy with efficient classical verification

So it's not just a 2^n vs. 2^n cat-and-mouse game!
Proposal by Bremner-Shepherd 2008, unfortunately now broken (Kahanamoku-Meyer 2019)

Replicate in other hardware platforms, and with more qubits, higher fidelity, …

Design new classical simulation algorithms!

Better complexity-theoretic evidence for hardness

Generating more and more certified random bits by running the same circuit C over and over?

Conclusions

Google and USTC **may** have achieved quantum supremacy for sampling tasks—building on a lot of "useless complexity theory" over the past decade!

Even if true, this leaves the huge challenges of **scalability** and **fault-tolerance**. But it already refutes those who said quantum speedups are impossible

It was thought obvious for years that sampling-based supremacy experiments had no applications. Certified randomness might change that—though challenges remain in making it secure and practical