The Physics of Quantum Information

Quantum computer science

Quantum hardware

Quantum matter

Quantum gravity

Modeling computation

What is computable?

What is *efficiently* computable?

P ≠ NP, NP-hardness.

Public key cryptography. Security based on computational hardness.

Turing, Cook, Levin, Karp, Diffie-Hellman, Rivest-Shamir-Adleman, …

Quantifying information

How compressible is a message?

How much information can be transmitted robustly through a noisy communication channel?

Error-correcting codes and robust computation.

Practical codes for modern communication systems.

Shannon, Hamming, Von Neumann, …

Quantum information

Bell inequalities: quantum correlations are a stronger resource than classical correlations (“quantum entanglement”).

Quantum cryptography: security from quantum physics.

Unknown quantum states cannot be copied accurately.

Tradeoff between acquiring information and causing disturbance.

How much information can be acquired by measuring a quantum system?

Einstein, Schrödinger, Bell, Clauser-Horne-Shimony-Holt, Aspect, Wiesner, Bennett-Brassard, Helstrom, Holevo, …

Quantum computation

Conjecture: classical systems cannot simulate quantum systems efficiently.

Thesis: a *quantum* computer can efficiently simulate any process that occurs in nature.

Quantum speedups are superpolynomial for some problems.

Quantum speedup is quadratic for exhaustive search (quantum computation time scales like square root of classical time).

Feynman, Manin, Deutsch, Bernstein-Vazirani, Shor, Kitaev, Grover, …

What is a quantum computer?

1. Scalable number of qubits.
2. Preparation of standard initial state.
3. Universal set of (entangling) quantum gates.
4. Classical computer to design uniform quantum circuit families.
5. Readout in the standard basis.

DiVincenzo, …

Quantum hardware

Atomic clocks → ion-trap quantum processors

Josephson junction → superconducting quantum processors.

Nanoscale devices → electron spin qubits.

Single-photon sources and detectors → photonic qubits.

Optical tweezers → Rydberg atom arrays.

+ *more*

Cirac-Zoller, Wineland-Monroe, Blatt, Schoelkopf-Devoret, Martinis, …

Ions

Tens of qubits in a linear trap.

Stable laser → state preparation, single-qubit gates, readout.

Manipulate normal modes of vibration → two-qubit gates, all-to-all coupling (tens of microseconds).

Scaling: modular traps with optical interconnects or ion shuttling.

Superconductors

~ 100 qubits in a two-dimensional array with nearest-neighbor coupling.

Transmons: artificial atoms, carefully fabricated and calibrated.

Microwave resonator for readout, microwave pulses for single-qubit gates.

Two-qubit gates via tunable frequency or cross-resonance drive (tens of nanoseconds).

Scaling: modular devices, microwave control lines, materials, fabrication, alternative qubit designs.

Quantum error correction

Decoherence: formidable enemy of quantum computing.

Quantum error-correcting codes: hide the protected quantum information from the environment.

Scalable quantum computing for reasonable noise.

Surface code: high error threshold and local processing in two dimensions.

Daunting overhead cost.

Unruh, Landauer, Shor, Steane, Kitaev, Aharonov-Ben-Or, Gottesman, …

Quantum matter

Topological order. Quantum phases of matter with long-range entanglement.

Symmetry-protected topological order.

Entanglement “area law”: tensor networks for exotic materials.

Universal properties of entanglement entropy and spectra.

Hamiltonian complexity. (Quantum) hardness of simulating ground states.

Information scrambling. (Classical) hardness of simulating chaotic quantum dynamics.

Wen, Haldane, Kane-Mele, Hastings, White, Vidal, Cirac-Verstraete, Kitaev, …

Quantum gravity

Hawking radiation: entanglement between inside and outside of black hole.

Black hole information: entropy = ¼ area.

Holographic duality: bulk geometry from boundary entanglement.

Holographic dictionary as a quantum error-correcting code.

Black holes as fast scramblers.

Hawking, Bekenstein, Maldacena, Ryu-Takayanagi, Almheiri-Dong-Harlow, Sekino-Susskind, …

Connections

Information scrambling: quantum circuits, chaotic dynamics, black holes, …

Quantum error correction: scalable computing, topological phases of matter, holographic correspondence.

Computational complexity: hardness of computational problems, preparing quantum phases of matter, geometry of the black hole interior.

Lots more.

Open Questions

How will we scale up to quantum computing systems that can solve hard problems?

What are the important applications for science and for industry?

What to do with near-term quantum computers?

Learn how to build more powerful quantum computers.

And learn how to use them for advancing science and for practical applications.

Prospects for the next 5 years

Encouraging progress toward scalable fault-tolerant quantum computing.

Scientific discoveries enabled by programmable quantum simulators and circuit-based quantum computers.

Quantum error correction

Repeated rounds of accurate error syndrome measurement.

Quantum memory times that improve sharply as codes increase in size.

Logical two-qubit gates with (much) higher fidelity than physical two-qubit gates.

Logical gate fidelities that improve sharply as codes increase in size.

We’re not there yet. But soon?

Quantum error correction circa 2022

Google 2021 (superconducting): 11-qubit *repetition code* + 10 ancilla qubits (Sycamore processor). 50 rounds of syndrome measurement, each taking about 1 microsecond. Logical error rate improves by 10X when code distance increases by 4.

Honeywell = Quantinuum 2021 (ions): 7-qubit color code + 3 ancilla qubits. 6 rounds of syndrome measurement, each taking about 200 milliseconds.

Also notable: ETH (9-qubit code + 8 ancilla qubits, superconducting), IBM (9-qubit code + 14 ancilla qubits, superconducting), UMD/Duke (9-qubit code + 4 ancilla qubits, ions), Innsbruck (two 7-qubit code blocks + 2 ancilla qubits, ions), Delft (5-qubit code + 2 ancilla qubits, NV centers in diamond).

Fault tolerance with the surface code

Logical error (per round of syndrome measurement):

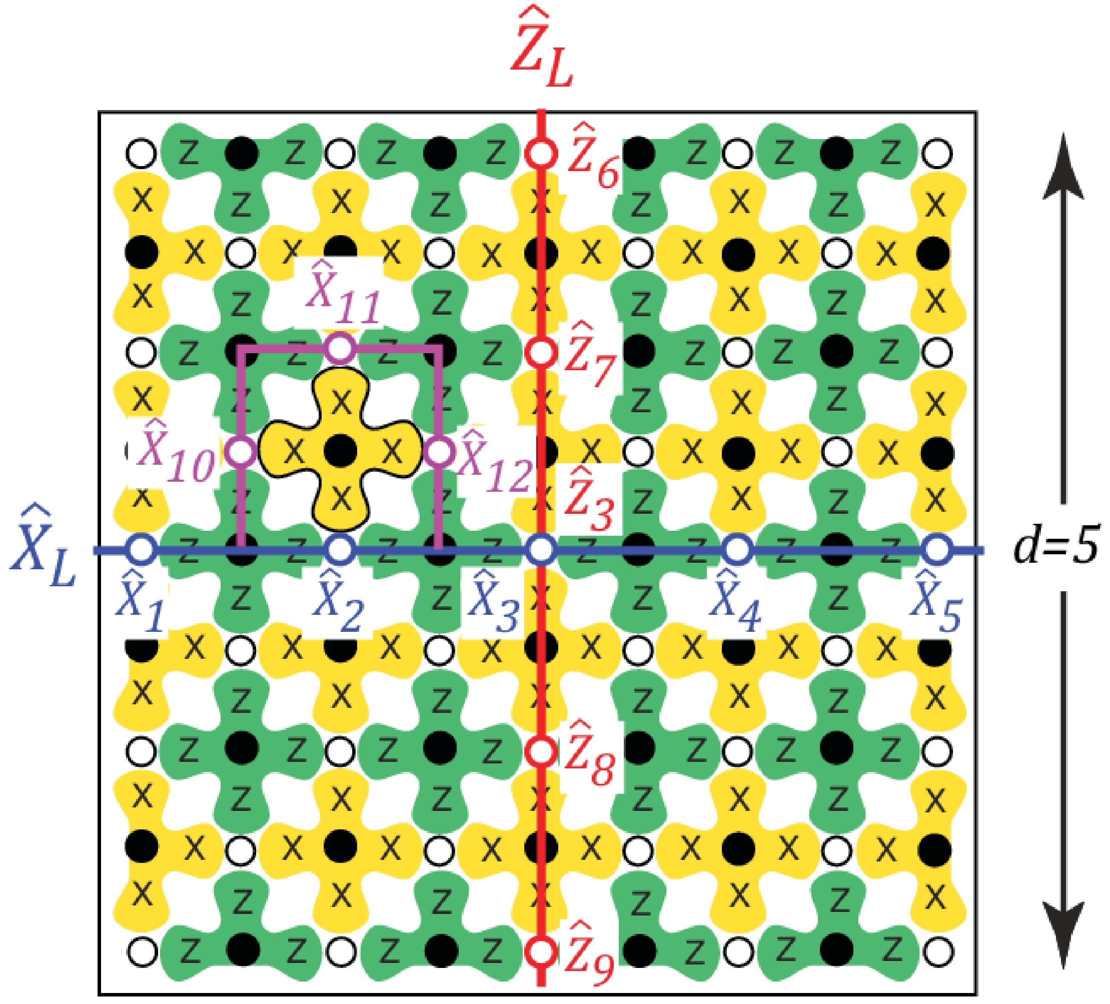
$$p_L(p_{\mathrm{phys}}, d) = 0.1(100p_{\mathrm{phys}})^{(d+1)/2}$$

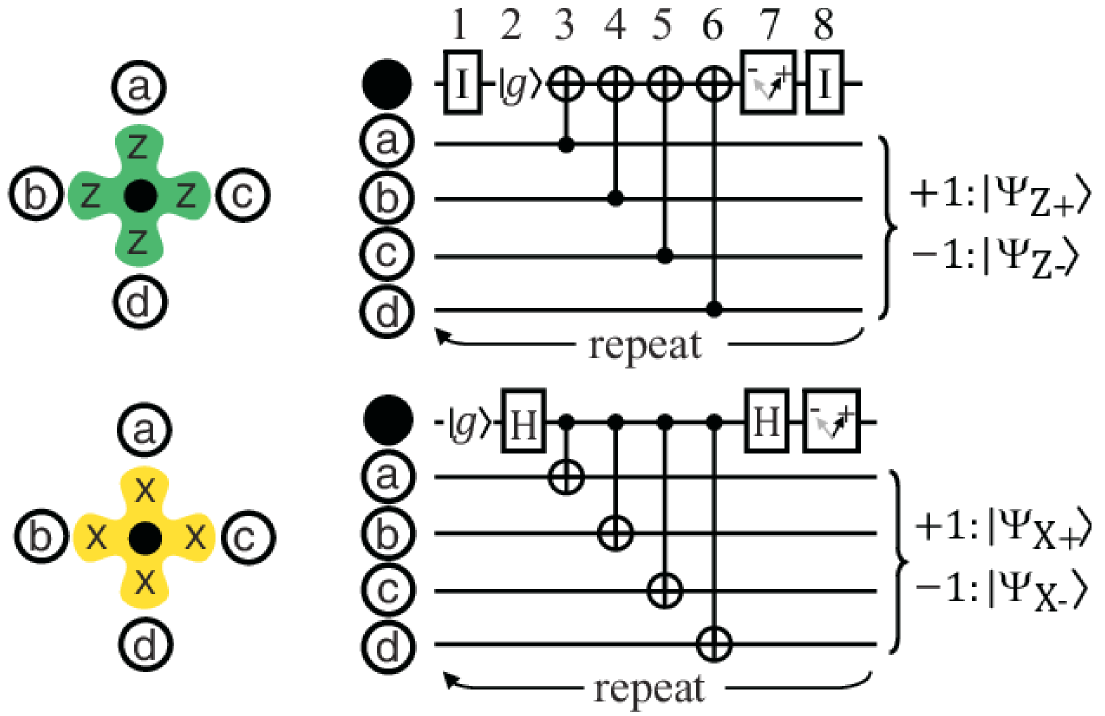
physical qubits per block: $2(d+1)^2$ (Fowler et al. 2013)

	d=5	d=9	d=15
p_{phys}= 0.5%	1.2%	0.3%	4x10^{-4}
p_{phys}= 0.1%	10^{-4}	10^{-6}	10^{-9}
p_{phys}= 10^{-4}	10^{-7}	10^{-11}	10^{-17}
# qubits	72	200	512

currently: $p_{\mathrm{phys}} \cong$ 1%

To break RSA for N = 2048 with $p_{\mathrm{phys}} \cong$ 0.1%:
d=27 → $2(d+1)^2$ = 1568 physical qubits per logical qubit.
(Gidney and Ekerå 2021)

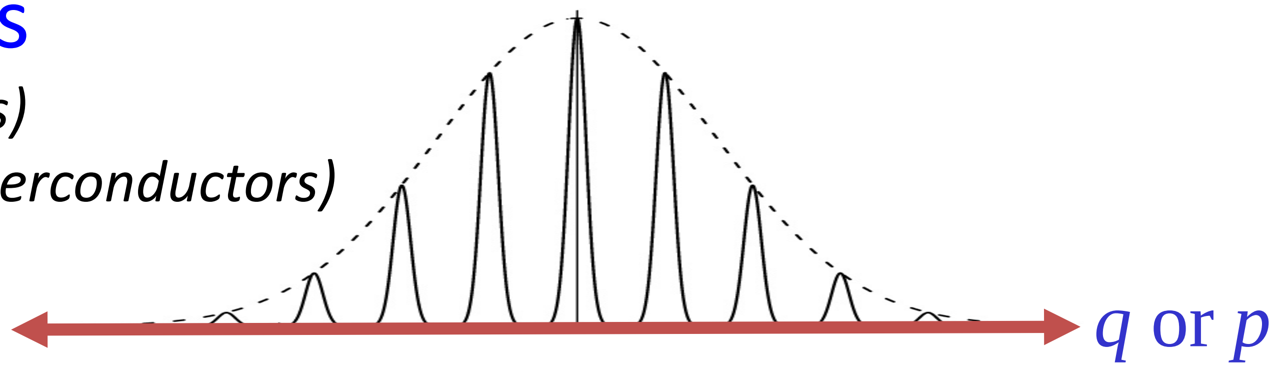




(Much) better gate error rates?

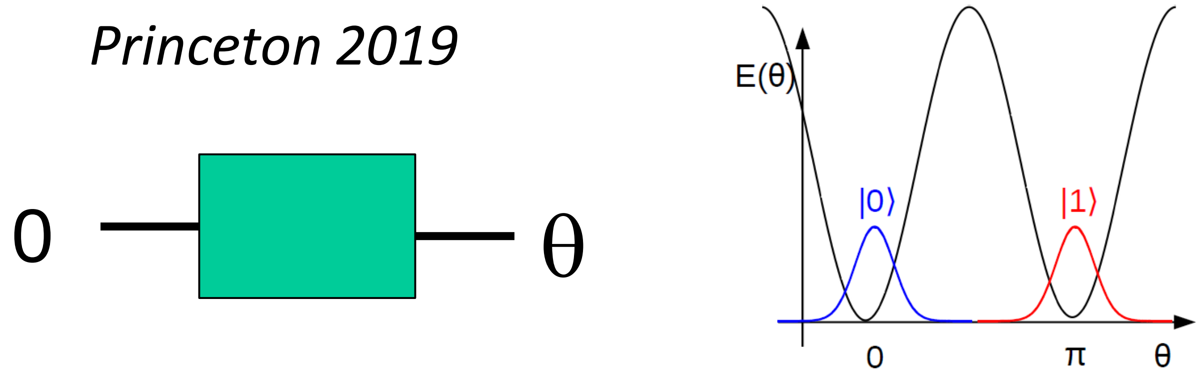
GKP codes

ETH 2018 (ions)
Yale 2019 (superconductors)



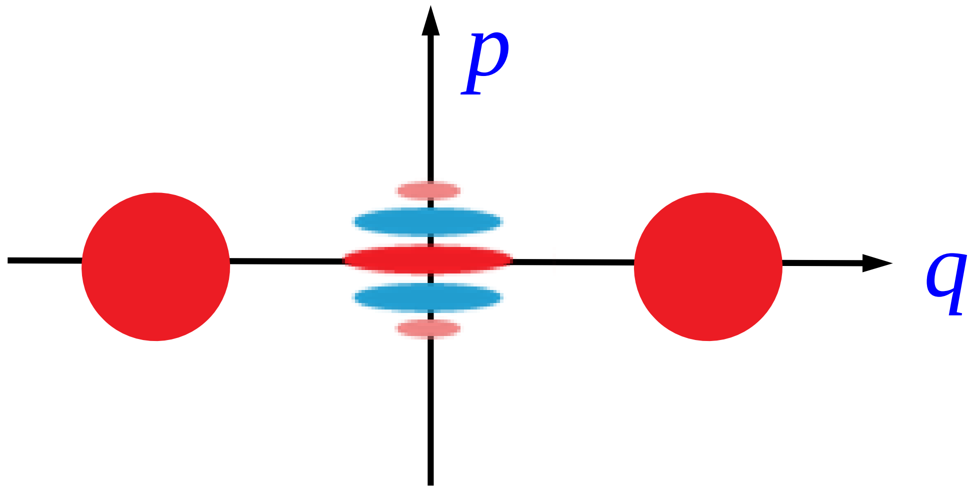
Zero-pi qubit

Princeton 2019

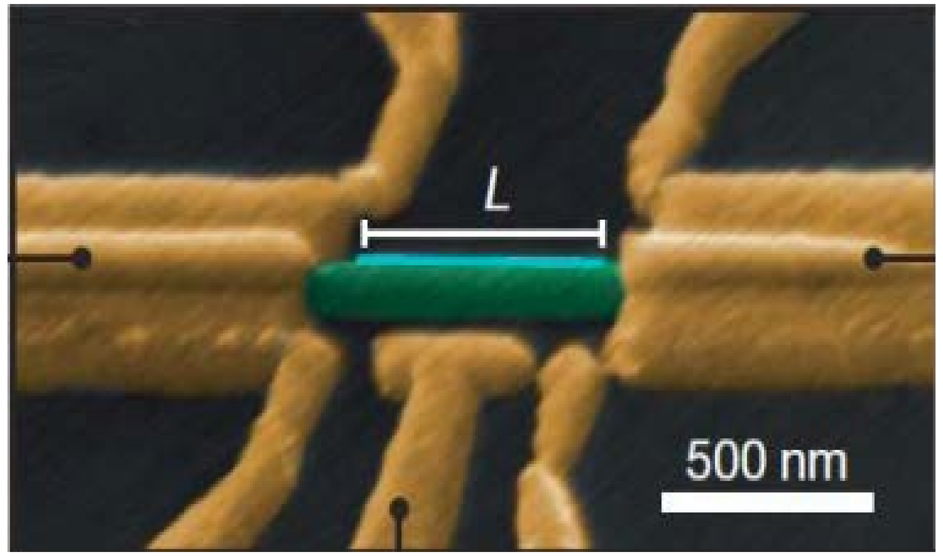


Concatenated cat codes

Yale 2019
Paris 2019



Majorana qubit



Quantum phases of matter circa 2022

Harvard/MIT 2021 (Rydberg atoms): Experimental confirmation of a topologically ordered quantum spin liquid. 219 atomic qubits in a programmable quantum simulator, frustrated by “Rydberg blockade.” Measurement of topological string operators.

Google/Stanford/MPI/Princeton/etc. 2021 (superconducting): Observation of a discrete time crystal, a periodically driven disordered phase which spontaneously breaks discrete time-translation invariance. 20 transmon qubits in a gate-based quantum computer. Measurement of temporal autocorrelations.

Also notable: ultracold atoms in optical lattices. Fluctuating string order in doped Hubbard model (Harvard), many-body localization (MPQ), etc.

What next? Observations of other novel quantum phases, both in equilibrium and far from equilibrium?

Opportunities in quantum simulation

What problems are (1) hard classically, (2) feasible quantumly, (3) of scientific or practical interest?

Classical methods are expected to fail for quantum systems that are highly entangled.

Numerical evidence suggests that heuristic classical methods scale reasonably in simulations of low energy-states of molecules and materials.

Quantum methods are also heuristic, because state preparation can be expensive.

Substantial quantum advantage is expected for simulations of highly-excited dynamics.

Challenges in quantum gravity

Locality in bulk spacetime at distances much less than the curvature scale.

Quantum gravity in asymptotically flat and de Sitter spacetime.

What’s inside a black hole?

What happens at the singularity?

What boundary theories have *useful* holographic bulk duals?

How hard is it to simulate quantum gravity with a quantum computer?

Quantum gravity: how experiments might help

Probe bulk geometry by measuring *boundary entanglement* structure.

Probe *bulk locality*, e.g. by studying boundary linear response.

Probe *fast scrambling*, Lyapunov spectrum.

Measure higher-order *quantum gravity corrections*.

Holographic dictionaries *beyond anti-de Sitter*.

Use gravitational intuition to understand emergent phenomena (e.g., relating coherent teleportation to traversable wormholes).

Some things I haven't mentioned

Post-quantum cryptography. Classical public-key protocols resistant to quantum attacks.

Quantum networks. Quantum key distribution. Untrusted devices. Transduction. Quantum repeaters. Other applications?

Quantum sensing. Improved strategies based on squeezing, entanglement, error correction. Navigation, surveying, scanning living matter. Detection of electric dipole moments, dark matter, gravitational waves.

Verification. How do we know a quantum computation is correct? Protocols based on post-quantum crypto assumptions.

Conclusions

A long road to practical applications. Quantum error correction is the key.

Next 5 years: progress toward fault-tolerant quantum computing, unprecedented explorations of exotic properties of quantum matter.

Advances in sensing, networking, computing will enable practical applications and new tools for exploring fundamental physics.

The Physics of Quantum Information provides unifying concepts and powerful technologies for controlling and exploring complex many-particle quantum systems of both practical and fundamental interest.

We've only just begun.