Quantum computing in the second quantum century

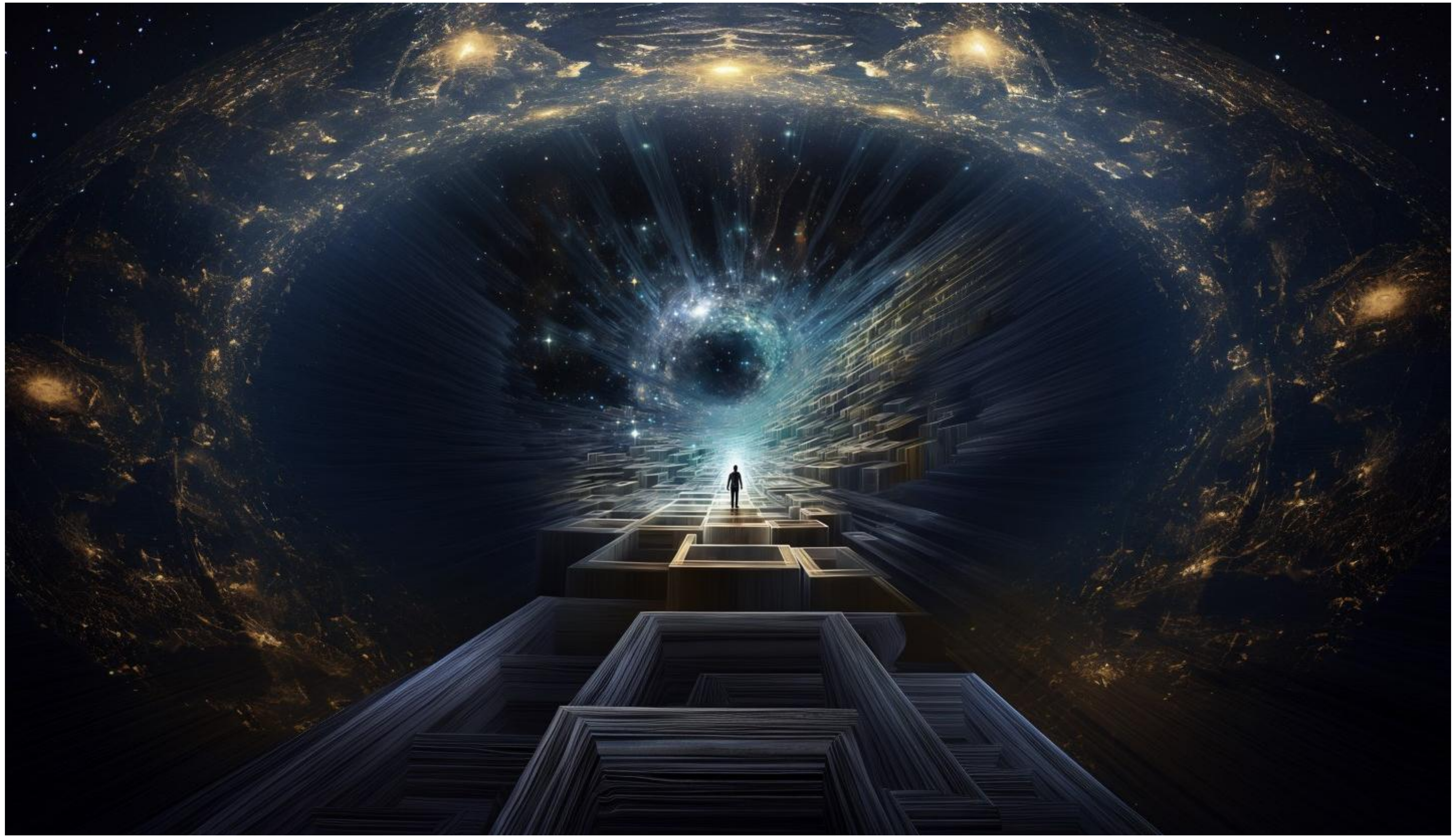
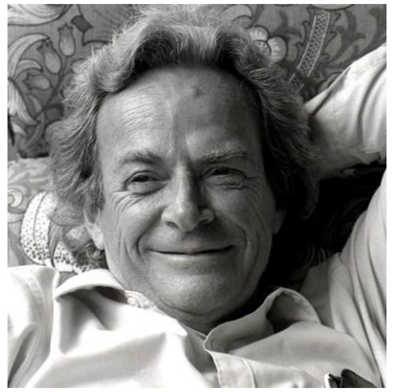


Image generated using Midjourney



aws

INSTITUTE FOR QUANTUM INFORMATION AND MATTER

John Preskill

Q2B 2025 Silicon Valley

10 December 2025

CALIFORNIA INSTITUTE OF TECHNOLOGY 1891

@preskill

On June 6, 1925, a swollen-faced, stuffy-nosed Werner Heisenberg, then 23 years old and suffering from hay fever, left his home in central Germany for the fresh air of the North Sea island of Helgoland, hoping for relief. There, he had a breakthrough, becoming the first to articulate a mathematical framework of quantum mechanics and resolve the then-glaring contradictions of quantum theory.

APS News, 1 July 2025

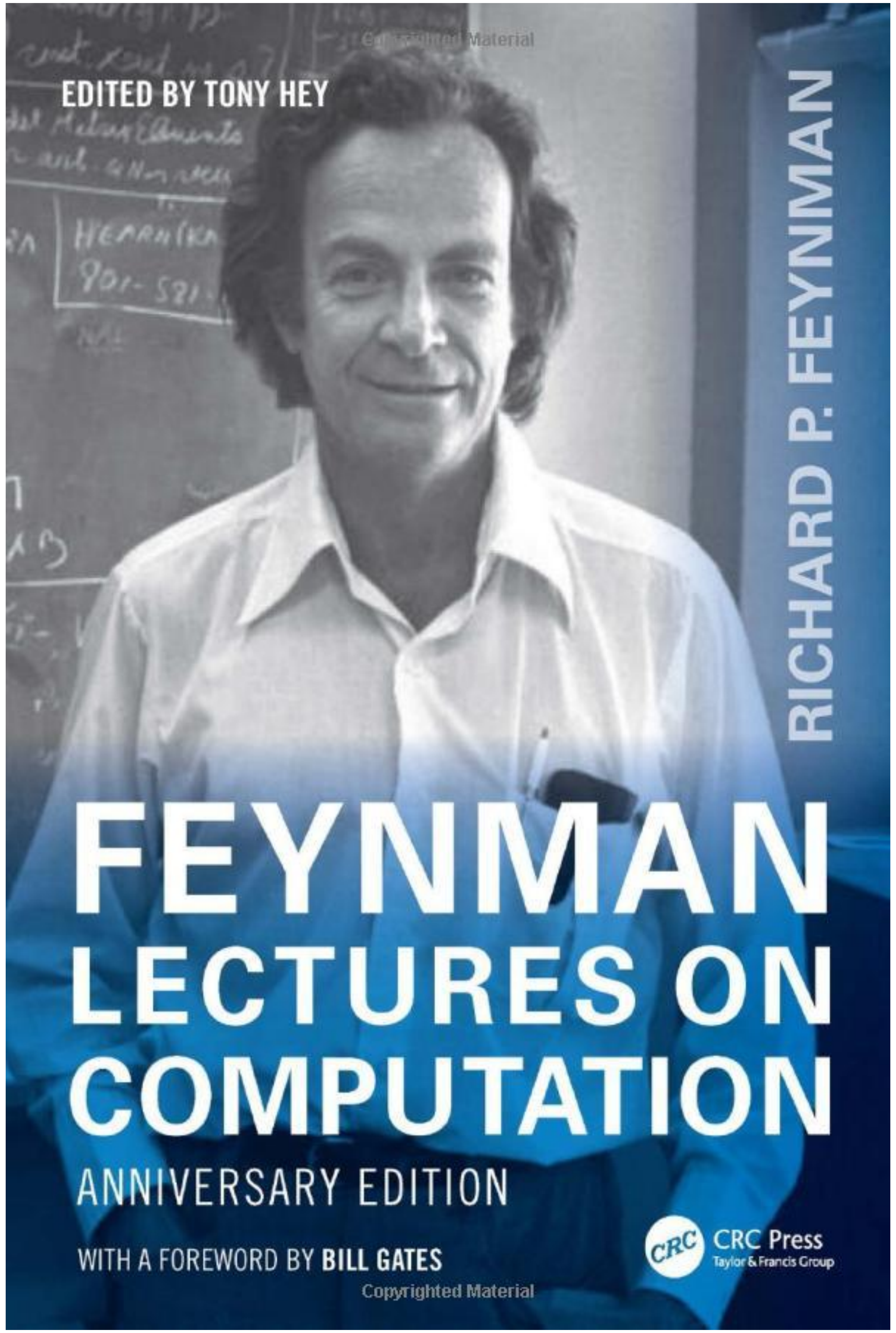
Heisenberg in the 1920s

The underlying physical laws necessary for the mathematical theory of a large part of physics and the whole of chemistry are thus completely known, and the difficulty is only that the exact application of these laws leads to equations much too complicated to be soluble.

Paul A. M. Dirac, Quantum Mechanics of Many-Electron Systems, Proceedings of the Royal Society, 1929

Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy.

Richard Feynman
Simulating Physics with Computers
May 1981



How Peter Shor Changed the World

1994: "These algorithms take a number of steps polynomial in the input size, for example, the number of digits of the integer to be factored."

1995: "It is shown how to reduce the effects of decoherence for information stored in quantum memory, assuming that the decoherence process acts independently on each of the bits stored in memory."

1996: "This paper shows both how to correct errors in encoded qubits using noisy gates and also how to compute on these encoded qubits without ever decoding the qubits."

arXiv.org > quant-ph > arXiv:quant-ph/9610011

Search or

Quantum Physics

Threshold Accuracy for Quantum Computation

E. Knill, R. Laflamme, W. Zurek

(Submitted on 8 Oct 1996 (v1), last revised 15 Oct 1996 (this version, v3))

We have previously (quant-ph/9608012) shown that for quantum memories and quantum communication, a state can be transmitted over arbitrary distances with error ϵ provided each gate has error at most $c\epsilon$. We discuss a similar concatenation technique which can be used with fault tolerant networks to achieve any desired accuracy when computing with classical initial states, provided a minimum gate accuracy can be achieved. The technique works under realistic assumptions on operational errors. These assumptions are more general than the stochastic error heuristic used in other work. Methods are proposed to account for leakage errors, a problem not previously recognized.

arXiv.org > quant-ph > arXiv:quant-ph/9611025

Search or A

Quantum Physics

Fault Tolerant Quantum Computation with Constant Error

Dorit Aharonov (Physics and computer science, Hebrew Univ.), Michael Ben-Or (Computer science, Hebrew univ.)

(Submitted on 14 Nov 1996 (v1), last revised 15 Nov 1996 (this version, v2))

Recently Shor showed how to perform fault tolerant quantum computation when the error probability is logarithmically small. We improve this bound and describe fault tolerant quantum computation when the error probability is smaller than some constant threshold. The cost is polylogarithmic in time and space, and no measurements are used during the quantum computation. The result holds also for quantum circuits which operate on nearest neighbors only. To achieve this noise resistance, we use concatenated quantum error correcting codes. The scheme presented is general, and works with all quantum codes that satisfy some restrictions, namely that the code is ``proper''.

Scalable quantum computing using recursive simulations.

"This paper … shows how to perform fault tolerant quantum computation when the error probability is smaller than some constant threshold. The cost is polylogarithmic in time and space."

Aharonov and Ben-Or, 1996

Things are changing

(1) *NISQ quantum advantage.*

(2) *Error correction gets real.*

(3) *Multiple billions invested.*

From NISQ to FASQ

What we have now:

-- *Noisy Intermediate-Scale Quantum (NISQ) machines*.

-- Capable of performing thousands of two-qubit operations.

-- Becoming useful for scientific exploration.

-- Limited commercial value.

What we want to have:

-- *Fault-Tolerant Application-Scale Quantum (FASQ) machines*.

-- Capable of performing billions or trillions of two-qubit operations.

-- Opening a wide variety of scientific and commercial applications.

-- Need to improve error rates by many orders of magnitude!

-- Quantum error correction is essential for crossing from NISQ to FASQ.

Some 2025 Highlights

Applications: Simulations of quantum dynamics.

Hardware: Rapid progress in atomic processors.

Error correction: Advantages from nonlocal connectivity.

Algorithms: Reduced cost for Shor’s algorithm.

Quantum machines for science

Quantinuum Helios: 98 qubits, 2Q gate F=.9992 (MS, all pairs)

IBM Heron: 156 qubits, 2Q gate F=.9988 (median CNOT)

Google Willow: 105 qubits, 2Q gate F=.9988 (mean CZ)

Harvard/QuEra/MIT: 448 qubits, 2Q gate F=.9954 (CZ, low depth)

More than 5K 2Q gates for correlated dynamics, mitigated.

Tradeoff: Higher fidelity and nonlocal connectivity vs. more shots.

Verifiable quantum advantage

Classical vs. quantum verification

Factoring / discrete log

Peaked quantum circuits

BlueQubit: hidden string on Quantinuum H2

Operator expectations after dynamics

Time-reversed ergodic evolution on Google Willow

Correlated fermions in 2D (digital)

Phasecraft / Google Willow (superconducting): Fermi-Hubbard dynamics on 6 x 6 lattice, 2 qubits per site, compare with free fermions for mitigation. 72 qubits, 4372 2Q gates.

Quantinuum Helios (ions): Fermi-Hubbard pairing correlations on 6 x 6 lattice + 18 ancillas, local fermion encoding. 90 qubits, 3439 2Q gates.

Harvard (neutral atoms): Non-abelian spin liquid and Fermi-Hubbard quench dynamics. 72-qubit honeycomb + 32 ancillas, low depth circuits.

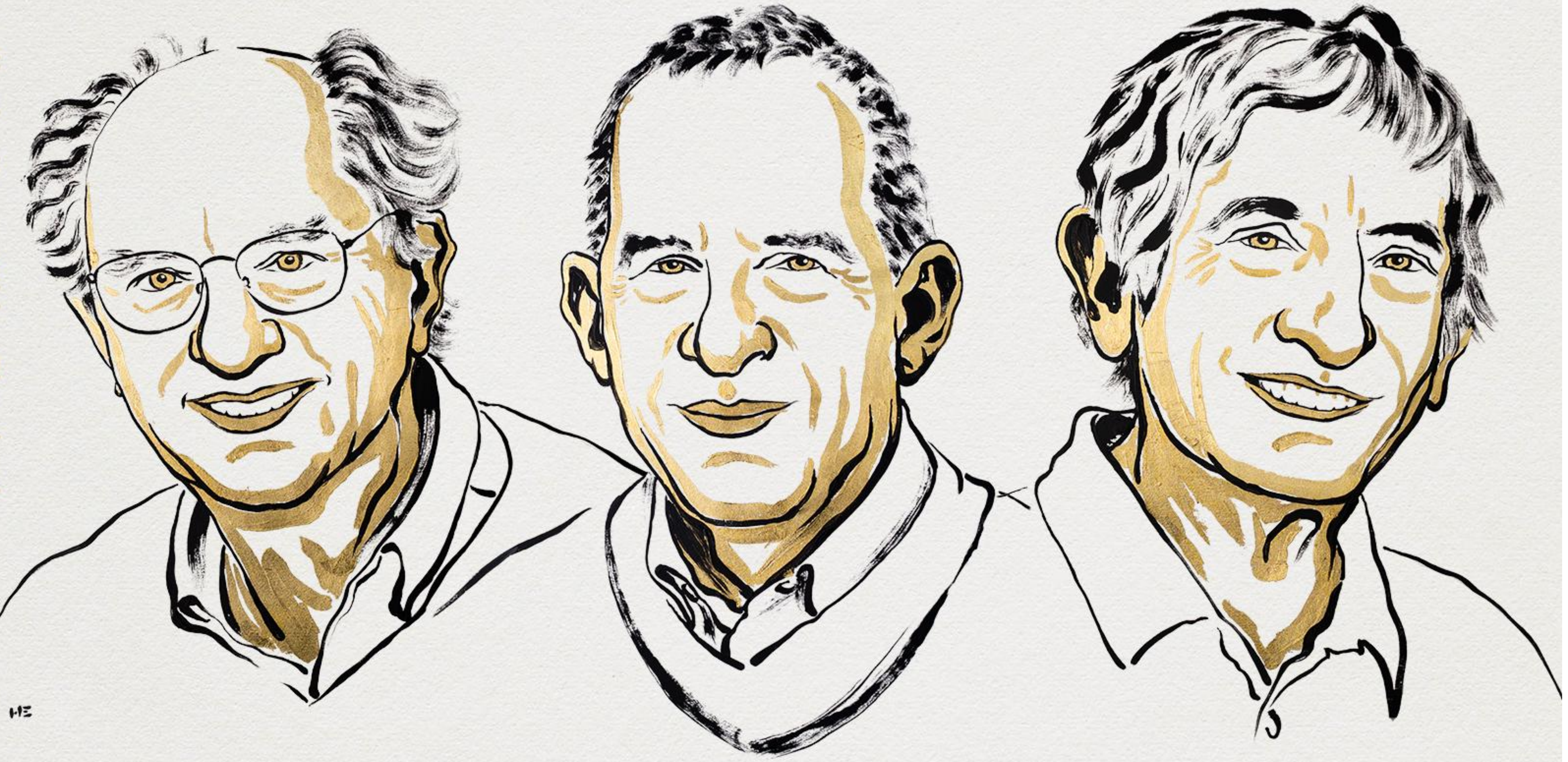
Analog simulations (neutral fermionic atoms in optical lattices): Thousands of lattice sites, but digital provides more flexible initial states, output observables and tunable Hamiltonians.

Will AI eat quantum's lunch?

We'll need training data from quantum computers, simulators, experiments.

THE NOBEL PRIZE IN PHYSICS 2025

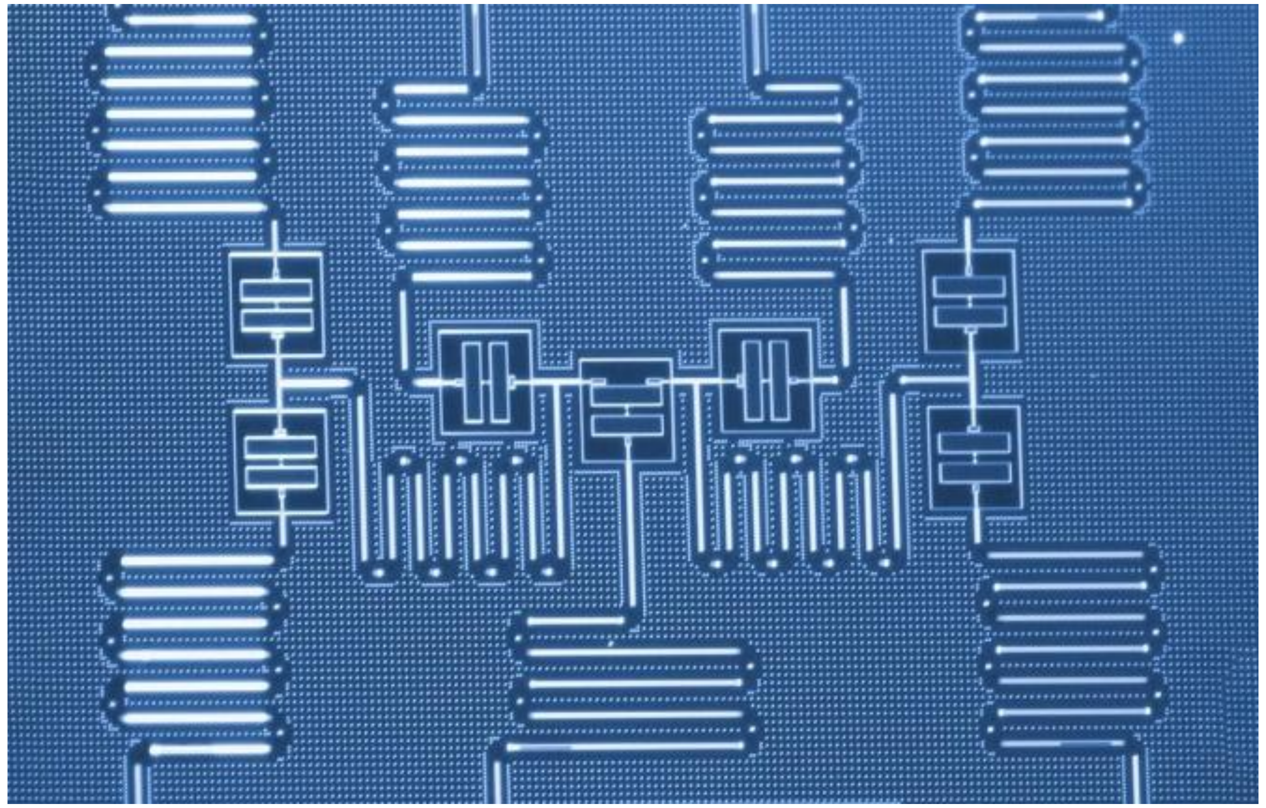
Illustrations: Niklas Elmehed



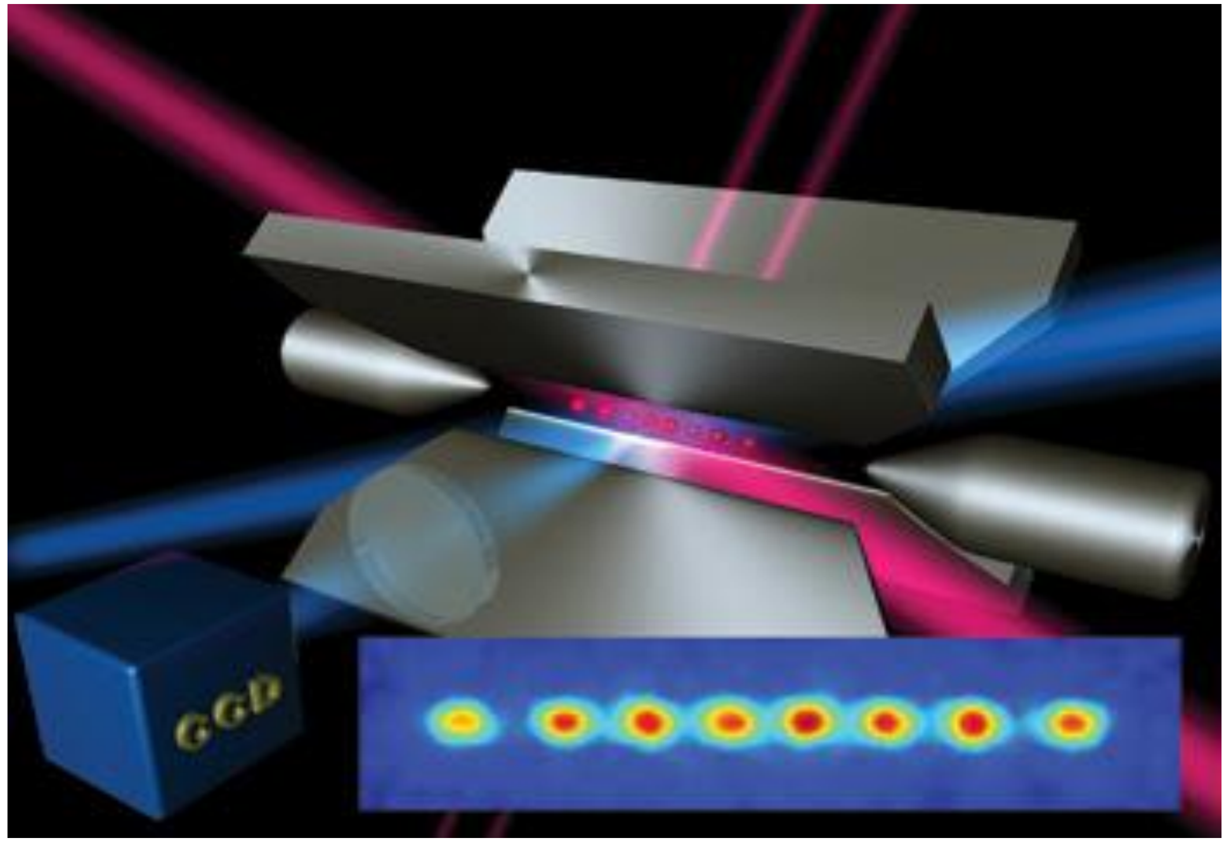
John Clarke | **Michel H. Devoret** | **John M. Martinis**

"for the discovery of macroscopic quantum mechanical tunnelling and energy quantisation in an electric circuit"

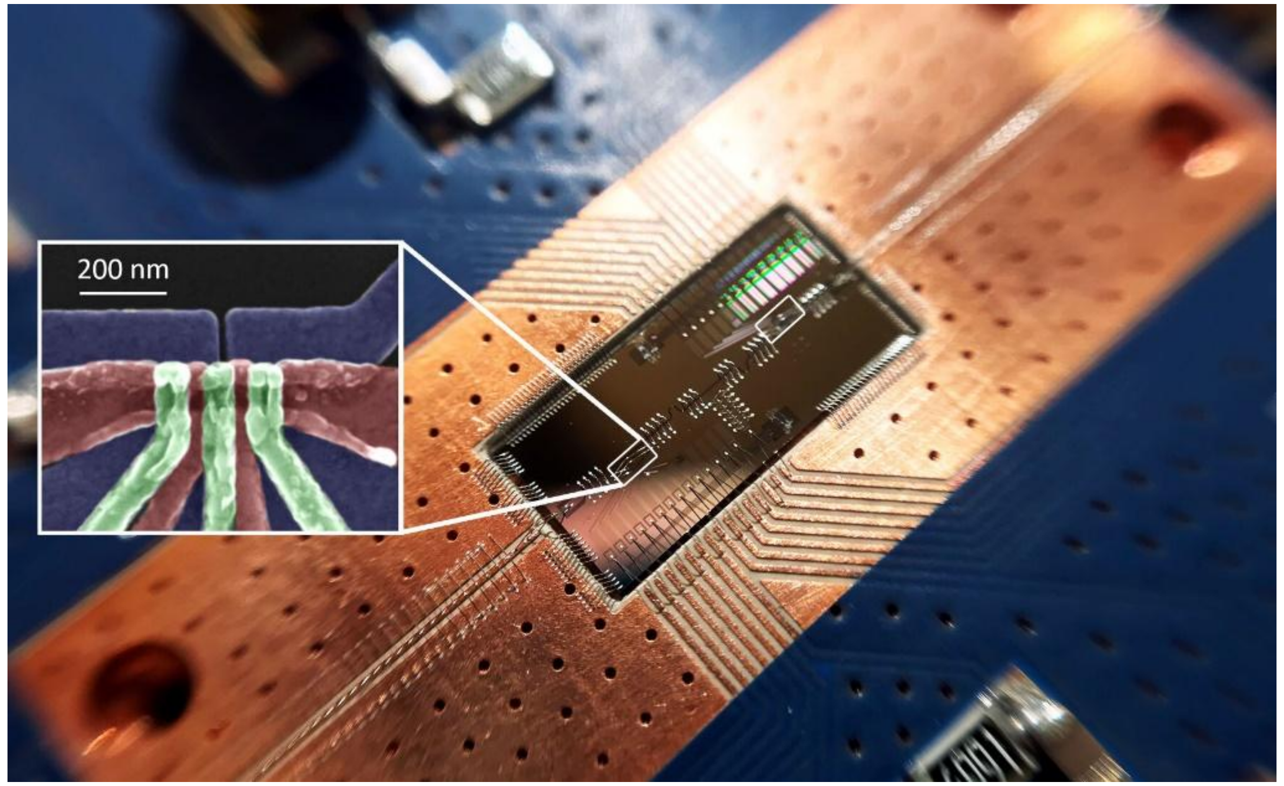
THE ROYAL SWEDISH ACADEMY OF SCIENCES



superconducting qubits



trapped atoms/ions



electron/nuclear spin qubits

photonics

The joy of nonlocal connectivity

An advantage for ion traps and neutral atoms in optical tweezers.

Transversal Clifford operations in the surface code: time blowup reduced from O(code distance) to O(1). Improved parallelism.

Higher encoding rates with quantum low-density parity-check (qLDPC) codes. Reduced number of physical qubits, high threshold, feasible decoders.

Universal gate gadgets for qLDPC with reduced spacetime cost.

These advantages partially compensate for the slow clock speed.

Tweezer arrays with thousands of atoms already exist.

Moving forward: improved fidelity and replacement of lost neutral atoms.

Breaking RSA

Factor 2048 bits in a few days using fewer than 1M physical qubits (assuming 10^{-3} 2Q error rate and 2D processing). [Gidney 2025]

(1) Truncated residue arithmetic to save space.

(2) “Yoked” (concatenated) surface code for more efficient cold storage.

(3) Magic state cultivation reduces cost of non-Clifford gates.

Highlights the urgency of migration to quantum-safe cryptography.

Imagining the future

In 1945, John von Neumann wrote to Lewis Strauss about the potential uses of fast electronic computers:

"... Uses which are not, or not easily, predictable now, are likely to be the most important ones. Indeed they are by definition those which we do not recognize at present because they are farthest removed from what is now feasible, and they will therefore constitute the most surprising and farthest-going extension of our present sphere of action in mathematics and in applied mathematics."

Prospects for the next 100 years

Past 100 years:

The relatively simple quantum behavior of weakly correlated particles like electrons, photons, etc.

Next 100 years:

The extraordinarily complex quantum behavior of many profoundly entangled particles.