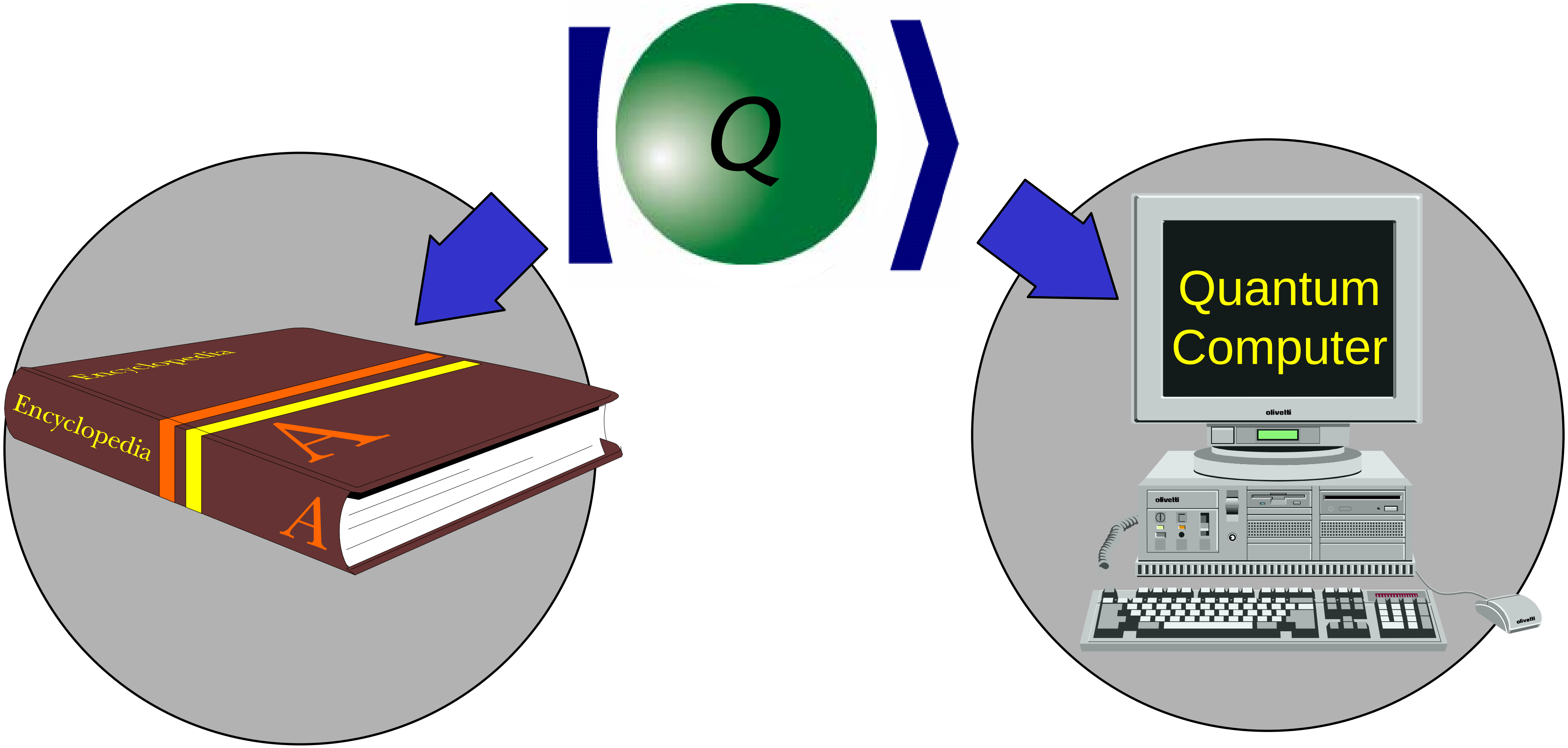
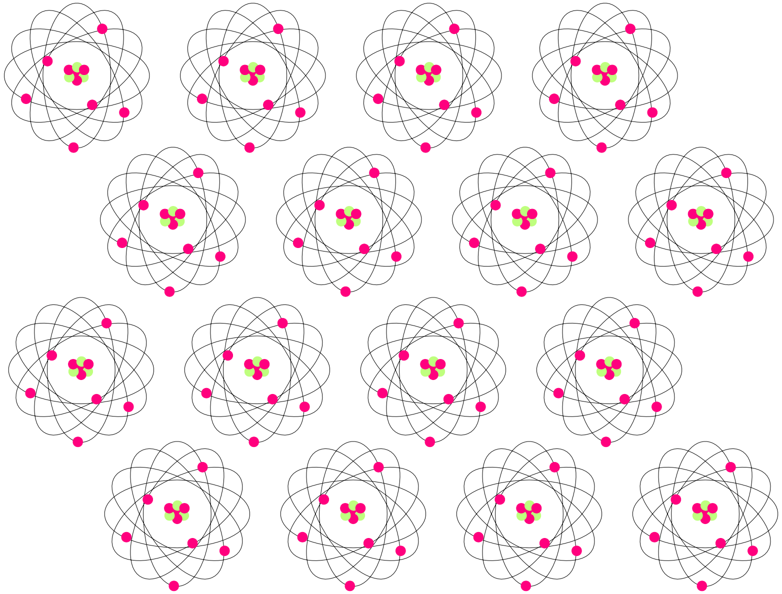
Quantum information and the future of physics

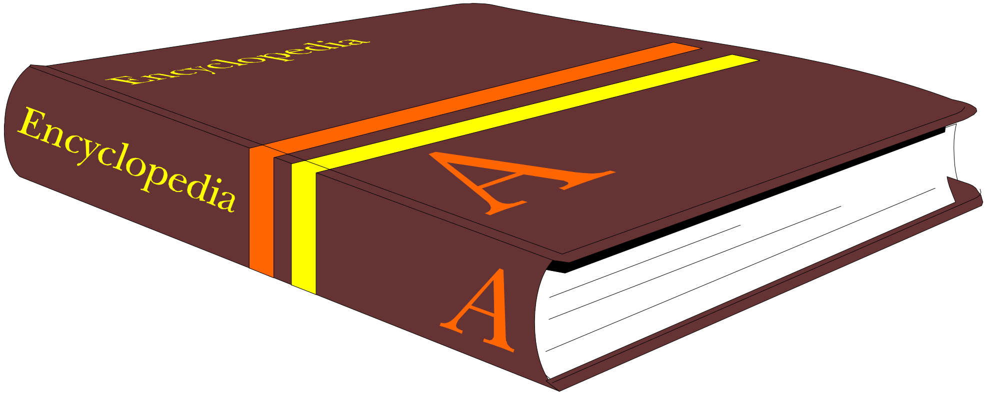


John Preskill
NSF workshop
15 March 2007

The ***Quantum*** Century

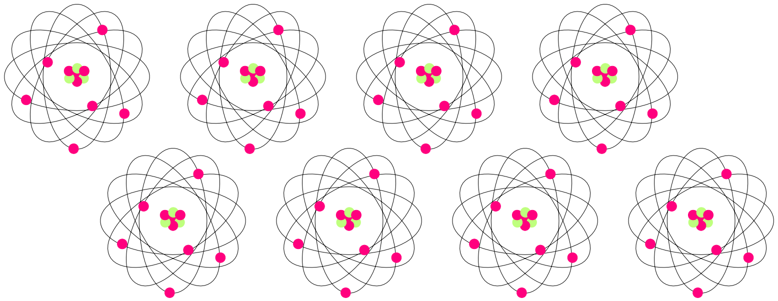


Though quantum theory is over 100 years old, there are profound aspects of the difference between quantum and classical systems that we have begun to understand in just the past few years. Many of these differences concern the *physical* properties of information …



Information

is encoded in the state of a *physical* system.



Information

is encoded in the state of a *quantum* **system.**

Put

Weirdness

to work!

Theoretical Quantum Information Science

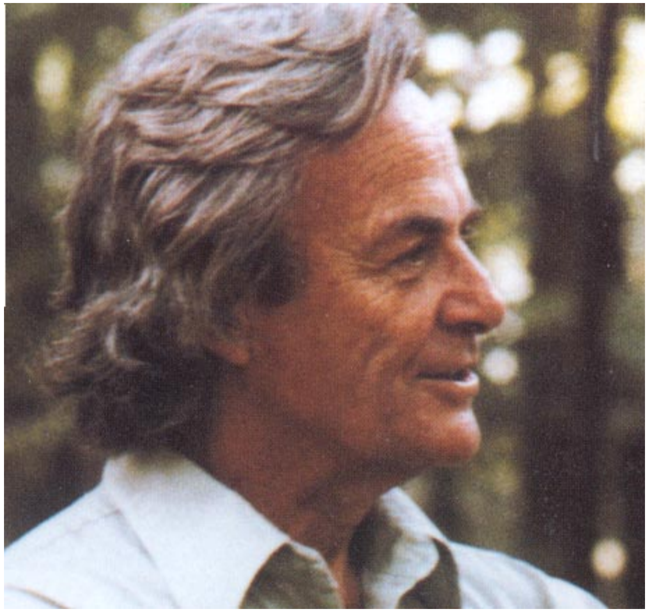
is driven by ...

Three ***Great*** Ideas:

1) Quantum Computation
2) Quantum Cryptography
3) Quantum Error Correction

These ideas originated during the past 30 years, and have been pursued aggressively for less than 15 years.

(1) Quantum Computation

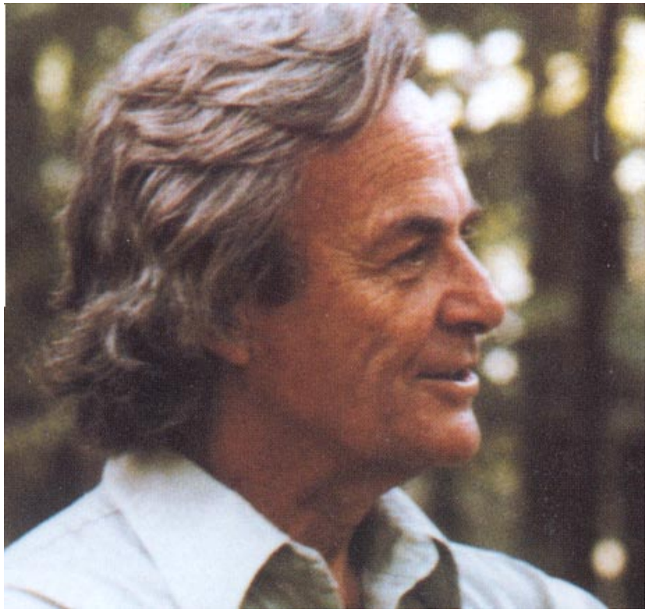


Feynman ‘81

Deutsch ‘85

Shor ‘94

A computer that operates on quantum states can perform tasks that are beyond the capability of any conceivable classical computer.



Feynman ‘81

Deutsch ‘85

Shor ‘94

Finding Prime Factors

1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

= ? × ?

Finding Prime Factors

1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

=

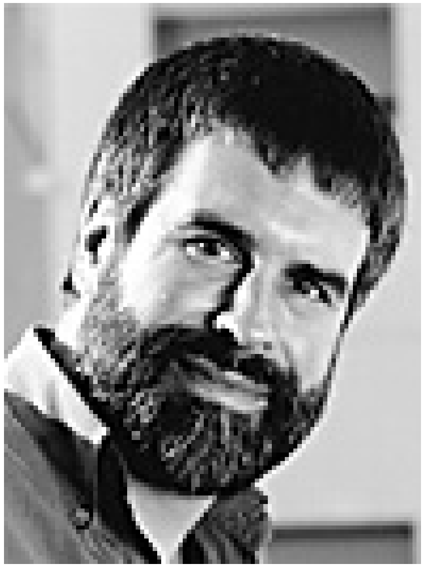
3968599945959
7454290161126
1628837860675
7644911281006
4832555157243

×

4553449864673
5972188403686
8972744088643
5630126320506
9600999044599

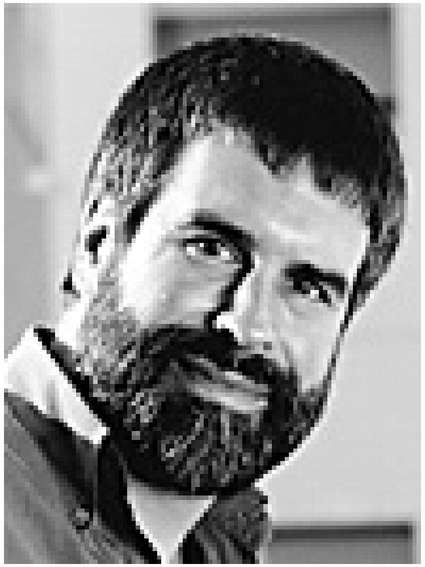
Shor ‘94

(2) Quantum Cryptography



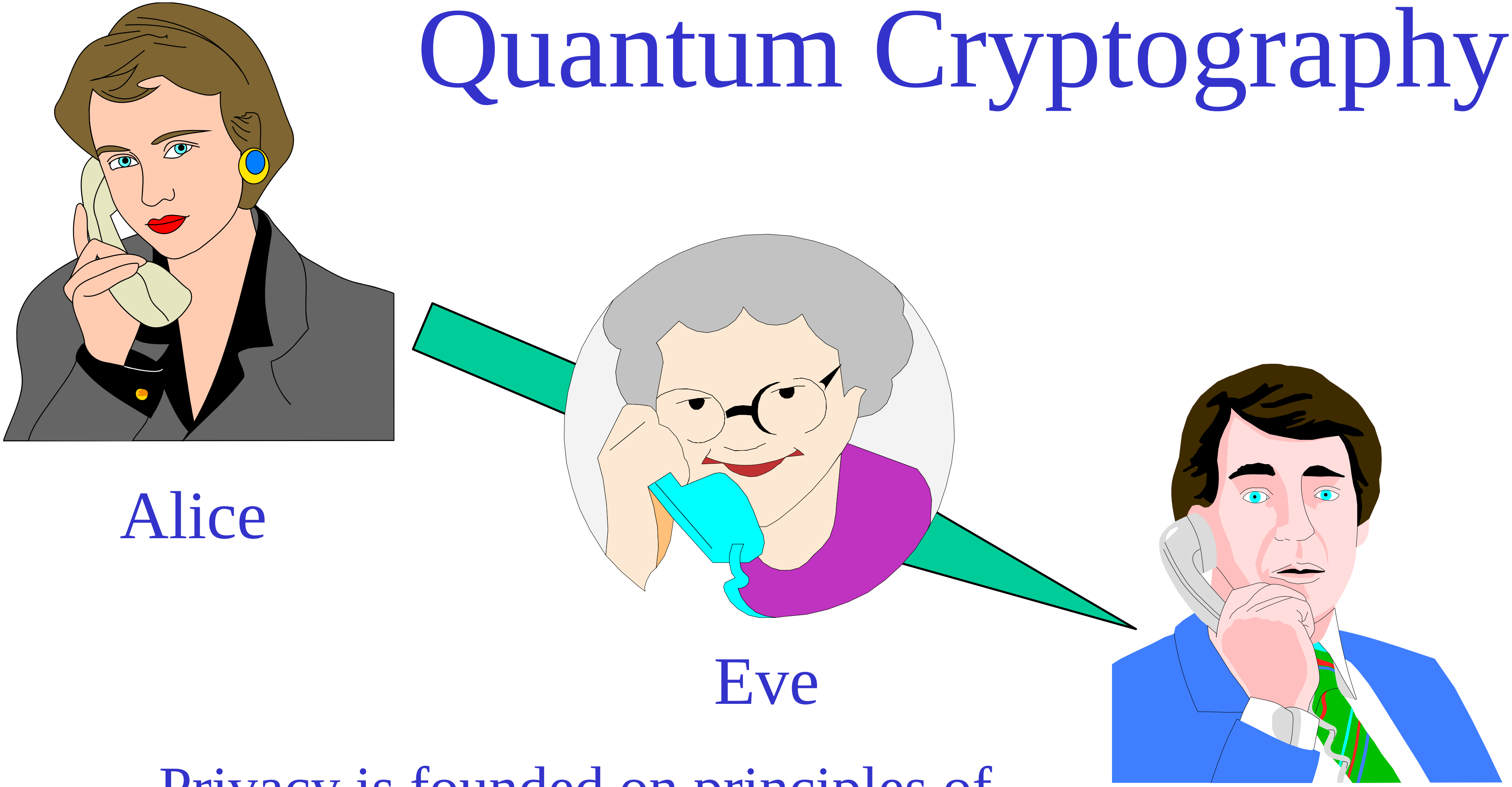
Bennett Brassard '84

Eavesdropping on quantum information can be detected; key distribution via quantum states is *unconditionally* secure.



Bennett   Brassard ’84

Quantum Cryptography



Alice

Eve

Bob

Privacy is founded on principles of fundamental physics, not the assumption that eavesdropping requires a difficult computation. Gathering information about a quantum state unavoidably disturbs the state.

(3) Quantum Error Correction

Shor ‘95

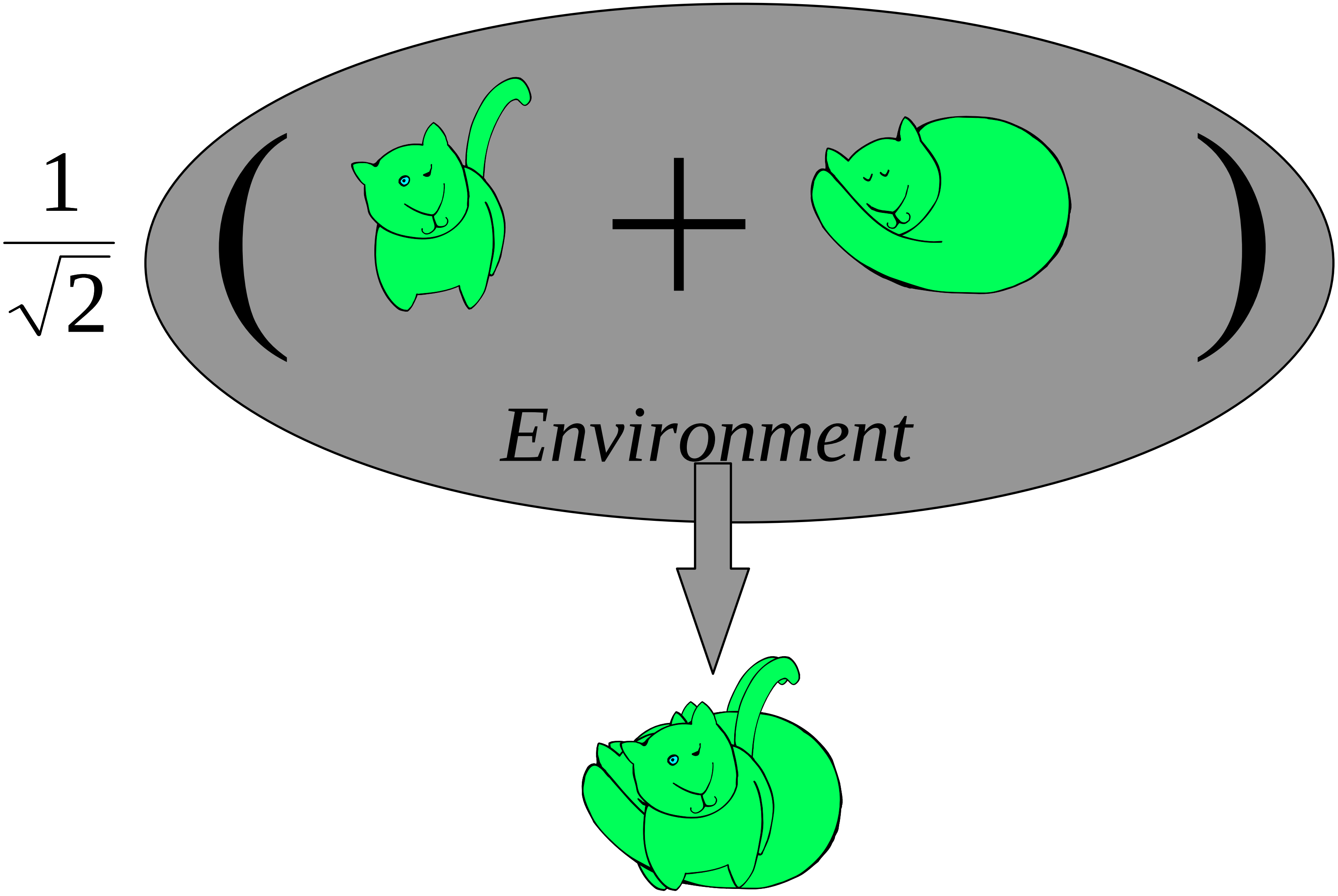
Steane ‘95

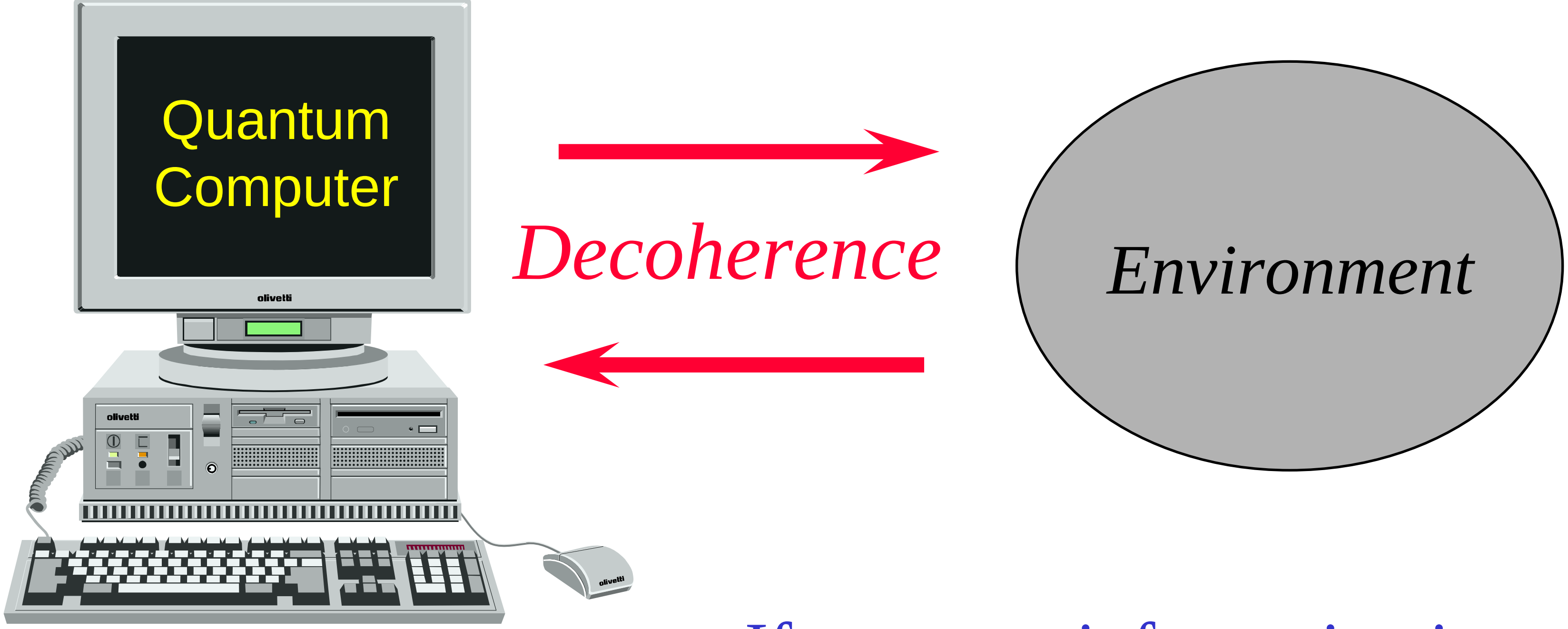
Quantum information can be protected, and processed fault-tolerantly.

Shor ‘95

Steane ‘95

Decoherence





Quantum Computer

Decoherence

Environment

ERROR!

If quantum information is cleverly encoded, it *can* be protected from decoherence and other potential sources of error. Intricate quantum systems *can* be accurately controlled.

Theoretical Quantum Information Science

is driven by ...

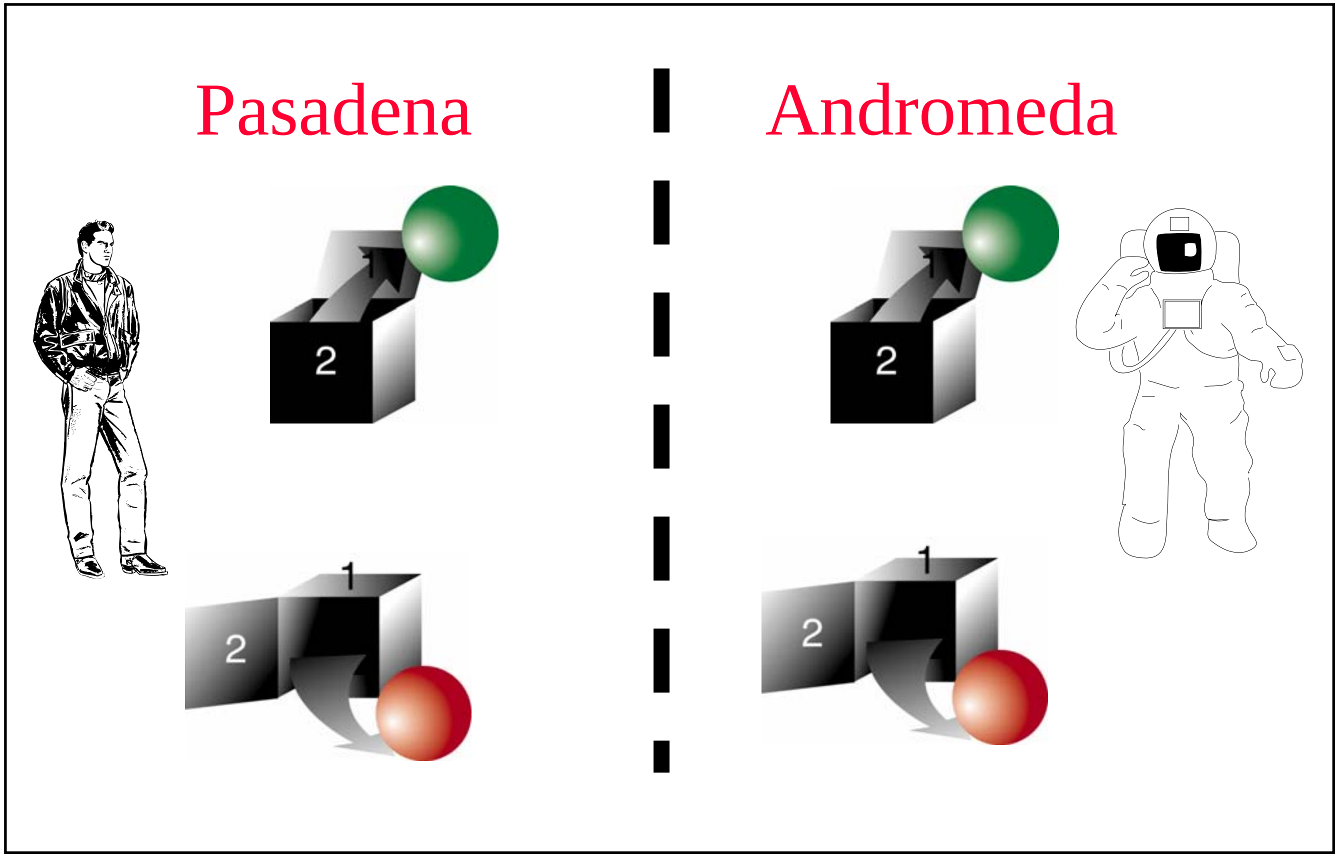
Three ***Great*** Ideas:

1) Quantum Computation
2) Quantum Cryptography
3) Quantum Error Correction

These ideas originated during the past 30 years, and have been pursued aggressively for less than 15 years.

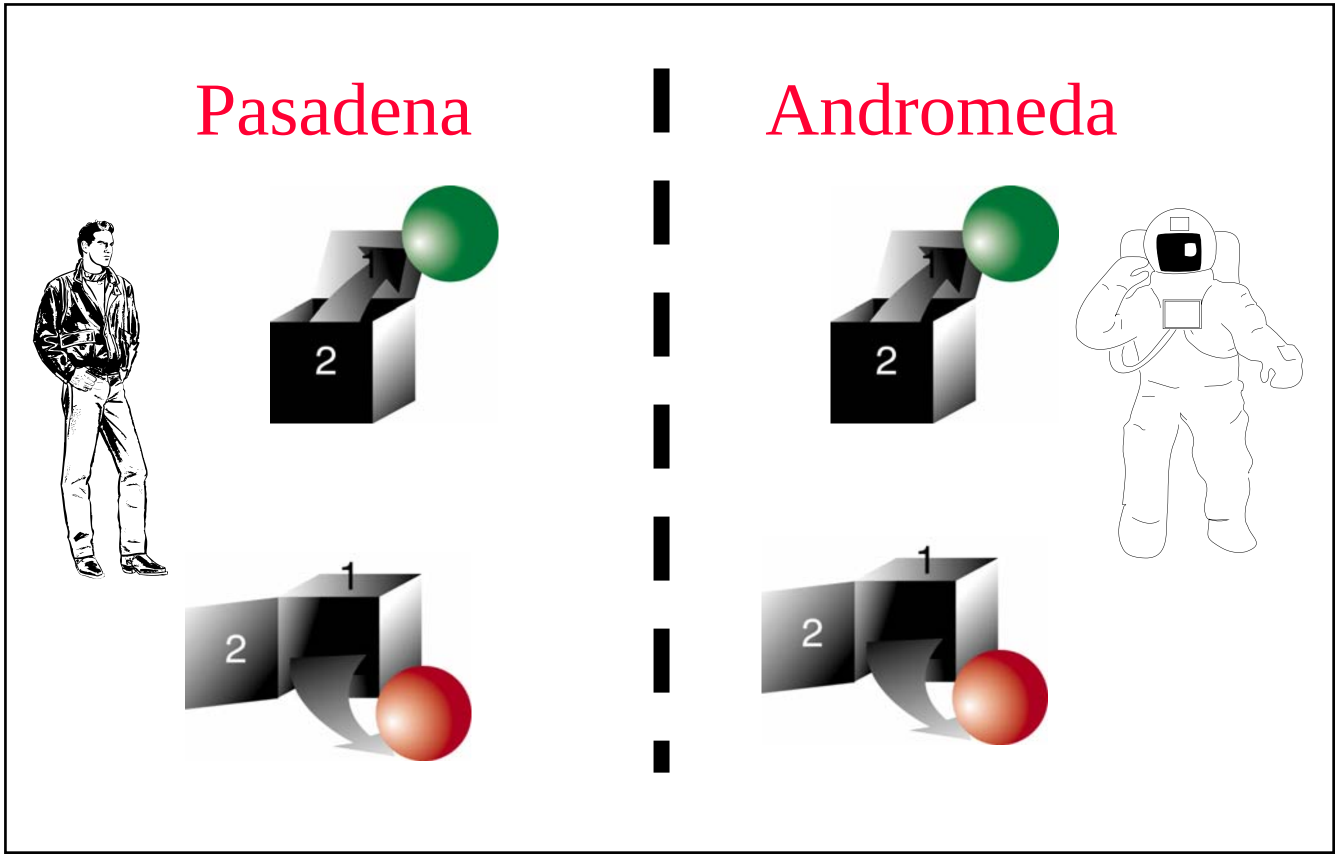
Quantum Entanglement

Bell ‘64



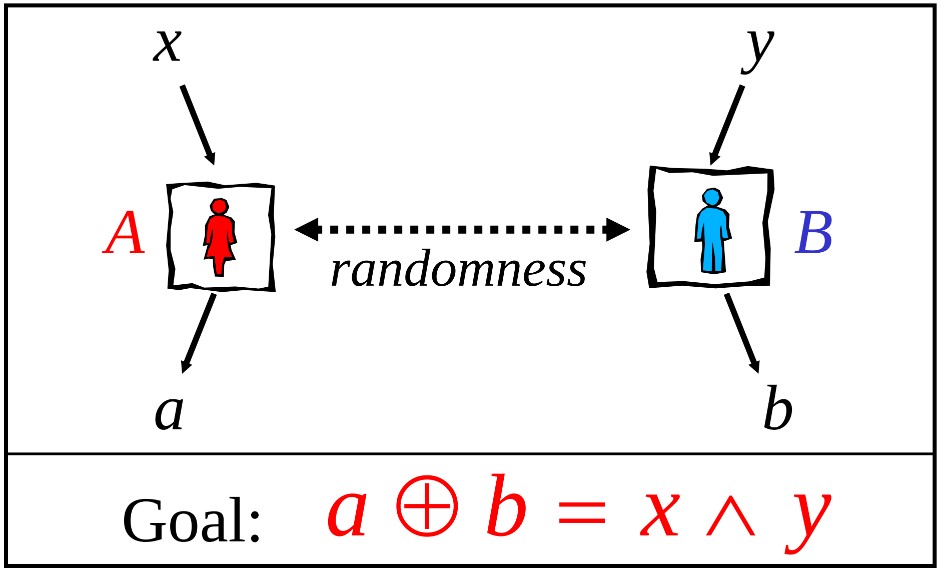
Quantum information can be *nonlocal*; quantum correlations are a stronger resource than classical correlations.

Bell ‘64



Quantum entanglement

Alice and Bob are cooperating, but distantly separated, players on the same team, playing a game. They cannot communicate, but in order to win the game, they must make correlated moves.



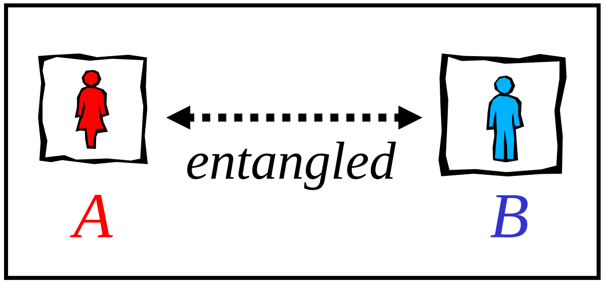
Goal: $a \oplus b = x \wedge y$

Bell’s theorem (1964): If Alice and Bob share classically correlated bits (which were prepared before the game began), they can win the game with probability no higher than 75% (averaged over all possible inputs), but if they share quantumly correlated qubits (quantum entanglement), they can win the game with probability 85.4%.

This example illustrates that *quantum correlations are a stronger resource than classical correlations*, enabling us to perform tasks that would otherwise be impossible.

Quantum entanglement

Bell’s theorem (1964): Alice and Bob have a higher probability of winning the game if they share quantumly correlated qubits (quantum entanglement) than if they shared classically correlated bits.



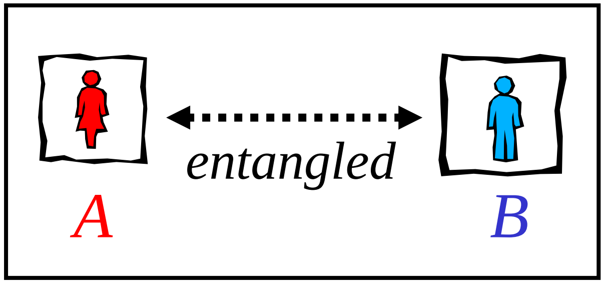
In experimental tests, physicists have played the game (e.g. with entangled photons – Aspect, 1982) and have won with a probability that exceeds what is possible classically (though there are still loopholes to these tests!).

Quantum information can be *nonlocal*; quantum correlations are a stronger resource than classical correlations.

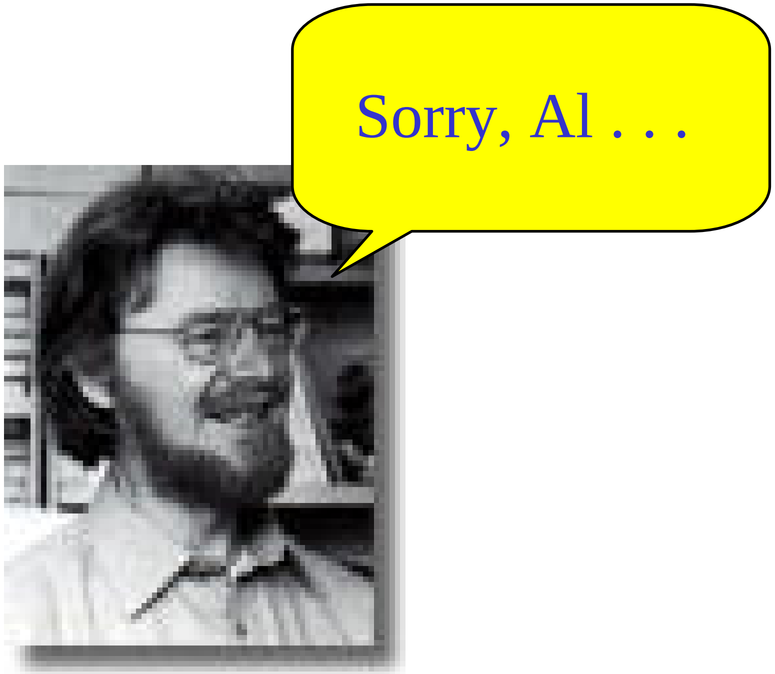
* Spooky action at a distance!!

Quantum entanglement

Bell's theorem (1964): Alice and Bob have a higher probability of winning the game if they share quantumly correlated qubits (quantum entanglement) than if they shared classically correlated bits.



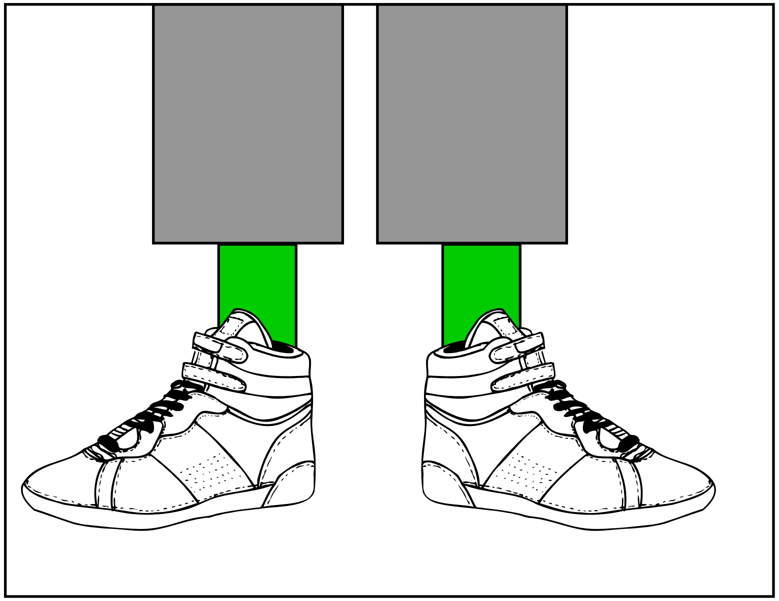
In experimental tests, physicists have played the game (e.g. with entangled photons – Aspect, 1982) and have won with a probability that exceeds what is possible classically (though there are still loopholes to these tests!).



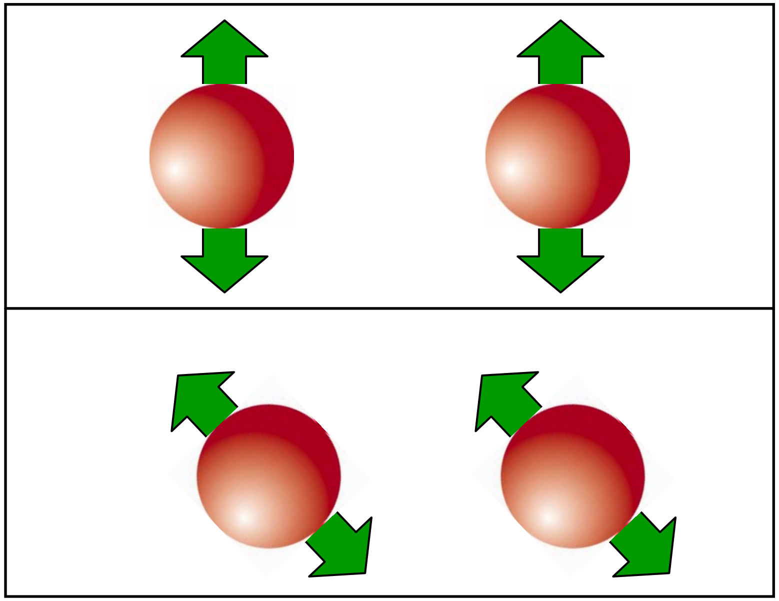
* Spooky action

at a distance!!

Quantum Entanglement



classically correlated socks



quantumly correlated photons

- There is just one way to look at a classical bit (like the color of my sock), but there are complementary ways to observe a quantum bit (like the polarization of a single photon). Thus correlations among *qubits* are richer and much more interesting than correlations among classical bits.

- A quantum system with two parts is *entangled* when its joint state is more definite and less random than the state of each part by itself. Looking at the parts one at a time, you can learn everything about a pair of socks, but not about a pair of qubits!

The quantum correlations of many entangled qubits cannot be easily described in terms of ordinary classical information. To give a complete classical description of one typical state of just a few hundred qubits would require more bits than the number of atoms in the visible universe!

It will never be possible, even in principle to write down such a description.

The power of quantum computation

Quantum correlations admit no succinct description using classical information. A complete description of a typical quantum state of 300 *qubits* would require of order 2^{300} classical bits, more than the number of atoms in the visible universe.

Therefore, a classical digital computer, in order to simulate a quantum computer, would have to manipulate matrices of exponentially large size. It seems that such a classical simulation of a quantum computation, using reasonable resources, is impossible.

A quantum computer would be a powerful tool for solving number theoretic problems: factoring, calculating discrete logarithms, finding units in algebraic number rings, etc.

Therefore, a quantum computer would be able to break widely used public key cryptosystems, which are based on the presumed hardness of such problems.

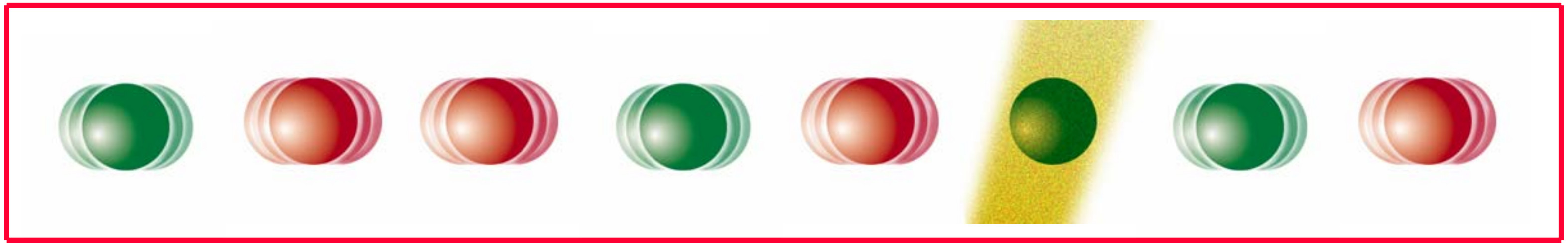
ten
entangled
qubits

The power of quantum computation

A quantum computer could simulate efficiently the real time evolution of a many-body quantum system, solving important problems in *ab initio* chemistry, simulation of exotic materials, quantum many-body physics, and quantum field theory.

Quantum computers can find solutions to hard combinatorial search problems (NP-complete problems) by exhaustive search, with a quadratic speed-up (quantum search time is square root of classical search time). The conventional wisdom, for which there is strong evidence, is that quantum computers *cannot* achieve an exponential speedup in finding solutions to hard instances of NP-complete problems.

Experimentally, small scale quantum computations have been demonstrated using cold electromagnetically trapped ions manipulated with lasers, and using liquid state nuclear magnetic resonance methods.



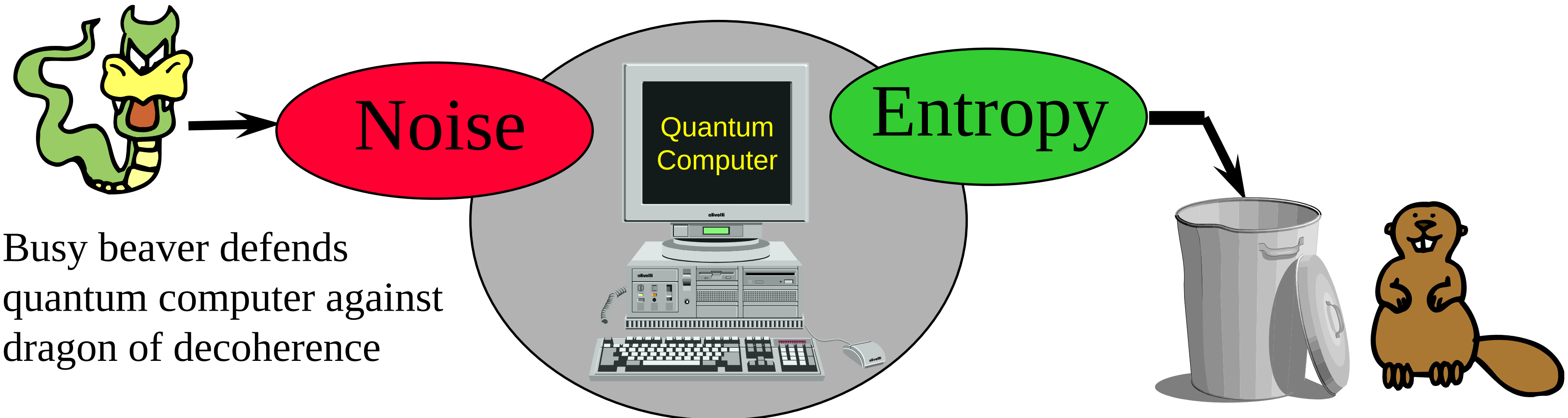
ion trap quantum computer

Battling decoherence using quantum error correction

Quantum information can be protected by hiding the information in quantum correlations among many qubits, so that local noise cannot easily damage the information.

A quantum computation can be executed *fault tolerantly,* provided that the (1) noise is weak and not too strongly correlated, (2) quantum gates can operate in parallel (to control noise in different parts of the computer simultaneously), (3) quantum memory can be refreshed (to remove entropy).

There is a *quantum threshold of accuracy* --- if the noise is weak enough, an arbitrarily long quantum computation can be executed reliably, with reasonable overhead.



Noise

Quantum Computer

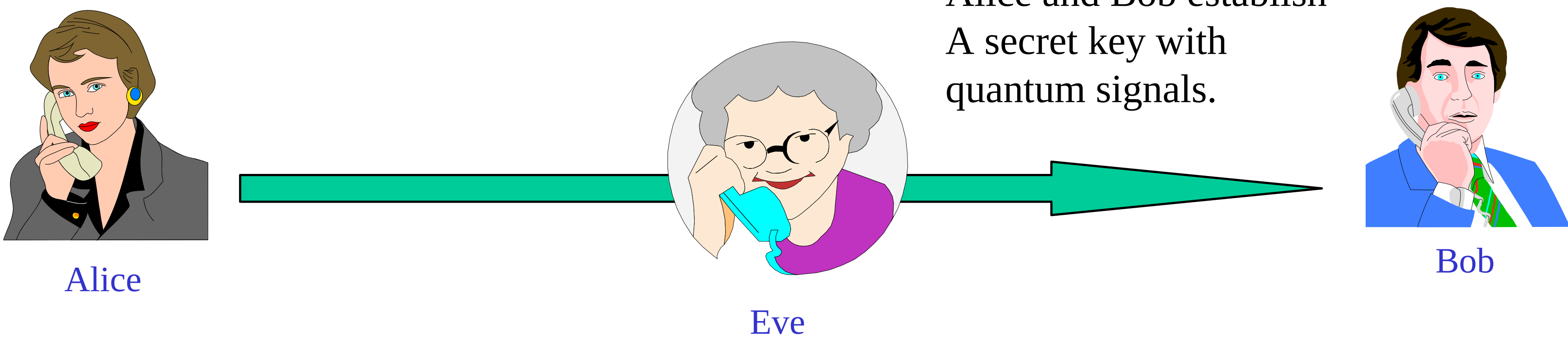
Entropy

Busy beaver defends quantum computer against dragon of decoherence

Quantum key distribution

In quantum key distribution, Alice and Bob use quantum signals (and an authenticated classical channel) to establish a shared private key that can be used to encrypt and decrypt classical messages. An eavesdropper (Eve) who collects information about the key by interacting with the signals produces a detectable disturbance; therefore Alice and Bob can detect Eve's activity, and they can reject the key if they fear that Eve knows too much about it.

Alice and Bob can generate a key that, with high probability, is almost perfectly private. The protocol is secure for any attack by Eve allowed by the known principles of quantum physics.

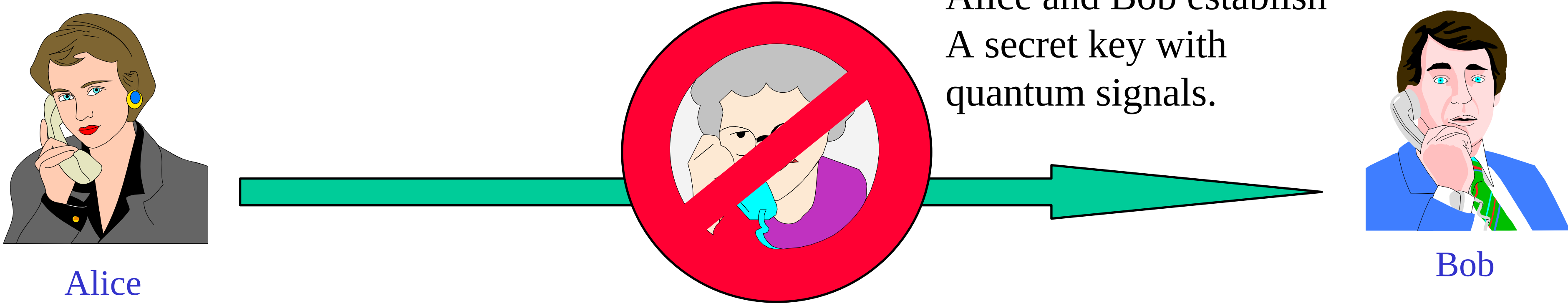


Alice and Bob establish
A secret key with
quantum signals.

Quantum key distribution

In quantum key distribution, Alice and Bob use quantum signals (and an authenticated classical channel) to establish a shared private key that can be used to encrypt and decrypt classical messages. An eavesdropper (Eve) who collects information about the key by interacting with the signals produces a detectable disturbance; therefore Alice and Bob can detect Eve's activity, and they can reject the key if they fear that Eve knows too much about it.

Alice and Bob can generate a key that, with high probability, is almost perfectly private. The protocol is secure for any attack by Eve allowed by the known principles of quantum physics.



Alice and Bob establish
A secret key with
quantum signals.

QKD for sale!

Security is based on the principle that copying of quantum signals can be detected, a property not shared by classical information.

Experiments have demonstrated the feasibility of quantum key distribution (QKD) protocols in which single-photon pulses are sent through (150 km) telecom fibers, or through free space.

Furthermore, quantum key distribution systems are now *commercially available*. You can order one over the (classical) Internet.

Quantum Security...
at last

Quantum Key Distribution System

Key distribution over optical fiber with absolute security

Main features

- First quantum cryptography system
- Security guaranteed by quantum physics
- Point-to point key distribution
- Standard optical fiber
- Distances up to 70 km
- Key rate up to 1000 bits/s
- Compact and reliable

Key distribution is a central problem in cryptography. Currently, public key cryptography is commonly used to solve it. However, these algorithms are vulnerable to increasing computer power. In addition, their security has never been formally proven.

Quantum cryptography exploits a fundamental principle of quantum physics - observation causes perturbation - to distribute cryptographic keys with absolute security.

id Quantique is introducing the first quantum key distributionsystem. It consists of an emitter and a receiver, which canbe connected to PC's through the USB port.

id Quantique

10, rue Cingria 1205 Genève Switzerland
Tel: (+41) 022 702 69 29 Fax: (+41) 022 781 09 80
email: info@idquantique.com
web: http://www.idquantique.com

id Quantique
A Quantum Leap for Cryptography

[illegible]

Some quantum challenges

Better characterize the power of quantum computation and discover new algorithms. How can quantum computers be used? What quantum simulation problems are hard for classical computers?

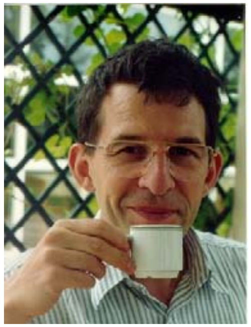
Fault tolerance and control: How much noise can be tolerated? How can we best protect against noise in real devices? What are the best ways to control quantum systems in real time under actual experimental conditions. Are there clever encodings of quantum information that are *intrinsically* robust?

Cryptography: What are the other applications, beyond key distribution, for a quantum Internet? Are there classical public key cryptography schemes that are secure against quantum attacks?

Hardware: Quantum repeaters and memory nodes to extend the reach of quantum cryptography (easier than large-scale quantum computation, and a potential application for modest-scale quantum computing). Implementations of quantum gates that are potentially scalable to a large computer. Realistic fault-tolerant architectures.

Quantum Hardware

Kimble



Devoret

Two-level ions in a Paul trap, coupled to “phonons.”

Two-level atoms in a high-finesse microcavity, strongly coupled to cavity modes of the electromagnetic field.

Charge in a Cooper-pair box; fluxons through a superconducting loop.

Electron spin (or charge) in quantum dots.

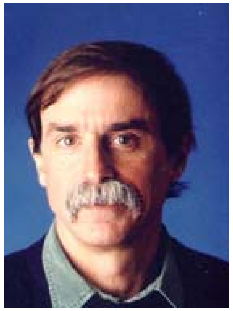
Cold atoms in optical lattices.

Nuclear spins in semiconductors, and in liquid state NMR.

Linear optics with efficient single-photon sources and detectors.

Anyons in fractional quantum Hall systems.

Electrons floating on liquid He, etc.

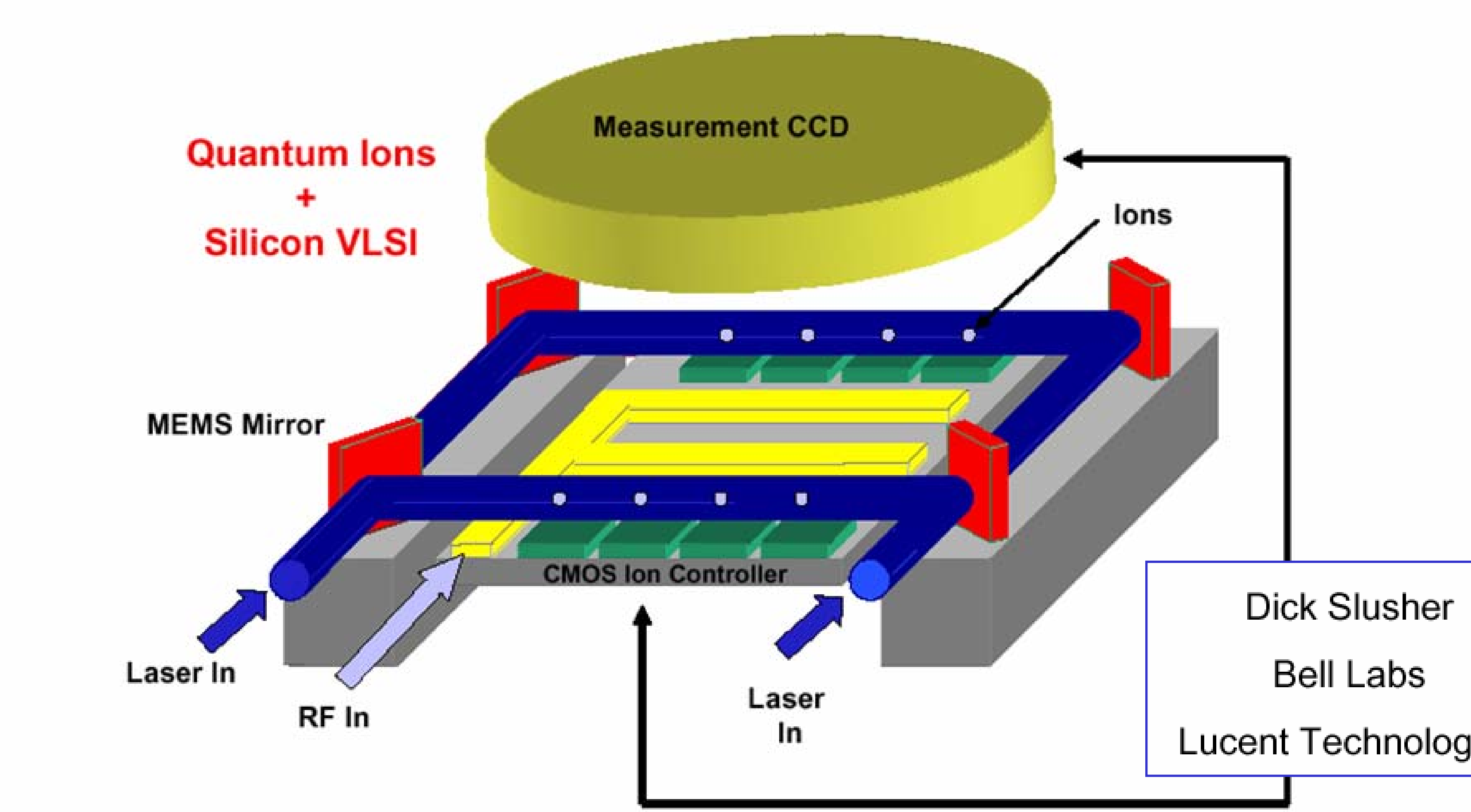


Wineland

Blatt

A factoring engine in 25 years?
Unlikely, but not impossible.

Scalable ion trap quantum computer: The Dream

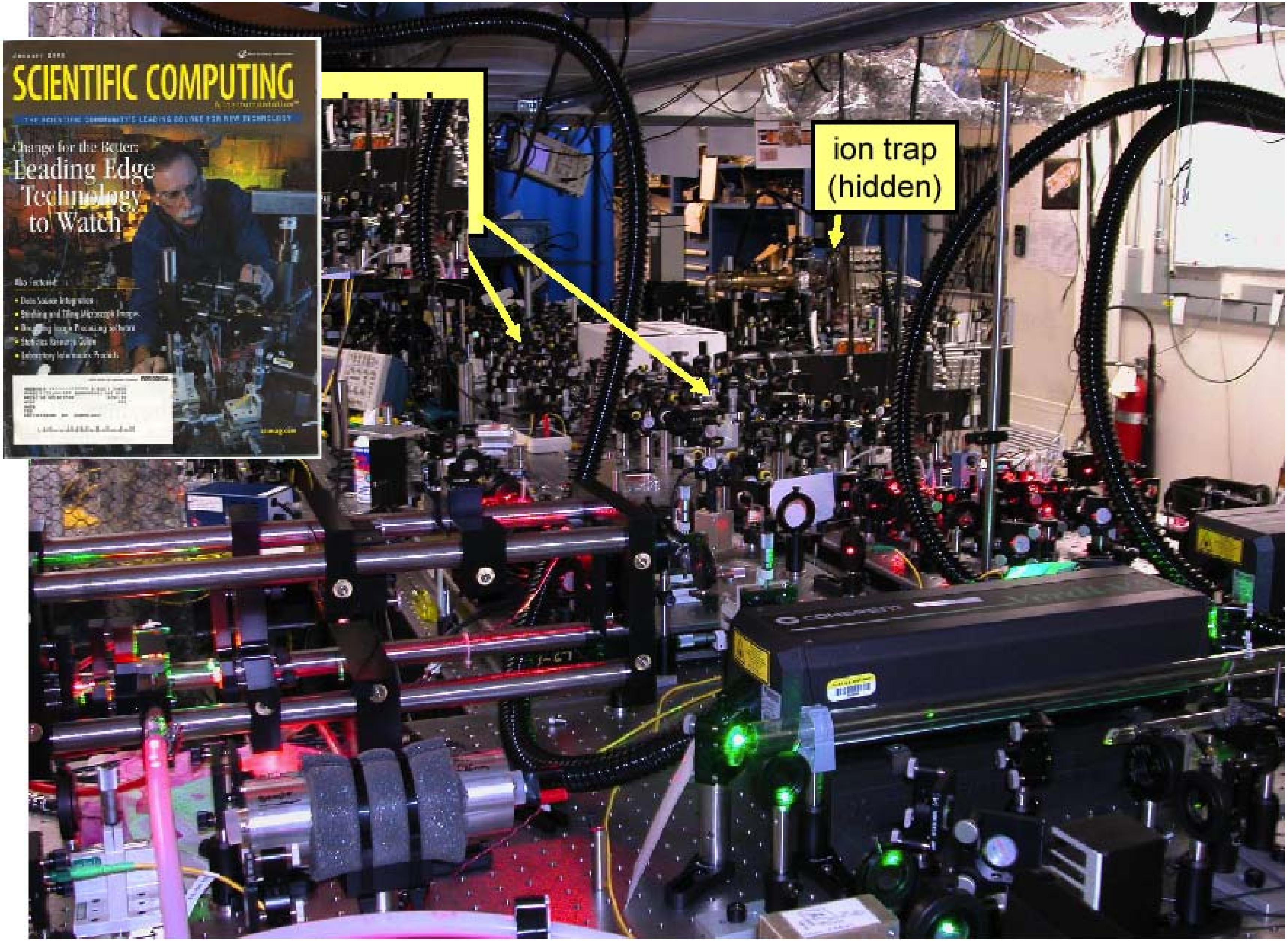


Dick Slusher

Bell Labs

Lucent Technologies

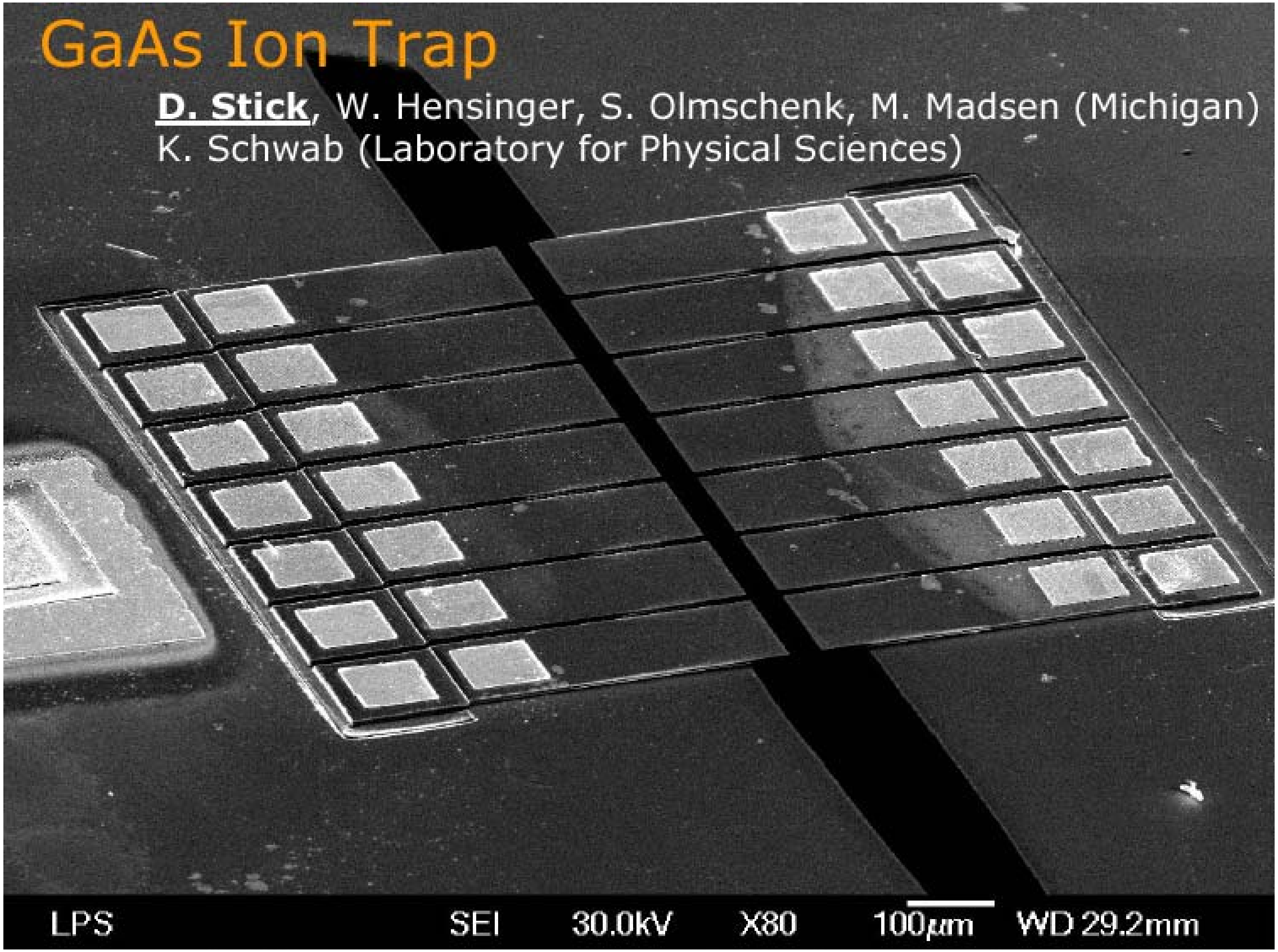
System Compatibility of Quantum & Classical: Spatial Pitch, Clock Speed
Operating Temperature, Power Dissipation



Ion trap quantum computer: The Reality

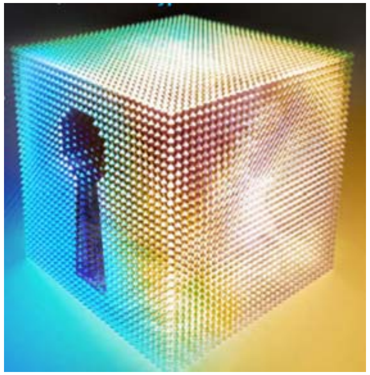
GaAs Ion Trap

D. Stick, W. Hensinger, S. Olmschenk, M. Madsen (Michigan)
K. Schwab (Laboratory for Physical Sciences)



Quantum Information Challenges

Cryptography



Privacy from physical principles

Algorithms

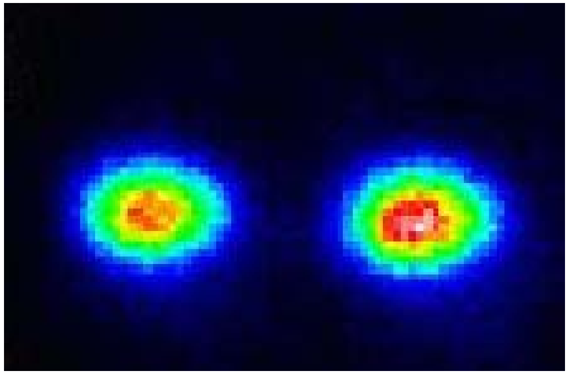
$$\sum_{x \in G} | x \rangle \otimes | f(x) \rangle$$

What can quantum computers do?

Error correction

Reliable quantum computers

Hardware



Toward scalable devices

And …what are the implications of these ideas for basic physics?

Challenges in theoretical (quantum) physics?

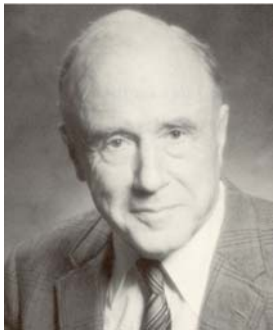
Weinberg

- "Dreams of a final theory." What theory describes the fundamental constituents of matter and their interactions? (What *computational model* is realized in Nature?)

Anderson

- "More is different." What emergent collective phenomena can arise in condensed matter? (What is the potential *complexity* of quantum many-body systems?)

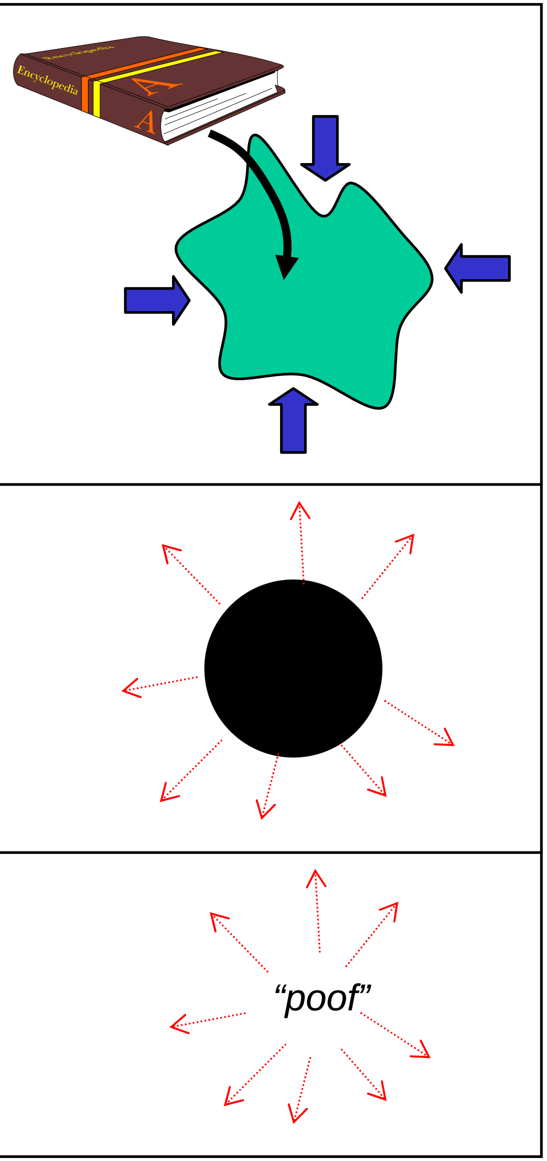
- "How come the quantum?" *Why* do the rules of quantum mechanics apply to Nature? (Is *everything* information?)



Wheeler

What (if anything) do these challenges have to do with (quantum) computation? How might computational concepts illuminate the big questions at the core of physics?

Dreams of a final theory: quantum gravity



The deepest questions about fundamental particle physics concern the properties of information under *extreme conditions*, particularly in the regime where *quantum fluctuations of spacetime* are strong.

Black holes: Does information escape from an evaporating black hole, and if so, how?

Cosmology: Why is the quantum state of the universe simple, and what does it mean that it is “simple.” Why is the universe “classical” on large scales?

M theory: Can computational approaches help us to answer “What is M theory?” How would we simulate M theory with a quantum computer? Can the simulation be efficient? Would an M theory computer be more powerful than a garden variety computer?

Holography: What does the holographic principle imply about the computational power written into the laws of Nature? Can quantum codes illuminate the origin of “emergent geometry”?

How come the quantum?

New foundations? If quantum mechanics is flawed, what is the alternative? If it is not flawed, can we understand why it must be the way it is? What *deformations* of quantum theory make sense?

Alternative computational models: Some ways of modifying quantum theory seem to give rise to "unreasonable" computational or cryptographic power. Is there a physical principle that says that some classes of problems are required to be hard?

Quantum mechanics as an effective long-distance theory: Could there be strong deviations from quantum theory at very short distance that are suppressed at the longer distances that are currently accessible experimentally?

Will we probe fundamental physics, not at Fermilab, but at "Feynmanlab"? Will we discover that large-scale quantum computation is impossible (not just in practice but in principle) because the currently understood laws of quantum physics fail for highly entangled states built from a sufficiently large number of qubits?

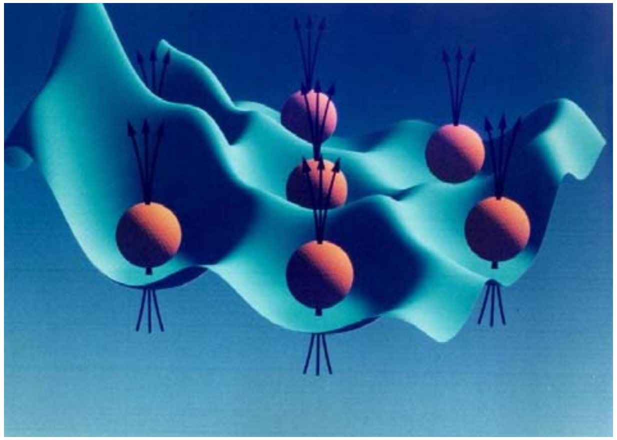
More is different: condensed matter physics

In a nutshell:

$$\boxed{whole > \sum (parts)}$$

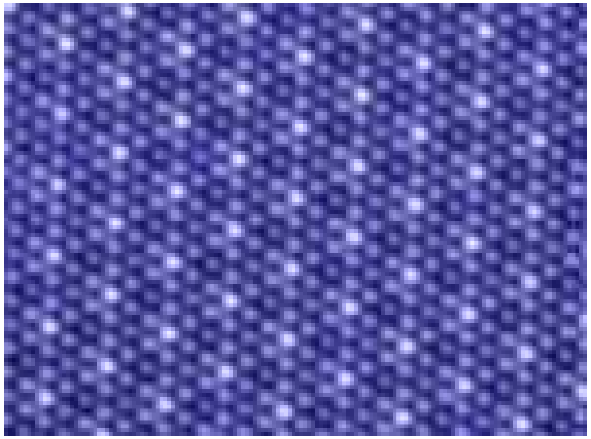
Emergent phenomena: the collective behavior of many particles cannot be easily guessed, even if we have complete knowledge of how the particles interact with one another.

Entangled quantum many-particle systems have an enormous capacity to surprise and delight us.



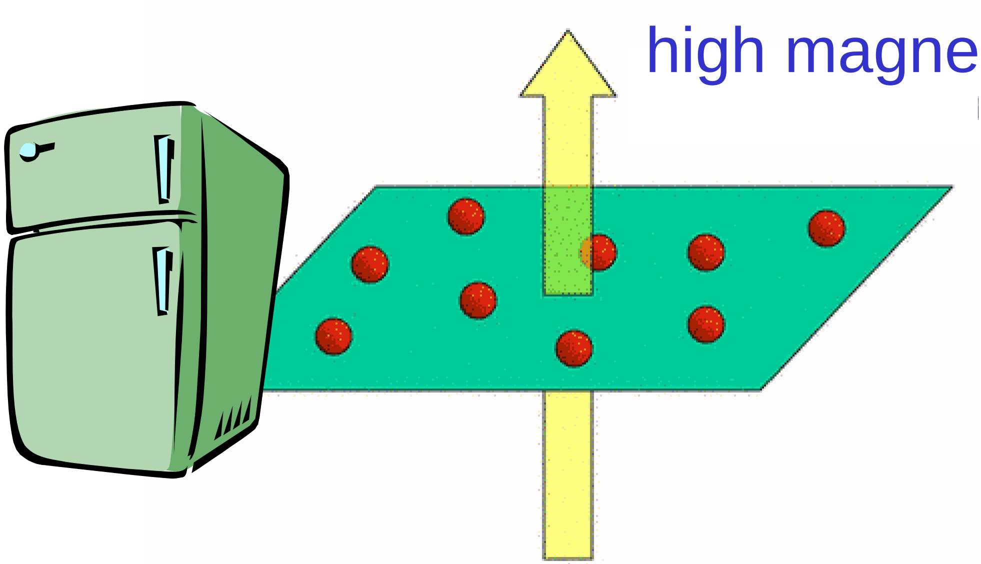
Fractional quantum Hall state

High temp. superconductor



Crystalline material

Emergence: the fractional quantum Hall effect



high magnetic field

electrons moving freely on a “table,” at very low temperature

An exotic new phase of matter, with local particle excitations (“quasi-particles”) that are profoundly different than the constituent electrons. In fact, a single quasi-particle carries an electric charge that is a fraction (for example, 1/3) of the charge of an electron.

More is different: Quantum many-body physics

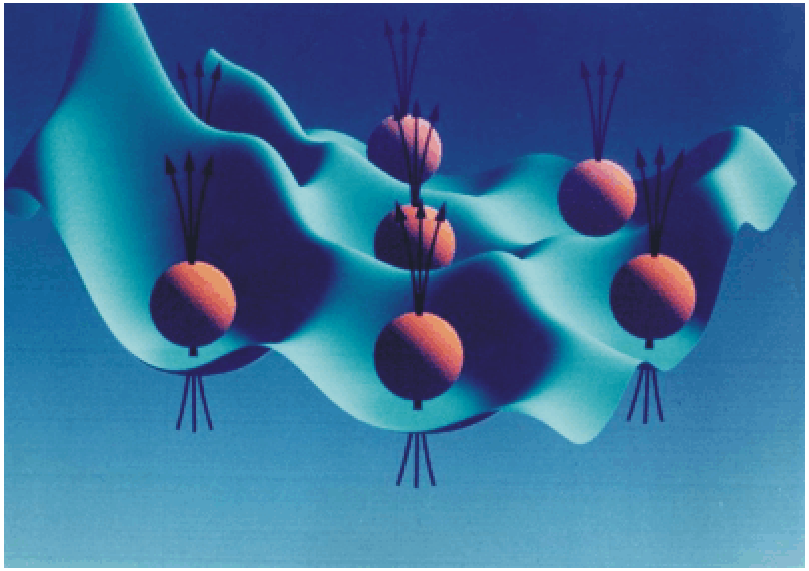
What are the possible manifestations of *many-particle quantum entanglement*? What collective phenomena arise when quantum fluctuations are large? [For example, systems composed of “strongly correlated electrons” such that the elementary excitations do not resemble electrons.]

What phases of matter are possible at zero temperature? What physical properties are robust (invariant under small changes in the Hamiltonian)? What are the (universal) properties of the transitions between the phases? Can there be a “final theory” of (quantum) condensed matter, or are collective phenomena inexhaustible?

- High-temperature superconductivity.

•What microscopic mechanism explains the properties of the high-T_c cuprates?

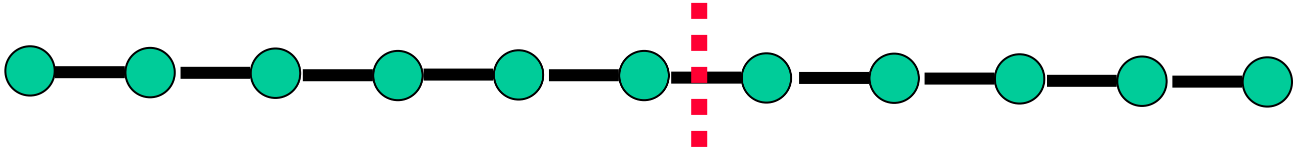
- Quantum Hall systems. What phases can be realized by a highly correlated two-dimensional gas of highly mobile electrons in a strong magnetic field?



Fractional quantum Hall state

Are these the tip of an iceberg?

Efficient classical simulation of quantum systems with bounded entanglement



Vidal

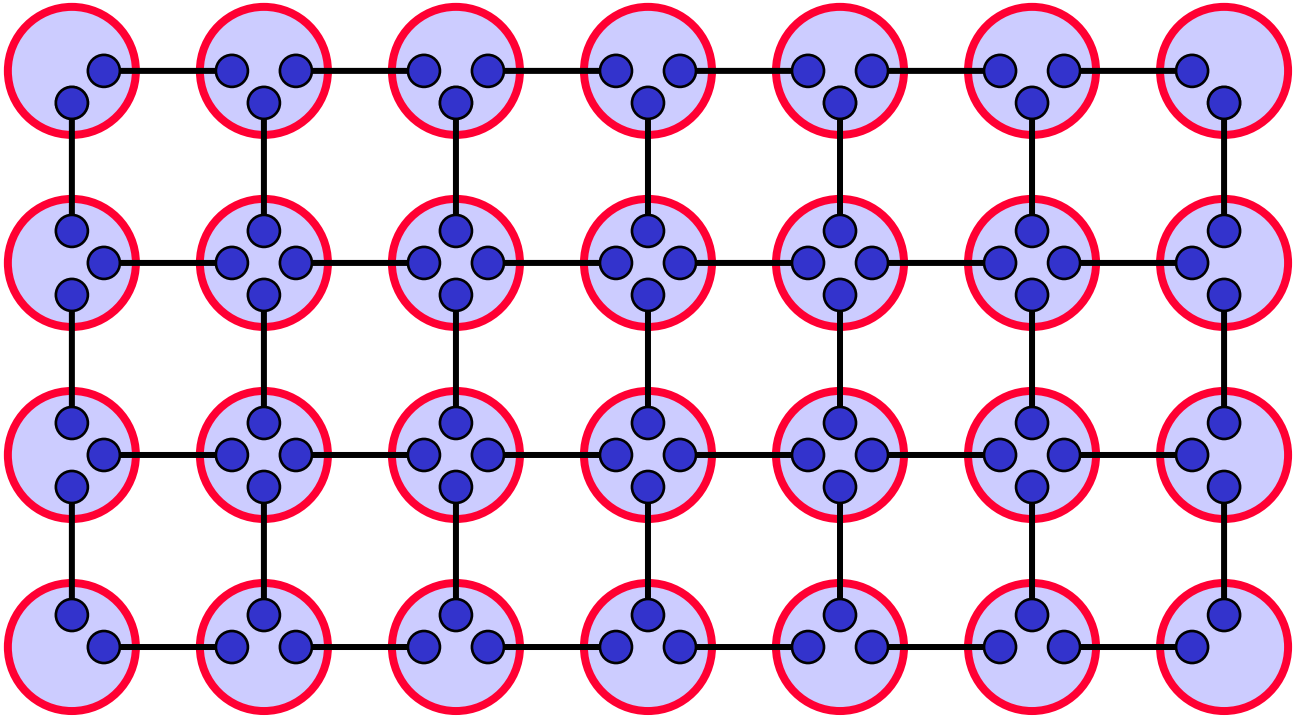
In general, there is no succinct classical description of the quantum state of a system of *n* qubits. But suppose, e.g., for qubits arranged in one dimension, that for any way of dividing the line into two segments, the strength of the quantum correlation (the amount of entanglement) between the two parts is bounded above by a constant, independent of n.

Vidal ('03) showed that in that case a succinct description is possible, with $O(n)$ parameters rather than 2^n, and that the description can be easily updated as the state evolves (if the interactions are local).

This makes precise the idea that entanglement is the source of a quantum computer's power: if the quantum computer does not become highly entangled, it can be efficiently simulated by a classical computer.

Furthermore, in one-dimensional systems with local interactions, the entanglement increases no more rapidly than $\log n$, and an efficient classical simulation of real time evolution is possible.

Projected entangled-pair states



Affleck

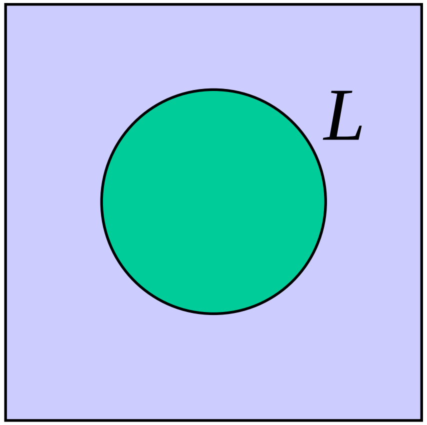
Werner

Cirac

Verstraete

Many-body quantum states can be described as *projected entangled-pair states* (Cirac and Verstraete ’04), extending the matrix product formalism (Affleck et al. ’88, Werner et al. ’92) to two or more dimensions. Lines are maximally entangled pairs of D-state auxiliary spins, and in each red circle, these auxiliary spins are projected onto the physical spins. For many systems, this technique provides a relatively succinct description that can be updated efficiently as the physical spins evolve.

Universal properties of entanglement



For the ground state of a large *two-dimensional* system, consider the entanglement of a disk (circumference L) with the rest of the system. For a system with a nonzero energy gap, the entanglement is:

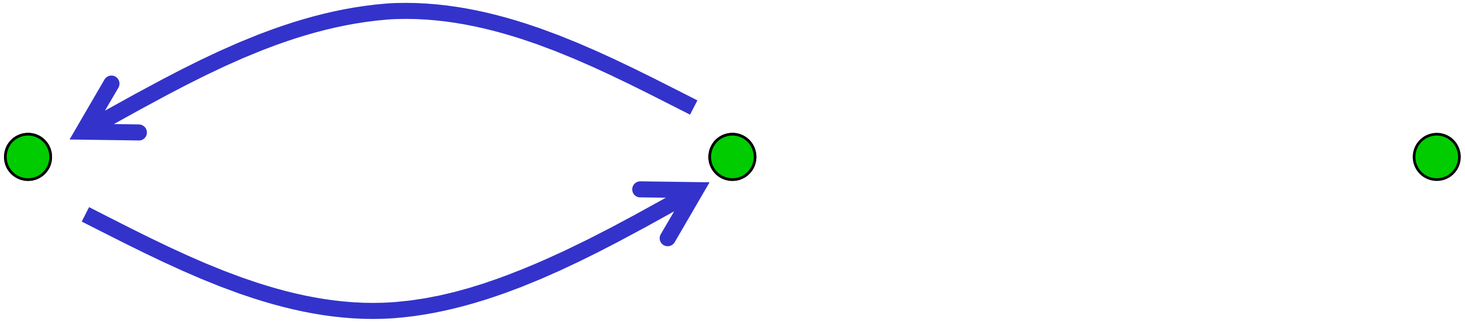
$$E = \alpha L - \gamma$$

The leading term proportional to L, arising from short distance fluctuations near the boundary, has a coefficient α that is cutoff dependent and nonuniversal. But there is also an additive correction γ, which is universal! (It does not depend on the geometry of the region, or on the microscopic details of the interactions in the system.) This term, the *topological entanglement entropy*, is a global feature of the the many-body quantum entanglement, characterizing the *topological order* of the gapped two-dimensional system (Kitaev-Preskill '06). There is a simple formula for the universal constant γ, in terms of the properties of the particle excitations of the system.

Thus, in this case a quantum phase of matter can be characterized by universal properties of many-body entanglement. And the topological order can be recognized on a topologically trivial surface (the plane).

Anyons

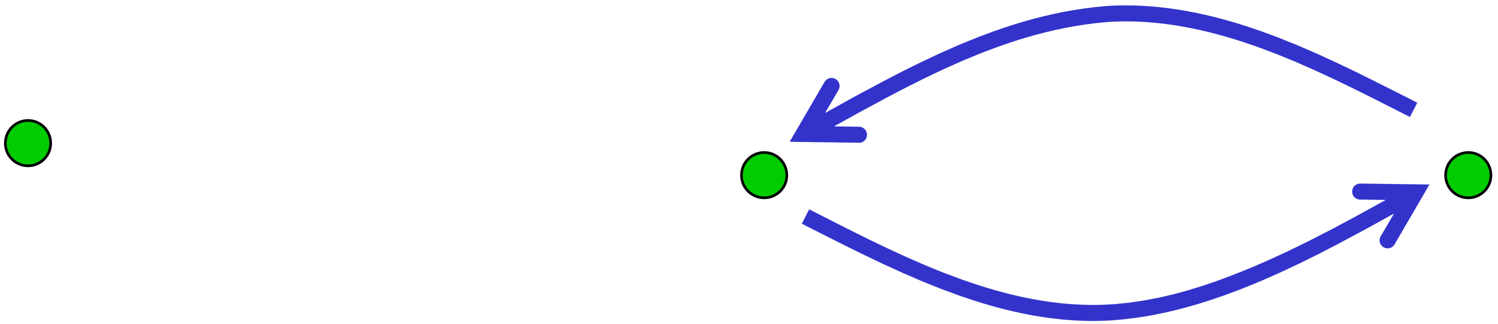
Quantum information can be stored in the collective state of exotic particles in two dimensions (“anyons”).



The information can be processed by exchanging the positions of the anyons (even though the anyons never come close to one another.

Anyons

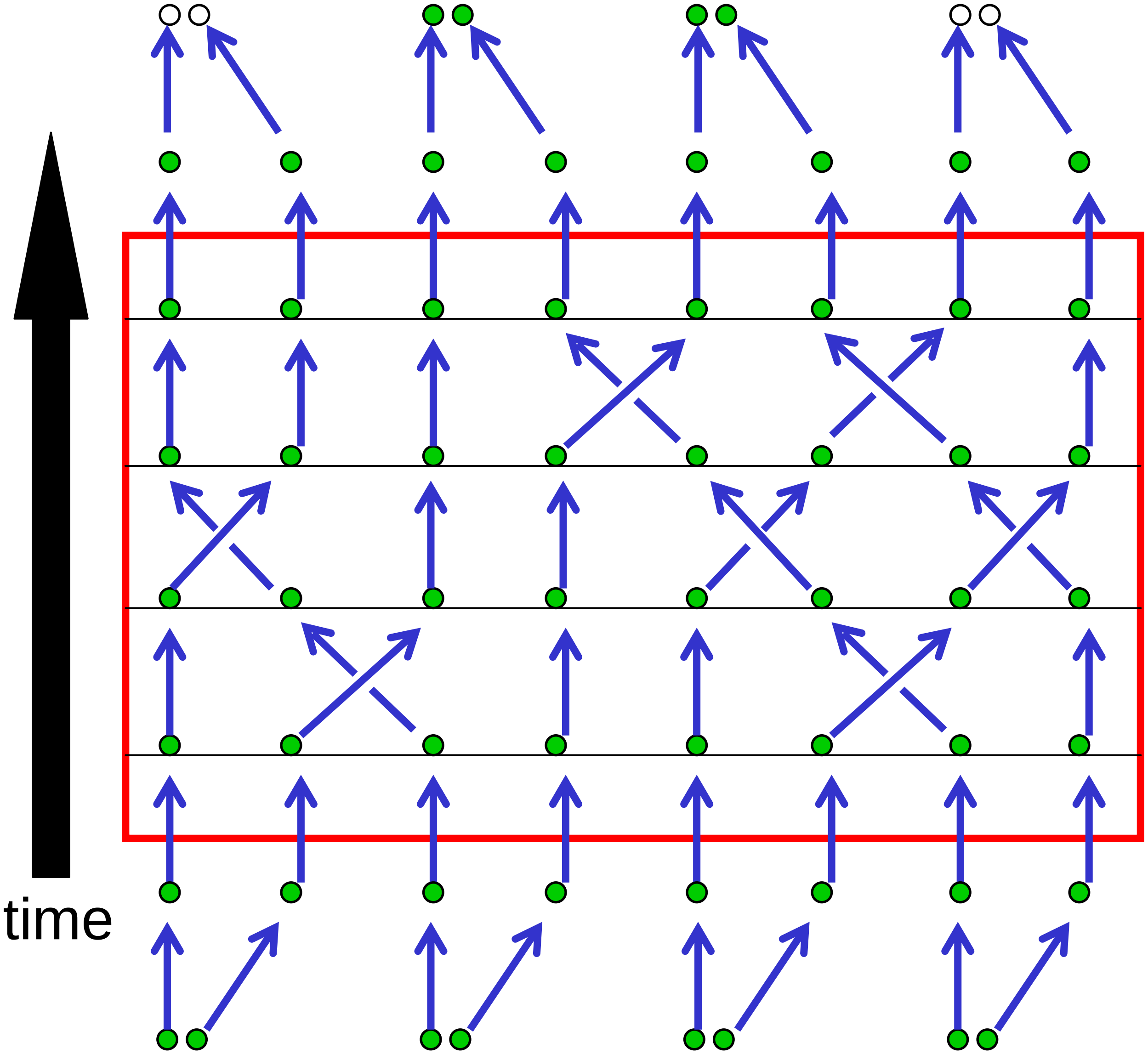
Quantum information can be stored in the collective state of exotic particles in two dimensions (“anyons”).



The information can be processed by exchanging the positions of the anyons (even though the anyons never come close to one another.

Topological quantum computation

(Kitaev '97, FLW '00)



annihilate pairs?

braid

braid

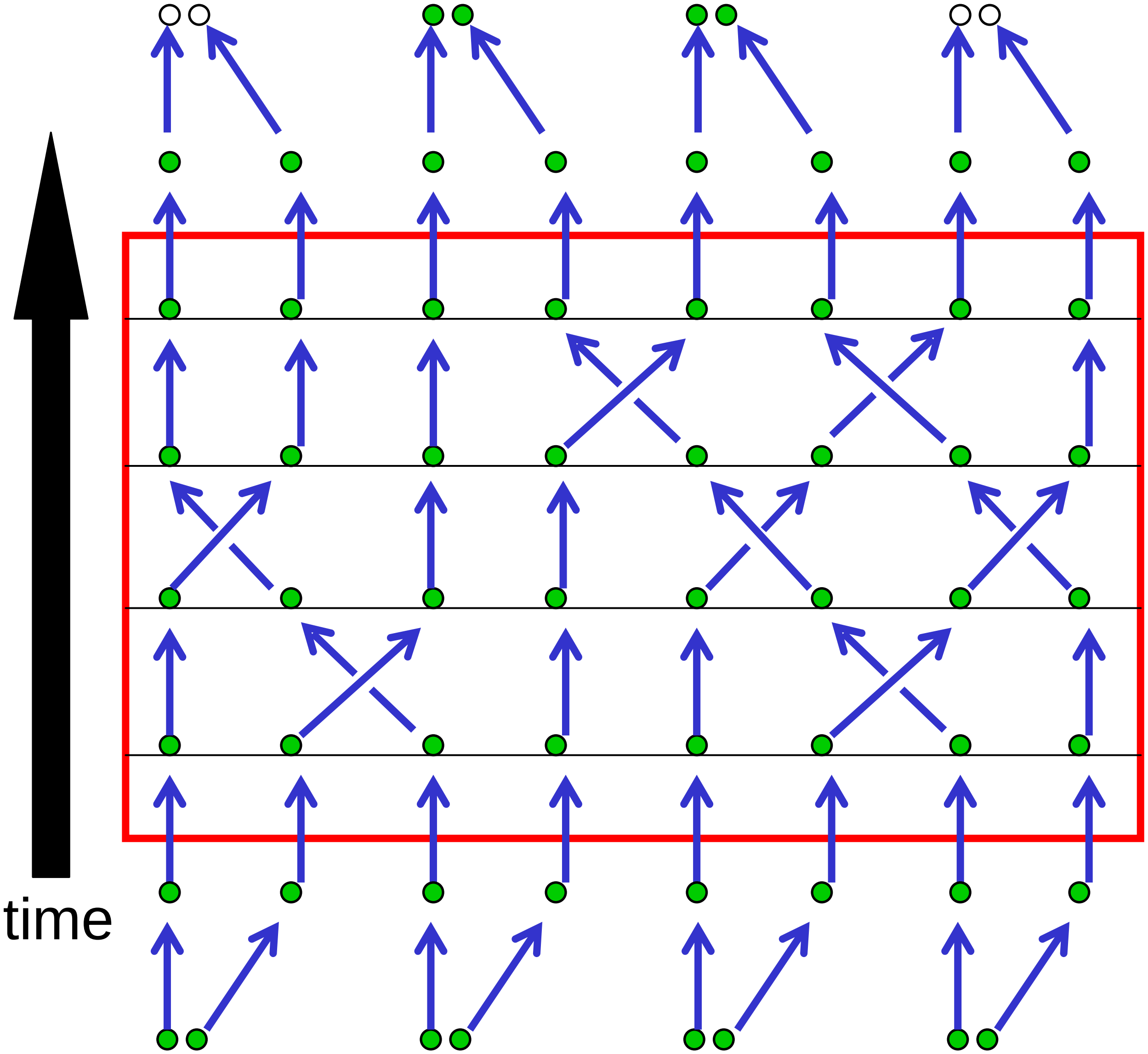
braid

create pairs

Kitaev

Freedman

Topological quantum computation (Kitaev ’97, FLW ‘00)



Physical fault tolerance with nonabelian anyons:

uncontrolled exchange of quantum numbers will be rare if particles are widely separated, and thermal anyons are suppressed...

Topological quantum computer:

The Dream

TO BEAT BACTERIA, STOP MUTATIONS • GLOBALIZATION AND POVERTY

SCIENTIFIC AMERICAN

How to Save Millions of Children from Rotavirus

APRIL 2006
WWW.SCIAM.COM

BIZARRE PARTICLES AND SPACETIME BRAIDS SOLVE IMPOSSIBLE PROBLEMS

COMPUTING WITH QUANTUM KNOTS

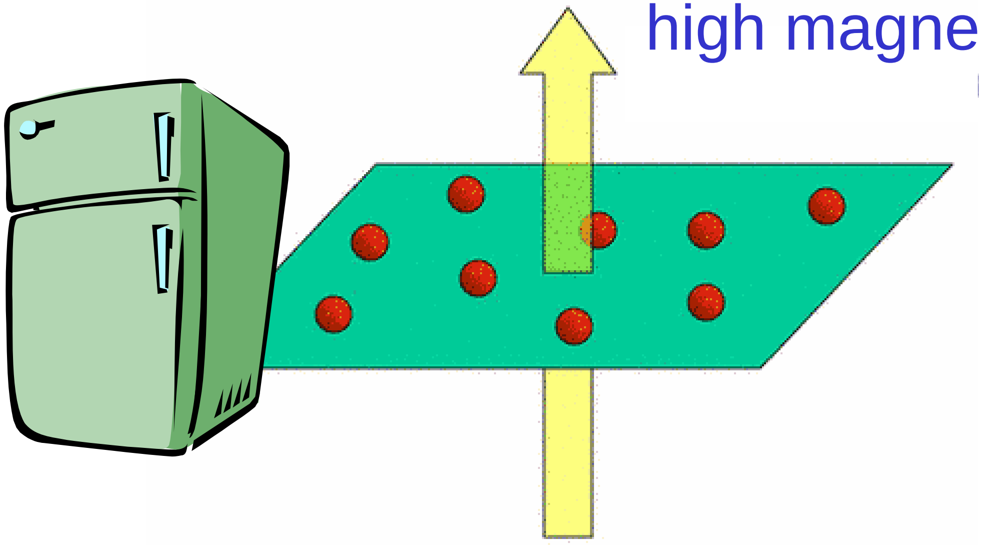
Cultured Apes and Evolving Intelligence

Magnetic Triggers of Solar Flares

Plugged-In Hybrid Cars

COPYRIGHT 2006 SCIENTIFIC AMERICAN, INC.

Anyons: the fractional quantum Hall effect

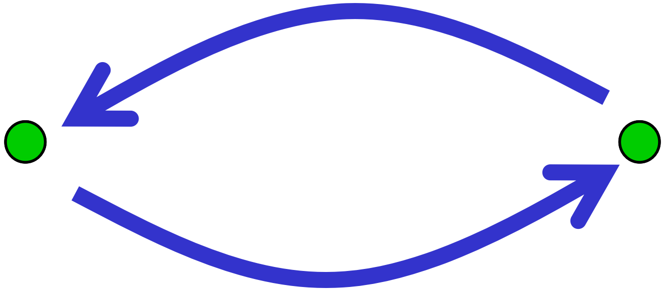


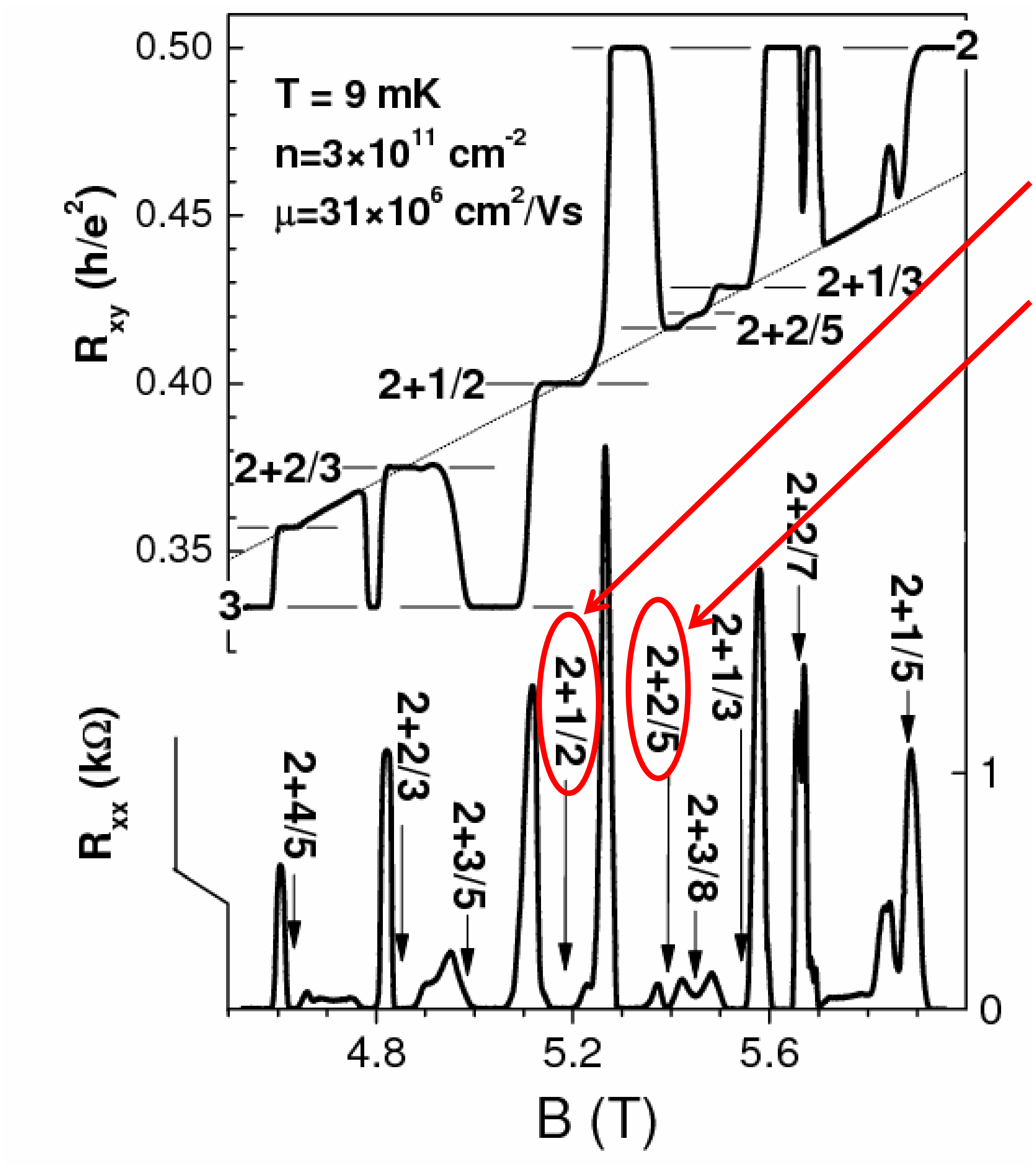
high magnetic field

electrons moving freely on a “table,” at very low temperature

An exotic new phase of matter, with particle excitations that are profoundly different than electrons.

These particles are *anyons*: they have topological interactions.





Pfaffian?

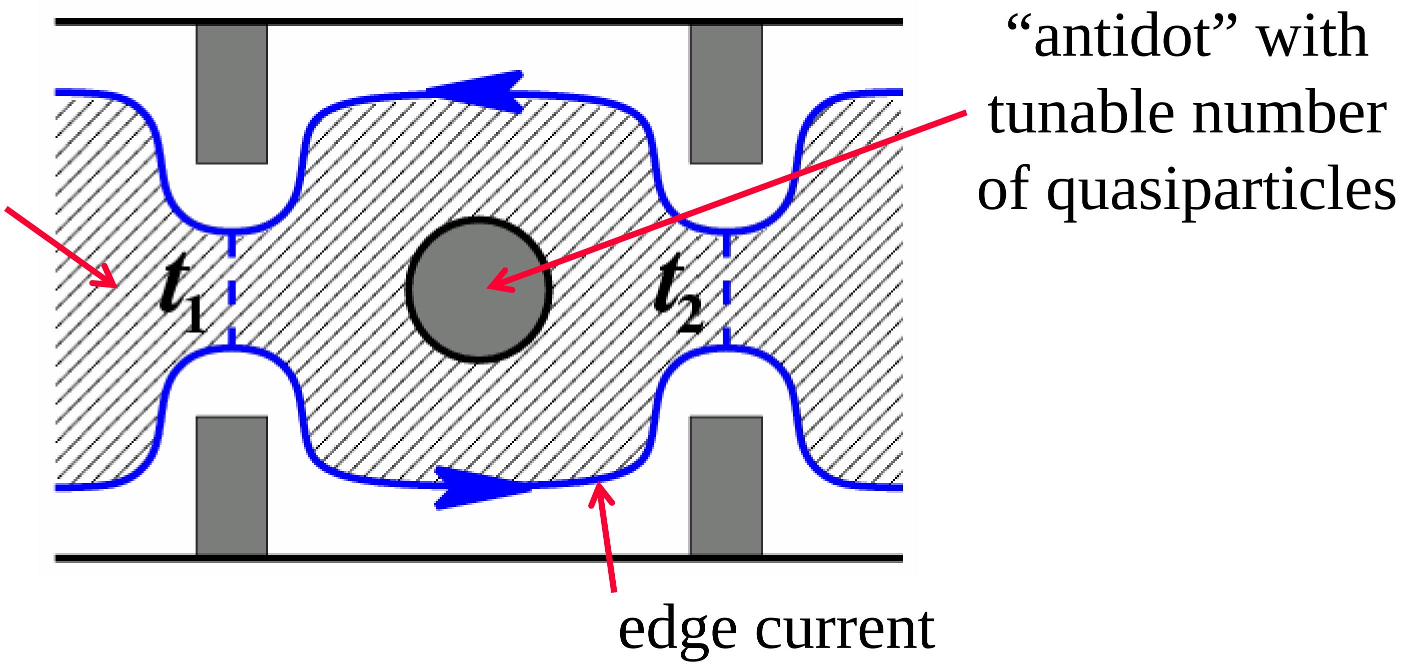
Read-Rezayi?

Topological quantum computer:

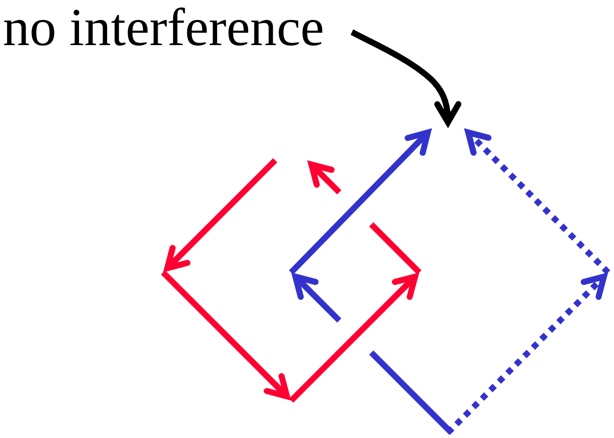
The Reality

J. S. Xia et al. (2004)

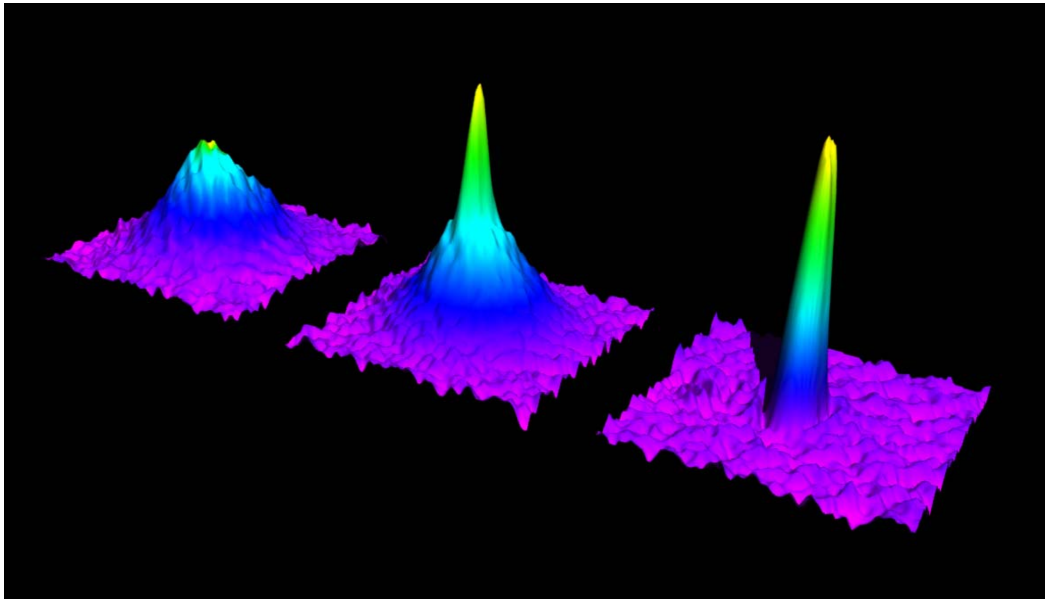
Nonabelian anyons in the laboratory



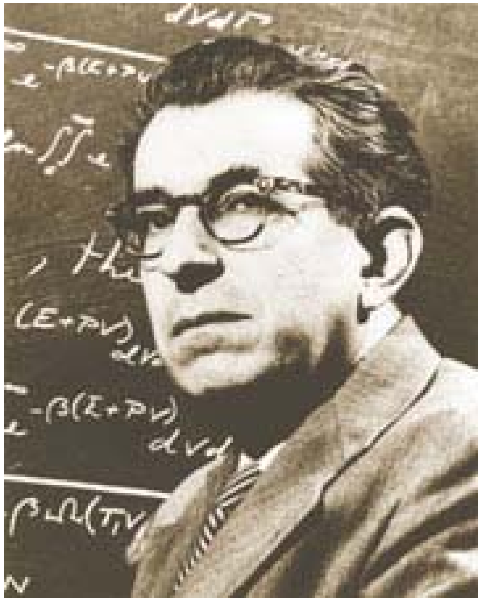
The two tunneling paths can interfere. When the number of quasiparticles on the antidot is even, there are Aharonov-Bohm oscillations in the (transverse and longitudinal) conductivity as the magnetic field varies. But if the the number of quasiparticles is odd, there is no interference and hence no oscillations. (Bonderson-Kitaev-Shtengel cond-mat/0508616, Halperin-Stern cond-mat/0508447.)



Atomic Physics Meets CMP

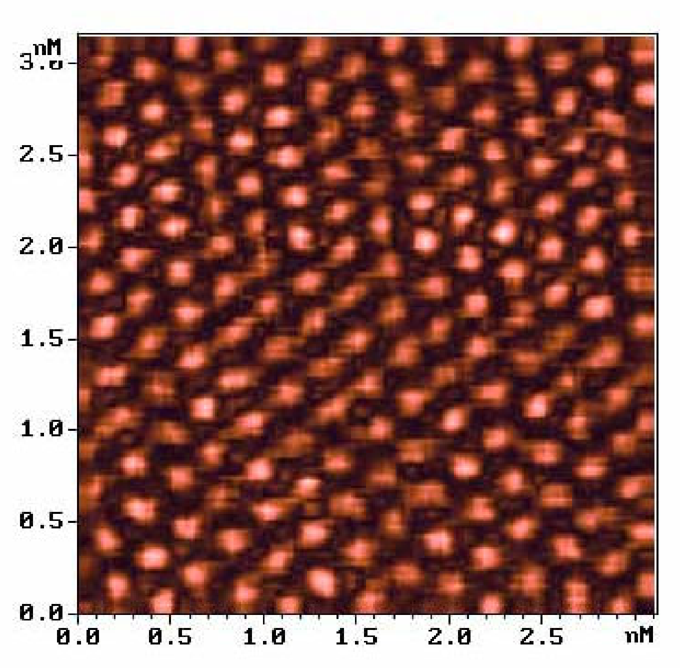


Bose-Einstein condensation in dilute gas (1995)

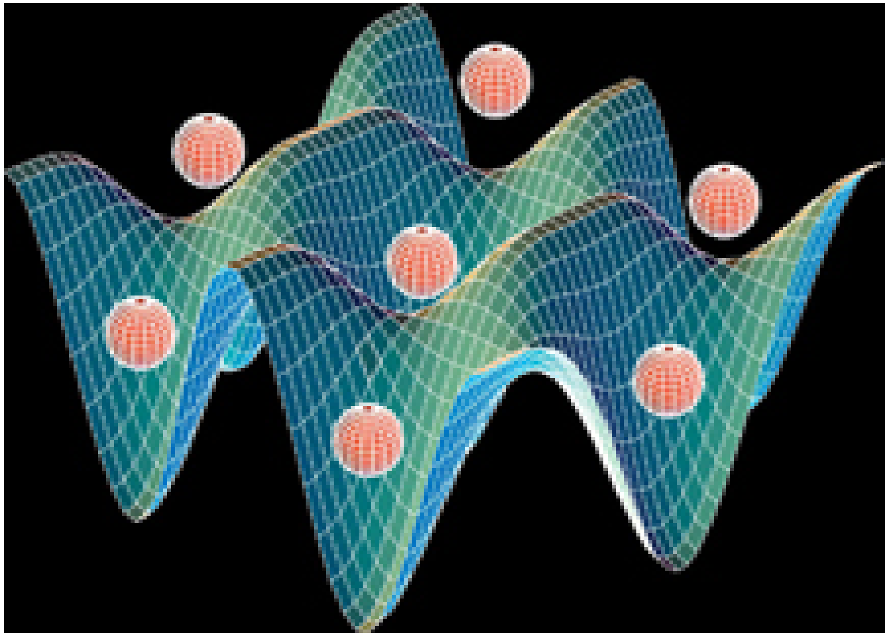


Fritz London and BEC in superfluid liquid ^{4}He (1938)

Quantum simulators:
Condensed matter meets atomic physics



atomic lattice (graphite):
Angstrom scale



optical lattice filled with cold
rubidium atoms: micron scale

The atomic physicists have developed remarkable tools for cooling and controlling atoms. Exploiting these tools, we can study (and discover) quantum many-particle phenomena that up until now have been experimentally inaccessible.

Simulation of a quantum phase transition: a tunable and nearly perfect (optical) lattice!

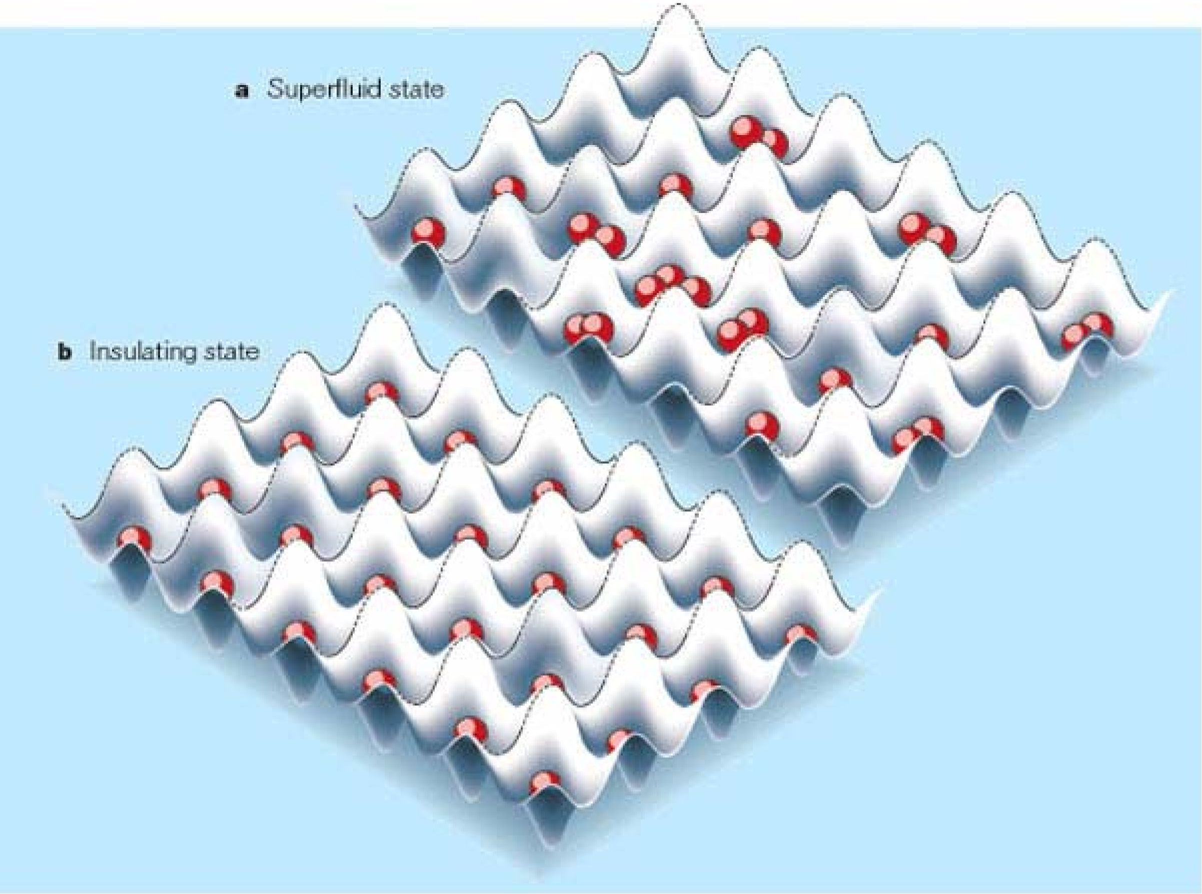


Figure 1 A quantum phase transition in an ultracold gas. By using a web of laser beams to create an energy landscape of mountains and valleys (an optical lattice), Greiner *et al.*[1] can reversibly switch a gas of rubidium atoms from a superfluid to an insulating phase. **a,** At a temperature of 10 nanokelvin or less the rubidium atoms share the same quantum state and are in a superfluid phase, in which they can move freely between valleys. **b,** By increasing the intensity of the laser beams in the optical lattice, the researchers force the gas into an insulating phase, in which each atom is trapped in an individual valley. Such control is vital to most proposals for building a quantum computer.

Jaksch

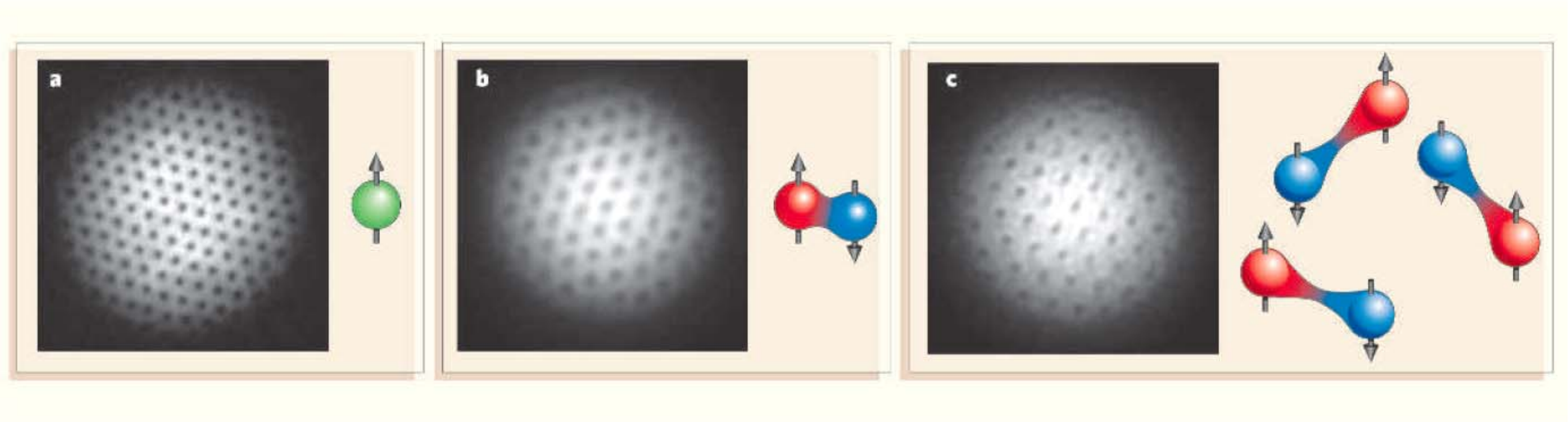
Bloch

M. Greiner, O. Mandel, T. Esslinger, T. W. Hänsch, and I. Bloch, "Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms," *Nature* 415, 39-44 (2002).

Quantized vortices in fermion pair condensates

W. Ketterle, et al. (2005)

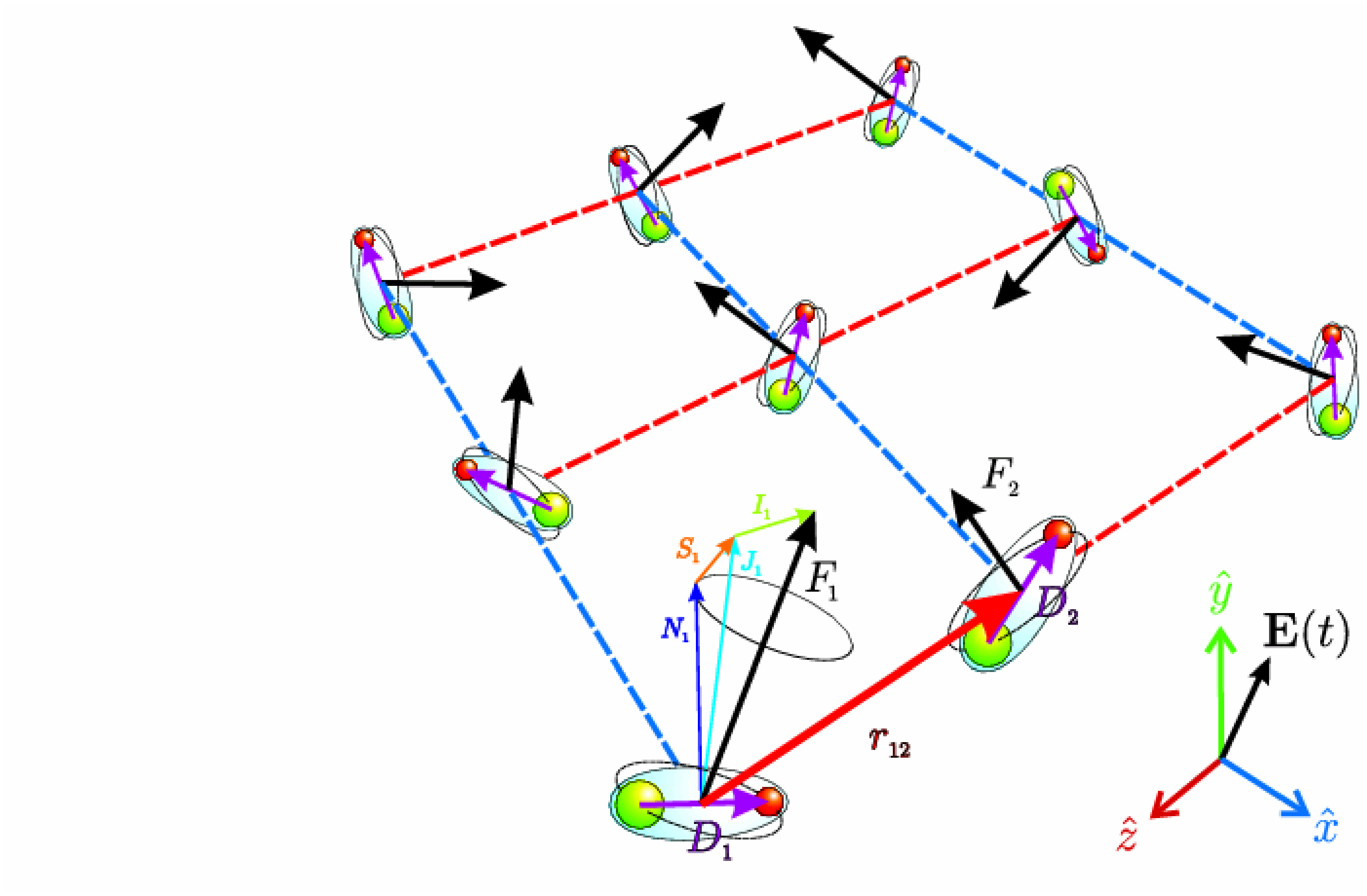
Superfluidity persists through the crossover from a molecular condensate of tightly bound pairs of fermionic lithium atoms (BEC) to a condensate of loosely bound Cooper pairs (BCS) analogous to a superconducting state of a system of electrons.



Because a superfluid flows without resistance, a rotating superfluid organizes into vortices, each carrying a tiny fraction of the angular momentum, and because the vortices repel one another, they crystalize into a regular lattice. The strength of the interactions between lithium atoms can be modulated by varying a magnetic field, so that the crossover from (b) to (c) can be studied experimentally.

Many-body physics with polar molecules

Brennan,
Micheli,
& Zoller
(2006)



Polar molecules, trapped in an optical lattice, have dipole moments, which provide a useful handle for manipulating the interactions among the molecules and realizing exotic quantum many-body states.

Condensed matter and quantum information – looking ahead

- Quantum information science did not exist 30 years ago. There will be many more surprises in the next 30 years.

- Condensed matter physics, atomic-molecular-optical physics, and quantum information science will continue to converge and advance synergistically.

- Computationally inspired methods for describing and analyzing quantum many-body systems will deepen our understanding of exotic quantum phases of matter.

- Unexpected emergent phenomena will be discovered using the experimental tools of ultracold atomic physics, guided by insights into quantum entanglement and quantum circuits.

- Exotic quantum states simulated using (analog) quantum computers will lead to the synthesis of new materials with important applications.