

Quantum Computing

Researchers are optimistic, but a practical device is years away.

SINCE QUANTUM ALGORITHMS and architectures will ultimately need hardware on which to run, we've explored how the principal experimental efforts are striving to produce it. Even 15 years ago, a quantum computer was generally viewed by computer scientists and physicists alike as an intriguing but probably unattainable theoretical curiosity. But interest exploded in 1994 after Peter Shor, then at Bell Laboratories (now at MIT), published his famous quantum factoring algorithm capable of undermining widely used cryptosystems that relied on the difficulty of factoring large numbers. Today, several thousand physics, computer science, and engineering researchers in more than 100 groups in universities, institutes, and companies around the world are exploring the frontiers of quantum information, encompassing quantum computing, as well as recently commercialized quantum cryptography and quantum teleportation communication techniques. Accelerating progress on virtually all fronts in this worldwide research community is yielding confidence that a practical quantum computer is indeed achievable.

Quantum computing's potential has always been tantalizing: Exponentially scalable computing power that could solve problems beyond the capabilities of conventional computers. The key is exploiting the superposition of quantum-entangled information units, or qubits. But the research challenges are daunting: How to create and reliably compute with the qubits, which require the seemingly mutually exclusive conditions of exquisite classical control while being isolated from any external influences that could destroy the entanglement.

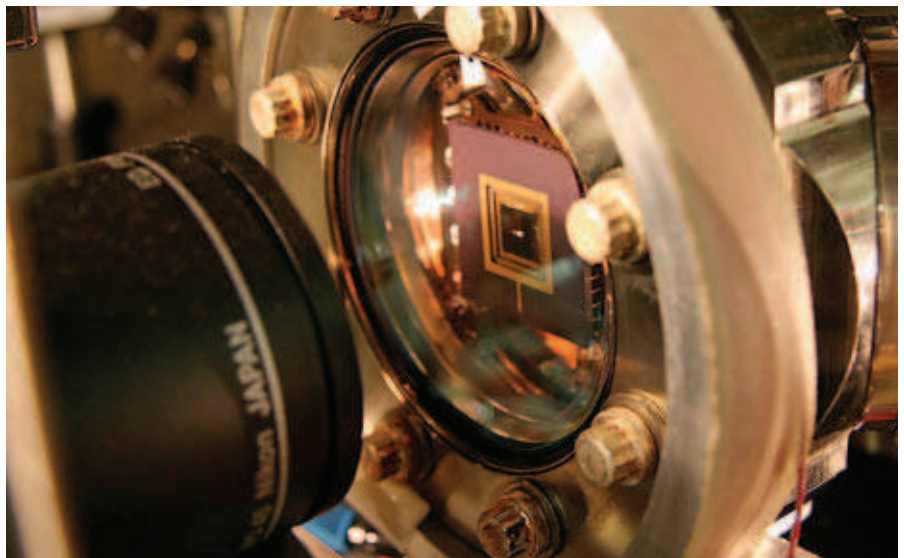
The computing power of a quantum computer grows exponentially with the number of qubits it uses. Dozens to hundreds of qubits will be needed for a

quantum computer to solve interesting problems using quantum algorithms (along with appropriate quantum error-correction techniques needed to be sure the answer is correct). The qubits must also be connected by quantum communication channels into logic gates that can be manipulated to implement the algorithms.

However, merely having and connecting qubits is not sufficient for a quantum computer. They must remain entangled long enough to complete the number of gate operations required by

ing. Typically, the qubit is a two-level motion mode for a trapped ion. The modes are modulated by laser pulses. The ion motion acts like a data bus, and gates are implemented by modulating neighboring ions.

"Our decoherence times can be up to 10 minutes—very long compared with other quantum computing techniques," says Dave Wineland of the National Institute of Standards and Technology, Boulder, CO. "But our gates are rather slow, about five microseconds for our two-qubit gates." Since



Miniature ion trap manufactured by Sandia National Laboratories.

the algorithm and mandatory error correction. Faster gate operation, higher fidelity (percentage of gate operations completed correctly), and greater error-correcting efficiency can speed the calculation or reduce the number of qubits needed to solve the problem.

More than a dozen different ways of creating qubits—each with its own strengths and challenges—have been developed to date. The following is a rundown of the leading candidates:

Ion traps use electrical and/or magnetic fields and laser-cooling to create a "pseudo-molecule" quantum register with micron-scale inter-ion spac-

ing a 100-to-200-digit number would require a million operations, even error-free implementation would take far longer than the qubit could be maintained. Researchers, led by Rainer Blatt of the Institut für Experimentalphysik Universität Innsbruck in Austria, recently set the record for qubit fidelity: 99.3%.

Integrating CMOS chips with ion traps is a recent innovation that permits quantum communication but uses classical control and measurement. One design created at Lucent by Richard Slusher (now at the Georgia Tech Quantum Institute) and Jungsang Kim

(now at Duke) is an ion-trap analogue to the electron-based charge-coupled device chips used in digital cameras. “This design gives addressability to an enormous number of ions,” says MIT’s Isaac Chuang.

Quantum dots are a popular solid-state host for qubits. Lieven Vandersypen’s research group in Delft, The Netherlands, reported last November that it had used an alternating electrical field to control single electrons contained in gallium arsenide quantum dots. Electrical control is more selective than the previously used magnetic fields. Their fidelity of flipping a single-electron spin (a simple gate) is a little lower than the 73% attained with magnetic-field control but is expected to increase as they gain experience. Future research will venture into no-spin hosts, such as silicon and carbon (carbon-12, nanotubes, graphene), that are expected to have much longer decoherence times.

Linear optic qubits are created by simultaneously producing forward and backward photons and encoding their logical states into vertical and horizontal polarizations. This approach has the advantage of long decoherence times and compatibility with fiber optics but needs higher photon-creation and -detection efficiencies. Last December, Andrew White’s group from the University of Queensland reported that it had used a linear optic circuit involving four qubits to find the prime factors of 15 (5 and 3) thus demonstrating that system’s ability to perform the core processes required for implementing Shor’s algorithm.

In April, Prem Kumar of Northwestern University announced a quantum gate created within an optical fiber. A few years ago, Kumar showed that photons can remain entangled within a fiber for a distance of 100 kilometers. The recent result will be useful in creating quantum repeaters for a distributed quantum information network.

Superconducting qubits can be made in three types: charge, flux, and phase. Each uses excitation states of Josephson junctions: two superconductor pieces separated by an insulator thin enough for Cooper pairs of electrons to tunnel across. This approach is scalable, since superconductivity enables fast control and readout and large,

More than a dozen different ways of creating qubits have been developed to date.

controllable couplings between widely separated qubits. However, it also requires extremely low temperatures—milliKelvins—and tends to have short decoherence times (to date only a few microseconds). John Martinis’s group at the University of California, Santa Barbara, recently measured single-qubit fidelity of 98% in a phase-qubit system. And Robert Schoelkopf’s group at Yale developed a “transmon” qubit 300 microns long and very stable against noise.

Hybrid approaches combine the best features of their parents. Chuang’s research group is integrating ion traps into superconducting qubits. “Ion traps are very hard to connect to anything,” Chuang says. “It would be really nice to have an ion trap with wires coming in and out.” Vandersypen says that as ion traps get smaller they might eventually look similar to quantum dots.


D-Wave Systems, a venture-backed company based in Vancouver, BC, made news twice last year when it announced the operation of a 16-qubit (in February) and 28-qubit (in November) “adiabatic” quantum computer. However, many scientists are skeptical of both the claims and their importance. The adiabatic method, which is a quantum version of simulated annealing, involves slowly evolving a system toward the solution. Skeptics say this approach will prove to be neither fault-tolerant nor scalable. Although the company revealed scant scientific detail about its approach, its president and CEO, Geordie Rose, says it has no proof yet of entanglement—the hallmark of quantum computation.

Diamond-based systems are an intriguing recent entrant. The qubit is the spin state of a nitrogen impurity adjacent to a vacancy in the carbon crystal.

Stemming from Tom Kennedy’s 2003 research at the Naval Research Laboratory, “nitrogen-vacancy color centers” have two compelling advantages: their spin state can be both initialized and read out optically at room temperature and weak spin-orbit coupling in diamond makes this qubit well-decoupled from its environment. Several groups have jumped in to study this system, and its decoherence time has increased from about 50 microseconds to nearly a millisecond.

Challenges include devising ways to control individual qubits and couple them together. But David Awschalom of the University of California, Santa Barbara, is optimistic. “If you had told me,” he says, “a few years ago that you were going to try to control a single electron at gigahertz frequencies in a solid-state material at room temperature, I’d have said, ‘Good luck!’ Now we’re doing just that.”

This system is also useful as an accessible test bed for studying spin interaction in solid-state materials that may contribute to the success of other systems and quantum physics knowledge in general. Awschalom’s group recently watched quantum information from a single “nitrogen-vacancy center” spin disappear into the “bath” of spins associated with the much more common nitrogen impurities not associated with vacancies...then reappear. “In quantum physics, this is a big deal,” Awschalom says. “It’s an age-old problem. There have been 1,000 theory papers on this, but no experiments.”

The recent across-the-board progress, however, has stimulated optimism in the eventual success and impact of quantum computing inconceivable 15 years ago. For example, IBM Research’s David DiVincenzo, who proved in 1995 that quantum algorithms could be executed using only two-qubit operations and later devised seven widely accepted criteria for a practical quantum computer, says, “I’m confident that the quantum computer will eventually change the world and will deeply influence how information processing will be done in the future.” 

Michael Ross writes about science and technology from San Jose, CA.

Mark Oskin, University of Washington, Seattle, contributed to this article.