A Quantum Leap for Computers?

Once the stuff of dreams, computers that could harness "quantum parallelism" to speed up certain computations by many orders of magnitude are edging toward reality

Computer scientists pride themselves on their logic—after all, logic gates are their stock in trade. But lately some of them have been looking a bit like Alice down the rabbit hole: wide-eyed at the paradoxes that prevail in an entirely new realm of computing. The new world they've disappeared into is the realm of the tiny—individual atoms and quanta of light.

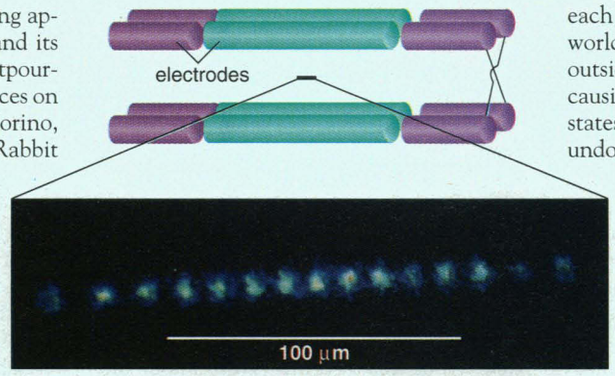
In that strange world, quantum mechanics reigns, and the same rules that let a particle be in many places at once allow it to perform many computational tasks simultaneously. "It's almost like magic," says Dan Simon of Microsoft Corp. in Redmond, Washington, one of the researchers whose work has shown that "quantum parallelism" can be exploited to perform in a few seconds certain calculations that would take billions of years on the most powerful classical computers.

Over the past few months, a growing appreciation of this paradoxical world and its accompanying magic has led to an outpouring of articles, proposals, and conferences on the topic—including a workshop in Torino, Italy, last week. Appropriately for a Rabbit Hole world, "things are out of control," jokes Massachusetts Institute of Technology researcher Seth Lloyd. And the whirlwind could get wilder with the news that at least rudimentary quantum computers (QCs) can actually be built.

In one of three papers on QCs in the 15 May *Physical Review Letters* (*PRL*), Ignacio Cirac of the University of Castilla-La Mancha in Spain and Peter Zoller of the University of Innsbruck in Austria show that, in theory, ions trapped in an electric field and cooled to fractions of a degree above absolute zero could be coupled to produce a quantum logic gate—the working heart of a computer. And researchers at the National Institute of Standards and Technology (NIST) in Boulder have already built and tested a simplified version of their suggestion.

Before the Cirac-Zoller paper, says Richard Hughes of Los Alamos National Laboratory, most theorists' suggestions for building QCs "seemed like they required 'unobtainium'—a material that didn't exist." Now, he says, the idea "isn't so crazy." Still, like Alice, these researchers are finding that the Rabbit Hole has its drawbacks. Among them are sharp limits on the sorts of computations a QC could perform and the exquisite sensitivity of quantum systems to slight errors. Such errors—which can stem from unwanted interactions with the "normal" world outside the system—could make the concept unworkable, some researchers say.

Much of the strangeness that dominates the world of QCs can be traced to the superposition principle, which holds that a quantum-mechanical system—say, an atom with several possible energy states or spin directions—can exist simultaneously in all of them until the states are actually measured. While a classical data bit, represented by voltages in a semiconductor, can carry only one value—a binary 0 or 1—an atom can carry both values at once, with 0 corresponding to its ground state, say, and 1 to its excited state. Likewise, two quantum bits, or "qubits," can simultaneously hold all combinations of their values—(0,0), (1,0), (0,1), and (1,1)—and a collection of n qubits can hold 2^n sets of values at a time.



SOURCE: DAVID WINELAND *ET AL.*

Quantum connection. These mercury ions, held in an electromagnetic trap, can act as quantum bits, storing superpositions of states. The atoms' collective motion can link the bits to one another to create a logic gate, the heart of a quantum computer.

Bursts of light, say, can flip the bits in various ways, independently changing each part of a superposition to a different value, and interactions among these bits can in principle create logic gates that let calculations proceed down many paths at once. When the calculation is finished, information about it can be extracted—measured—again using light pulses.

Looked at in this way, QCs "are in a sense just reinterpretations of spectroscopy," says David DiVincenzo of IBM's Thomas J. Watson Research Center in Yorktown Heights, New York. In nuclear magnetic resonance spectroscopy, for example, radio frequency pulses flip atomic spins. The operation is generally exploited to probe the atoms' chemical environment, but it also amounts to a logical NOT operation on a qubit, says DiVincenzo—an operation that changes a bit's value from 0 to 1 or vice versa.

What's more, instead of flipping the qubits completely, certain pulses can "tip" them into the superpositions of 0s and 1s that take advantage of quantum parallelism. But the qubits, like the bits in a conventional computer, still need to be coupled to create the logic gates of a computer, in which the state (or states, in this case) of one bit affects the state of another.

And there quantum mechanics throws up a big stumbling block. To form a logic gate, the qubits have to "interact strongly with each other and weakly with the outside world," says Rolf Landauer, also at IBM. Any outside interactions act as a "measurement," causing superposed quantum mechanical states to "collapse" into a single state and undoing the advantage of a QC. And coupling qubits without measuring them "is a tall order," says Landauer.

Making qubits count

Last year, however, Peter Shor of AT&T Bell Laboratories in Murray Hill, New Jersey, came up with just the incentive physicists needed to fill that order. Building on work by Microsoft's Simon, Shor found a quantum algorithm for quickly factoring numbers so huge that they might take the age of the universe to factor on classical machines. Quantum logic, says Shor, makes it possible to sort through a space of solutions that grows exponentially with the size of the number to be factored.

"Before Shor's algorithm, there was no concrete evidence that you could do something interesting with a quantum computer that you couldn't do with a classical computer," says Simon. The result could shake up the science of cryptography, in which the latest schemes are based on the difficulty of factoring large numbers (see box). And it concentrated the minds of researchers looking for ways to wire qubits together into a complete logic gate.

It was after listening to a talk on QCs by

Keeping Secrets Safe From Quantum Code-Cracking

Quantum computers, with their potential for cracking codes based on the factors of large numbers, could threaten the peace of mind of spies, diplomats, and others bent on secret communications (see main text). But quantum mechanics can also make amends, as a recent breakthrough by Richard Hughes and his colleagues at Los Alamos National Laboratory shows. At a conference held last month at the University of Rochester in New York, Hughes announced that the group had transmitted information through 14 kilometers of optical fiber by encoding it in the quantum properties of photons, where the quantum mechanical uncertainty principle shields it from observation by eavesdroppers.

Hughes's work isn't the first demonstration of quantum cryptography, as it is known. But, for the record, it's the longest, surpassing by 40% a previous effort by a team at British Telecom and the Defense Research Agency in the United Kingdom. Still more impressive, says Charles Bennett, a pioneer in quantum encryption at IBM's Thomas J. Watson Research Center in Yorktown Heights, New York, Hughes didn't send his message through a high-tech custom-built system. Instead, he sent the perishable quantum states through existing fiber "out with the chipmunks" on the grounds of Los Alamos.

Like other quantum cryptography schemes, Hughes's provides a way for people in different locations (usually dubbed Alice and Bob by cryptographers) to develop a key that either can use to decode messages sent via an unsecured public channel. The apparatus isolates individual photons, then uses a fiber-optic splitter to divide each photon's quantum-mechanical wave function—which gives the odds that the photon exists at any particular point in space—into halves. Before its 14-kilometer journey, the split wave function passes through separate short lengths of optical fiber; differences in the path lengths alter the timing of the two pulses, encoding information that "Alice" can transmit to "Bob."

Instead of using the split pulses to send a definite key—which could be intercepted—Alice and Bob create one in the course of their quantum communication. They independently choose strings of random binary numbers. Alice then sends quantum pulses to Bob in which her 0s are encoded with one particular phase shift and her 1s with another.

With a split path arrangement of his own, Bob can add a phase shift to the pulses received at his end. Knowing how Alice is encoding her 0s and 1s, he calibrates the shifts so that whenever his string calls for a 1 but Alice has sent a 0, or vice versa, the pulses will end up with a net offset of half a wavelength. In that case, the pulses will interfere destructively and Bob's detector will not see a photon. If the numbers agree, however, the pulses will be offset by a different amount and Bob will sometimes measure a photon—but only sometimes, for this is quantum mechanics. Through an unsecure channel, he lets Alice know when he measured a photon, and they build up a key consisting of the shared numbers corresponding to these photons.

Meanwhile, if an eavesdropper—Eve for short—tries to tap into the quantum channel, she will find it impossible to cover her tracks. Because of quantum mechanical uncertainty, she won't be able to reconstruct the exact sequence of pulses she intercepted. If Bob and Alice share some of their key, the jig will be up.

Playing both Alice and Bob roles, Hughes was able to transmit and receive information with an error rate of roughly 1%. Future efforts to send quantum code over even greater distances, though, may run up against the constraint that quantum signals can never be amplified without altering them. But Bennett thinks further improvements in detectors and quantum cryptography schemes might eventually allow those bent on secrecy to "just bury fibers and thumb their noses" at potential eavesdroppers.

–J.G.

Artur Ekert of Oxford University—a co-author, along with David Deutsch and Adriano Barenco of Oxford, of one of the recent *PRL* papers—that Cirac and Zoller realized that a line of ions chilled to fractions of a kelvin in an electrostatic trap could serve as a "quantum wire" for passing information without measuring it. The key, they realized, is the ions' shared motion; coupled by their electric charges, they can rock in synchrony, like a chorus line.

The rocking motion is itself quantized into ground and excited states that can encode qubit information. The challenge, Cirac and Zoller realized, was getting information from one qubit onto this wire, then moving it along the wire to another qubit. They took advantage of the fact that the internal energy states of the ions, just like the rocking motion of the whole line, can be regarded as quantum-mechanical pendulums that have known oscillation frequencies.

Cirac and Zoller hypothesized that, if a small laser beam were focused on an individual ion and tuned to a frequency equaling the difference between the ion's internal frequencies and those of the rocking motion, it would set up a resonance between ion and wire—in effect, opening up a connection. The ion's qubit information could be imprinted on the wire's motional states, without any need for a measurement to determine what that information is. Irradiating a second ion with the proper frequencies could transfer quantum information from the wire to the ion; the procedure could also make the ion's bit flip or not flip depending on the state of the first ion.

"They've figured out a way to have any ion interact with any other ion on the chain," says Tycho Sleator, a physicist at New York University. "It's a beautiful piece of work." Already NIST's Chris Monroe and David Wineland have tested part of the scheme by swapping quantum information between the rocking motion and a single ion, and they have written a proposal to do factoring—of the number 15—using Shor's algorithm. The hardware requirements? "About 10 ions," says Wineland. In the final, read-out stage after the quantum calculation, a burst of laser light would cause the ions holding 1s to glow and leave those holding 0s dark, like the display of a 1950s-vintage digital computer.

This isn't the only effort to make the Wonderland machine come true. Other experimentalists, such as Jeff Kimble at Caltech, are pursuing entirely different schemes, attempting to couple atoms to photons, which would act as the "wires." But amid all these advances, skeptics continue to raise serious questions about the ultimate feasibility of QCs. Calculations show, for instance, that small errors in a QC can accumulate exponentially during its operation, and no one has yet figured out a satisfactory way of reaching into the quantum world to correct them. The problem is "pretty severe at first glance," says William Unruh of the University of British Columbia in Vancouver.

And there may be limited incentive to solve it, because so far, Shor's factoring algorithm remains the only scheme for putting quantum wonders to work on a practical challenge. "There's no question that Shor's procedure works," says IBM's DiVincenzo. But, he asks, "is it just some accident"—not a technique that will be generally applicable to other problems? For now, though, QC researchers are finding too many delights in the Wonderland realm to want to go home.

–James Glanz