wants users to speak up if they see anything fishy.

Another challenge for both the specialized and general-purpose search engines is the "hidden Web"—databases that search engines do not index, either because their content has a short shelf life (such as daily weather reports) or because they are available to subscribers only. The publishers of *Science*, *Nature*, and other journals charge fees for online access to the full text of research papers. Although abstracts may be available, and the citations can readily be discovered by search engines such as Google, the data and full text may never be seen by search engines. This is partly why Elsevier cranked up the Scirus Project. "Because of our firewalls and subscriptions, engines like Google cannot get in and index us," says Markus.


**Unbiased?** Publishers who run search engines say they are resisting the temptation to push their own products.

These barriers pose a dilemma for researchers who want the stamp of peer-review approval and publication in a high-profile journal but who also want the world to know about their work. It has also led to a continuing debate about whether scientific research publications should be free and available without restriction on the Web (*Science*, 14 July 2000, p. 223). At the moment, *Science* and *Nature* both allow authors to post copies of papers on their Web pages after a period of time. By then, however, it may no longer be the breaking news that researchers are looking for.

Other researchers believe that the highest quality search tools will come not from rejiggering the search engines but from a whole new way of creating Web content. One initiative, called the "semantic Web," is being promoted by a team that includes Tim Berners-Lee, the father of the World Wide Web, who is now at the Massachusetts Institute of Technology. The goal is to incorporate "metadata"—a description of what a document is about—into every Web page, in a form that computers can easily digest and understand. To scientists wrestling with information overload, that might mark the first big step toward paradise regained.

–DAVID VOSS

NEWS

# The Quandary of Quantum Information

**Scientists are excited by the potential of quantum computing but increasingly confused about how it works**

If even the newest, speediest personal computers don't thrill you, consider what's in store if quantum computing lives up to its promise. By using the strange properties of quantum objects to store and manipulate information, quantum computers, if they can ever be built, would crack the codes that safeguard the Internet, search databases with incredible speed, and breeze through hosts of other tasks beyond the ken of ordinary computing.

Useful quantum computers are still at least years away; right now, the most advanced working model can barely factor the number 15. Nonetheless, the past few years have seen a flurry of advances, as physicists figure out how to use quantum information to perform feats that are impossible in the classical world. Yet even as theorists crank out quantum software, they have been astonished to discover that a phenomenon long considered essential for quantum computing appears to be dispensable after all. That leaves them wondering just which exotic properties of the quantum realm combine to give quantum computers their incredible potential. "People are looking for where the power of quantum computing is coming from," says Raymond Laflamme, a physicist at the University of Waterloo in Ontario. And the deeper they peer beneath the surface, the more paradoxes they discover.

At first glance, a quantum computer shouldn't be more inscrutable than the computer on your desktop; both are essentially machines that process information. In 1948, Bell Labs scientist Claude Shannon laid the groundwork for modern computing by founding information theory, a new discipline that did for information what the laws of thermodynamics did for heat. A PC, true to Shannon's vision, processes information by manipulating "bits," binary digits that can have a value of either 0 or 1. A 1 can be a high voltage, a closed switch, or a bright light, whereas a 0 can be a low voltage, an open switch, or a dim light: The medium is certainly not the message. But however the bits are represented, the computer uses an algorithm to make those ons and offs dance a jig, and out pops the desired answer.

What makes quantum information much more intricate than classical Shannon information is that quantum computers, unlike their classical counterparts, can exploit the laws of the subatomic realm. Instead of manipulating bits, quantum computers store information on quantum-mechanical objects such as atomic nuclei, photons, or superconductors. A "qubit" might be a 1, for instance, if a photon is polarized vertically rather than diagonally, if an atom's spin is pointing up rather than down, or if current in a loop of superconductor is moving clockwise rather than counterclockwise.

But the laws of quantum mechanics make qubits quite different from bits. Instead of having to choose between being a 0 or a 1, a qubit can be both at once—an idea that physicist Erwin Schrödinger mocked with his famous half-alive, half-dead cat. But this "superposition" of different quantum states is quite real; for instance, last year, teams from Delft, in the Netherlands, and New York state, showed that superconducting loops can carry currents that run both clockwise and counterclockwise at the same time (*Science*, 31 March 2000, p. 2395). Under the right circumstances, manipulating a single qubit in superposition is equivalent to running a classical computer twice—once with the bit set to 0 and another time with the bit set to 1, potentially giving a quantum computer a speedup over a classical one.

A second quirk of qubits that makes the quantum computer incredibly powerful is entanglement. When two quantum objects are entangled, their fates are linked. The most famous incarnation of entanglement is Einstein's "spooky action at a distance," in which, if one entangled atom is poked, its entangled twin feels the prod, even if it's halfway across the universe. In theory, any number of particles can be entangled. Mathematically, such clusters are yoked together to form, in effect, a single object—you can't manipulate one member without considering the effect on the others. In principle, this more-than-the-sum-of-their-parts effect allows qubits to be linked into larger and larger quantum systems capable of storing staggering amounts of information. Two entangled qubits can be equivalent to four sets of two bits—(0, 0), (0, 1), (1, 0),

and (1, 1)—all at once. Three entangled qubits are equivalent to the eight different combinations of three bits all at once, and so on and so on exponentially.

When quantum computing began to blossom in the early 1990s, most experts thought this exponential effect would form the heart of a quantum computer. "It was fairly well accepted in the community that you need entanglement to do the power of quantum computation," says John Smolin, a physicist at IBM's Thomas J. Watson Research Center in Yorktown Heights, New York. "Without entanglement, you lose the ability to get exponential compression in quantum representation." Where a 10-bit classical computer might take 1024 separate calculations to perform a task, a quantum computer could do the same task by means of a single calculation with 10 entangled qubits instead.

Such exponential compression has some drastic consequences. In the mid-1990s, mathematician Peter Shor of Lucent Technologies' Bell Labs in Murray Hill, New Jersey, proved that a quantum computer would be able to factor large numbers much more quickly than an ordinary computer can. Because public-key cryptography—the technique that protects transactions on the Internet—relies upon the difficulty of factoring large numbers, a quantum computer would crack the Internet's encryption schemes.

A quantum computer could do many other things that classical computers can't. For example, it could query a database in a way that no classical computer could ever do. In essence, tracking down an element in a database is equivalent to picking a combination lock. Imagine a lock with 25 possible combinations. An ordinary computer would try each combination, one by one, until it found the correct one that opened the lock. On average, it would take 12 or 13 attempts to find the correct combination; in the worst case, it can take 25. In 1997, Bell Labs computer scientist Lov Grover showed that a quantum computer could solve that same database problem in no more than five tries. That is, instead of requiring about $N/2$ tries to try $N$ combinations, it takes the square root of $N$—a significant speedup that would be impossible in the world of classical computing. But quantum computers aren't merely more efficient than ordinary ones. This year, Nicolas Gisin of the University of Geneva and his colleagues at the Swiss Federal Institute of Technology found a quantum-mechanical procedure for solving an information-theory conundrum (colorfully known as the Byzantine generals problem) that classical algorithms cannot solve in any amount of time.

For years, scientists assumed that such spectacular results showed the power of entangled particles. Recently, though, they have been shocked to discover that the limits of classical computing can be exceeded without even using entanglement. In fact, some experimenters have been doing it all along.

The most sophisticated quantum computers to date, developed by physicists such as Neil Gershenfeld of the Massachusetts Institute of Technology (MIT) and Isaac Chuang of IBM's Almaden Research Center in San Jose, California, perform quantum-type computations with atomic spins as qubits. By nudging molecules such as chloroform with magnetic fields, Chuang and colleagues force the atomic spins to reverse their orientations (or dance more intricate dances) to carry out quantum logic operations. These nuclear magnetic resonance (NMR) quantum computers, which include the one that can factor the number 15, are still quite rudimentary. But by executing some basic quantum algorithms—error correction, Grover's algorithm, and others—they prove that quantum-computing theorists are on the right track.

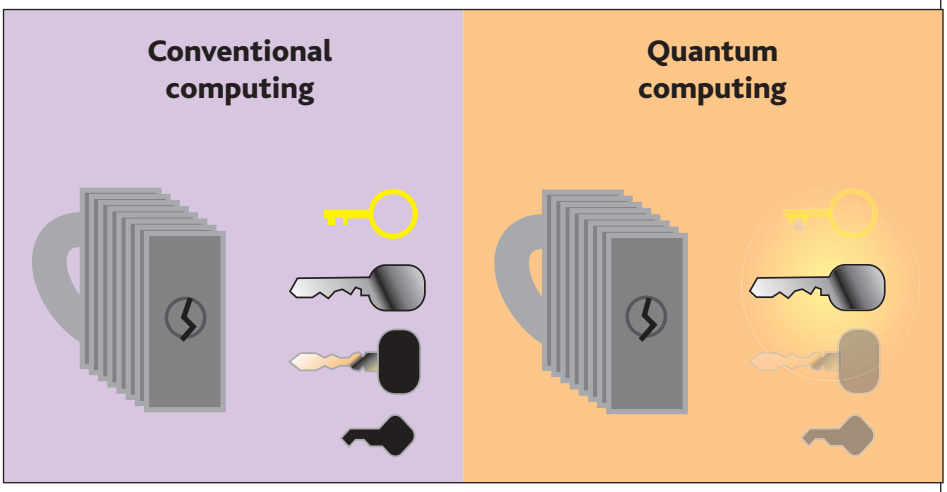
Or so it seemed. In 1999, Carlton Caves of the University of New Mexico, Albuquerque, showed that under the room-temperature conditions of the NMR experiments, large-scale entanglement of atoms is impossible. Bewilderingly, the NMR quantum computers had executed Grover's algorithm without having access to the entanglement that the algorithm required. In another unsettling twist, last year, MIT physicist Seth Lloyd showed how to mimic Grover's quantum database-searching speedup without using entanglement at all. By exploiting interference effects made possible by the wavelike nature of particles, Lloyd's algorithm also gets a square-root-of-$N$ improvement over classical computers. The penalty for jettisoning entanglement is that any quantum computer running Lloyd's algorithm would need exponentially growing resources. As the problem gets bigger and bigger, the computer requires many, many more beamsplitters, detectors, and other necessary equipment, making it impossible to solve any but the tiniest problems. So even though Lloyd's algorithm outpaces any classical computer, it is inherently limited in a way that quantum computing with entanglement is not. "There's something funny that happens," says Smolin. "[Lloyd's algorithm] really does sit in between a quantum algorithm and a classical algorithm."

Clearly, Laflamme says, "entanglement is not the whole answer to where the power of quantum computing comes from." What gives quantum computers their power, then? "What it is, we're not 100% sure," he says. "It's not something we always want to say to our sponsoring agency, but to a researcher, it's absolutely great."

Exploring the limits of unentangled quantum computing, Laflamme and colleagues at Los Alamos National Laboratory recently figured out a way to create a quantum computer by using simple lenses, mirrors, and other optics to manipulate a beam of unentangled light. "It's an idea I like: a way to manipulate quantum information in a totally unexpected way," he says. The drawback is that the computer needs a source of light that spits out a single photon at a time and a detector sensitive enough to detect that photon—equipment that is easy to sketch on paper but difficult and expensive to build.

Such theoretical insights won't hasten the day quantum computers appear in your local mall. "We understand [quantum information] more deeply," Smolin says, "but it doesn't get you any closer to quantum computers." But by puzzling through the seeming paradoxes of quantum information, theorists think that they will understand the strange realm of quantum theory in unprecedented detail. Says Laflamme: "We're just on the border of the territory, and we're just making excursions into it."

–CHARLES SEIFE




**Quantum edge.** Whereas a classical database search (left) tries to match every possible "key," Lov Grover's quantum technique saves steps by making mismatches fade into improbability.