TRN's
Making the Future report
The State of an Emerging Technology and a Look at What Lies Ahead
Report Number 10 December, 2003/January, 2004

Quantum Computing: Prospects and Pitfalls

Executive Summary

Researchers began trying to make quantum computers, which use particles like atoms, electrons and photons to compute, about 20 years ago. Quantum computing research is moving steadily forward, fueled largely by U.S. government funding, but it will be at least another two decades before quantum computers live up to their considerable potential.

The laws of physics cause things to behave differently in the realm of atoms and molecules than in the much larger world. These differences, particularly the abilities of superposition and entanglement, would allow quantum computers to check all possible answers to a problem at once, in contrast to the much slower classical computer method of checking answers one at a time.

This ability means quantum computers would be fantastically fast — many orders of magnitude faster than classical computers' ultimate potential — for certain types of very large problems, including searching large databases and factoring the large numbers whose solutions would render today's encryption useless.

Using infinitesimally small particles to compute is also very difficult, and at this stage it is difficult to be sure that all the challenges can be met.

Researchers are exploring many different methods to make quantum bits and to connect quantum bits into quantum architectures. Quantum bits, or qubits, equate to the transistors that make up today's computer chips.

The well-established qubit candidates are ion traps, semiconductor impurities, superconductor circuits, quantum dots, neutral atom optical traps, and linear optics.

Less established possibilities include molecular magnets, spectral hole burning devices, and Wigner crystals.

Nuclear magnetic resonance (NMR) qubits are well-established and useful for testing but will likely prove impractical.

The major challenges include making qubits whose states last enough to carry out computing; keeping quantum computing free from errors; connecting thousands of qubits together; controlling an array of at least several thousand qubits; and efficiently manufacturing qubits.

What to Look For

Qubits and Logic:

Encoding information in logical qubits
Creating entanglement on demand
Qubits that last for whole seconds
Reliably transferring information from atoms to photons and back

Computers:

Fault-tolerant operation of a multi-qubit computer
10-qubit computer
100-qubit computer
1,000-qubit computer
A quantum computer that outperforms classical computers

Communications:

Electric, room-temperature single-photon sources
Efficient sources of entangled photons
Efficient room-temperature photon detectors
Quantum repeaters or relays

Algorithms:

Proof of a quantum speedup for route optimization-type problems
Proof of a quantum speedup for pattern recognition problems
Proof of a quantum speedup for simulating chaos

The concept

The concept of astoundingly fast quantum computers emerged around 20 years ago. Despite the seemingly hypersonic speed of scientific and technological development, however, it will be a long time before anyone, even governments, can

unwrap a shiny new quantum computer and plug it into the wall.

Quantum computing research is moving steadily forward, however, fueled largely by U.S. government funding. Most of the challenges of building practical quantum computers are well understood, and researchers are pursuing a range of approaches, including about half a dozen that are likely to contribute significantly to the field or even end up as direct ancestors of practical technologies.

The widely divergent equipment used in the different approaches — lenses and mirrors, magnetic fields, lasers, test tubes, superconducting circuits, and silicon chips — is evidence that no one knows yet what practical quantum computers will look like. But researchers are coming to a consensus about what computers that are based on the attributes of atoms and subatomic particles will need to be able to do, what parts they will need to have and how those parts will have to work together.

This report outlines the state of quantum computing research, describes the competing technologies, and points out the next steps on the long road ahead.

Quantum weirdness

The laws of physics cause things to behave differently in the realm of atoms and molecules than in the much larger world where we have honed our instincts about how things work.

An atomic particle — unlike, say, a slice of toast — not only does the equivalent of spinning clockwise or counterclockwise, but it can also reside in any mix of both clockwise and counterclockwise, an ability known as superposition.

When quantum particles like atoms, electrons and photons are in superposition they can become entangled, meaning properties like spin can become linked, or synchronized, between a pair of particles. Entangled particles also remain linked regardless of the physical distance between them.

These abilities are counterintuitive, but well-proven by experimentation. They are also potentially very useful for computing.

Unimaginable power

Superposition allows a single string of quantum bits, or qubits, to represent many numbers at once. The two spin positions of a quantum particle can represent the 1s and 0s of computing, just as a classical computer uses the on and off positions of a transistor to represent binary numbers. Quantum spin positions are usually referred to as spin up and spin down.

A string of seven transistors and a string of seven qubits can each represent the 128 possible seven-digit binary numbers. The difference between these two types of switches is that those made from transistors can only represent one number at a time, while qubits can represent all of the possible combinations at once. The advantage becomes more marked with longer strings: 15 qubits, for instance, could represent 32,768 combinations at once.

Entanglement allows a quantum computer to do computations on all of these numbers at once. When a string of qubits are entangled with each other, a single set of logic operations affects all of the

How It Works

Quantum bits, or qubits, are the atomic equivalent of the transistors that make up today's computers. In order to carry out the logic of computing, there must be some way to represent the 1s and 0s of computer information. The many candidate qubits all have one thing in common — the ability to switch from one state to a second state. These states are used to represent binary information.

Qubits use properties of one of four types of quantum particles: photons, electrons, atoms and ions.

Photons

The electric field of unpolarized photons vibrates in a plane perpendicular to the photon's course. Polarized photons' electric fields, however, vibrate in only one of four directions within that plane: vertical, horizontal and the two diagonals. Two pairs of polarizations can represent 1 and 0 respectively.

Photons can be controlled by mirrors and polarizing filters, which block all photons but those with one particular polarization orientation.

Electrons

Electrons are oriented in one of two directions, spin up and spin down, which are akin to the two poles of a magnet. Electrons can be switched between the two states using electric, magnetic or optical fields. An electron's position within a quantum dot can also be used to represent a binary number.

Atoms and ions

Atoms and ions are more complicated objects than electrons and have several ways of representing information. Ions are atoms that contain a charge because they have an extra or missing electron.

Like electrons, atoms have a spin orientation that can be used to represent binary numbers in a qubit. The position of an atom's outer electron — at the low-energy level or at a higher-energy level — can also be used to represent 1s and 0s. Atoms that are trapped and cooled vibrate in discrete quantum steps that can also be used in a qubit. A fourth type of atomic qubit is based on hyperfine levels, or subtle variations in electron orbital levels caused by the magnetic interactions between the nucleus and electrons.

Qubits

Qubits are made up of controlled particles and the means of control — devices that trap particles and switch them from one state to another. There are four established qubit candidates: ion traps, quantum dots, semiconductor impurities, and superconducting circuits.

qubits at once. Like waves that reinforce and cancel each other, quantum logic operations cancel out wrong answers so that when qubits are examined, causing them to assume a definite state, they represent the correct answer.

Computing problems that involve looking through large numbers of possibilities for a solution — like cracking the security codes underpinning encryption and searching very large databases — could potentially be solved very quickly using quantum computers. The first quantum computer that contains at least several thousand qubits, has the potential to do lightning-fast searchers across huge databases and also obliterate security as we know it.

In short, quantum computers have the potential to be many orders of magnitude faster than today's classical computers could ever be for certain types of problems.

The challenge

The trillion dollar question, then, is can working quantum computers of at least several thousand quantum bits be made.

Ask a researcher who works in the field and you are likely to get an answer of "in around 20 years," often followed by an "if ever" qualifier.

Using particles to reliably store information and carry out computations is extremely difficult. Just for starters, particles are fantastically small: the size difference between a hydrogen atom and a ping-pong ball is about the same as the size difference between a ping-pong ball and the Earth. Particles are also easily disturbed, which causes them to lose the information they are holding. Given their size and fragility, it is a serious challenge to coordinate even a few qubits, let alone thousands or millions.

At this stage it is difficult to be sure that all of the challenges can be met.

Researchers from the University of Arkansas and Texas A&M University have calculated that the statistical nature of quantum data, the practical requirements of inputting data into systems capable of carrying out entanglement, and the difficulty of quantum error correction will require quantum computers to draw very large amounts of power, making them less efficient than classical computers for all but a few types of problems. (See "Quantum Computing Has Limits", page 67.)

Many research teams are continuing to work on quantum computers despite the difficulties. Historically, scientists have found ways around many seemingly unworkable situations. The potential payoff of fantastically fast computing makes the challenge impossible to resist. And the national security implications mean that U.S. federal funding for quantum computing research has been robust.

There are several major steps that must be reached before quantum computers can become practical:

- Making qubits whose states last long enough to carry out computing
- Keeping quantum computing free from errors
- Connecting thousands of qubits together
- Controlling arrays of at least several thousand qubits

Ion traps

Ion traps use optical and/or magnetic fields to contain individual ions. Researchers have entangled as many as four ions in a single ion trap. Ion trap technology is well-established and is likely to be able to scale up to large numbers of qubits. Because ions are charged, they are more vulnerable to environmental noise than neutral atoms.

Quantum dots

Quantum dots are bits of semiconductor material that contain one or a few electrons. Quantum dots can be reliably loaded with individual electrons, and they can be readily integrated into electronic devices. Current prototypes, however, work only at extremely low temperatures.

Semiconductor impurities

Atoms embedded in semiconductor materials are commonly found as impurities, or flaws in computer chips. It is difficult to make a pure chip — there tends to be an unwanted atom of some kind in every few billion semiconductor atoms. Semiconductor impurity qubits use electrons contained in phosphorus or other atoms intentionally introduced into semiconductor materials; the electron states can be controlled using lasers or electric fields.

Superconducting circuits

Superconducting circuits are electrical circuits made of superconducting material, which allows electrons to flow with almost no resistance at extremely low temperatures. Superconducting circuits can form qubits in several ways, including the flow of current itself, which can be made to flow in both directions at once in the quantum state of superposition.

Electrons pair up to flow through a superconductor, and billions of these pairs form a single entity that behaves as one giant subatomic particle when the superconductor contains a tiny break. When one of the circuits, dubbed Josephson junctions, is connected to a reservoir of electron pairs, the number of pairs in the reservoir can be changed by exactly one, and this change can be reliably measured.

Superconducting circuits can be made using semiconductor manufacturing techniques. The principal advantage is that they use millions or billions of electrons rather than requiring control over individual particles. The drawback is that they operate at extremely low temperatures.

Optical traps

Neutral atoms in optical traps are another candidate type of qubit. Optical traps work because light waves are strong enough at the atomic level to trap and

- Efficiently manufacturing qubits

Hardware, Software and Communications

Like classical computing, quantum computing requires hardware capable of taking in information, carrying out computations, and returning readable results; communications equipment capable of transporting information from one place to another; and software capable of characterizing complicated problems.

Researchers are working on many types of quantum hardware, from qubits to storage devices to whole computers. They are also working on various tools aimed at easing the production of quantum computing hardware.

There are also major efforts underway to find ways to send particles containing quantum information over communications lines so that quantum computers can exchange information.

And many research groups have come up with quantum software: logical rules, or algorithms, that take advantage of superposition and entanglement to solve real problems. Without working qubits, however, the software is useless.

Many potential models

The first step in constructing a quantum computer is making working qubits and connecting a few of them together. Many research papers explore ways to store binary information in particles and to connect qubits by allowing the particles to affect each other. Several research teams have demonstrated ways to make a few connected qubits.

To get this far, each of these teams has had to find ways to use particles to represent the 1s and 0s of computing. There are many candidate qubits and there are many different methods of containing and controlling particles that could lead to new types of qubits.

Quantum denominations

The three principal types of particles used in quantum computing are photons, electrons and atoms. (See How It Works, page 2.)

Photons have the distinct advantage of being resistant to noise from the environment, which means photonic qubits can be readily manipulated and even transmitted over relatively long distances. The main drawback of photonic qubits is that it is hard to make photons interact with each other; these interactions are needed to carry out quantum computing.

Electrons are a natural for qubits because they are oriented in one of two directions, spin up and spin down, because individual electrons can be confined within tiny pieces of semiconductor, and because electric circuits, magnetic fields and lasers can be used to rapidly control trapped electrons. Electrons are infinitesimal, however. It's difficult to read the states of individual electrons. And though the physics of controlling interactions between two electrons is well understood, such control is challenging to achieve.

Atoms, and their electrically charged alter egos, ions, are larger and easier to confine than electrons, and researchers have years of control particles, much like wind pushing a windmill. Atoms are less vulnerable to noise than ions, but it's harder to make atoms interact.

Who to Watch

Qubits and Logic

Michael Chapman, Georgia Institute of Technology
Atlanta, Georgia
www.physics.gatech.edu/ultracool/

Robert Clark, University of New South Wales
Sydney, Australia
http://www.phys.unsw.edu.au/STAFF/ACADEMIC/clark.html

David G. Cory, Massachusetts Institute of Technology
Cambridge, Massachusetts
mrix4.mit.edu/Cory/Cory.html

David Kielpinski, Massachusetts Institute of Technology
Cambridge, Massachusetts
web.mit.edu/physics/research/pappalardofellowshipsprogram/pappalardofellowsbios.html#kielpinski

Paul G. Kwiat, University of Illinois
Urbana-Champaign, Illinois
www.physics.uiuc.edu/People/Faculty/profiles/Kwiat/

Daniel Lidar, University of Toronto
Toronto, Canada
qubit.chem.utoronto.ca/Lidar.html

Daniel Loss, University of Basel
Basel, Switzerland
theorie5.physik.unibas.ch/loss/

Yuriy Makhlin, University of Karlsruhe
Karlsruhe, Germany
www-tfp.physik.uni-karlsruhe.de/~makhlin/

Florian Meier, University of California, Santa Barbara
Santa Barbara, California
theorie5.physik.unibas.ch/meier/

Terry P. Orlando, Massachusetts Institute of Technology
Cambridge, Massachusetts
www.rle.mit.edu/superconductivity/

Eugene Polzik, University of Aarhus
Aarhus, Denmark
www.dfi.aau.dk/amo/qoptics/qoptics.htm

Mark Saffman, University of Wisconsin
Madison, Wisconsin
hexagon.physics.wisc.edu

Mark Sherwin, University of California, Santa Barbara
Santa Barbara, California
www.physics.ucsb.edu/People/person.php3?userid=sherwin

Jens Siewert, University of Regensburg
Regensburg, Germany
homepages.uni-regensburg.de/~sij05914/

experience in manipulating individual atoms. The relative stability of atoms makes them well-suited to storing quantum information and serving as processor qubits. It is difficult, however, to move atoms while preserving their quantum states, so they are not particularly suited to quantum communications, and shuttling information between atoms is likely to involve using photons as intermediaries.

Ensembles of atoms can also be made to behave like a single atom, and small groups of electrons can be made to behave like a single electron. Researchers have used these groups of particles in qubits, taking advantage of their larger size to ease the requirements of controlling qubits.

A Josephson junction, which is a type of superconducting circuit, can make billions of electrons behave like a single virtual particle, and so can be used as a qubit.

Even whole laser beams have enough of a quantum nature that researchers are working out how to use them in quantum communications and are exploring the theoretical possibility of using them for quantum computing.

Qubits

Qubits include particles and the means of particle control. The major types of qubits are ions contained in ion traps, electrons confined to quantum dots, atoms embedded in semiconductors, and groups of electrons whizzing around superconducting circuits. (See How It Works, page 2.)

Quantum dots, made from semiconductor material, have the distinct advantage of being able to be integrated with existing electronics and manufactured using existing semiconductor facilities.

Researchers from Hewlett-Packard Laboratories and Qinetiq PLC in England have demonstrated that it is possible to use voltage pulses and magnetic fields to take a two-electron quantum dot qubit through all the necessary operations needed to compute. (See "Electron Pairs Power Quantum Plan", page 15.)

Researchers from the University of California at Santa Barbara have demonstrated that individual electrons associated with semiconductor impurities can serve as qubits when energy is added to the system via high-frequency lasers. Semiconductor impurities are atoms of a different substance that appear every few billion atoms even in fairly pure semiconductor materials. An advantage of this type of qubit is that it can be made using today's semiconductor manufacturing processes. (See "Chip Impurities Make Quantum Bits", page 17.)

Although much of quantum research is focused on the major candidate qubits, the field is young enough, and the challenges of working with particles difficult enough, that researchers are also looking for new ones. Other possibilities include molecular magnets, electrons on supercooled helium, and devices based on spectral hole burning.

Molecular magnets are molecules whose electrons have more or less the same spin orientation, resulting in a strong overall spin and thus magnetization.

Jaw-Shen Tsai, NEC Research and RIKEN
Wako, Japan
www.riken.go.jp/engn/r-world/research/lab/frontier/quantum/coherence/

K. Brigitta Whaley, University of California, Berkeley
Berkeley, California
www.cchem.berkeley.edu/~kbwgrp

David J. Wineland, National Institute of Standards and Technology
Boulder, Colorado
www.boulder.nist.gov/timefreq/ion/

Peter Zoller, University of Innsbruck
Innsbruck, Austria
th-physik.uibk.ac.at/qo/zoller/

Architectures

Neil Gershenfeld, Massachusetts Institute of Technology
Cambridge, Massachusetts
web.media.mit.edu/~neilg

Robert Joynt, University of Wisconsin
Madison, Wisconsin
uw.physics.wisc.edu/~joynt

Bruce Kane, University of Maryland
College Park, Maryland
www.glue.umd.edu/~bekane/QC/QC@UMD's_LPS_Bruce_Kane.htm

Franco Nori, University of Michigan
Ann Arbor, Michigan
www-personal.engin.umich.edu/~nori

Communications and Storage

Jon Dowling, Jet Propulsion Laboratory
Pasadena, California
home.earthlink.net/~jpdowling/

Philippe Grangier, French National Scientific Research Center (CNRS)
Orsay Cedex, France
www.iota.u-psud.fr/~grangier/Quantum_optics.htm

Philip Hemmer, Texas A&M University
College Station, Texas
ee.tamu.edu/People/bios/hemmer.html

H. Jeff Kimble, California Institute of Technology
Pasadena, California
www.its.caltech.edu/~qoptics/

Prem Kumar, Northwestern University
Evanston, Illinois
www.ece.northwestern.edu/~kumarp/

Selim M. Shahriar, Northwestern University
Evanston, Illinois
www.ece.northwestern.edu/faculty/Shahriar_Selim.html

Harald Weinfurter, University of Munich
Munich, Germany
scotty.quantum.physik.uni-muenchen.de

Anton Zeilinger, University of Vienna
Vienna, Austria
www.ap.univie.ac.at/users/Anton.Zeilinger/

Researchers from the University of London and the University of Copenhagen have found a way to make electrons flow across the surface of superfluid liquid helium contained in tiny channels etched into a wafer of gallium arsenide. The electrons form two-dimensional solid arrays, ubbed Wigner crystals. (See "Cold Electrons Crystallize", page 17.)

Spectral hole burning involves tuning atoms to respond to specific wavelengths of light. Researchers from the Massachusetts Institute of Technology are building a quantum computer that uses atoms trapped in a transparent solid. Each atom is tuned to two different wavelengths and serves as a qubit. When a wavelength from one atom overlaps a wavelength from another, the atoms can become entangled. The technique may allow the researchers to build a computer that has as many as 300 qubits. (See "Hue-ing to quantum computing", page 18.)

Light logic

Optical quantum computers use photonic properties like horizontal and vertical polarization to represent the ones and zeros of computing. The fleeting nature of photons and their weak interactions makes them less suited to computing than atoms and electrons, and in many schemes they are relegated to the role of transporting quantum information within and between quantum computers.

There are several schemes, however, that call for using photons in quantum processors. A common approach generates entangled qubits by firing high-power laser beams into special crystals that split individual high-energy photons into pairs of entangled lower-energy photons.

Researchers from Los Alamos National Laboratory have shown that it is also possible to control single photons using linear optics equipment like mirrors, beam splitters and photon detectors. Controlling single photons using linear optics equipment is simpler than controlling individual or small numbers of particles. (See "Ordinary Light Could Drive Quantum Computers", page 19.).

Johns Hopkins researchers have refined the idea with a linear optical quantum computer architecture that minimizes the probability of errors in this type of computer. The new design reduces by two orders of magnitude the amount of optical equipment needed, making it more likely that a linear optical computer quantum computer could be built. (See "Quantum Scheme Lightens Load", page 21.)

The main drawback to optical quantum computing is that it requires a lot of very fast, highly efficient equipment.

MRI technology

One quantum computing scheme that that has largely fallen out of favor is nuclear magnetic resonance (NMR) computing. In this type of computer, atoms within the molecules of a liquid are qubits, and they are controlled using the same technology used to take medical magnetic resonance images (MRIs). The possible show-stopper of nuclear magnetic resonance computing is the difficulty

Theory and Algorithms

Dorit Aharonov, Hebrew University
Jerusalem, Israel
www.cs.huji.ac.il/~doria/

Simon Benjamin, University of Oxford
Oxford, England
www.materials.ox.ac.uk/peoplepages/benjamin.html

Sougato Bose, Oxford University
Oxford, England
www.qubit.org/people/sougato/

Isaac Chuang, Massachusetts Institute of Technology
Cambridge, Massachusetts
feynman.media.mit.edu/ike

Richard E. Cleve, University of Calgary
Calgary, Canada
pages.cpsc.ucalgary.ca/~cleve/

David DiVincenzo, IBM Research
Yorktown, New York
www.research.ibm.com/ss_computing/

Artur Ekert, University of Oxford
Oxford, England
cam.qubit.org/users/artur/index.php

Lucien Hardy, Oxford University
Oxford, England
www.qubit.org/people/lucien_hardy/

Daniel Gottesman, Perimeter Institute
Waterloo, Canada
perimeterinstitute.ca/people/researchers/dgottesman/

Lov K. Grover, Bell Laboratories
Murray Hill, New Jersey
www1.bell-labs.com/user/lkgrover/

Bernardo A. Huberman, Hewlett-Packard Laboratories
Palo Alto, California
www.hpl.hp.com/shl/people/huberman/

Richard Jozsa University of Bristol
Bristol, England
www.cs.bris.ac.uk/~richard/

Emanuel Knill, Los Alamos National Laboratory
Los Alamos, New Mexico
www.c3.lanl.gov/~knill/

Seth Lloyd, Massachusetts Institute of Technology
Cambridge, Massachusetts
www-me.mit.edu/people/personal/slloyd.htm

David A. Meyer, University of California, San Diego
La Jolla, California
www.math.ucsd.edu/~dmeyer/

Gerard J. Milburn, The University of Queensland.
Brisbane, Australia
www.qcaustralia.org/bio/staff_milburn.htm

John Preskill, California Institute of Technology
Pasadena and, California
www.theory.caltech.edu/people/preskill/

Leonard J. Schulman, California Institute of Technology
Pasadena, California
www.cs.caltech.edu/~schulman/

of reading the spin flips of more than a half-dozen atoms at once. The seemingly insurmountable problem is that as the number of qubits grows, the signal from each qubit gets weaker.

A team of researchers at Stanford University and IBM research have breathed new life into the scheme by finding a way to strengthen the signals in a two-qubit nuclear magnetic resonance quantum computer. (See "Laser Boosts Liquid Computer", page 22.)

Though NMR quantum computers are unlikely to ever scale up to useful proportions, the technology is perhaps the most advanced form of quantum computing today, and nuclear magnetic resonance quantum computers are serving as testbeds for research into many aspects of quantum computing.

Umesh Vazirani, University of California at Berkeley
Berkeley, California
www.cs.berkeley.edu/~vazirani/

Vlatko Vedral, Imperial College, London
London, England
www.qubit.org/people/vlatko/

John Watrous, University of Calgary
Calgary, Canada
www.cpsc.ucalgary.ca/~jwatrous/

Colin P. Williams, Jet Propulsion Laboratory
Pasadena, California
cism.jpl.nasa.gov/sando/cwilliams.html

Controlling quantum information

Using qubits to carry out computing means controlling the behavior of qubits. Several teams of researchers are working on using electronics to control spin information.

Researchers from the Max Planck Institute and the Technical University of Munich in Germany have used an electric switch to transfer spin information from a group of electrons to the nuclei of atoms in a semiconductor. (See "Electric Switch Flips Atoms", page 25.)

Researchers from the University of California at Santa Barbara have built a semiconductor device that uses an electric field to rapidly reverse the spin of electrons. The device can pinpoint an area of electrons that's 10,000 times smaller than the head of a pin, and can change electron spin in less than one millionth of a second. (See "Semiconductors Control Quantum Spin", page 26.)

Several research teams are aiming to sidestep some of the difficulties of dealing with single particles by finding ways to use a group of particles to access superposition.

Researchers from the University of Basel in Switzerland and the University of Pittsburgh have devised a way to make qubits from groups of electrons rather than from harder-to-control single electrons. (See "Electron Teams Make Bigger Qubits", page 23.)

An international team of researchers has found a way to use clouds of atoms per qubit rather than having to control single atoms. (See "Atom Clouds Ease Quantum Computing", page 24.)

Several teams of researchers are also working with superconducting quantum interference devices, or SQUIDS. These tiny loops of superconductor carry an electric current that, when exposed to a magnetic field, enters into the state of superposition. Superposition in this case is a single set of electrons flowing in both directions at the same time. The two directions can represent the 1s and 0s of binary computing. (See "Oversize Oddity Could Yield Quantum Computers", page 27.)

Holding it together

It is not enough simply to find a way for a particle to represent a 1 or 0. A qubit must store the information long enough for it to be used in a computation. The challenge is that the fragile quantum states of atoms and subatomic particles that make up qubits are easily disturbed by small amounts of energy from the environment, including radio waves, magnetic fields and light.

When environmental noise intrudes on quantum particles' isolation, the quantum mechanical properties used to store information can change, or decohere, in a fraction of a second.

Researchers have come up with several ways to deal with decoherence. Some research teams have found ways to carve out decoherence-free zones. Others are working on error-correction schemes.

Logical vs. physical

Decoherence-free subspaces use aspects of multiple physical qubits to create a single logical qubit that is immune to noise.

Researchers from the National Institute of Standards and Technology (NIST) have built an ion trap qubit that contains a pair of beryllium ions controlled by lasers. The researchers used portions of two physical qubits to encode a logical qubit that lasted about three times as long as an unprotected qubit. (See "Quantum Bit Hangs Tough", page 29.)

Researchers from Los Alamos National Laboratory and the Massachusetts Institute of Technology used a set of three carbon atoms to create one sheltered, logical qubit. (See "Quantum Bit Withstands Noise", page 30.)

Two separate teams from the University of Toronto have demonstrated quantum algorithms running on decoherence-free subspace qubits: the Grover search algorithm running on a nuclear magnetic resonance quantum computer, and the Deutsch-Jozsa algorithm for examining both sides of a virtual coin at once running on an optical quantum computer.

A team of scientists from the University of California at Berkeley and IBM Research has proposed another type of encoding scheme. The scheme uses qubit interactions that are more natural and easier to control than the usual methods, but also adds an extra level of logic to the system. (See "Alternative Quantum Bits Go Natural", page 31.)

Living with errors

One way to deal with the errors introduced by decoherence is to find ways to automatically correct them. Like ordinary computers, quantum computers will always be subject to some degree of error, and like ordinary computers, quantum computers will need error correction codes.

Researchers from the University of Wisconsin at Madison have come up with an error correction method that reduces quantum computing error rates by two orders of magnitude. The method changes the usual quantum analog, or continuous, variable signal to a digital signal that has a discrete on and off state. (See "Quantum Computers Go Digital", page 32.)

Entangled logic

The point where quantum physics and computer science converge is the conditional NOT, or CNOT, logic gate. All of the necessary logic of computing can be built up from the CNOT gate and a few single-bit logic gates. The CNOT gate involves two bits: a control bit and a target bit. If the control bit is 1, the target bit changes from 1 to 0, or vice versa, and if the control bit is 0 the target bit remains unchanged.

In quantum computing a pair of entangled particles can make a CNOT gate. The CNOT two-qubit gate is the linchpin of the set of logic gates required for quantum computing, and the implementation of a CNOT gate is a key benchmark for quantum computer technologies.

Researchers from NEC Research and the Japanese Institute of Physical and Chemical Research (Riken) have implemented a CNOT gate using a pair of superconducting circuits.

Researchers from the University of Michigan and the University of California, San Diego have implemented a CNOT gate using a pair of electrons in a quantum dot. (See "Light Drives Electron Logic", page 34.)

In separate demonstrations, a research team from the National Institute of Standards and Technology, University of Colorado and University of Oxford, and a team from the University of Innsbruck in Austria have implemented CNOT gates using trapped ions.

Researchers from the University of Maryland have entangled qubits made from superconducting circuits that contain billions of electrons acting as one giant particle. (See "Big Qubits Linked over Distance", page 42.)

Blueprints

Researchers are also working out ways to put large numbers of qubits together in quantum computer architectures that define whole computers.

Scientists from the Institute of Physical and Chemical Research (Riken) in Japan have devised a scheme to connect qubits made from tiny loops of superconducting material in such a way that the qubits can carry out all the basic logic operations needed for computing. (See "Design Links Quantum Bits", page 37.)

National Institute of Standards and Technology (NIST) researchers have found a way to allow distant qubits to communicate as though they were in contact. Quantum computing architectures usually shunt information between qubits by passing the information through every qubit in between, bucket-brigade fashion. The NIST scheme uses a chain of entangled pairs of qubits to allow any qubit in a system to swap information with any other. (See "Quantum Computing Catches the Bus", page 35.)

Researchers from the University of Oxford and University College London in England have proposed a quantum computer architecture that simplifies qubit control by allowing qubits to be controlled all at once and allows them to be constantly connected to each other instead of repeatedly connected and disconnected. (See "Quantum Computer Keeps It Simple", page 34.)

Researchers from the University of Innsbruck in Austria have devised a quantum computing architecture that uses one- and two-qubit geometric operations to carry out the binary logic of computing. The scheme is designed for trapped ion qubits, but

could be generalized to other quantum computer hardware. (See "Quantum Logic Counts on Geometry", page 40.)

Quantum chips

Quantum designs that use semiconductor chips have a distinct potential advantage over other types of qubits: they can be manufactured using methods similar to those used to make today's computer chips.

The original solid-state quantum computer architecture called for electrons trapped in quantum dots. University of Wisconsin researchers have advanced this architecture with a design that would incorporate thousands of single-electron quantum dots in a silicon chip. The quantum dots contain a bottom layer of silicon germanium that serves as an electron reservoir and is chemically altered to allow electrons to flow more easily. Three additional layers make up a sandwich of silicon and silicon germanium that traps a single electron in place when it is needed for computing. (See "Chip Design Aims for Quantum Leap", with page 38.)

Another well-known solid-state quantum computer architecture, developed by University of Maryland researcher Bruce Kane, calls for regularly spaced phosphorous atoms embedded in silicon chips. A research team from the University of New South Wales in Australia has advanced this design by making a prototype: individual phosphorus atoms spaced four nanometers apart on a silicon surface. (See "Positioned Atoms Advance Quantum Chips", page 42.)

Scientists from the Institute of Physical and Chemical Research (Riken) in Japan and the State University of New York at Stony Brook have entangled a pair of superconducting qubits in an integrated circuit. (See "Quantum Chips Advance", page 42.)

A team of researchers from the Italian National Institute for Material Physics and the Polytechnic Institute of Torino in Italy have devised a quantum computer made from quantum dots, ultrafast lasers and an alternative type of particle. Rather than electrons, the quantum dots trap excitons. An exciton is a negatively-charged electron and positively-charged hole that reside in a temporarily stable orbit around each other. The advantage of the architecture is that excitons survive in superposition for a relatively long time — nanoseconds or microseconds. This is long enough for thousands of computational operations to take place. (See "Quantum Computer Design Lights Dots", page 41.)

Relative Scale

An electron is 100 billion times smaller than a hydrogen atom.

A row of 10 hydrogen atoms is one nanometer long.

Visible light photons range from 400 to 700 nanometers in diameter.

An E. coli bacterium is 1,000 nanometers, or one micron, wide.

A human hair is about 75 microns in diameter.

Tools of the trade

As with any emerging technology, researchers are building tools designed to help build and run quantum computers. These include tools to form quantum circuits, techniques to control spin currents, and methods of strengthening entanglement.

Researchers from Cambridge University in England and the Massachusetts Institute of Technology have developed a lithographic technique that involves drawing electric charges on a surface to form quantum dots and wires. The technique takes a few hours, which is much faster than the standard method of using electron beams to etch lines and dots into semiconductor material. (See "Tool Sketches Quantum Circuits", page 44.)

Researchers from the University of California and Pennsylvania State University have demonstrated that it is possible to efficiently move a current of electrons, with their collective spin intact, from one semiconductor material to another. The researchers also showed that this spin state can last as long as 100 nanoseconds — long enough to perform computations. (See "Quantum Current Closer to Computing", page 44.)

Researchers from the University of Toronto have proposed a way of generating and controlling electron spins in semiconductors using a pair of light beams of slightly different colors. The interface between light beams sorts electrons, sending those of one spin in one direction and those of the other spin in the opposite direction. (See "Shining a New Light on Electron Spin", page 45.)

Entangling particles

Entanglement is a critical but elusive resource for quantum computing. The more the better, generally.

Researchers at Los Alamos National Laboratory and the University of Geneva in Switzerland have found a way to distill a collection of partially entangled pairs of photons down to a smaller number of more highly entangled photon pairs. The method uses a type of polarization filter. (See "Filters Distill Quantum Bits", page 46.)

Massachusetts Institute of Technology researchers have found a way to make entangled-photon beams that contain specific wavelengths of light and are relatively bright. (See "Rig Fires More Photon Pairs", page 47.)

And a research team at the University of Oxford in England has made a laser that emits entangled photons. (See "Laser Emits Linked Photons", page 47.)

Measuring Entanglement

It's difficult to determine how entangled a pair of particles is, or even if two particles are entangled at all. Entanglement requires that particles not be in contact with the environment, but measuring a particle means hitting it with some form of energy. In most cases, researchers have to calculate the probabilities for whether and how much a pair of particles are entangled.

Researchers are also beginning to develop techniques for directly measuring entanglement. Scientists from the University of Rome La Sapienza in Italy have demonstrated a technique for detecting entanglement in pairs of photons.

Researchers from the Technical University of Gdansk in Poland and the University of Cambridge in England have come up with a general scheme for measuring entanglement. (See "Method Measures Quantum Quirk", page 48.)

Wichita State University researchers have showed that a quantum neural network could calculate entanglement, an ability that could in turn help in building quantum computers. (See "Self-Learning Eases Quantum Computing ", page 49.)

Reading the answers

Being able to compute the answers to very large problems is useless if those answers cannot be read. Researchers are working on ways to read particle spins in order to extract answers from quantum systems.

Researchers from the University of California at Berkeley have found a way to measure the spin of an electron associated with a nickel impurity embedded in a copper oxide crystal. (See "Tool Reads Quantum Bits", page 50.)

Bottling chance

Memory is a basic element of computing. Information is fleeting in classical computer processors and more so in quantum computers, requiring at least short-term storage capabilities.

Researchers from NASA's Jet Propulsion Laboratory have proposed a type of linear optical quantum memory that uses an error correction code to recover lost qubits in fiber-optic lines. Putting the device in a fiber loop forms a memory device.

Researchers from Johns Hopkins University have demonstrated a quantum memory device that captures photonic qubits for a tiny fraction of a second by switching them into a fiber-optic loop. The qubits can be read when they are switched out of the loop (See "Fiber Loop Makes Quantum Memory", page 52.)

Researchers from the Harvard-Smithsonian Center for Astrophysics have shown that it is possible to transfer quantum information from a light pulse to gas atoms and back again. They have also shown that it is possible to alter the light information as it is stored in the atoms. (See "Stored Light Altered", page 54.)

Researchers from the Massachusetts Institute of Technology, Texas A&M University and the Electronics and Telecommunications Research Institute in South Korea have shown that it is possible to store the quantum information contained in light pulses in a crystal for a few tenths of a millisecond. (See "Crystal Stores Light Pulse", page 53.)

Making connections

Communications is also a critical component of computing, both for moving information within and moving information between computers. Researchers are still grappling with the basics of how to move information between qubits within a quantum computer, but they are also planning ahead for full-blown quantum networks.

Signals fade as they travel down communications lines because some photons are inevitably lost as they bounce around optical fibers. Today's optics solve the fading signal problem by using repeaters, which simply make fresh copies of fading information and send the copies on.

The traditional setup won't work with information stored in particles that are in superposition. Quantum information is fragile because particles come out of superposition when observed. Observing signals in order to copy them would destroy the information.

The incentive to make quantum repeaters is high, however, because transmitting quantum information can potentially provide perfect security as well as the means to link quantum computers. The incentive is especially strong because practical quantum computers would render most of today's security codes useless. Quantum cryptography, however, has been thoroughly demonstrated in the laboratory, and is likely to be deployed well before practical quantum computers arrive. (See TRN's Making the Future report Quantum Cryptography: Potentially Perfect Security)

Scientists from the University of Innsbruck in Austria have found a way to boost quantum signals. They got around the observation problem by using a repeater made from a cloud of atoms. The device would transfer quantum information carried by inbound photons to an atom cloud, which would then transfer it to outbound photons to produce a stronger signal. (See "Device Would Boost Quantum Messages ", page 56.)

Another possibility echoes a concept out of science fiction. Particles can be teleported using entanglement, a process akin to faxing a particle. A pair of entangled particles that are physically separated form the teleportation machine. Teleportation occurs when a target particle comes into contact with one of the two entangled particles and is then measured, which destroys the target particle. With the information gained from the measurement, however, researchers can measure the second entangled particle and in doing so turn it into an exact copy of the target particle.

Teleportation can be used to make quantum repeaters. The devices would teleport particles from one repeater to the next.

Researchers at the University of Geneva in Switzerland and the University of Aarhus in Denmark have teleported a photon from one laboratory to a second laboratory by bringing the photon to be teleported in contact with a local photon entangled with a photon at the second location; the two labs were 55 meters away, but the setup simulated a distance of two kilometers. (See "Teleportation Goes the Distance", page 55.)

Researchers from the Harvard-Smithsonian Center for Astrophysics have proposed a way to entangle atom-photon particle pairs that involves firing a laser into a Bose Einstein condensate, an exotic form of matter formed by chilling atoms to near absolute zero. Entangled atom-photon pairs could be used for quantum communications, including teleportation. (See "Proposal Would Marry Atom and Photon", page 57.)

Researchers from the Massachusetts Institute of Technology and the U.S. Air Force Research Laboratory have come up with a scheme to network quantum computers that involves entangling a pair of photons, sending each to a separate node, or computer, on a quantum network, and transferring the information to single atoms contained at the nodes. The atoms are entangled with each other, and key to the plan is a scheme to entangle distant atoms via teleportation. (See "Quantum Network Withstands Noise", page 58.)

Quantum software

The promise of quantum computing is that it could very quickly solve needle-in-a-haystack problems — those that contain many, many possibilities to sort through. Two significant quantum algorithms have shown that quantum computers would be better for solving two types of problems than classical computers.

Shor's algorithm, published in 1994, showed that quantum computers could factor numbers — and thus break encryption codes — at a dramatically faster rate than classical computers. This includes factoring numbers so large that no conceivable classical computer could ever factor them. Researchers from IBM and Stanford University have factored the number 15 using a seven-qubit nuclear magnetic resonance quantum computer as a demonstration of Shor's factoring algorithm and of techniques for controlling quantum computers. (See "Quantum Demo Does Tricky Computing", page 59.)

Grover's algorithm, published in 1996, showed that quantum computers could search large, unstructured databases dramatically faster than classical computers.

Researchers are attempting to develop algorithms that apply quantum computing to other broad classes of problems.

To that end, researchers at the Massachusetts Institute of Technology have devised a quantum algorithm that raises the possibility of solving NP-complete problems. (See "Simulation Hints at Quantum Computer Power", page 60.)

These types of very large problems include the traveling salesperson problem. Planning the best route for a salesperson to take through several cities seems like a fairly simple problem. But the number of possibilities increases exponentially with each additional city. Even with a fairly moderate number of cities — 15 — there are billions of possible routes. Increase the number of cities to 500, and you get an impossibly large number of possibilities that no classical computer could ever hope to solve.

Filling in the picture

Several other algorithms have been developed that solve particular problems in mathematics and that would render certain encryption codes vulnerable.

A University of British Columbia physicist has come up with algorithm that shows that quantum computers would be faster than classical computers at finding patterns. (See "Quantum Software Gets the Picture", page 61.)

Researchers from the University of Amsterdam, the Center for Mathematics and Computer Science (CWI) in the Netherlands, and the University of Calgary in Canada have found a mathematical fingerprinting scheme that would allow quantum computers to compare two sets of data much more efficiently than is possible with classical computers. (See "Quantum Data Compares Faster", page 62.)

IBM researchers have shown that adding a quantum component to secret-sharing cryptographic protocols that break a cryptographic key into pieces would make it harder for the people holding the pieces to cheat or be coerced into revealing the secret. (See "Quantum Code Splits Secrets", page 63.)

Researchers from Lucent Technologies' Bell Labs have modified Grover's algorithm to allow quantum computers to do sampling computations. According to the researchers, the algorithm will allow quantum computers to do statistical sampling, to search using sketchy information, and to approximate answers to scientific problems that are too difficult to solve. (See "Sampling Ability Broadens Quantum Computing", page 64.)

Researchers from Hewlett-Packard Laboratories and Stanford University have shown that quantum software, like classical computing software, would benefit from a strategy of using a mix of algorithms rather than a single algorithm to solve computer problems that take varying amounts of time for each attempt. (See "Portfolios Boost Quantum Computing", page 65.)

Researchers from Trento University in Italy, the University of Innsbruck in Austria and the Institute for Scientific and Technological Research at the Trentino Institute of Culture in Italy are building a programming architecture for quantum computing in the form of a C++ class library, or vocabulary for the C++ programming language. (See "Programming Goes Quantum", page 66.)

Most researchers working on quantum algorithms are counting on entanglement being part of the equation. A researcher at the University of California in San Diego, however, has demonstrated that a particular quantum search algorithm does not necessarily have to use entanglement. (See "Quantum Computing without Weirdness", page 68.)

The lay of the land

Quantum computing is unlikely to ever replace classical computing for everyday tasks, but work in the last ten years has shown that quantum computers have the potential to solve otherwise unsolvable problems. That only two broadly applicable quantum algorithms have been developed in the last decade, and none in the last seven years, however, suggests that using particles to compute is difficult, limited in applicability, or both.

Though the factoring algorithm alone is enough to ensure that quantum computing research will be well funded, uncertainty about the overall usefulness of quantum computing could begin to diminish some of the enthusiasm the field currently enjoys. A key milestone is the development of a third algorithm that shows quantum computers have an advantage over classical computers for a broad class of problems. In particular, definitive proof that quantum computers can solve NP-complete problems that are out of the range of classical computers would assure that the technology will be vigorously pursued.

Of course, no amount of enthusiasm can guarantee that quantum computers large enough to be useful can be built.

The long road ahead

The last year has seen significant progress in quantum computing, particularly the factoring algorithm running on a seven-qubit nuclear magnetic resonance computer and the method of entangling of two solid-state qubits. But these are still baby steps, and a quantum computer that outperforms classical computers is off in the multi-decade future.

Even optimistic goals that aim for working quantum computers in a decade are focused on testbed technology. The U.S. government's Advanced Research and Development Activity (ARDA), under the direction of the National Security Agency (NSA), is one of the principal funders of quantum computing research. A panel of 17 quantum computing researchers has prepared a roadmap for ARDA that last year set goals for the next ten years of research. (See qist.lanl.gov)

The first set of goals, set for 2007, calls for researchers to thoroughly control qubits and qubit interactions by creating entanglement on demand, encoding information in logical qubits, extending qubit lifetime, and communicating quantum information from one qubit to another. The 10-year goal, for 2012, calls for the fault-tolerant operation of a multi-qubit quantum computer running a quantum algorithm. Such a computer would allow researchers to begin to explore the practical issues relating to quantum computer architectures and algorithms.

Recent Key Developments

Advances in quantum computing schemes:

- A scheme to compute using qubits made from quantum dots containing two electrons (Electron Pairs Power Quantum Plan, page 15)
- A scheme to use electrons from individual atoms embedded in semiconductors as qubits (Chip Impurities Make Quantum Bits, page 17)
- A prototype that allows a set of electrons to be controlled on the surface of a tiny amount of supercooled helium (Cold Electrons Crystallize, page 17)
- A scheme for quantum computing by tuning the wavelengths of light that embedded atoms respond to (Hue-ing to Quantum Computing, page 18)
- A breakthrough proposal for a way to carry out quantum computing using ordinary light and standard optical equipment (Ordinary Light Could Drive Quantum Computers, page 19)
- An improved scheme for making quantum computers using ordinary light (Quantum Scheme Lightens Load, page 21)
- A laser technique that combats noise in NMR quantum computers (Laser Boosts Liquid Computer, page 22)
- A method that makes multiple electrons behave like one that could enable qubits that are easier to control (Electron Teams Make Bigger Qubits, page 23)
- A method that makes many atoms behave like one to make a qubit that is a bigger target (Atom Clouds Ease Quantum Computing, page 24)

Advances in qubits:

- An electronic switch that transfers electron spins to the nuclei of atoms (Electric Switch Flips Atoms, page 25)
- An electronic device that rapidly controls the spins of electrons (Semiconductors Control Quantum Spin, page 26)
- A pair of demonstrations of quantum superposition in superconducting circuits (Oversize Oddity Could Yield Quantum Computers, page 27)
- A logical qubit encoded in two nuclear spins using liquid nuclear magnetic resonance techniques, Massachusetts Institute of Technology, Los Alamos National Laboratory and Columbia University, February 2002
- A noise-resistant logical qubit formed from two beryllium ions (Quantum Bits Hangs Tough, page 29)
- A demonstration of a noise-resistant logical qubit made from three carbon atoms (Quantum Bit Withstands Noise, page 30)
- A scheme to use the natural behavior of quantum dots to form qubits (Alternative Quantum Bits Go Natural, page 31)
- A scheme to make digital qubits from analog electron signals (Quantum Computers Go Digital, page 32)

Advances in logic gates:

- A two-qubit CNOT logic gate made from superconducting circuits, NEC Research and the Japanese Institute of Physical and Chemical Research (RIKEN), October 2003
- A two-qubit logic gate made from two electrons in a quantum dot controlled by light (Light Drives Electron Logic, page 34)
- Two demonstrations of two-qubit logic gates made from trapped ions, the National Institute of Standards and Technology, University of Colorado and University of Oxford, and the University of Innsbruck in Austria, March 2003
- A universal NOT logic gate, La Sapienza University in Italy, Slovak Academy of Sciences and National University of Ireland, October 2002

Advances in computer architectures:

- A scheme that controls all of the qubits in a quantum computer at the same time using one set of control signals (Quantum Computer Keeps It Simple, page 34)

- A scheme to connect qubits that reside in different parts of a quantum computer (Quantum Computing Catches the Bus, page 35)
- A scheme to link qubits made from superconducting loops (Design Links Quantum Bits, page 37)
- A scheme to control multiple quantum dot qubits (Chip Design Aims for Quantum Leap, page 38)
- A scheme to compute using arrays of ion traps, Massachusetts Institute of Technology, University of Michigan and the National Institute of Standards and Technology, June 2002
- A scheme to compute using qubits made from ammonium molecules trapped in carbon nano cages, University of Cambridge and University of Oxford, March 2002
- A scheme to compute using the geometry of virtual spaces formed by the math describing particles (Quantum Logic Counts on Geometry, page 40)
- A scheme to compute using quantum dots and ultrafast laser pulses (Quantum Computer Design Lights Dots, page 41)
- A pair of linked superconducting circuit-based qubits that are separated by nearly a millimeter (Big Qubits Linked over Distance, page 41)
- A pair of linked superconducting circuit-based qubits (Quantum Chips Advance, page 42)
- A silicon chip that contains precisely positioned individual phosphorous atoms (Positioned Atoms Advance Quantum Chips, page 43)

Advances in tools and resources:

- A faster way to make quantum dots, wires and hills (Tools Sketches Quantum Circuits, page 44)
- A demonstration showing it is possible to move a current of spin-segregated electrons from one semiconductor to another (Quantum Current Closer to Computing, page 44)
- A way to use light to control the flow of electrons (Shining a New Light on Electron Spin, page 45)
- A method that employes polarization to sort out highly entangled pairs of photons (Filters Distill Quantum Bits, page 46)
- A way to make entangled photon beams that are relatively bright and contain specific wavelengths of light (Rig Fires More Photon Pairs, page 47)
- A way to use a laser to multiply entangled photon pairs (Laser Emits Linked Photons, page 47)
- A method of detecting the entanglement of pairs of photons, University of Rome La Sapienza, November 2003
- A scheme for directly measuring entanglement (Method Measures Quantum Quirk, page 48)
- A simulation that shows that a quantum neural network could calculate the quantum mechanical property of entanglement (Self-Learning Eases Quantum Computing, page 49)
- A way to measure the spin of a single atom (Tool Reads Quantum Bits, page 50)

Advances in storage:

- A scheme for an optical quantum memory based on an error correction code, NASA's Jet Propulsion Laboratory, November 2003
- A demonstration showing that it is possible to store a pair of entangled photons in a group of rubidium atoms, Harvard University, Harvard-Smithsonian Center for astrophysics and the P. N. Lebedev Institute of Physics in Russia, May 2003
- A fiber-optic loop switch that stores photonic qubits for tens of billionths of a second (Fiber Loop Makes Quantum Memory, page 52)
- A demonstration showing that it is possible to map the quantum state of light onto a group of cesium atoms, University of Aarhus in Denmark, July 2002
- A way to store photonic quantum information in a crystal for a few tenths of a second (Crystal Stores Light Pulse, page 53)
- A way to alter quantum photon information as it is stored in a group of atoms (Stored Light Altered, page 54)

Advances in communications:

- A demonstration showing a way to identify successfully teleported photonic qubits, University of Vienna, February 2003

- A demonstration showing that it is possible to teleport photons across two kilometers (Teleportation Goes the Distance, page 55)
- A demonstration showing that a laser beam can be teleported, Australian National University, June 2002
- A demonstration of quantum cloning of photons that showed that high-quality but not perfect copies can be made, University of Oxford and University of California at Santa Barbara, March 2002
- A quantum repeater scheme that transfers quantum information from photons to an atom cloud and back (Device Would Boost Quantum Messages, page 56)
- A scheme for entangling an atom and photon that calls for firing a laser into a Bose Einstein condensate (Proposal Would Marry Atom and Photon, page 57)
- A scheme for transmitting and storing quantum information in a series of quantum network nodes spaced as far as 10 kilometers apart (Quantum Network Withstands Noise, page 58)

Advances in algorithms:

- A demonstration of the Grover search algorithm running on nuclear magnetic resonance quantum computer made more stable by decoherence-free subspaces, University of Toronto, November 2003
- A demonstration of the Deutsch-Jozsa algorithm for examining both sides of a virtual coin at once running on an optical quantum computer made more stable by decoherence-free subspaces, University of Toronto, October 2003
- A demonstration of the Deutsch-Jozsa algorithm running on a single trapped ion, University of Innsbruck in Austria and the Massachusetts Institute of Technology, January 2003
- A seven-atom quantum computer that can factor the number 15 (Quantum Demo Does Tricky Computing, page 59)
- A simulation that shows that quantum computers might be able to solve NP-complete problems (Simulation Hints at Quantum Computer Power, page 60)
- An algorithm that proves the quantum computers would be faster than classical computers at finding patterns (Quantum Software Gets the Picture, page 61)
- A mathematical fingerprinting scheme that would allow quantum computers to compare sets of data more efficiently than is possible using classical computers (Quantum Data Compares Faster, page 62)
- A secret-sharing scheme that taps entanglement to split information into two pieces (Quantum Code Splits Secrets, page 63)
- An algorithm that would allow quantum computers to do sampling computations (Sampling Ability Broadens Quantum Computing, page 64)
- Proof that a mix of algorithms would make for more efficient quantum computing (Portfolios Boost Quantum Computing, page 65)
- A C++ class library for quantum computing (Programming Goes Quantum, page 66)

Advances in theory:

- Calculations that show that quantum computers are likely to always need very large amounts of power (Quantum Computing Has Limits, page 67)
- Evidence that a quantum search algorithm does not require entanglement (Quantum Computing without Weirdness, page 68)

Quantum Computing Schemes

Electron Pairs Power Quantum Plan

By Eric Smalley, Technology Research News
January 1/8, 2003

The shortest route to practical quantum computers, which promise to be phenomenally powerful, may be through proven manufacturing processes, namely the semiconductor technology of today's computer chips. It wouldn't hurt if the machines also used aspects of quantum physics that are relatively easy to control.

Researchers from Hewlett-Packard Laboratories and Qinetiq plc in England have mapped out a way to manipulate a pair of very cold electrons that could eventually lead to practical quantum computers made from quantum dots, or

tiny specks of the type of semiconductor material used in electronics.

The researchers showed that at low temperatures, a pair of trapped electrons operate relatively simply and can be manipulated using electric and magnetic fields. "For... two electrons in a square-shaped quantum dot, there are just two states," John Jefferson, a senior fellow at Qinetiq.

The electrons repel each other to diagonally-opposite corners of the quantum dot, leaving the two electrons in one of two possible configurations: upper right corner and lower left corner, or upper left corner and lower right corner.

These two states can represent the 1s and 0s of digital information; the quantum dots, or qubits, that contain them are the quantum computing equivalent of today's computer transistors, which use the presence or absence of electricity to represent 1s and 0s.

Quantum computers have the potential to solve very large problems fantastically fast. The weird rules that quantum particles like atoms and electrons follow allow them to be in some mix of states at once, so a qubit can be a mix of both 1 and 0. This means that a single string of qubits can represent every possible answer to a problem at once.

This allows a quantum computer to use one set of operations to check every potential answer to a problem. Today's electronic computers are much slower, in contrast, because they must check answers one at a time.

Key to the researchers method is the square shape of the microscopic quantum dot—a speck of the semiconductor gallium arsenide measuring 800 nanometers a side—that they used to trap the electrons. A nanometer is one millionth of a millimeter. "Two electrons in a square quantum dot repel each other [to the corners] due to the usual Coulomb repulsion force between them," said Jefferson.

The Coulomb force kicks in when particles carry a charge. Particles of the same charge, like electrons, which are negatively charged, repel each other.

Due to the weird nature of quantum particles, however, the electron pair may also jump, or tunnel, from one position, or state, to the other, said Jefferson. "This happens periodically... and the system can also be in a strange superposition state where it is partly in one state and partly in the other," he said. "This is the basis of our two-electron semiconductor quantum-dot qubit."

The researchers showed that they could use voltage pulses and magnetic fields to take this type of qubit through all the necessary operations needed to compute, said Jefferson.

This was tricky because it is not possible to turn the Coulomb force on and off, said Jefferson. "A severe potential problem with the Coulomb interaction is that it is always there," he said. The researchers showed, however, that it is possible to control the effects of the force, and thus harness it to do computing.

The researchers scheme differs from many other quantum dot quantum computing designs because it uses the positions of two electrons rather than their spin, which is a quality that can be likened to a top spinning clockwise or counterclockwise. The electrons' positions determine the charge states of the quantum dot, meaning if an electron is in one corner of the quantum dot that corner has a charge. "It is often easier to manipulate charge states compared to spin states," said Jefferson. In addition, "it is... certainly easier to measure charge states compared to spin states," he said.

To turn this building block into a practical computing device, however, the qubits must be stable. This requires "some means of preparing the qubits in a specific state, after which they have to [be affected only] according to the basic laws of quantum mechanics," said Jefferson. This includes isolating them from other interactions, he said.

Practical quantum computers would require hundreds or thousands of connected qubits. "It should be possible to add more qubits," said Jefferson. There must also be a way to measure the final results when the computation has taken place, he said.

The researchers showed that these requirements can theoretically be satisfied using the two-electron qubits, said Jefferson. "In principle, these criteria may be met, though to do so in a practical device would be technologically very challenging," he said.

Researchers generally agree that practical quantum computing of any type is one to two decades away. "Ten to 20 years is more realistic than 2 to 5," for a practical application of the two-electronic quantum dots, said Jefferson.

Rather than using semiconductor quantum dots, the researchers' basic method could possibly be achieved more quickly and effectively using a series of individual molecules, said Jefferson. "The energy and temperature scales [for molecules] are higher and thus less prone to random errors," he added.

This could address one of the main hurdles to using qubits practically, Jefferson said. "One of the main challenges is to reduce the interaction of a quantum system with its environment—the so-called decoherence problem," he said.

The other main technical challenge to using the system practically would be to produce quantum dots containing precisely two electrons, and to coax the electrons to switch states with acceptable error rates, he said.

Jefferson's research colleagues were M. Fearn and D. L. J. Tipton of Qinetiq and Timothy P. Spiller of Hewlett-Packard Laboratories. They published the research in the October 30, 2002 issue of the journal *Physical Review A*. The research was funded by the British Ministry of Defense, the European Union, Hewlett-Packard and Qinetiq.

Timeline: 10-20 years
Funding: Corporate, Government
TRN Categories: Physics; Quantum Computing and Communications
Story Type: News

Related Elements: Technical paper, "Two-Electron Quantum Dots as Scalable Qubits," Physical Review A, October 30, 2002

TRN

Chip Impurities Make Quantum Bits

By Eric Smalley, Technology Research News
March 14, 2001

It's difficult to make a semiconductor computer chip that is pure. Usually for every few billion or so semiconductor atoms there's an unwanted atom of some kind. These impurities are little more than a nuisance to chip makers, but they could become the key to phenomenally powerful quantum computers.

Researchers based at the University of California at Santa Barbara have demonstrated that individual electrons associated with these impurities can serve as quantum bits, or qubits. The research opens a route to solid-state quantum computers that would be compatible with today's semiconductor manufacturing processes.

The researchers made qubits by firing intense, high frequency lasers at electrons of donor atoms, according to Mark S. Sherwin, a professor of physics at UC Santa Barbara.

A donor is an atom of a different element that has one more valence electron than the atom it replaces, he said. Electrons reside around an atom's nucleus in specific bands or orbitals; valence electrons reside in the outermost band.

"If a silicon atom substitutes for a galium atom, three of the silicon's four valence electrons will be tied up in bonds to neighboring [galium] atoms, but the fourth will be left over with nowhere obvious to go," Sherwin said.

The laser drives the electron from its ground, or low-energy, state to a higher energy state. The two states can be used to represent the 0 and 1 of binary computing. The electron then oscillates between the two states and during this oscillation the electron enters the quantum state of superposition in which it is in both states at the same time.

Quantum computers hold the promise of being faster than the most powerful possible ordinary computer for certain applications like cryptography and database searches. The power of a quantum computer comes from manipulating many qubits in superposition at once, thereby processing at the same time all the possible numbers those qubits represent.

The researchers are working on containing the donor atoms' electrons in quantum dots or other structures in order to preserve the electrons and separate them from each other, said Sherwin. In the current setup, the electrons can be freed with relatively little energy, and the number of donor atoms means the electrons are on average about 200 nanometers apart, which makes it difficult to address each one individually, he said.

The researchers also plan to drive the electrons to a different higher energy state because the one they used in the experiment is relatively unstable, allowing for only one oscillation between the high and low energy states, said Sherwin. The researchers will need the superposition of states to last long enough to perform the thousands of operations necessary to implement a quantum algorithm.

"Using the qubits in our present experiment, I don't think we could perform any quantum algorithms," said Sherwin. "We know things will get much better, but it is difficult to predict how much better."

It will be at least 10 to 20 years before practical quantum computing applications are developed, said Sherwin.

Sherwin's research colleagues were Bryan E. Cole, Jon B. Williams and B. Tom King of the University of California at Santa Barbara and Colin R. Stanley of the University of Glasgow. They published the research in the March 1, 2001 issue of *Nature*. The research was funded by the Army Research Office and the Defense Advanced Research Projects Agency (DARPA).

Timeline: 10 to 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Coherent manipulation of semiconductor quantum bits with terahertz radiation," Nature, March 1, 2001

TRN

Cold Electrons Crystallize

By Kimberly Patch, Technology Research News
December 12, 2001

When electrons travel together in a current through electrical wire, they usually do so haphazardly, randomly bumping into each other as they push forward.

Researchers from the University of London and the University of Copenhagen have found a way to make electrons line up in a type of crystal as they travel.

The work promises to increase researchers' understanding of one of nature's most basic and useful particles, and is a step forward in using electrons to do extremely fast computations in quantum computers.

Electrons are one of the three basic particles that make up atoms. Between 1 and 117 electrons circle around an atom's nucleus depending on its type. Hydrogen, for example, holds onto just one electron, while copper has 29.

In a metal or semiconductor, the outermost electrons become detached from the atoms to form free electrons that can flow as electrical current through a wire.

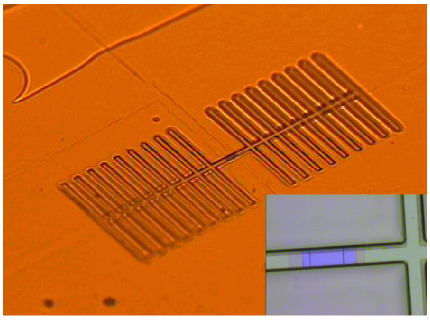
The electrons the researchers worked with were flowing across the surface of superfluid liquid helium that was

contained in tiny channels etched into a wafer of gallium arsenide.

Helium becomes a superfluid at about two degrees Kelvin, or -271 Celsius, and provides a smooth surface for the flowing electrons.

The channels formed a field-effect transistor, which controls electrical current.

Quantum particles like electrons have many weird properties. The electrons in the researchers' device are a type known as two-dimensional electrons because they can only move in the two-dimensional plane of the liquid's surface. The researchers controlled the electrons using positively charged metallic electrodes that attracted the negatively charged electrons.



Source: University of London

These tiny channels contain liquid helium cooled to just above absolute zero. Electrons moving across the surface of the helium in the center of the device (blue portion of inset) line up to form a Wigner crystal, which is a type of solid.

In the researchers' device, the electrons behaved like normal free electrons at temperatures above one degree Kelvin. But below that the electrons packed together into offset rows similar to a single layer of ping-pong balls pushed together on the surface of a table.

These two-dimensional, solid arrays of electrons, or Wigner crystals, interacted with waves on the helium surface, said Michael Lea, a professor of physics at the University of London. As a Wigner crystal approached the speed of the waves it encountered increased resistance, "a bit like a sound barrier for airplanes," said Lea. This resistance is evidence that the electrons formed a type of solid.

Individual electrons that are part of a Wigner crystal could eventually be used as quantum bits, or qubits in a quantum computer, he said. "Such a computer would use localized electrons—as in a crystal—to perform calculations," said Lea.

The researchers are currently studying smaller numbers of electrons in similar structures that form single electron transistors, which need only one electron to switch on or off.

The work is an "experimental tour de force" that produced a new type of object, said Mark Dykman, a physics professor at Michigan State University. "Quite remarkably, the results demonstrate not only the onset of crystallization, but also that the wires can move past each other, [which shows that] ordered wires are well-defined objects," he said.

Understanding electrons better is essential in many facets of nanotechnology, said Dykman.

For example, one goal in miniaturizing computers is to make single-electron transistors. The Wigner wires demonstrate "what happens when several electrons are placed into confined space," he said, adding that the knowledge also has the potential to contribute to proposals that involve entirely new devices.

The effect has potential in quantum computing, said Dykman. "The work shows that... a small group of electrons can be controlled. This is certainly an important step," toward using those electrons for computing, he said.

It will take three to five years before proof-of-principle experiments determine whether the effect can be used for quantum computing, said Lea. Researchers generally agree that practical quantum computers will take a least 20 years to develop.

Lea's research colleagues were Philip Glasson, Vladimir Dotsenko, Parvis Fozooni, William Bailey and George Papageorgiou of the University of London, and Soeren Andresen and Anders Kristensen of the University of Copenhagen in Denmark.

They published the research in the October 22, 2001 issue of *Physics Review Letters*. The research was funded by the UK Engineering and Physical Sciences Research Council (EPSRC), the European Union (EU), the Royal Society and International Association for the promotion of cooperation with scientists from the New Independent States of the former Soviet Union (INTAS).

Timeline: 3-5 years, 20 years or more
Funding: Government
TRN Categories: Quantum Computing; Materials Science and Engineering
Story Type: News
Related Elements: Technical paper, "Wigner Wire: Electrons Act Orderly," Physical Review Letters, October 22, 2001

TRN

Hue-ing to Quantum Computing

By Eric Smalley, Technology Research News
September 20, 2000

The starting gun has sounded in the marathon of developing solid-state quantum computers, and one lead team jockeying for position is betting that shining different color lasers on impure diamonds will get them across the finish line.

The researchers are building their quantum computer using spectral hole burning, which tunes atoms or molecules trapped in a transparent solid to specific light wavelengths, or colors.

The researchers have tuned nitrogen atoms embedded in diamond to a range of slightly different wavelengths, said Selim M. Shahriar, a research scientist in the Research Laboratory of Electronics at the Massachusetts Institute of Technology. The differences in color are imperceptible to humans, he added.

Each atom is tuned to two wavelengths. If a laser beam of one of the wavelengths hits it, the atom will emit light of the other wavelength, Shahriar said. In addition, a pair of atoms each tuned to two wavelengths can be linked to each other. For example, if atom A is tuned to wavelengths 1 and 2 and atom B is tuned to wavelengths 2 and 3 and the atoms are hit with lasers tuned to wavelengths 1 and 3, both atoms emit light of wavelength 2, he said.

This allows the atoms to be coupled by quantum entanglement. When two atoms are entangled, a change in the state of one is immediately reflected by a corresponding change in the other regardless of the physical distances between the atoms.

An atom can serve as a quantum bit, or qubit, because it spins in one of two directions, and its spins can represent the ones and zeros of binary computing. Because isolated bits are of little use, linking atoms is a prerequisite for quantum computing.

The researchers expect their spectral hole burning technique to yield 300 or more qubits, Shahriar said. That number is significant because a 300-qubit quantum computer would be able to factor numbers larger than any conventional computer will likely ever be able to handle.

"The experiment is already in progress. We have already demonstrated that each atom has the two-color response that we need. We have already demonstrated how we can line [the atoms] all up to be spinning in the same direction. That's the starting point of the quantum computer," Shahriar said.

How long the qubits last is as important as the number of qubits. Qubits are fragile because the slightest influence from the outside environment can knock the atoms out of their quantum state. The nitrogen-infused diamond spectral hole burning technique would probably last long enough to yield 40,000 quantum operations, Shahriar said.

"You need to be able to do more operations, but there are ways to increase that number," he said.

The other early favorites in the race for solid-state quantum computing are techniques based on superconductors, electron spins in quantum dots and nuclear spins in semiconductors.

"It's very important to pursue a lot of different things at this stage because it's very unclear exactly what type of hardware is going to be useful in the long run," said John Preskill, professor of theoretical physics and director of the Institute for Quantum Information at the California Institute of Technology. "So it's a healthy thing that there are a lot of different ideas floating around, spectral hole burning being one of them."

The first step toward solid-state quantum computers is demonstrating good control over a qubit in a system "which has at least the potential to be scaled up," Preskill said.

Other researchers have demonstrated seven-qubit systems using nuclear magnetic resonance (NMR). However, NMR techniques are not expected to scale up significantly, hence the race to develop solid-state quantum computing. Solid-state devices are based on semiconductors or other crystalline solids.

Schemes that are good candidates for quantum computing should support reliably readable results, reliable preparation of the initial states of their qubits, and logic gates with good fidelity, Preskill said. NEC researchers in Japan have gone the furthest in solid-state quantum computing with a superconducting implementation in which they have established a qubit, he said.

The nitrogen-diamond spectral hole team is in the last year of a three-year project to establish the viability of the technique, Shahriar said.

"We expect to demonstrate quantum entanglement within nine months," he said. "At the end of the next three-year [period] we expect to have at least 10 of these atoms coupled to one another. And that'll be a pretty significant step."

Though useful quantum computers are at least 20 years away, quantum information processing could be used for secure communications in five to ten years, Shahriar said.

Shahriar's colleagues are Philip R. Hemmer of the U.S. Air Force, Seth Lloyd and Jeffery A. Bowers of MIT, and Alan E. Craig of Montana State University. The research is funded by the Air Force Office of Scientific Research, the Army Research Office and the National Security Agency.

Timeline: 5-10 years; >20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper "Solid State Quantum Computing Using Spectral Holes" posted on the Computing Research Repository (CoRR) at arxiv.org/abs/quant-ph/0007074

TRN

Ordinary Light Could Drive Quantum Computers

By Eric Smalley, Technology Research News
January 31, 2001

One reason quantum computers are not likely to show up in your neighborhood electronics store any time soon is the laboratory equipment needed to build today's prototypes is hard to come by and difficult to use.

With some improvements to a couple of key devices, though, that could change. Thanks to a scheme concocted by researchers at the Los Alamos National Laboratory, researchers should be able to build quantum computers using common linear optics equipment.

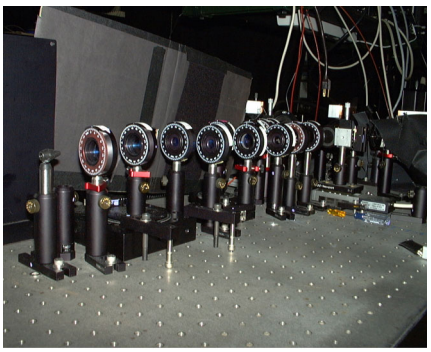
Practical quantum computers could be developed sooner with the means for building prototypes within reach of a

greater number of researchers. Quantum computers are expected to solve certain problems like cracking codes and searching large databases much faster than any other conceivable computer.

To achieve quantum computing, researchers manipulate the quantum states of photons or atoms to perform logic operations. Photon manipulation traditionally requires nonlinear optics methods, which use powerful lasers to coax photons from special materials.

The effect the lasers have on the atoms of these materials increases faster than the increase in intensity of the light. Ordinarily, the effect is proportional. This nonlinearity produces strange phenomena, like entangled pairs of photons, that are useful for quantum computing.

"We show that nonlinear optical elements can be simulated using linear optics and photo-detectors, a very surprising result," said Emanuel Knill, a mathematician at Los Alamos National Laboratory. "It opens up an entirely new path toward realizing quantum computers."



Source: Los Alamos National Laboratory

Common linear optics equipment like these beam splitters and phase shifters could be used to build quantum computers.

Quantum computers based on the Los Alamos linear optics scheme would create quantum bits, or qubits, by using two opposite conditions of individual photons to represent the 0 and 1 values used in binary computing.

There are two sets of opposite conditions. The first is the two possible paths a photon can take when it encounters a beam splitter. The second is either of two pairs of polarizations. Photons are polarized, or oriented, in one of four directions: vertical, horizontal, and two diagonals. Each polarization is paired with its opposite: vertical with horizontal and diagonal with diagonal.

Multiple bits can be used to represent larger numbers. Four bits can represent 24 or 16 numbers and 24 bits can represent 224 or more than 16 million numbers. Ordinary computers process these numbers one at a time. So, for example, in order to find one number out of 16 million an ordinary computer will have to look through an average of eight million numbers.

What makes a qubit different from an ordinary bit is that it can be in a third state, the quantum mechanical condition of superposition, which is essentially a mix of both 0 and 1. This means it's possible to perform a series of quantum mechanical operations on a series of qubits all at once. For some applications, the number of quantum mechanical operations is exponentially smaller than the number of steps required for a classical computer.

The quantum mechanical operations are sequenced to make up logic gates, which perform the basic mathematics of computing. Most quantum logic gate schemes require particles in more complicated quantum arrangements like entanglement. According to Knill, however, it is possible to create logic gates by manipulating the photons that are in the superpositions created by the linear optics.

Quantum computers based on photons rather than atoms will be easier to network because there will be no need to transfer quantum information between atoms and photons. "The only realistic proposals for long distance quantum communication are based on photons," Knill said.

Before the scheme can be implemented, however, researchers will need to improve both the light source and the photon detector. Two recently developed single-photon emitters hold out the promise that the necessary equipment could be available to researchers within a few years, said Knill.

"I think it's a neat idea," said John Preskill, professor of theoretical physics and director of the Institute for Quantum Information at the California Institute of Technology. "Any theoretical ideas that help make realizations of quantum logic technically less demanding might turn out to be important ideas."

Preskill led a research team that proposed a different scheme for quantum computing using linear optics, though that scheme requires its initial state to be prepared using nonlinear optics.

"There have been a lot of previous discussions of using information encoded in photons to [make] universal quantum gates, but always involving some kind of nonlinear coupling between photons, and those are hard to manage," said Preskill. "The stuff that Knill et al are talking about in principle is much easier. It uses tools that are available in lots of laboratories," he said.

Despite the potential for linear optics to speed things up, it would be a significant achievement if in 25 years a quantum computer can solve problems that are beyond the reach of classical computers, said Knill.

"Quantum computation by any means is a long way off," he said. "Our proposal adds to the tool box of possible experimental realizations, which may help speed things up. The fact is, the necessary experiments are extremely demanding."

Knill's research colleagues were Raymond Laflamme of Los Alamos National Laboratory and Gerard J. Milburn of the University of Queensland in Australia. They published the research in the January 4, 2001 issue of Nature. The research was funded by the Department of Energy and the National Security Agency.

Preskill's research colleagues were Daniel Gottesman of the University of California at Berkeley and Alexei Kitaev of

Microsoft Research. Their work is scheduled the published in the journal *Physical Review A*. The research was funded by the Department of Energy and the Defense Advanced Research Projects Agency.

Timeline: 25 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "A scheme for efficient quantum computation with linear optics," Nature, January 4, 2001; Technical paper, "Encoding a qudit in an oscillator," arXiv.org/abs/quant-ph/?0008040

TRN

Quantum Scheme Lightens Load

By Eric Smalley, Technology Research News
October 16/23, 2002

Two years ago, scientists proved it possible to build a quantum computer from simple optical equipment commonly found in university classrooms and laboratories. Now researchers at Johns Hopkins University have refined the approach, reducing the amount of equipment linear optical quantum computers would need by about two orders of magnitude.

Quantum computers use the weird nature of particles like atoms, electrons and photons to perform many computations in parallel. If a big enough quantum computer could be built, it would far outstrip classical computers for solving certain problems like cracking secret codes. So far, however, only the most rudimentary quantum prototypes have been constructed.

The Johns Hopkins plan shows that equipment like mirrors, half mirrors and phase shifters could be used to make practical, photon-based quantum computers, said James Franson, principal staff at the Johns Hopkins University Applied Physics Laboratory and a research professor the university's electrical and computer engineering department. "Our approach may make it more feasible to develop a full-scale quantum computer," he said.

Controlling single photons using linear optics equipment is simpler than manipulating individual or small numbers of atoms or electrons, which are the basic units of most other quantum computing schemes.

Capturing and manipulating atoms and electrons involves precisely tuned lasers or magnetic fields, or carefully constructed microscopic devices. It's also much harder to transport isolated atoms and electrons than it is to move photons. "An optical approach to quantum computing would have a number of potential advantages, including the ability to connect different devices using optical fibers in analogy with the wires of a conventional computer," said Franson.

Linear optical quantum computers, like ordinary electronic computers, would use circuits that link simple logic devices in intricate patterns that make the output from one device the input to the next. The 1s and 0s of linear optical quantum computing would be represented by properties of photons like horizontal versus vertical polarization rather than the presence or absence of a current of electrons.

The potential power of any type of quantum computer comes from its ability to examine all possible solutions to a problem at once rather than having to check one at a time.

This is possible because when a particle like a photon is isolated from its environment it is in the weird quantum state of superposition, meaning it can be horizontally and vertically polarized at once, and so can represent a mix of 1 and 0. This allows a string of photons in superposition to represent every combination of 1s and 0s at the same time so that a quantum computer could process all the numbers that represent possible solutions to a problem using one set of operations on the single string of photons.

Linear optical devices perform quantum logic operations by altering photons according to probabilities. Half mirrors, or beam splitters, for example, can direct photons along one of two paths, with an even chance for each path.

The challenge of linear optical quantum computing is to pass the correct result of a quantum logic operation from one device to the next without directly observing the states of the photons that represent the results, because this would change the states and therefore destroy the information the photons contain.

The trick is to put additional photons through the logic operation at the same time. These additional, ancilla photons trigger the optical circuitry that passes along the output of the logic operation when the result of the operation is correct. The ancilla photons are absorbed in photon detectors in the circuitry, but the output photons are preserved and passed on.

The key advance in the Johns Hopkins researchers' approach is that it uses fewer ancilla photons by entangling input and ancilla photons in a way that minimizes the probability of errors, said Franson. When two or more particles in superposition come into contact with each other, they can become entangled, meaning one or more of their properties change in lockstep even if the particles are separated.

Fewer ancilla photons means fewer pieces of equipment are needed. "Using the current error correction techniques, our high-fidelity approach should reduce the [equipment] required by roughly two orders of magnitude," said Franson. The amount of equipment required to generate the entangled ancilla state and the probability of an error "both increase rapidly with increasing numbers of ancilla photons," he said.

The original linear optical quantum computing scheme had an average error rate of 2/n, while the researchers' refined scheme has an average error rate of 4/n2, according to

Franson. N represents the number of ancilla photons. This translates to error rates of 20 percent versus 4 percent for 10 ancilla photons, and 2 percent versus 0.04 percent for 100 ancilla photons.

This gives the Johns Hopkins scheme a practical error rate with far fewer ancilla photons, said Franson. Quantum error correction will require error rates on the order of 0.1 to 0.01 percent, he said. "That range of errors could be achieved with 100 ancilla in our case, but that would require 5,000 ancilla in the original... method."

Because the scheme requires fewer mirrors and beam splitters to manipulate the smaller number of ancilla photons, it makes it more likely that a practical linear optical quantum computer could be built, said Jonathan Dowling, supervisor of the quantum computing technologies group at NASA's Jet Propulsion Laboratory. The researchers' method "seems to be a substantial improvement over the original scheme," he said.

Devices enabled by this new approach will be used in quantum communications systems before they are used in full-blown quantum computers, said Dowling. With experience gained from making quantum communications devices, the researchers' approach will eventually lead to "a practical, compact, all-optical quantum computer," he said.

Dowling's group has developed a plan for a quantum repeater, a device necessary to boost quantum communications over long distances, that is based in part on the researchers' linear optical quantum logic, said Dowling.

The researchers have shown that the overhead needed to achieve a given fidelity for linear optical quantum logic gates can be significantly improved, said Emanuel Knill, a mathematician at Los Alamos National Laboratory and one of the scientists who developed the concept of linear optical quantum computing.

The Johns Hopkins researchers' approach does not address logical qubits, however, said Knill. Logical qubits are encoded from two or more physical qubits, and this makes them more resistant to errors. "My preference is to use logical qubits," said Knill. "If one wishes to use physical, not logical, qubits, then the authors' approach would help significantly," he said.

Quantum repeaters could be developed in five years, said Franson. "Full-scale quantum computers would be much more difficult and would probably require 15 to 20 years in the most optimistic scenario," he said.

The researchers are working on making photon-based logic gates and memory devices, and single-photon sources, said Franson. "These are the basic building blocks of a linear optics approach to quantum computing," he said.

Franson's research colleagues were Michelle Donegan, Michael Fitch, Bryan Jacobs, and Todd Pittman. They published the research in the September 23, 2002 issue of the journal *Physical Review Letters*. The research was funded by the Office of Naval Research (ONR), the Army Research Office (ARO), the National Security Agency (NSA) and the Department of Defense (DOD) Independent Research and Development Program (IR&D).

Timeline: 5 years, 15-20 years
Funding: Government
TRN Categories: Physics Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "High-Fidelity Quantum Logic Operations Using Linear Optical Elements," Physical Review Letters, September 23, 2002

TRN

Laser Boosts Liquid Computer

By Eric Smalley, Technology Research News
October 24, 2001

The most advanced experimental quantum computers use the same technology medical magnetic resonance images use to make images of our insides.

MRIs make images of soft tissue by aligning the body's hydrogen atoms with a continuous magnetic field, and then using pulses from other magnets to knock the hydrogen atoms out of alignment in the areas being imaged. After each pulse, the atoms realign with the continuous magnetic field and in the process they emit radio waves whose frequencies are specific to different types of tissue.

Nuclear magnetic resonance (NMR) quantum computers make qubits, which represent the ones and zeros of computing, by flipping the orientations of atoms within the molecules of a liquid. However, it's extraordinarily difficult to read the spin flips of more than a half a dozen of these qubits, or quantum bits, at a time.

Although a growing number of researchers are calling NMR quantum computing a dead end, some who are pressing ahead with the technology have moved it a small step forward.

The seemingly insurmountable problem with NMR quantum computers is that as they gain more qubits the signals from the qubits get weaker and are eventually drowned out by the random noise of the system. The largest NMR quantum computer built to date consists of seven qubits. They're not likely to get much bigger using current designs, and it will probably take thousands of qubits to make a practical quantum computer.

A team of researchers at Stanford University and IBM Research, however, has found a way to strengthen the signals from a two-qubit NMR quantum computer.

Nuclear magnetic resonance devices manipulate atoms magnetically in order to detect them. When some types of atoms are placed in a strong external magnetic field, their nuclei emit radio signals. The nucleus of an atom behaves like a tiny magnet, a property called spin. In order for nuclear magnetic resonance to work, enough atoms have to be

polarized, or have their spins aligned either with or opposite an external magnetic field, that the collective signal cuts through the noise produced by randomly oriented atoms.

The signal decreases as the number of qubits increases in NMR quantum computers, said Anne S. Verhulst, a researcher at Stanford University. But because the NMR signals are "proportional to the polarization of the nuclear spins, our technique increases the signals. Hence we can allow more qubits before the signals disappear in the noise," she said.

To do this, the researchers mixed rubidium vapor with xenon gas and aimed a laser into the mixture. The laser light was circularly polarized, so that its electric field rotated. The laser polarized, or aligned the electrons of the rubidium atoms, which in turn polarized the xenon. The researchers then separated out the xenon, froze it into a liquid and mixed it with liquid chloroform. The xenon polarized some of the carbon and hydrogen atoms in the chloroform, and those atoms served as the stronger qubits in the researchers' quantum computer.

Boosting the polarization this way increased the strength of the spin signals by a factor of 10, said Verhulst. In order to use the scheme on a practical level, the researchers will have to increase the strength of the signals by 1,000 times and show that it works on computers made of more than two qubits, she said.

Despite the success of the initial results, the odds are still heavily against NMR yielding practical quantum computers. "Even though NMR quantum computers are the only ones existing so far, the problems related to the scaling issue are really huge. If one wants to make it work with liquids, then either some very special molecules or NMR technique or some additional source of high polarization has to be found, or a combination of all these things. And all of those are not straightforward to discover," she said.

The research doesn't have to lead to practical quantum computers to be useful, said John M. Myers, a project scientist at Harvard University, who helped build a 5-qubit NMR quantum computer in 1999.

"What is worthwhile about this research is the advance of molecular control," said Myers. "The techniques of NMR quantum computing can help to determine structures of large molecules, such as proteins. That is something special about NMR, in contrast to other quantum information processing schemes," he said.

It will take at least 15 to 20 years before practical quantum computers can be built, said Verhulst. "A lot of the efforts involve… nanofabrication, building extremely sensitive probes, trying to manipulate single electrons. And all of those are interesting for technological evolution as a whole," she said.

Verhulst's research colleagues were Oskar Liivak and Mark H. Sherwood of IBM Research, Hans-Martin Vieth of the Free University of Berlin, and Isaac L. Chuang now at the Massachusetts Institute of Technology. They published the research in the October 8, 2001 issue of the journal *Applied Physics Letters*. The research was funded by the Defense Advanced Research Projects Agency (DARPA).

Timeline: 15-20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Non-Thermal Nuclear Magnetic Resonance Quantum Computing Using Hyperpolarized Xenon," Applied Physics Letters, October 8, 2001

TRN

Electron Teams Make Bigger Qubits

By Eric Smalley , Technology Research News
September 10/17, 2003

One of the biggest challenges in building quantum computers is making quantum bits that are small enough to have the requisite quantum behavior, yet large enough to be reliably controlled by electronic circuits.

Quantum bits, or qubits, use traits of particles like electrons or photons to represent the 1s and 0s of computing. An electron can serve as a qubit because it is oriented in one of two directions, spin up and spin down.

Researchers from the University of Basel in Switzerland and the University of Pittsburgh have come up with a candidate qubit made from groups of electrons rather than harder-to-control single electrons.

The researchers have shown that as long as a spin cluster is made up of odd numbers of electrons it can behave like a single electron, according to the Florian Meier, a researcher at the University of Basel.

The method can potentially produce qubits that are relatively easy to control.

Spin clusters are groups of electrons that are close enough to each other that their spins are aligned. In cases where spin alignment is antiferromagnetic, meaning the magnetic orientations alternate from one electron to the next, spins from an even number of electrons cancel each other out and for odd numbers of electrons there is a net spin equivalent to the spin of one electron.

Electron spins are promising candidates for qubits because they can be built into computer chips, they are relatively well insulated from environmental disturbances like electronic noise and heat, and existing techniques allow electron-spin qubits to be controlled by magnetic and electric fields.

In practice, however, controlling magnetic and electric fields at the scale of individual electrons is extremely challenging, said Meier. The researchers' method eases the burden by widening the focus to a set of electrons rather than just one. "The conditions on local control of electric and magnetic fields are substantially relaxed," said Meier. "For quantum

computing with electron spins in quantum dots, magnetic and electric fields need not be controlled on the length scale of 50 nanometers, but only on typical scales of 250 nanometers."

The placement of the spins and the size of the cluster can also vary considerably, he said.

Quantum computers gain their power from the weird traits of particles like electrons. When an electron is isolated from its environment, it enters into superposition, which is some mix of spin up and spin down. This allows a long enough string of qubits to represent every possible answer to a problem. The power of a quantum computer comes from being able to check all of the possible answers using a single set of operations instead of having to checking them one by one as is done by classical computers.

Quantum computers based on spin cluster qubits would work the same way as quantum computers made of single-spin qubits, said Meier. "Although the cluster is composed of many spins, with respect to its magnetic properties the large cluster behaves very similarly to a single electron spin," he said.

The researchers have shown theoretically that spin cluster quantum computers can use the same techniques for initialization, gate operation, error correction and readout as quantum computers that use single electron spins.

Spin-cluster-qubits can be made using any of a wide range of artificial magnetic molecules that have been synthesized during the past decade, said Meier.

Though such spin cluster hardware would be smaller than quantum dots, which are microscopic bits of semiconductor material used to trap electrons for some quantum computing schemes, they are easier to produce, he said. "Nature provides identical copies of these systems."

The researchers' next step is to form one-and two-qubit quantum gates using spin cluster qubits, said Meier. The main challenge in making practical spin cluster qubits is developing a method for measuring the tiny magnetic orientations produced by single-electron spins, he said. Practical, general-purpose quantum computers are 20 years away, according to Meier.

Meier's research colleagues were Jeremy Levy from the University of Pittsburgh and Daniel Loss from the University of Basel. The work appeared in the January 31, 2003 issue of *Physical Review Letters*. The research was funded by the University of Basel, the University of Pittsburgh, the European Union, the Defense Advanced Research Projects Agency (DARPA) and the Swiss National Science Foundation.

Timeline: 20 years
Funding: Government, University
TRN Categories: Quantum Computing and Communications
Story Type: News
Related Elements: Technical papers "Quantum Computing with Antiferromagnetic Spin Clusters," posted on the physics archive at arxiv.org/abs/cond-mat/0304296, and "Quantum Computing with Spin Cluster Qubits," Physical Review Letters, January 31, 2003

TRN

Atom Clouds Ease Quantum Computing

By Eric Smalley, Technology Research News
January 16, 2002

Computers that use the internal properties of atoms to perform calculations promise to solve problems that will always be impossible for classical computers, which compute using electrical current running through transistors made up of millions of atoms.

One of the challenges of building a quantum computer, however, is controlling matter and energy at the level of individual atoms and photons. First, these particles are fantastically small. The difference in size between a hydrogen atom and a ping pong ball is about the same as the size difference between a ping pong ball and the Earth. Add the complication that particles vibrate and flit about and it's not hard to see why it's so difficult to isolate and control them.

Researchers at Harvard University, the University of Kaiserslautern in Germany, the University of Connecticut and the University of Innsbruck in Austria have sidestepped the problem with a scheme for building quantum computers out of clouds of atoms.

"We do not need to control atoms one by one," said Mikhail Lukin, an assistant professor of physics at Harvard University.

Atoms act like tiny tops that spin either clockwise or counterclockwise. These two spin states can represent the ones and zeros of computer logic. Researchers can flip the value of these quantum bits, or qubits, between one and zero by switching the spin of the atom with a laser beam or magnetic field.

Atoms also contain magnetic fields with North and South poles that, like ordinary refrigerator magnets, either attract or repel each other. In both refrigerator magnets and atoms, these interactions cause the magnetic field around each magnet or atom to stretch. Atoms with stretched poles interact more strongly with other atoms.

When these dipole atoms are polarized, or lined up magnetically, they form a dipole blockade, said Lukin. "The interactions are so strong that not more than one single spin can be flipped in an entire atomic cloud. In this situation an entire small atomic cloud can behave as a single quantum bit," he said.

These atomic clouds are easier to work with than single atoms, and the quantum states of the atom clouds last for several seconds, which is long enough to perform the thousands or millions of individual operations needed for practical computing. The quantum states of individual

particles, in contrast, usually last only thousandths or millionths of a second.

A second challenge in making quantum computers is finding a way to transfer information from atoms to photons and back again in order to use the more mobile photons to transmit information. The larger target of a whole cloud of atoms should make this transfer easier to accomplish, said Lukin.

The atom cloud scheme can be used in a range of hardware that has been developed to corral individual atoms, including semiconductor devices and ions held in magnetic traps, according to Lukin.

A full-scale quantum computer is at least two decades away, according to many researchers in the field. "Whereas some minor applications could become technologically relevant within [a] five- to ten-year time-frame, a discussion of practical, full-scale quantum computers is very premature," said Lukin.

Even with the advantages of using clouds of atoms, the researchers' scheme may not lead to full-scale quantum computers because it uses light to link qubits, said Jonathan P. Dowling, supervisor of the quantum computing technologies group at NASA's Jet Propulsion Laboratory. "You have this limit that the light beams can't be any smaller than the wavelength of the light, and that's pretty big," he said.

Practical quantum computers would consist of hundreds of thousands or millions of qubits, said Dowling. "A scalable quantum computer, in my opinion, is not likely with these optical schemes," he said.

The scheme could be used for quantum communications repeaters, however, said Dowling. Repeaters, which boost fading communications signals, are what allow today's conventional communications lines to span long distances. Quantum communications, which carry information in specially prepared photons, would also require a series of repeaters in order to pass signals over long distances.

Lukin's research colleagues were Michael Fleischhauer of the Harvard-Smithsonian Center for Astrophysics and the University of Kaiserslautern in Germany; Robin Cote of the University of Connecticut; and Luming Duan, Dieter Jasch, Ignacio Cirac and Peter Zoller of the University of Innsbruck in Austria.

They published the research in the July 16, 2001 issue of the journal *Physical Review Letters*. It was funded by the Austrian Science Foundation, the European Union, the European Science Foundation, and the National Science Foundation (NSF).

Timeline: 5-10 years; Unknown
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Dipole Blockade and Quantum Information Processing in Mesoscopic Atomic Ensembles," Physical Review Letters, July 16, 2001

Qubits

Electric Switch Flips Atoms

By Eric Smalley, Technology Research News
February 13, 2002

Atoms and subatomic particles are like microscopic tops that can spin in one of two directions, up or down. Spintronics and quantum computing use these spin directions to represent the ones and zeros of digital information. Today's electronics, in contrast, use the presence or absence of electric charge to represent binary numbers.

A team of researchers from the Max Planck Institute and the Technical University of Munich in Germany has used an electronic switch to transfer the spin of a group of electrons to the nuclei of atoms in a semiconductor.

Information transfer between electrons and atoms is a key component of spintronics and quantum computing. Atoms in semiconductor crystals are better suited to preserving spin and thereby storing information than electrons because they are fixed in position and they are better insulated from the environment than electrons. Electrons, however, can flow in currents, which makes them better suited to transmitting information.

Computers based on spintronics would be faster, use less electrical power and store data more densely than electronic computers. Data would also remain in memory after the power was turned off, allowing spintronics computers to start instantly.

Quantum computers can use the interactions of individual particles to solve certain problems, like cracking secret codes and searching large databases, that are beyond the abilities of the fastest classical computer possible.

The researchers' experiment proved that it is possible to transfer spin between atoms and electrons, but a lot of work remains before the capability can be put to practical use, said Jurgen Smet, a scientist at the Max Planck Institute. The experiment "brings us one step closer, but we have a large number of giant leaps to go to make something useful and practical," said Smet. "We have succeeded... in a very crude manner for a large ensemble of nuclei, however under extreme conditions, like nearly absolute zero temperature and... a large, stationery magnetic field."

Ordinarily, the spins of electrons and atoms in a semiconductor are isolated from each other. The energy associated with electron spin is considerably greater than the energy associated with atomic spin, and this energy mismatch usually keeps the electrons from changing the atomic spin. But by using a gate, or electronic switch, to control the density of electrons in the semiconductor, the researchers found that at certain densities the interactions between electrons affect the spins of the semiconductor's atoms.

Atomic spins can also be flipped using magnetic fields, which is how hard disk drives in today's computers work.

But disk drives are larger, slower and require more energy than the integrated circuits on computer chips. "One would like all-electronic nuclear solid-state devices so that one can marry the benefits of the technology used in present-day electronics with those of quantum computation or spintronics," said Smet.

The researchers' experiment shows that electronic control of atomic spin in semiconductors is possible. However, their technique is unlikely to lead directly to practical technology, said Smet. "The physics we exploit to flip the nuclear spins actually also requires these low temperatures, so there is at least no straightforward rule on how to scale this up," he said.

Still, the research shows that spintronics could be a viable successor to today's electronics. "Atoms... are the smallest unit of which a semiconductor crystal is composed. If you were to extrapolate Moore's Law... you'll find that in the next decade or so we end up with a dimension on the order of the atom," said Smet. Moore's Law, which has held true for the past couple of decades, states that computer speeds double every 18 months as manufacturers shrink computer circuits. "Clearly a paradigm shift has to occur. That is one reason why long-term researchers fervently think about ways to explore the spin degree of freedom of the nucleus of atoms," he said.

Controlling atomic spin could also be used in quantum computing. But to do so, however, the researchers' technique would need to be applied to individual atoms. "This kind of control is not something we will manage to achieve within the next two decades," said Smet.

The researchers device serves as a miniature laboratory for probing the fundamental interactions between electrons and nuclei and exploring the basis for exchanging information between the two spin systems, said David Awschalom, a professor of physics at the University of California at Santa Barbara. "This is a beautiful experiment," he said. "Many people envision that future quantum computing will use nuclear spins for information storage, and thus it is important to explore these basic interactions."

Smet's research colleagues were Rainer Deutschmann, Frank Ertland and Gerhard Abstreiter of the Technical University of Munich, Werner Wegscheider of the Technical University of Munich and the University of Regensburg, and Klaus von Klitzing of the Max Planck Institute. They published their research in the January 17, 2002 issue of the journal *Nature*. The research was funded by the German Ministry of Science and Education (BMBF) and the German National Science Foundation (DFG).

Timeline: > 20 years
Funding: Government
TRN Categories: Materials Science and Engineering; Quantum Computing
Story Type: News

Related Elements: Technical paper, "Gate-Voltage Control of Spin Interactions between Electrons and Nuclei in a Semiconductor," Nature, January 17, 2002

TRN

Semiconductors Control Quantum Spin

By Eric Smalley, Technology Research News
December 12, 2001

An electron is like an infinitesimal top spinning either clockwise or counterclockwise. The two directions can represent the ones and zeros of computing, which has tempted researchers to find new ways to build computers.

The possibilities range from ultra-powerful quantum computers to ordinary computers that require far less electricity. The trick is being able to control the direction of the particles' spin.

A research team based at the University of California at Santa Barbara has built a semiconductor device that uses an electric field to rapidly reverse the spin of electrons confined to an area 10,000 times smaller than the head of a pin. The device can change the spin of an electron in less than a millionth of a second.

The research shows it is possible to use conventional electronics to construct a 'spin gate' that controls the electron spin, said David D. Awschalom, a physics professor at the University of California at Santa Barbara. The technology can be applied "rapidly, locally and with conventional technologies," he said.

The key advantage of controlling spin in a semiconductor device is that thousands or millions of the devices could be combined to make a new kind of computer processor in the same way that millions of transistors make up today's computer chips.

Today's computers use the charge of electrons—the presence or absence of an electric current in a circuit—to represent the ones and zeros of computing. But in order to store digital information, the ones and zeros have to be translated into the positive and negative fields of tiny bits of magnetic material in disk drives.

Spin, however, could be used for both processing and storing information. Spintronic computers would be much faster than today's computers because they could store information without using magnetic disk drives, which are much slower than computer chips, and they would require much less power. Longer term, controlling electron spin could make it easier to use the weird quantum properties of the particles to build phenomenally powerful quantum computers.

The researchers achieved their high degree of control over electron spin using a quantum well—a relatively simple

microscopic device made from layers of semiconductor material.

Electrons ordinarily either orbit an atom or hop from one atom to another. This hopping behavior is what allows electrical current to flow through a wire. Quantum wells catch electrons in flight and hold them in place. "Quantum wells are nanometer-scale structures used to trap electrons in specific locations. They are the basis for many of today's electronic devices, such as the laser in your CD player," Awschalom said.

The researchers shaped their quantum well like a parabola instead of the usual box shape, said Awschalom. The quantum well is made from a mixture of the semiconductors gallium arsenide and aluminum gallium arsenide and is 100 nanometers wide, or about one-tenth the width of an E. coli bacterium. A nanometer is one millionth of a millimeter.

The researchers created the parabolic shape by gradually varying the concentration of aluminum across the quantum well, with the lowest concentration at the center and the highest at the edges. The researchers moved electrons within a well by turning on an electric field and varying its strength.

The speed and direction of an electron's spin in the quantum well is related to the concentration of aluminum; by moving electrons to specific positions in the well the researchers were able to speed up, stop and reverse their spins. Most importantly, the researchers were able to move the electrons without changing their wave functions, which could allow the electrons to serve as a quantum bit, or qubit, said Awschalom.

One of the weird aspects of quantum physics is that when an electron is isolated from its environment it is in superposition, meaning it is in some mixture of both spin directions and it has some chance of being at any given point in the quantum well. The mathematical map of these possibilities is the particle's wave function. When the electron is observed or otherwise comes into contact with its environment, it's wave function collapses and it assumes a definite position and spin direction.

Multiple particles in the same space have a combined wave function, which is the case for the electrons in the researchers' quantum well.

The challenge for quantum computing is to preserve this fragile state of superposition while manipulating it to perform computations. In the researchers' device, moving the electrons changes their spins, which is the manipulation needed for computing, but preserves the wave function.

The reward for achieving precise control of particle spin is tremendous. A series of qubits that are in superposition can represent every binary number that has as many or fewer digits than the number of qubits. For example, three qubits can represent eight different binary numbers and 25 qubits can represent 33,554,432 binary numbers.

The wave functions of a series of qubits can also be linked, or entangled. When changes are made to one entangled particle, they all change the same way regardless of the physical distance between them, as long as they remain in superposition.

Using this bizarre property, quantum computers could examine every possible answer to a problem with one series of operations rather than having to check each individually, which means they could solve problems that would be impossible for the most powerful classical computer conceivable.

Quantum computing algorithms are sequences of single-qubit and two-qubit operations. The single-qubit operation—reversing the spin of an electron—is essentially what the researchers' spin gate does, said Michael E. Flatté, an associate professor of physics at the University of Iowa. Though the researchers have not demonstrated single-qubit operations yet, "their work indicates a plausible path to them," he said.

The researchers' next major objective is to entangle an array of qubits, said Awschalom. Entangling at least two qubits would allow for two-qubit operations; large numbers of entangled qubits would be necessary to make a practical quantum computer.

The spin gate could be used in practical applications in 10 to 20 years, said Awschalom.

Awschalom's research colleagues were Gian Salis, Yuichiro Kato, Dan C. Driscoll and Art C. Gossard of the University of California at Santa Barbara, and Klaus Ensslin of the Swiss Federal Institute of Technology. They published the research in the December 6, 2001 issue of the journal *Nature*. The research was funded by the Defense Advanced Research Projects Agency (DARPA), the Office of Naval Research and the National Science Foundation (NSF).

Timeline: 10-20 years
Funding: Government
TRN Categories: Materials Science and Engineering; Quantum Computing
Story Type: News
Related Elements: Technical paper, "Electrical Control of Spin Coherence in Semiconductor Nanostructures," Nature, December 6, 2001

TRN

Oversize Oddity Could Yield Quantum Computers

By Eric Smalley, Technology Research News
November 15, 2000

As it turns out, quantum effects don't have to be confined to the world of atoms and subatomic particles. Research efforts have shown quantum effects in electrical currents of thousands to millions of electrons, a result that raises hopes

for building quantum computers that can solve problems that are impossibly difficult for ordinary computers.

Researchers at Delft University of Technology in the Netherlands are one of two teams to produce a superposition in a superconducting quantum interference device (SQUID). Superposition is the quantum mechanical effect in which an atom or particle is in two different states simultaneously.

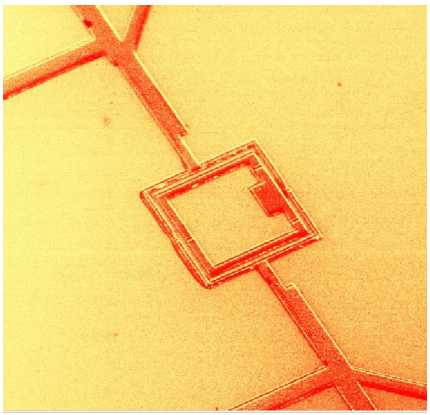
SQUIDs are tiny loops of superconductor that, when exposed to a magnetic field, carry an electrical current. Superposition in this case is a single set of electrons flowing in both directions at the same time.

"In our system the current can run both ways at the same time, so it has the potential to act as a qubit," said Casper van der Wal, a graduate student at Delft University of Technology. A qubit, or quantum bit, has two distinct states that can represent the ones and zeros of binary computing.

In the quantum state, the current flow of a SQUID has a certain probability of being in one of the two directions. A quantum computer would act on a set of SQUIDs by influencing their probabilities (posing the problem) so that when the SQUIDs leave their quantum state the resulting flow directions would represent a specific number (getting the result).

Researchers at the State University of New York at Stony Brook have created a superposition of a larger current flow in a SQUID. The current flow in the SUNY Stony Brook SQUID contains billions of electrons while the current flow in the Delft device contains millions of electrons.

"Our system is better in terms of testing the limits of quantum mechanics on the macroscopic scale," said Jonathan R. Friedman, a postdoctoral researcher in the department of physics and astronomy at SUNY Stony Brook. "The Delft device may have some advantages in terms of usefulness for quantum computation."



Source: Delft University of Technology

The square in the middle is a six nanometer superconductor loop that carries electrical current made of thousands of electrons.The breaks in the loop cause the electrons to behave as a single, giant particle.

The advantage lies in the number of breaks in the SQUID's superconducting loop. The breaks, called Josephson junctions, cause the flow of electrons to behave as a single, giant particle. The SUNY Stony Brook device uses a single junction and the Delft device uses three.

"Using three junctions allows for making the loop much smaller than a one-junction loop. Thereby the system can be better isolated from noise," said van der Wal. Quantum states are easily destroyed by influences from their environments, so quantum computers' quantum components will need to be well insulated.

Also, quantum computers' qubits will need to be linked. The qubits in SQUIDs-based quantum computers would most likely be linked by inductive coupling.

"Controlled inductive coupling means that the magnetic field produced by one loop can be picked up by a neighboring loop such that the behavior of the two depends on each other," said van der Wal. "We can engineer the strength of this coupling and probably make it even tunable. This is the main advantage of our system with respect to microscopic systems like atoms. Our microfabricated system allows for much more engineering of the system's parameters. The parameters of atoms are set by nature."

Though quantum computers are probably decades away, enough progress has been made that most research efforts are now focused on making practical devices.

"The big advantage about SQUIDs is that they can be fabricated en masse on a chip. Large-scale integration is quite conceivable," said Friedman.

The Delft team has produced chips containing many loops. However, just putting a bunch of loops on a chip falls far short of producing a working quantum computer.

"We [first have to prove] that we can push the control over individual systems to much higher precision than what we could do in our last experiment," said van der Wal. "On the way there we could run into fundamental physical phenomena that [show quantum computing] will never work at all with our loops."

It will likely be 20 to 30 years before SQUIDs-based quantum computers could be commercially available, said van der Wal. "It is like the path from experimental Nuclear Magnetic Resonance machines... in 1946 to MRI machines in hospitals [in] 1982," he said.

Van der Wal's colleagues were A. C. J. ter Haar, F. K. Wilhelm, R. N. Schouten, C. J. P. M. Harmans and Johan E. Mooij of Delft University of Technology, and Terry P. Orlando and Seth Lloyd of the Massachusetts Institute of Technology. They published their work in the October 27, 2000 issue of the journal *Science*.

The research was funded by the Dutch Foundation for Fundamental Research on Matter, the European Union Training and Mobility for Researchers Research Network on Superconducting Nanocircuits, and the U.S. Army Research Office.

Timeline: 20-30 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements:Technical paper "Quantum Superposition of Macroscopic Persistent-Current States" in Science Oct. 27, 2000

Quantum Bit Hangs Tough

By Eric Smalley, Technology Research News
January 17, 2001

Efforts aimed at building quantum computers face a common nemesis: noise.

The fragile arrangements of atoms and subatomic particles that make up today's rudimentary prototypes are easily disabled by small amounts of energy from the environment. Researchers at the National Institute of Standards and Technology (NIST) have built a quantum bit (qubit) that is immune to a key form of decoherence, or noise.

The Decoherence Free qubit can store a single bit's worth of information. It could also serve as the basic building block of a practical quantum computer.

The NIST team created the qubit in an ion trap, which is a device that uses radio waves and electric fields to suspend ions in space. The researchers trapped two beryllium ions and then used lasers to control how the ions were spinning and interacting with each other.

An atom or subatomic particle can serve as a qubit because it spins in one of two directions, which can represent the ones and zeros of binary computing. Quantum computers are potentially much more powerful than ordinary computers for certain applications because atoms and subatomic particles can exist in the quantum mechanical state of superposition in which they are essentially spinning in both directions at the same time. This allows a relatively small number of qubits to represent very large numbers.

The catch is that particles exist in quantum states for only tiny fractions of a second before decoherence sets in. Because a practical quantum computer will need to perform thousands of operations on its qubits, making them last is critical.

One way to make them last is to create Decoherence Free Subspaces (DFSs), which are essentially noise-free zones. When two or more physical qubits are subjected to the same noise, it's possible for a subset of their possible states to be immune to the noise. Researchers can use these protected states to create logical qubits.

The principal form of decoherence in the NIST ion trap is dephasing, which is the condition in which the ions' energy levels fluctuate randomly, said David Kielpinski, a research assistant at NIST.

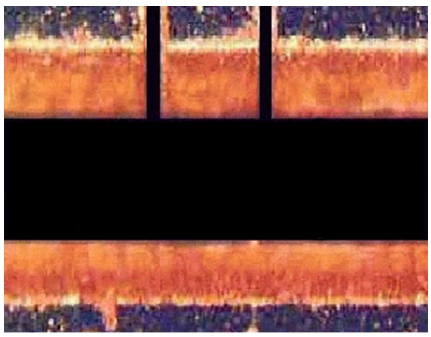
"What we demonstrated in our paper was that there are these two states and they are resistant to collective dephasing, and any superposition of these two states is resistant to collective dephasing," he said. "That makes one qubit which is resistant to collective dephasing."

The researchers showed that the Decoherence Free qubit lasted about three times as long as an unprotected qubit.

"The work by the NIST group is a crucial step towards employing noise-free methods in quantum computation," said Paul Kwiat, a physics professor at University of Illinois.

In October, Kwiat and a team of researchers at Los Alamos National Laboratory reported the first experimental verification of DFSs. Their experiment involved two photons and yielded a single decoherence free state.

Though the NIST results are significant, a mere tripling of the qubit's very short lifetime is not sufficient by itself for practical computing, said Kwiat. "Any system that you eventually come up with will have some residual [noise] effects so that using these decoherence-free methods will never be the whole story," he said.



Source: NIST

This device uses radio waves and electric fields to trap and hold ions suspended in space. The horizontal gap is two-tenths of a millimeter from top to bottom. Researchers can use the trapped ions as quantum bits. Note: the original image was a composite that included this image.

An alternative to DFSs are quantum error correction schemes, which essentially clean up errors introduced by decoherence. However, quantum error correction codes would require a lot of computer power. The ultimate answer will likely involve combining DFSs and quantum error correction, said Kwiat.

The NIST team's long-range plan is to build a practical quantum computer by linking many ion traps. "In our particular idea of how large-scale quantum computing would work, you want to be shuttling your qubits around over fairly big distances in space," said Kielpinski.

DFSs could play a key role because even though moving ions around in space subjects them to potentially destructive changes in the environmental energy, pairs of ions will experience the same changes and therefore could preserve DFSs.

It will likely be 20 years before quantum computing of any kind becomes practical, said Kielpinski.

Kielpinski's research colleagues were Volker Meyer, Mary A. Rowe, Cass A. Sackett, Wayne M. Itano and Dave J. Wineland of NIST, and Christopher Munro of the University of Michigan. They published the research in the January 4, 2000 issue of *SciencExpress*. The research was funded by the National Security Agency, the Office of Naval Research and the Army Research Office.

Timeline: 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "A Decoherence-Free Quantum Memory Using Trapped Ions," SciencExpress, January 4, 2000

Quantum Bit Withstands Noise

By Eric Smalley, Technology Research News
September 26, 2001

The everyday world we see around us rests on a foundation of atoms and subatomic particles and the interactions among them. Separated from the world at large, these particles behave according to a very different set of rules than the laws of physics we experience.

Physicists have been able to study quantum mechanics by isolating particles for fleeting moments, and what they have found has led some to devise schemes to make extraordinarily powerful computers by harnessing the bizarre behavior of the particles.

The main challenge to making useful quantum computers is being able to isolate the delicate particles from environmental energies, or noise, like radio waves, magnetic fields, and light for more than small fractions of a second.

"Because it is virtually impossible to isolate a real-world quantum system from its environment, decoherence is practically ubiquitous," said Lorenza Viola, a postdoctoral fellow at the Los Alamos National Laboratory.

Decoherence happens when noise from the environment intrudes on quantum particles' isolation, changing the quantum mechanical properties used to store information in quantum computing.

A team of researchers from Los Alamos National Laboratory and the Massachusetts Institute of Technology has come up with a way of fending off decoherence by using environmental noise rather than trying to block it.

Quantum computers use isolated atoms or subatomic particles to form quantum bits. Qubits, like bits in classical computing, have two positions that can represent the ones and zeros of binary logic, which is the basis of nearly all computers. For instance, an electron can be used as a qubit because, like a top, it can spin in one of two directions: spin up or spin down.

One of the strange qualities of quantum particles is that when a particle is isolated from its environment, which by definition means it cannot be observed directly, it acts differently from a particle that is not isolated and can be observed. An isolated particle is in superposition, which is some unknown mixture of all possible states. For example, an electron in superposition could be 1 percent spin up and 99 percent spin down or 50 percent spin up and 50 percent spin down.

The advantage of using a string of qubits in superposition to represent data is that it can effectively represent many numbers at once. A string of seven qubits could represent all 128 of the seven-digit combinations of spin up and spin down. Ten qubits could represent 1,024 combinations, and 15 qubits, 32,768 combinations at once. Classical bits can represent the same number of combinations, but must go through the combinations one at a time to find, for example, a combination that represents a solution to a problem.

One way of preserving qubits long enough for them to perform these useful computations is to control environmental noise in a way that leaves sheltered zones where some qubits can be protected. "If one has a bunch of qubits and, say, the noise affects all but the first qubit, then the information carried by qubit one is clearly preserved," said Viola.

One way of doing this is by making one logical qubit out of the interactions, or waves generated by several particles, rather than protecting the data in one physical qubit.

Quantum particles behave like both particles and waves. The geometrical shape of a particle's wave, its wave function, can be symmetrical, just like the left and right sides of a person. Interacting particles have a common wave shape, and when noise from the environment affects all of the particles equally, the shape of their collective wave contains symmetries.

The Los Alamos and MIT team has made a type of sheltered zone called a noiseless subsystem that makes a qubit out of the symmetries in the collective wave function of a set of three carbon atoms.

Using the wave function symmetries of quantum particles to store information requires more than one particle to represent a logical qubit, but that qubit preserves quantum information in the face of noise better than a qubit made of a characteristic like spin in a single particle. In fact, the noise that produces wave symmetries would be enough to destroy any single-particle qubit.

An earlier scheme demonstrated by the researchers at the National Institute of Standards and Technology (NIST) also uses sheltered zones and makes logical qubits from wave symmetries. The decoherence-free subspaces scheme uses noise to produce symmetries that do not otherwise affect the underlying set of particles. The scheme is also less complicated than noiseless subsystems, but it requires more precisely controlled noise, said Viola. They also require at least four particles per qubit, while the noiseless subsystem needs only three.

The noise that produces the wave symmetries in the noiseless subsystem scheme does change the quantum characteristics like spin in the underlying set of particles, which makes them more difficult to produce than decoherence-free subspace qubits, said Daniel Lidar, an assistant professor of chemistry at the University of Toronto.

On the other hand, noise that affects the particles is more common than noise that does not, which means noiseless subsystem qubits are potentially easier to sustain in the real world, said Viola. "Assuming the ability to identify or engineer quantum devices with the correct symmetries, noiseless subsystems would allow for more options in implementing robust [quantum] memories simply because noiseless subsystems are more common than decoherence-free subspaces," she said.

In addition, noiseless subsystems can be combined with a broader range of quantum error correction codes than decoherence-free subspaces, Viola said. Error correction codes catch errors that occur when one or more bits accidentally change from a one to a zero or vice versa.

The research is a significant step towards robust scalable quantum computing, said Lidar. As expected, noiseless subsystems produce a significant increase in coherence time for noise of arbitrary strength, he said. "The result holds for engineered noise, and hence its utility in real life remains to be seen," he said.

Although fewer particles are needed to encode qubits using noiseless subsystems than decoherence-free subspaces, the encoding process is somewhat more complicated, Lidar said. "A very valuable lesson learned from the [research] is that the encoding/decoding steps can take a significant amount of time and contribute to coherence degradation," he said.

The issue of number of particles versus ease of encoding presents researchers with a trade-off to consider when choosing between noiseless subsystems and decoherence-free subspaces, said Paul Kwiat, a physics professor at the University of Illinois at Urbana Champaign. "The trade-off of which is easier to deal with will depend on the particular system used for quantum computing."

Though the concept of noiseless subsystems might be important in developing quantum computers, the particular noiseless subsystem the Los Alamos and MIT researchers produced is not practical because it was created using Nuclear Magnetic Resonance (NMR) techniques, he said. NMR, which is also used for medical imaging, uses strong magnetic fields to align atoms.

NMR quantum computing "is now accepted not to be true quantum computing" because NMR quantum computers cannot be made with more than a few qubits, and they also cannot produce quantum entanglement, said Kwiat.

Particles in superposition can also be linked, or entangled, so that they share one or more quantum characteristics like spin; if environmental noise knocks an electron out of superposition and into the spin up position, an electron that was entangled with it also leaves superposition in the same spin up position, regardless of the physical distance between them. Entanglement would give practical quantum computers the ability to do many calculations efficiently.

The technique can be used in other quantum computer architectures, including trapped ions and solid-state quantum chips, according to Viola.

Practical applications of quantum information processing for cryptography and simulating quantum mechanics could be achieved in the next few years, said Viola. However, full-blown quantum computers that are able to, for example, improve on current capabilities for factoring large numbers are probably more than 20 years off, she said.

Viola's research colleagues were Emanuel Knill and Raymond Laflamme of Los Alamos National Laboratory and Evan M. Fortunato, Marco A. Pravia and David G. Cory of the Massachusetts Institute of Technology. They published the research in the September 14, 2001 issue of the journal *Science*. The research was funded by the Department of Energy, the National Security Agency (NSA), the Army Research Office and the Defense Advanced Research Projects Agency (DARPA).

Timeline: 2 years, > 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Experimental Realization of Noiseless Subsystems for Quantum Information Processing," Science, September 14, 2001

TRN

Alternative Quantum Bits Go Natural

By Eric Smalley, Technology Research News
April 18, 2001

One of the first hurdles to developing practical quantum computers is coming up with devices that let researchers precisely control qubits, the individual atoms, electrons or photons that are the basic building blocks of quantum computers.

Controlling qubits usually involves minute, finely tuned and precisely aimed laser, microwave or magnetic pulses. These control operations are very difficult for even a single qubit and the task of controlling as few as 10 is daunting. Ultimately, practical quantum computers will require systems that can control at least several hundred qubits.

A team of researchers based at the University of California at Berkeley has come up with an encoding scheme that sidesteps the problem. The trick is making qubits out of the natural interactions of two or more particles rather than changing the behavior of individual particles. The researchers are proposing to fit computer logic to the natural actions of qubits, rather than forcing qubits to do conventional logic operations.

There are two basic requirements quantum computers must satisfy in order to perform all the binary logic operations of ordinary computers: controlling all possible quantum mechanical states of each physical qubit and quantum mechanically linking two or more physical qubits to form a Controlled-Not (CNOT) logic gate. A CNOT gate has a control bit and a target bit. If the control bit is 1, it flips the target bit from 0 to 1 or 1 to 0. If the control bit is zero, it leaves the target bit alone.

These requirements, outlined in a 1995 paper, have become a sort of bible of universal quantum computation, said Daniel

Lidar, an assistant professor of chemistry at the University of Toronto.

The trouble is, it's very difficult to make physical systems that can satisfy these requirements, he said. "In... quantum dots, for example, implementing the single-qubit operations can be very hard," he said.

In a quantum computer whose qubits are individual electrons trapped inside quantum dots, which are microscopic specks of semiconductor material, flipping a bit from a 0 to a 1 or a 1 to a 0 requires extreme accuracy, said Lidar. "You need to apply a very, very local, microscopically accurate magnetic field," he said.

This is where the Berkeley encoding scheme comes in. Rather than forcing physical qubits to perform these difficult operations, the researchers propose to use "what we call the natural talents of the physical system," said Lidar. "The paradigm shift that we're proposing is that you start with whatever is natural for [a given] system," he said. "You investigate whether the system as such is capable of implementing universal [quantum] computation."

In a quantum dot system, one natural operation is switching information between two neighboring quantum dots, said Lidar. "If you have two physical qubits—two electrons on two separate quantum dots — [you can swap] the wave functions of these two electrons. It's a lot easier to perform than these single-qubit operations," he said.

The catch is that these natural operations don't translate directly to the necessary quantum computing functions.

"If you want to just use the naturally available interactions in the system, you'll have to play some tricks," said Lidar. "You're going to have to represent your logical zeros and ones in terms of some entangled combinations of [quantum mechanical] states of these physical qubits," he said.

And at some level the quantum computer still has to perform the same operations that implement universal quantum computation. "Again you use single qubit gates and a CNOT, but these single-qubit gates no longer operate on the physical... qubits, rather they operate on the encoded qubits," said Lidar.

The downside to encoding is that quantum computers will need at least twice as many physical qubits as non-encoded systems require.

"The trade-off in encoding is that you're using a number of physical qubits in order to encode one logical qubit," said Lidar. "Whether the net balance is positive, that's something that's going to depend on a particular implementation," he said. "What is easier to do, engineer a difficult operation or give access to more physical qubits?"

The encoding scheme grew out of research on decoherence-free subspaces, which protect qubits from decoherence. Decoherence occurs when energy from the environment knocks a physical qubit out of its quantum mechanical state. Limiting decoherence is one of the principal challenges to developing practical quantum computers.

The encoding research shows how this idea can be extended to general notions of fault-tolerant quantum computation, said Seth Loyd, an associate professor of mechanical engineering at the Massachusetts Institute of Technology.

"This scheme is potentially useful, [but] whether this or any other scheme will lead to large-scale quantum computation remains to be seen," he said.

In order to test the encoding scheme, researchers will need to build prototype solid-state quantum computers with between two and four qubits and test them first using the standard paradigm, said Lidar. That probably won't happen for another five years, he said.

Many researchers say that it will be at least two decades before practical quantum computers are developed.

Lidar's research colleagues were Dave Bacon, Julia Kempe and K. Birgitta Whaley of the University of California at Berkeley and David P. DiVincenzo of IBM Research. The research was funded by the Army Research Office, the National Security Agency, and the Advanced Research and Development Activity.

Timeline: >20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Encoded Universality in Physical Implementations of a Quantum Computer," posted to the Los Alamos National Laboratory e-Print archive February 27, 2001; Technical paper "Quantum Computation," Science, October 13, 1995

TRN

Quantum Computers Go Digital

By Eric Smalley, Technology Research News
January 29/February 5, 2003

Some of the same properties that would make quantum computers phenomenally powerful are also properties that make it difficult to actually build them.

Problems that would take the fastest possible classical computer longer than the lifetime of the universe to solve would be hours-long exercises for large-scale quantum computers. Such machines would be able to rapidly search huge databases and would render today's encryption methods useless.

The key to quantum computers' potential is that quantum bits, the basic building blocks of quantum computing logic circuits, can represent a mix of 1 and 0 at the same time, allowing a string of qubits to represent every possible answer to a problem at the same time. This means a quantum computer could check every possible answer using a single

set of operations. Classical computers, in contrast, check each answer one at a time.

But today's qubits are difficult to work with and prone to errors, and the faster they go the more errors they produce. One of the challenges of building a quantum computer is reducing errors. Researchers from the University of Wisconsin at Madison have eased the problem with a method that reduces error rates by two orders of magnitude.

Today's computers are digital, meaning they use signals that are either on or off to represent two states—a 1 or a 0 — and all computations are done using combinations of these binary numbers. One advantage of using just two states is the signals that represent those states don't have to be exact, they simply have to be clearly closer to 1 than 0 or vice versa.

Qubits are analog devices, meaning they produce variable, continuous signals rather than discrete on and off states. For example, a particle can be in one of two orientations, spin up and spin down, but also some mix of the two. The 1s and 0s of digital information are mapped to the spin up and spin down states, but quantum computations have to be precise to ensure that the given particle is actually in one of those two states. "Classical bits have only two states... quantum bits can be in between," said Robert Joynt, a physics professor at the University of Wisconsin at Madison.

A qubit continually rotates between 0 and 1, which makes it prone to errors, said Joynt. "A rotation of a qubit can, for example, fall a little bit short with only a very minor error in the input signal," he said.

The researchers' method makes quantum computing a pseudo-digital operation. "In our set-up, a definite rotation rate for the qubits is associated with a range of input signals. [This way] the input does not have to be exceedingly precise," said Joynt.

Easing the requirements for precision could go a long way toward making quantum computers viable. "The driving force [for the idea] was objections from experienced electrical engineers, particularly at IBM, who believed that quantum computing would not work... the because the specs for the driving electronics would be much too [demanding]," said Joynt.

The researchers are applying the pseudo-digital qubits to their ongoing efforts to build a solid-state quantum computer. Their design calls for thousands of individually-controlled electrons in a silicon chip. The chip would allow for careful control of the interactions between neighboring electrons so that the states of the electrons could be used to carry out computations. Some of the fundamental logic operations in quantum computers are carried out through the interactions of pairs of qubits.

The researchers added the pseudo-digital qubits concept to their design by having pairs of electrons slide past each other rather than crash into each other, said Joynt. When the electrons are well separated the interaction is off, representing a 0, and when they are within close range the interaction is on, representing a 1.

When the researchers simulated the technique, they found that it reduced operational error rates by more than two orders of magnitude, according to Joynt. The researchers' pseudo-digital qubits could be implemented in other types of quantum computers, he added.

The pseudo-digital approach is a good one, said Bruce Kane, a visiting associate research scientist at the University of Maryland. "My guess is that future quantum computers will use the pseudo-digital approach," he said. It remains to be seen whether the devices the researchers are building will work well, however, he said.

Quantum computing naturally has many similarities to analog rather than digital computing, said Kane. Because digital computers operate using just two states — 1 and 0 — inputs can always be rounded. This type of rounding, however, is impossible in quantum computing, he said. "It [is usually] necessary to control parameters very precisely to keep the computation on track," he said.

The researchers' method is an attempt to find systems that "pretty much automatically have only two interaction strengths," said Kane. No system can have exactly this behavior, so the method doesn't eliminate the problem of errors creeping into a quantum computation, but it can reduce the severity of the errors, he said.

The researchers have shown how to minimize the adverse effects of turning interactions on and off in quantum computing, said Seth Lloyd, a professor of mechanical engineering at the Massachusetts Institute of Technology. "Although I doubt that this exact architecture will prove to be the one that is used to construct large-scale quantum computers, it is exactly this sort of imaginative quantum-mechanical engineering that is required to solve the problems of large-scale quantum computation," he said.

One of the challenges in implementing the scheme in a real quantum computer is fabricating the tiny qubits precisely, said Joynt. "The real issue is fabrication of quite complicated nanostructures," he said.

The researchers are working on qubits made from two basic pieces—a semiconductor sandwich structure "which is really a monster club sandwich," said Joynt; and a gate structure, which controls the state of a qubit so that it can represent a one or a zero.

The researchers have made progress on the semiconductor sandwich structure and are gearing up now to produce the gate structure, "which is quite complex," Joynt said.

The researchers are also working on a readout apparatus that will fit on the chip. Reading the quantum states of particles is tricky because quantum states are easily disturbed.

It will take a decade to develop simple demonstration models, and probably 20 years before the devices can be used in practical quantum computers, said Joynt.

Joynt's research colleagues were Mark Friesen and M. A. Eriksson. They published the research in the December 9, 2002 issue of *Applied Physics Letters*. The research was funded by the National Science Foundation (NSF) and the Army research office (ARO).

Timeline: 10-20 years
Funding: Government
TRN Categories: Physics; Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Pseudo-Digital Quantum Bits," Applied Physics Letters, December 9, 2002

TRN

Logic Gates

Light Drives Electron Logic

Technology Research News, September 10/17, 2003

Although quantum computers have the potential to solve very large problems very quickly, and full-size quantum computers would render most of today's security software obsolete, building a quantum computer is extremely difficult, and working models are at least one to two decades away.

Researchers from the University of Michigan at Ann Arbor and the University of California San Diego at La Jolla have taken the proposition a step forward by demonstrating a conditional logic gate made from a pair of electrons trapped in a quantum dot.

The researchers' device acts as a two-bit conditional logic gate, and is controlled using light. It is the first such gate implemented in a solid-state device, according to the researchers.

A working quantum computer would require thousands or millions of such gates. The researchers are currently refining a method that includes a third electron, which will allow the system to hold information longer and be scaled up to large numbers of gates.

It will take at least ten years to assess the potential of different types of quantum computers, and longer than that to build one, according to the researchers. The work appeared in the August 7, 2003 issue of Science.

Computer Architectures

Quantum Computer Keeps It Simple

By Eric Smalley, Technology Research News
August 13/20, 2003

Quantum computers promise to be fantastically fast at solving certain problems like cracking codes and searching large databases, which provides plenty of incentive for overcoming the tremendous obstacles involved in building them.

The basic component of quantum computers, the qubit, is made from an atom or subatomic particle, and quantum computers require that qubits exchange information, which means the interactions between these absurdly tiny objects must be precisely controlled.

Researchers from the University of Oxford and University College London in England have proposed a type of quantum computer that could greatly simplify the way qubits interact.

The scheme allows qubits to be constantly connected to each other instead of repeatedly connected and disconnected, and it allows a computer's qubits to be controlled all at once, said Simon Benjamin, a senior research fellow at the University of Oxford in England. Global control is a fairly unconventional idea that "allows you to send control signals to all the elements of the device at once instead of having to separately wire up each element," he said.

The scheme can be implemented with different types of qubits. A common type uses the spin of an electron. Electrons can be oriented in one of two directions, spin up and spin down. These are analogous to the poles of a kitchen magnet and can represent the 1s and 0s of computer information.

Key to the potential power of quantum computers is a weird trait of quantum particles like electrons. When an electron is isolated from its environment, it enters into superposition, meaning it is in some mix of both spin up and spin down.

Linking two qubits that are in superposition makes it possible for a quantum computer to examine all of the possible solutions to a problem at once. But controlling how two qubits interact is extremely challenging, said Benjamin. Qubits "must be made to talk to each other, and when the operation is over they must be made to stop talking," he said.

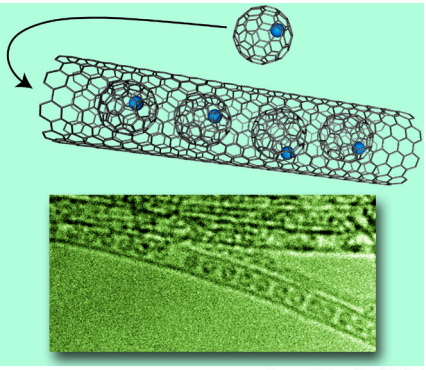
In traditional quantum computing schemes that use electron spins, pairs of qubits have a metal electrode between them. When the electrode is negatively charged, it repels the negatively charged electrons that make up the qubits, keeping them separated. But giving the electrode a positive charge draws the electrons toward each other, allowing them to interact by exchanging energy. Allowing the qubits to interact for half the time it takes to completely swap energy is the basis of two-qubit logic gates.

The energy of the two qubits has to be resonant or errors can arise, but off-resonant energy can also be harnessed, said Benjamin. Particles resonate at specific energies in the same way that larger objects vibrate more readily at certain frequencies. Different energies can be more or less resonant with each other much like certain musical notes sounding better together than others. "Something that we were used to thinking of as a source of error could in fact be a means of controlling the computer," he said.

The researchers' proposal replaces the electrode with a third electron. These three electrons are constantly interacting,

but they don't always exchange energy. When the middle electron is off resonant, the qubits are blocked from exchanging energy. This way, the interaction "is always on, but we can effectively negate it by ensuring that the energies of neighboring spins are completely incompatible," said Benjamin.

Avoiding electrodes is useful for several reasons. Fabricating qubits with electrodes between them "will require a fantastic degree of control," said Benjamin. "If a particular pair of electrons are too close, then the interaction will be jammed on, and if they are too far away then the interaction will be jammed off," he said.



Source: University of Oxford

This diagram and image depict a carbon nanotube containing four carbon buckyballs. The blue dots represent electrons. Each buckyball can serve as qubit.

Electrodes can also knock qubits out of superposition. "Each electrode can act as an [antenna], channeling electromagnetic noise from the room-temperature world right down to the qubits," said Benjamin.

The researchers took their proposal a step further by removing the need to control electrons individually. Every change to the energy of the electrons is applied to the whole device. The researchers divide a string of qubits into two groups, odd and even, with every other qubit in one group. A set of six specific changes to the energies of the electrons covers all of the logic gates required for quantum computing, according to the researchers. Quantum programs would consist of timed sequences of the changes.

The main disadvantage of the researchers' proposal is that it could require as many as two spins per qubit rather than the usual single spin, which would make for a larger device, said Benjamin. "Right now experimentalists are struggling to make even two qubits in solid-state systems," he said.

The researchers' work is valuable because it extends the range of candidates for quantum computing, said Barry Sanders, a professor of quantum information science at the University of Calgary in Canada. The work is "stoking the fires of creativity so that we physicists can dream up other quantum computing realizations that lead to easier control and less experimental complexity," he said.

There is a growing realization that there are many ways to perform qubit operations, said Robert Joynt, a physics professor at the University of Wisconsin at Madison. The Oxford and University College London work is significant for people trying to make a real machine, because it means that the constraints on the hardware are a lot looser than people thought at first, he said. This research "is particularly nice since it gets rid of the usual need to precisely tune two-qubit operations."

The researchers are currently exploring how the method would work in a two- or three-dimensional array of qubits, said Benjamin. "We'd also like to build up a more detailed description of how to implement our scheme with specific technologies like... electron spin," he said.

Researchers generally agree that practical quantum computers are two decades away. It is possible that quantum computers capable of computations that are impossible on conventional computers could be built within ten years, said Benjamin.

Such systems "will be mainly of interest to the scientific community because they will involve using quantum computers to simulate other quantum systems, such as fundamental biological processes," said Benjamin. "These first quantum computers may require an entire lab built around them, and may be treated as a national or international resource for research—a bit like today's supercomputers or... particle accelerators."

However, it is also possible that quantum computing research could stall if there's not enough experimental progress in the next few years, said Benjamin. "It's possible that quantum computing is an idea born before it's time. Our technology may simply be to crude to achieve it," he said.

Benjamin's research colleague was Sougato Bose. The work appeared in the June 20, 2003 issue of *Physical Review Letters*. The research was funded by the Royal Society, the Oxford-Cambridge-Hitachi Nanoelectronics at the Quantum Edge project in England, and the National Science Foundation (NSF).

Timeline: 10-20 years
Funding: Corporate, Government, University
TRN Categories: Quantum Computing and Communications Story
Type: News
Related Elements: Technical paper, "Quantum Computing with an Always-On Heisenberg Interaction," Physical Review Letters, June 20, 2003

TRN

Quantum Computing Catches the Bus

By Eric Smalley, Technology Research News
February 26/March 5, 2003

Before researchers can build large-scale quantum computers, they must work out ways to shunt information between computer components.

Quantum computers use traits of particles like atoms and electrons to compute, and are theoretically many orders of magnitude faster than today's computers in solving very large problems, including the number-factoring problems whose complexity underpins today's computer security software.

The challenges in building practical quantum computers include preserving the fragile quantum states of particles that represent the 1s and 0s of digital information and controlling the delicate interactions between particles that the computers tap to process information.

National Institute of Standards and Technology (NIST) researchers have tapped an aspect of classical computers and a pair of weird particle traits to allow distant particles, or qubits, to communicate as though they were in contact.

In today's computers, memory and processor chips pass data back and forth through a central communications bus. In contrast, many proposed quantum architectures shunt information between particles, or qubits by passing the information through every qubit in between, bucket-brigade fashion. Transferring information this way is slow and error prone.

The researchers' scheme uses empty qubits as a communications bus that allows distant memory bits to exchange information directly. "Memory qubits... do not need to be swapped throughout the computer," said Gavin Brennan, a physicist at NIST. This helps cut down on errors, which increase with each information transfer, he said.

The particles that make up qubits have states that can represent the 1s and 0s of computing. Electrons, for example, have two different spins, much like a top that can spin clockwise or counterclockwise.

Quantum computers have the potential to be phenomenally fast due to a couple of weird traits of particles. When particles are isolated from their environments, they enter the quantum state of superposition, and are in some mix of all possible states.

And when two or more particles in superposition come into contact, they can become entangled, meaning one or more of their properties are linked. The link remains even if the particles are separated, and if one particle interacts with its environment and is knocked out of superposition into a definite state, the other particle also leaves superposition and assumes the same state at the same instant regardless of the distance between them.

The key to quantum computers' potential is that qubits in superposition can represent every possible answer to a problem at the same time, allowing the computer to check all the answers with one set of operations. Quantum computers containing thousands of qubits would be able to solve problems that have so many possibilities it would take today's computers longer than the life of the universe to check them all serially.

In the nearest-neighbor quantum computer architectures that could be improved by the NIST scheme, neighboring qubits become entangled in order to pass along information during logic operations. The bus qubits in the researchers' scheme don't carry information directly, but become entangled to form a communications channel.

When distant memory qubits A and B need to interact, "one creates a chain of... entangled pairs of bus qubits between A and B using nearest-neighbor interactions," Brennan said. In a second step, entanglement swapping, the ends of the chain are entangled with each other, Brennan said. Qubits A and B can communicate by having qubit A interact with the bus qubit at one end of the chain and B interact with the bus qubit at the other end of the chain. "The effect is the same as if A and B interacted directly," he said.

The nearest-neighbor interactions needed to form a chain with entangled ends are easier to carry out and less error prone than the interactions needed to pass information from one qubit to the next.

A communications bus "will certainly be necessary for large quantum computers that use nearest-neighbor interaction," said David Kielpinski, a postdoctoral fellow at the Massachusetts Institute of Technology. The NIST method "is innovative and plausible, drawing on interesting recent results in quantum communication," he said.

Setting up quantum communications links between distant parts of a quantum computer to allow widely separated qubits to talk to each other reduces the computing time considerably, said Kielpinski. At the same time, however, "it takes some extra work to set up a good communications link, so more resources and time are needed than for proposals that don't have the nearest-neighbor limitation in the first place," he said.

Proposals to build quantum computers from quantum dots, semiconductor impurities and optical lattices all use nearest-neighbor architectures. Quantum dots are specks of semiconductor that trap individual or small numbers of electrons. Semiconductor impurities are individual atoms embedded in semiconductor material. Optical lattices are three-dimensional arrays of laser beams that trap individual atoms.

Other quantum computing architectures, including designs that use ions trapped in magnetic fields or electric current flowing through superconductor loops, do not link qubits via nearest-neighbor connections, and instead include a type of fixed, common bus. Though these schemes avoid the overhead of the researchers' communications channels, the common buses could be a source of crosstalk that could degrade computations, said Brennan.

There are several challenges to building large-scale quantum computers that need to be overcome before it will be possible to implement the researchers' communications scheme, including building hardware with precisely positioned and readily controllable qubits, and coming up with reliable basic logic gates.

One well-known proposal by Bruce Kane of the University of Maryland calls for using the properties of phosphorus atoms embedded in silicon. "Designing a regular array... is a technical challenge," said Brennan. It would be a similar challenge to isolate the single atoms trapped in optical lattices, he said.

Researchers agree that it will be a long time before quantum computers become practical. "We expect a modest sized—about 50 qubits—quantum architecture [in] the next 10 to 20 years," said Brennon. A 50-qubit computer could provide simulations of complex systems better than classical computers, he said.

Brennan's research colleagues were Daegene Song and Carl J. Williams. The researchers posted the work on the arXiv physics archive in January, 2003. The research was funded by the National Security Agency (NSA) and the Defense Advanced Research Projects Agency (DARPA).

Timeline: 10-20 years
Funding: Government
TRN Categories: Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "A Quantum Computer Architecture Using Nonlocal Interactions," posted to the arXiv physics archive, January 6, 2003

TRN

Design Links Quantum Bits

By Eric Smalley, Technology Research News
December 11-25, 2002

Much of today's effort to build quantum computers, which would use the attributes of atoms and subatomic particles to carry out blazingly fast computations, is focused on finding the best way to make quantum bits, or qubits, the basic building blocks needed to represent and process information using the quirks of quantum physics.

But getting quantum computing off the ground also means connecting thousands of qubits in much the same way transistors are wired together in ordinary computer chips.

Researchers at the Institute of Physical and Chemical Research (Riken) in Japan have moved a step toward making these connections with a design that calls for qubits made from tiny loops on superconducting material. The researchers have worked out a way to connect the loops so that they can efficiently carry out all the basic logic operations a quantum computer needs, according to Franco Nori, head of the digital materials laboratory at Riken and an associate professor of physics at the University of Michigan.

The payoff could be enormous; quantum computers have the potential to solve problems like cracking secret codes and searching large databases that are beyond the reach of the most powerful classical computer possible.

The loops provide access to the properties of subatomic particles because electrons pair up when they flow through a superconductor, and billions of electron pairs can be merged into a single entity that behaves as one giant subatomic particle in superconducting loops that have one or more small breaks, or Josephson junctions.

When one or two of the loops are connected to a reservoir of electron pairs, the number of pairs in the reservoir can be reliably changed by exactly one pair, which changes the reservoir's charge in a measurable way.

The two charge states can represent the 1s and 0s of computing. And because the electron pairs behave as one subatomic particle that follows the weird laws of quantum physics, the reservoir can be in both states at once. This characteristic is the basis of quantum computing's potential power.

The loops can be mass-produced using standard chipmaking processes, but linking the qubits requires more than simply wiring them together. The quantum states produced by the loops are fragile, and linking them also requires the presence of a carefully tuned magnetic field.

Other designs for building quantum computers from superconductor loops include ways to link neighboring qubits, but can only pair distant qubits in a bucket-brigade fashion through intervening qubits, which slows computing, said Nori. "A scalable quantum computer needs to couple any selected pairs of qubits, [whether they are] neighboring or far away," he said.

Time is of the essence in quantum computing because the quantum states that are used to store and manipulate information last for only fractions of a second, and the computers need to perform thousands of operations before the qubits decohere, or break down.

The Riken researchers' design can be likened to a series of water tanks connected by pipes that contain valves that can open a flow between any two tanks. The tanks represent qubits and the pipes the superconducting circuits between them.

Opening the correct valves by applying a magnetic field sends an electric current flowing between specific qubits, which makes it possible to link the qubits in the bizarre quantum state of entanglement.

When a subatomic particle or atom is isolated from the environment, it enters into superposition, meaning it is in some mixture of all possible states. Like a top, a particle can spin in one of two directions, but in superposition the particle spins in some mixture of both directions at the same time.

When two or more particles in superposition come into contact with each other, they can become entangled, meaning one or more of their properties, like spin or polarization, become locked together. This is a useful property for computing: if a pair of entangled photons have linked polarizations, when one of the photons is knocked out of superposition and becomes vertically polarized, the other

photon leaves superposition at the same instant and also becomes vertically polarized, regardless of the distance between them.

Entanglement is key to quantum computing's potential speed: it will allow a computer to check every possible answer to a problem with one series of operations across a group of entangled particles rather than having to check each possible answer one by one.

The researchers' design provides an efficient way of implementing two key quantum logic circuits, or gates:

CNOT and conditional phase shift. Each gate uses two qubits. In a CNOT gate, one of the qubits is a control bit and the other is a target bit. If the control bit is 1, the target bit changes—either from 0 to 1 or 1 to 0. If the control bit is zero, the target bit does not change. The operation entangles the two qubits. A conditional phase shift synchronizes two qubits.

These two types of gates, together with gates made from single qubits, form the basic logic of quantum computing, said Nori. "All quantum computing operations can be decomposed into these gates and the basic one-bit gates," he said. One-bit gates change the state of a single qubit to, for example, reverse the spin of an electron to change it from a 1 to a 0.

Existing schemes to build quantum computers from superconducting loops require several two-qubit operations rather than just one to make up CNOT and conditional phase shift gates, said Nori. Because two-qubit operations are time-consuming, it is important to use as few as possible in order to get the most out of the limited lifetimes of the quantum states, he said.

A CNOT gate that requires only a single two-bit operation is a distinct advantage, said Jens Siewert, a staff member of the Institute for Theoretical Physics at the University of Regensburg in Germany.

The researchers' work is an engineering rather than a conceptual contribution, said Yuriy Makhlin, a staff member of the Institute for Theoretical Physics at the University of Karlsruhe in Germany. When techniques for manipulating two or three qubits become well-established, it will be important to build circuits with larger numbers of qubits and to optimize their design, he said. "Already at this stage one has to plan ahead."

There's a long way go before researchers can build practical quantum computers, which will have thousands of qubits, said Nori. "The first step is to make good working qubits, then the next step is to couple two, and then three," he said. Performing logic operations with the qubits and reading the results are also difficult problems, he added.

The researchers next steps are to improve the circuit designs to gain more reliable and less disruptive readout of the qubits, and to extend the amount of time information stored by qubit lasts before it decoheres, said Nori. "There are many steps involved in designing and building a quantum computer," he said. "Our group is aiming at identifying and working on key steps; the work is scheduled to last a decade or longer."

There is broad agreement in the research community that it could take two decades or longer to develop practical quantum computers. "The PCs we are using now on our desks are quite different from the first computing machines of the 1930s and 1940s," said Nori. "It took over half a century to get to our PCs. It might also take decades for this new type of computing to become widespread," he said.

Nori's research colleagues were J. Q. You of Riken and Jaw-Shen Tsai of Riken and NEC Research. They published the research in the November 4, 2002 issue of the journal *Physical Review Letters*. The research was funded by the National Security Agency (NSA) Advanced Research and Development Activity (ARDA), the Air Force Office of Scientific Research (AFOSR), the National Science Foundation (NSF), and Riken.

Timeline: 20 years
Funding: Government
TRN Categories: Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Scalable Quantum Computing with Josephson Charge Qubits," Physical Review Letters, November 4, 2002

TRN

Chip Design Aims for Quantum Leap

By Eric Smalley, Technology Research News
August 21/28, 2002

The first step toward making phenomenally powerful quantum computers is capturing and manipulating individual subatomic particles, which is a bit like getting a fly to venture onto your desk, then perform tricks like "sit up" and "roll over" on command.

The second step is harnessing, controlling and coordinating thousands or millions of particles at once. Making a practical quantum computer also means doing this using ordinary electronics rather than exotic laboratory equipment.

University of Wisconsin researchers are tackling these issues with a quantum computer design that would incorporate thousands of individually-controlled electrons into a silicon chip that could be made much the same way as today's computer chips.

Practical quantum computers would be many orders of magnitude faster than today's computers for problems that involve massive amounts of data, like cracking secret codes and searching large databases.

The researchers' idea is to "trap single electrons in tiny silicon sandwiches about a millionth of an inch across," said Robert Joynt, a physics professor at the University of

Wisconsin at Madison. The silicon sandwiches are quantum dots, microscopic specks of semiconductor material that can hold one or a few electrons.

These dots can represent bits of information because an electron acts like a tiny spinning top, and depending on which way it is spinning it can represent a 1 or a 0. Conventional computers use the presence or absence of electric current running through transistors to indicate the 1s and 0s of digital information.

Proposals for making quantum computers out of quantum dots have been around for several years. The Wisconsin researchers' design plots out some of the difficult details — it allows individual electrons to be loaded into the quantum dots and allows interactions between electrons held in neighboring dots is to be closely controlled.

Each dot would consist of a bottom layer of silicon germanium that has been chemically altered to allow electrons to flow more easily. This layer would serve as a reservoir of electrons.

The middle layers would consist of an extremely thin layer of silicon sandwiched between layers of unaltered silicon germanium. The silicon layer would hold the individual electron used by the quantum computer, and the silicon germanium layers would act as barriers to keep additional electrons out. The researchers could coax individual electrons to tunnel through the barriers to the silicon layer by changing the electrical current running through the chip.

Metal electrodes that move the electrons laterally would form the chip's top layer. The electrodes would be used to bring pairs of electrons in adjacent dots together to perform the basic logic operations of computing. The quantum interactions of a pair of electrons can be represented mathematically, and that math can be used to generate the binary logic that is the foundation of computing. This allows logic operations like adding binary numbers to be carried out by controlling the electron interactions.

"The biggest hurdle is fabrication," said Joynt. "This needs to be done with exquisite control of the quality of the material and to very high measurement specs," he said.

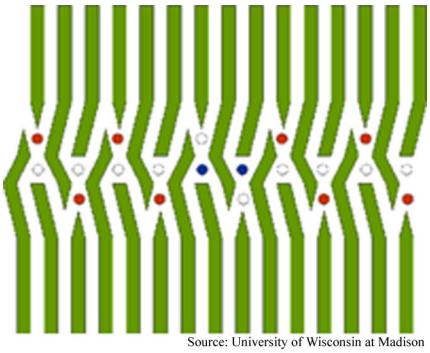
Because the quantum dots are made from layers of metal and semiconductors, like computer chips, the researchers' proposed device could be built using standard chipmaking processes, according to Joynt. "The dots are only slightly smaller than the features on commercial chips, which have millions of transistors," he said.

Unless the optical lithography used in the commercial chip industry improves, however, this minor decrease in size means that the researchers will have to use electron beam lithography, said Joynt. "This is slower and more expensive, but perhaps not prohibitively so," he said.

Today's optical lithography uses ultraviolet light with wavelengths ranging from 200 to 300 nanometers and can etch features as small as 130 nanometers. Electron beams can be focused with magnetic fields to around 10 nanometers and so can etch much smaller features.

The potential benefits of a practical quantum computer are enormous.

"Quantum computing is massively parallel," said Joynt. This means that many inputs can be processed at the same time, which makes for a computer that can solve problems that would take a regular computer "essentially forever" to work out, he said.



Source: University of Wisconsin at Madison

The dots in this quantum computer diagram represent individual electrons. The green lines are electrodes that move electrons back and forth. The blue electrons are interacting to carry out basic quantum logic operations.

When an electron is isolated from its environment it is in the weird quantum state of superposition, meaning it is spinning in both directions at once. An electron in superposition can represent a mix of 1 and 0, and a string of electrons in superposition can represent every combination of 1s and 0s at the same time.

The power of a quantum computer comes from the ability to check every possible combination of numbers at once to find the answer to a problem that can have more possibilities than there are atoms in the universe. Ordinary computers have to check each possible answer one at a time.

Researchers have already come up with software that would allow quantum computers to crack secret codes and search massive databases.

The Wisconsin work is a good effort that adds "many realistic details" to quantum dot research, said IBM Research physicist David DiVincenzo. DiVincenzo and Daniel Loss, a physics professor at University of Basel in Switzerland, developed an earlier quantum dot quantum computer proposal.

"I am very encouraged generally by the efforts of the University of Wisconsin group," said DiVincenzo. "They have started a big, integrated effort involving both theory and experiment," he said.

Practical quantum computers are likely to take 25 years to develop, said Joynt. "And I'm an optimist," he said. "We are working on fabricating a prototype, step by step," he added. "The next step is to make sure that our [silicon layer] is properly trapping the electrons."

Joynt's research colleagues were Mark Friesen, Paul Rugheimer, Donald Savage, Max Lagally, Daniel van der Weide and Mark Eriksson. They published the research in the July 15, 2002 issue of the journal *Physical Review B*.

The research was funded by the U.S. Army Research Office (ARO) and the National Science Foundation (NSF).

Timeline: 25 years
Funding: Government
TRN Categories: Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Design and Proof of Concept for Silicon-Based Quantum Dot Quantum Bits," posted on the arXiv physics preprint archive at arXiv.org/abs/cond-mat/0204035; Technical paper, "Decoherence of Electron Spin Qubits in Si-Based Quantum Computers," Physical Review B, July 15, 2002

TRN

Quantum Logic Counts on Geometry

By Eric Smalley, Technology Research News
July 25, 2001

Imagine you are holding a beach ball in one hand and a doll in the other. Place the doll on its back on top of the ball and slide it feet first half way down the side of the ball, then slide it sideways halfway around the ball, and then slide it head first back to the top. Notice that even though you kept the doll straight, the doll's head and feet are reversed from their original orientation.

You have just demonstrated a basic principle of spheres. If you consider the doll's head 1 and the doll's feet 0, you have also computed. You have performed a NOT gate, which is a logic operation that flips a bit from a 0 to a 1 or a 1 to a 0.

This idea of computing by geometry is at the heart of a proposed scheme for quantum computing that could yield prototype systems that are sturdier and easier to control than experimental computers based on previous schemes, which involve manipulating the energy levels of particles.

Quantum computers could solve certain types of very large problems almost instantaneously because quantum bits, or qubits, can represent every possible solution to a problem and quantum computers can check every possibility in relatively few steps. Ordinary computers have to check each possibility one at a time.

Researchers at the University of Innsbruck have devised a scheme for quantum computing that builds all the necessary binary logic operations from one- and two-qubit geometric operations.

The scheme is designed for trapped ions, but it can be generalized to other quantum computer hardware, said Luming Duan, a researcher at the University of Innsbruck and an associate professor of physics at the University of Science and Technology in China.

An ion is an atom that has an electric charge because it has gained or lost one or more electrons. An ion trap is a device that uses magnetic fields to hold an ion in one position so that researchers can focus laser beams and/or radio waves on it.

In geometric quantum computing, the ion doesn't move through physical space but through a virtual space determined by the range of possible changes to the subtle interactions between the ion's nucleus and its electrons.

Electrons occupy regions, or orbitals, around the nucleus. These orbitals exist only at certain distances from the nucleus, but the magnetic interactions between the nucleus and electrons cause slight variations, termed hyperfine levels, in these orbitals. The parameters of an ion's hyperfine levels form a mathematical space that, like a real space, can be described using geometry.

Quantum bits perform geometric computations by walking through parameter space, said Duan. These transformations, which compose all the quantum computation tasks, "result from nontrivial geometric structures, such as curves, of this... space."

Using the scheme, the 1 and 0 of a bit could be encoded as two hyperfine levels of an ion's low-energy state. An ion is in its low-energy state when its electrons are in the lowest orbitals. Computing would be performed by firing a series of laser pulses at the trapped ion. The wavelength and polarization of the lasers would be tuned to subtly alter the relationship between the ion's nucleus and its electrons, resulting in one of the two hyperfine levels.

The transformations in most other quantum computing schemes are dynamic, meaning they shift particles from one energy state to another. In some cases this makes the information the particles hold more susceptible to interactions with the environment, said Duan. When particles interact with the environment they are knocked out of their quantum state, which destroys the bits encoded in the particles' quantum attributes.

Many researchers say it will be at least 20 years before quantum computers that outperform classical computers can be developed. The geometric quantum computing scheme is not likely to accelerate this timeframe, said Duan.

However, "some interesting demonstration-of-principle experiments and experimental demonstration of some special advantages of geometric quantum computation [could happen] quite soon," he said.

Duan's research colleagues were Juan-Ignacio Cirac and Peter Zoller of the University of Innsbruck. They published the research in the June 1, 2001 issue of the journal *Science*. The research was funded by the Austrian Science Foundation, the European Union, the European Science Foundation and the Chinese Science Foundation.

Timeline: 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News

Related Elements: Technical paper, " Geometric Manipulation of Trapped Ions for Quantum Computation," Science, June 1, 2001

TRN

Quantum Computer Design Lights Dots

By Eric Smalley, Technology Research News
February 21, 2001

Figuring out how to hit atoms and subatomic particles with thousands of laser pulses or radio waves while keeping them isolated from the environment is one of the main thrusts of quantum computing research.

Another important focus is making quantum computers that can be manufactured relatively cheaply rather than cobbled together with expensive laboratory equipment.

A team of researchers in Italy has proposed a scheme for building quantum computers using microscopic specks of semiconductor and ultrafast lasers that could achieve both goals.

The scheme is one of several proposals based on using quantum dots, which are pieces of semiconductor that are usually no larger than a few hundred atoms across. Quantum dots are often referred to as artificial atoms or macroatoms because they corral small numbers of electrons. They have the potential to be mass-produced because they are made using the same processes as today's computer chips.

"The idea is to use quantum hardware fully compatible with current microelectronics technology," said Fausto Rossi, an associate professor of physics at the Polytechnic Institute of Torino.

But this quality could make it harder to achieve the other goal of squeezing in enough laser pulses before the quantum bits, or qubits, decohere, or come out of the quantum state of superposition due to interactions with the environment. Practical quantum computers made from quantum dots will likely have qubits based on electrical charge, and charge-based qubits decohere quickly.

The Italian scheme's qubit is made from an exciton, which is an electron and a hole in a temporarily stable orbit around each other. Holes are positively charged gaps where negatively charged electrons can reside.

The researchers propose to get around the decoherence limitation by using only ultrafast lasers to perform logic operations on the qubits. Other quantum dot quantum computing schemes use radio waves or magnetic fields, either alone or with ultrafast lasers. Laser's can be pulsed on the order of picoseconds, which is millions of times faster than radio waves or magnetic fields. A picosecond is one trillionth of a second. A picosecond is to one second as one second is to 31,709 years.

Because excitons can survive in the required quantum mechanical state of superposition for nanoseconds or even microseconds, which are thousands or millions of times longer than the pulses, the scheme could allow for the many thousands of laser pulses that will make up the computational operations needed for useful quantum algorithms.

The principal drawback to the Italian researchers' scheme is the lack of a method for addressing individual qubits. Because the quantum dots have to be spaced more closely than the wavelengths of light, the researchers can't use light to observe individual qubits, said Rossi.

The researchers are considering getting around the problem by using a cellular automata scheme instead of attempting to address each qubit individually. If quantum dots are spaced closely enough, the position of electrons in one quantum dot determines the position of electrons in the adjacent dot, which allows information to be transferred along a series of dots.

The goal of the researchers' project is to demonstrate basic quantum computing operations on a two-qubit prototype within three years, said Rossi. "If this [works], then we will start thinking about practical issues like large-scale integration and scalability," he said.

Most researchers say they believe that practical quantum computers are at least 20 years away.

Rossi's research colleagues were Eliana Biolatti, Rita C. Iotti and Paolo Zanardi of the Italian National Institute for Material Physics. They published the research in the December 25, 2000 *Physical Review Letters*. The research was funded by the European Commission's Future and Emerging Technologies program.

Timeline: <3 years, 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Quantum Information Processing with Semiconductor Macroatoms," Physical Review Letters, December 25, 2000

TRN

Big Qubits Linked over Distance

Technology Research News, May 21/28, 2003

Quantum computers promise to be fantastically fast for solving certain problems, including code breaking that would render today's computer security useless.

The trouble with tapping the traits of particles like atoms and electrons to compute, however, is that they are notoriously difficult to control.

One solution is to bring quantum mechanical behavior into a larger realm.

Researchers from the University of Maryland have moved this approach a step forward by entangling a pair of large

quantum bits that were spaced nearly a millimeter apart. Entanglement is a weird quantum property that will allow quantum computers to simultaneously check every possible answer to a problem. Entanglement links a pair of qubits, the building blocks of quantum computers, so that when a logic operation is performed on one, the other changes as well, regardless of the distance between them.

The researchers' prototype entangled qubits were superconducting circuits containing billions of electrons acting as one giant particle. The qubits were 700 microns apart—a vast expanse by quantum standards, and several hundred times further apart than previous chip-based entanglement experiments.

Researchers generally agree that practical quantum computers are least two decades away. The work appeared in the May 15, 2003 issue of *Science*.

TRN

Quantum Chips Advance

By Eric Smalley, Technology Research News
March 12/19, 2003

Today's rudimentary quantum computer prototypes come in many unusual forms, including laser beams, liquids and sets of single atoms.

Many researchers, however, are trying to make quantum computers that look more like their electronic predecessors. A promising avenue is superconducting circuits, and several research teams have used the technology to form the particle-based qubits that quantum computers use to manipulate the 1s and 0s of computing.

Researchers from the Institute of Physical and Chemical Research (Riken) in Japan and the State University of New York at Stony Brook have entangled a pair of electronic qubits in an integrated circuit. The work is a milestone on the road to chip-based, mind-bogglingly fast quantum computers.

The device "is the first solid-state electronic circuit that is capable of creating entanglement, the most important property required for an efficient quantum computer," said Jaw-Shen Tsai, a research fellow at NEC Fundamental Research Laboratories in Japan and head of the Macroscopic Quantum Coherence Laboratory at Riken.

Entanglement is a weird quantum phenomenon in which two or more particles like atoms or electrons become linked, changing in lockstep regardless of the distance between them. This property is key to the immense power of quantum computing because it allows a quantum computer to check every possible answer to a problem at once.

Classical computers, in contrast, must check each possible answer one at a time. A full-scale quantum computer could solve problems like cracking strong encryption codes that are beyond the reach of even the most powerful possible classical computers.

Quantum computers use opposite states of a particle to represent the 1s and 0s of digital information. An electron, for example, can spin in one of two directions, up or down, similar to a top spinning clockwise or counterclockwise.

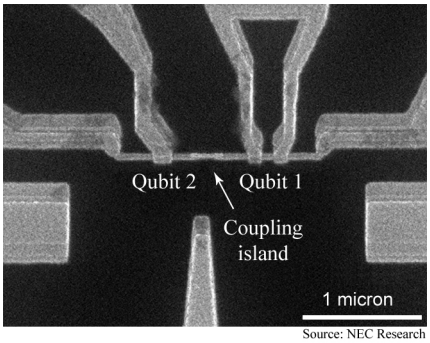
When an atom or subatomic particle is isolated from its environment, it enters into superposition, which is a mixture of all possible states. An electron in superposition, for example, is spinning both up and down at the same time. This means that a qubit can represent both 1 and 0 at once, and a long enough string of qubits can represent every possible answer to a problem.

Two or more particles can become entangled when they are in superposition, and they stay entangled as long as they remain in superposition. This is the key to quantum computers' potential for phenomenal speed. A quantum computer can check every possible answer to a problem using a single series of operations across a set of entangled qubits.

The researchers' device is unusual because it can tapped these weird quantum traits on a larger-than-atomic scale.

The device consists of a pair of Josephson junction qubits connected to a capacitor, which briefly stores electric charges. Josephson junctions are tiny breaks in superconducting circuits. Electrons pair up to flow through a superconductor, and billions of these pairs form a single entity that behaves as one giant subatomic particle when the superconductor contains a Josephson junction.

When a Josephson junction circuit is connected to a reservoir of electron pairs, the number of pairs in the reservoir can be changed by exactly one, and this change can be reliably measured. The two states—the original number of pairs and the original number plus one—can represent 1 and 0.



Source: NEC Research

The circuits in this image form a pair of quantum bits, or qubits, that can be entangled. Entanglement is a weird quantum property that gives quantum computers the potential to be extraordinarily fast. The circuits are a precursor to quantum computer chips.

And because the electron pairs behave as one entity, they can be in a superposition of the two states, which means they can serve as qubits. Josephson junction qubits are also much larger, and therefore easier to work with, than qubits that are individual particles.

The researchers tested the prototype by using an electric pulse to join the two qubits via the capacitor between them. When they measured the qubits' oscillation frequency they found that when the qubits were joined the oscillation pattern

became more complex, a sign of quantum entanglement, said Tsai. "We have observed quantum oscillation in a two-qubit Josephson charge qubit system," he said.

If the researchers' results are confirmed, it would be the first demonstration of entanglement for macroscopic objects in solid-state devices, said Jens Siewert, a staff member of the Institute for Theoretical Physics at the University of Regensburg in Germany. "The [researchers] are careful enough not to claim that they have unambiguously obtained this result, but it is very likely that they did," he said.

Entangling solid-state charge qubits is of utmost importance not only for quantum computation but for understanding quantum mechanics in general, said Siewert. "It is the experiment quite a few people are trying to do at the moment," he said.

The researchers' next step is to make two-qubit logic gates from the Josephson junction qubits, said Tsai. It is likely to take 10 to 20 years before the research can be applied practically, he said.

Josephson junctions only work in temperatures close to absolute zero, so even if large Josephson junction quantum computers can be built they would likely be expensive, specialized systems.

Tsai's research colleagues were Oleg Astafiev of Riken, Yuri A. Pashkin of Riken and the Lebedev Physical Institute in Russia, Tsuyoshi Yamamoto and Yasunobu Nakamura of Riken and NEC Research, and Dima E. Averin of the State University of New York at Stony Brook. The work appeared in the February 20, 2003 issue of *Nature*. The research was funded by NEC and Riken.

Timeline: 10-20 years
Funding: Corporate, Government
TRN Categories: Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Quantum Oscillations in Two Coupled Charge Qubits," Nature, February 20, 2003

TRN

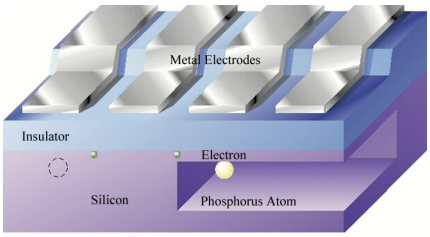
Positioned Atoms Advance Quantum Chips

By Eric Smalley, Technology Research News
August 1/8, 2001

A team of researchers at the University of New South Wales in Australia has laid the foundation for quantum computer chips that closely resemble today's mass-produced semiconductor chips. This is in sharp contrast to today's rudimentary prototype quantum computers, which are built out of complicated laboratory equipment.

The researchers have placed individual phosphorus atoms at regular intervals on a silicon surface. The work is the first step in implementing a silicon-based quantum computer architecture that uses phosphorus atoms embedded in silicon as quantum bits, or qubits.

"Our [research is] a demonstration of the controlled placement of single molecules on a semiconductor surface," said Jeremy O'Brien, a graduate student at the University of New South Wales.

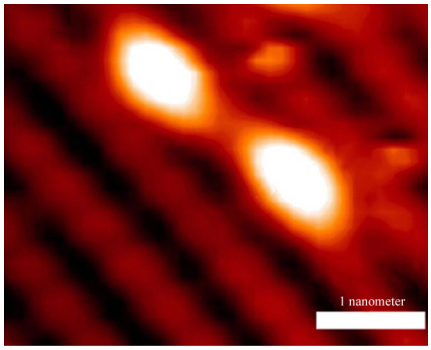


Source: University of New South Wales

In the phosphorus-in-silicon quantum computer architecture, the electrodes directly above the phosphorus atoms control the atoms' quantum states and the electrodes above the spaces between the atoms control the interactions between the atoms via their electrons.

This was challenging because individual phosphorus atoms readily bond to silicon, which makes it impossible to align phosphorus atoms by moving them around on a silicon surface. The researchers got around the problem by coating the silicon with a one-atom-thick layer of hydrogen and then using the probe tip of a scanning tunneling microscope to remove individual hydrogen atoms at regular intervals.

The researchers put phosphorus atoms into the holes left after removing the hydrogen atoms by exposing the hydrogen-coated silicon to phosphine gas. Phosphine gas molecules are composed of phosphorus and hydrogen atoms. The phosphine bonded to the silicon, one molecule to a hole.



Source: University of New South Wales

The bead-like rows in this scanning tunneling microscope image are hydrogen atoms that cover a layer of silicon. The two bright spots are phosphine molecules that fill holes where individual hydrogen atoms have been removed.

This showed that "it is possible to fabricate an atomically precise linear array of single, phosphorus-bearing molecules on a silicon surface with the required dimensions for the fabrication of a silicon-based solid-state quantum computer," said O'Brien.

The researchers were able to position the phosphorus atoms at four-nanometer intervals, which is smaller than the 20-nanometer intervals required for the phosphorus-silicon architecture. A nanometer is about 10 hydrogen atoms long.

"One of the major drawbacks to the [phosphorus-silicon] scheme was [the need to] to position phosphorus atoms with atomic precision on a silicon crystal," said Jonathan P. Dowling, supervisor of the quantum computing technologies

group at NASA's Jet Propulsion Laboratory. "This phosphine idea is really neat, somewhat miraculous, and appears as if it might really work," he said.

The next step in the process is to cover the phosphine molecules with another layer of silicon, said O'Brien. "This will require very high-quality crystal growth to avoid defects which could disrupt the operation of the quantum computer. We must ensure that the phosphorus qubits incorporate into the silicon crystal and remain in the ordered atomic array," he said.

Once the phosphorus atoms are sandwiched in silicon, the next challenge is linking them together and to the outside world. The phosphorus-silicon architecture calls for a metal electrical contact positioned above each atom on the top layer of silicon to control the quantum state of the atom and read the state to determine whether it represents a 1 or a 0. Another metal contact positioned between two atoms could control the quantum interactions between them, according to O'Brien.

Quantum computers would be much faster than ordinary computers at certain tasks like cracking secret codes and searching large databases. Many researchers in the field say quantum computers are not likely to be ready for practical use for at least 20 years.

O'Brien's research colleagues were Steven R. Schofield, Michelle Y. Simmons, Robert G. Clark, Andrew S. Dzurak, Neil J. Curson and N. S. McAlpine of the University of New South Wales in Australia, Bruce E. Kane of the University of Maryland, and Marilyn E. Hawley and Geoffrey W. Brown of Los Alamos National Laboratory. Their research has been accepted for publication in the journal *Physical Review B*. The research was funded by the Australian Research Counsel, the Australian Government, the National Security Agency and the Advanced Research and Development Activity.

Timeline: > 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Towards the fabrication of phosphorus qubits for a silicon quantum computer," posted on the Los Alamos National Laboratory archive at arXiv.org/abs/cond-mat/0104569

TRN

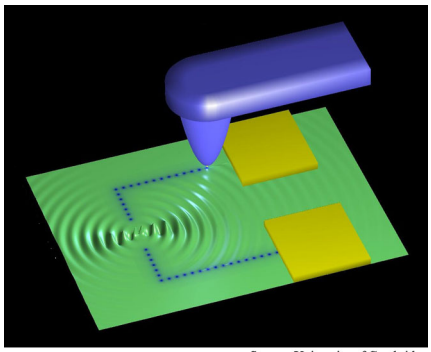
Tools and Resources

Tool Sketches Quantum Circuits

Technology Research News, August 27/September 3, 2003

Computer chips are manufactured using photo lithography—a technique that employs light and chemicals to etch microscopic features into silicon.

Researchers routinely use electron beam lithography, which uses beams of electrons instead of photons, to etch even smaller devices, like the quantum dots that trap single electrons to form the building blocks of quantum computers.



Source: University of Cambridge

This graphic depicts an atomic force microscope that has been modified to make prototype quantum computer circuits.

Electron beam lithography is a very slow process, however.

Researchers from Cambridge University in England and the Massachusetts Institute of Technology have developed a lithographic technique, dubbed erasable electrostatic lithography, that allows a quantum device to be drawn in a few hours rather than a couple of weeks.

The researchers modified a scanning tunneling microscope so that they could sketch charge patterns onto the surface of a piece of the semiconductor gallium arsenide and erase the patterns using red light. The surface charge, which draws from a subsurface sheet of electrons, defines working quantum components.

The researchers have used the method to define quantum wires, dots and hills, and are currently working on improving the technique's resolution, according to the researchers.

The method could be used practically in five years, according to the researchers. The work appeared in the August 14, 2003 issue of *Nature*.

TRN

Quantum Current Closer to Computing

By Kimberly Patch, Technology Research News
September 5, 2001

One way to significantly improve computers is to use something other than the presence or absence of electric current to signal the ones and zeros that form the binary logic of computing. One promising alternative takes advantage of the quantum nature of electrons.

Spintronics is an emerging field that uses the spin of electrons to represent ones and zeros. Electrons spin in one of two directions, up or down, which is roughly analogous to a top spinning clockwise or counterclockwise.

In theory, these two states of an electron would allow for ultra low-power conventional computers and would provide the means for moving information within and between

quantum computers. Proposed schemes for quantum computers use atoms or subatomic particles to represent ones and zeros and use quantum mechanics to check every possible answer to a problem at the same time.

In practice, there are many details to be worked out.

In order to use electron spin to signal a one or zero, the spins of a group, or current of electrons have to be aligned, and this collective spin must survive the electrons' transfer from one transistor to another and then last long enough to be useful.

Researchers from the University of California and Pennsylvania State University have moved spintronics a significant step forward by demonstrating that it is possible to efficiently move a current of electrons, with their collective spin intact, from one semiconductor material to another. In addition, the research shows that the spin state can be made to last as long as 100 nanoseconds, which is long enough to work for traditional computing.

"We have shown that spin lifetimes can exceed 100 nanoseconds and can be transported over distances exceeding 150 microns. In both cases, this exceeds the time and length scales used in today's technology," said David Awschalom, a physics professor at the University of California at Santa Barbara.

That this was fairly easy to accomplish surprised even the researchers. The implication of the results is that it should be possible to fabricate spin transistors, said Awschalom.

To investigate how practical using electron spin for computing could be, the researchers measured the spin of a current of electrons that was moving from a gallium arsenide semiconductor to a zinc selenide semiconductor. "I thought that this would be the simplest laboratory in which to test the basic idea: an atomically clean interface between two well-studied semiconductors," said Awschalom.

The researchers started by using polarized laser beams to create in a layer of gallium arsenide a reservoir of electrons whose spins were aligned. Ordinarily, only a small number of electrons from this reservoir would cross the barrier to a layer of zinc selenide and their spins would become random within a few hundred picoseconds, or trillions of a second. The researchers found that applying an electric field increased the number of electrons crossing the barrier by 40 times and also boosted the lifetime of the spins to usable levels.

Ultimately, the researchers hope to use electron spins for high-density information technology and fundamentally new methods of information processing like quantum computation, said Awschalom. If practical quantum computers can be built, they would be phenomenally fast for solving certain problems like cracking codes and searching large databases.

The experiments are something of a milestone in the spintronics field, said Jay Kikkawa, an assistant professor of physics and astronomy at the University of Pennsylvania.

In the experiments, the spin of the electron acts as an identification tag, said Kikkawa. "Its response to a magnetic field reveals the electron's magnetic history, which, in part, includes how long spins have spent in different layers," he said.

The researchers use this information to distinguish among several different channels within a spin current flowing across an interface between materials. "It's a very clever trick that one could never pull off in a purely electrical system," Kikkawa said. This is because electrical current consists of electric charge and the spins of its electrons are random.

Electron spins could be used in computing within the decade, Awschalom said.

Awschalom's research colleagues were Irina Malajovich of the University of California at Santa Barbara, and Joseph J. Berry and Nitin Samarth of Pennsylvania State University. They published the research in the June 14, 2001 issue of the journal *Nature*. The research was funded by the Defense Advanced Research Projects Agency (DARPA), the Office of Naval Research (ONR) and the National Science Foundation (NSF).

Timeline: < 10 years
Funding: Government
TRN Categories: Semiconductors and Superconductors; Quantum Computing
Story Type: News
Related Elements: Technical paper, "Persistent Sourcing of Coherence Spins for Multifunctional Semiconductor Spintronics," Nature, June 14, 2001

TRN

Shining a New Light on Electron Spin

By Ted Smalley Bowen, Technology Research News
January 3, 2001

Researchers are beginning to get a handle on how to build phenomenally powerful quantum processors, but figuring out how to shuttle data in and out of them is a major obstacle to making quantum computers practical.

University of Toronto researchers propose to solve the problem by using laser pulses to move electrons without introducing an electrical charge.

Because particles like electrons spin in one of two directions, the spin directions can represent the ones and zeros of binary computing. "The method allows us to sort electrons by their spin," said John Sipe, a physics professor at the University of Toronto.

Using light to control the flow of electrons could foster new data processing and data storage methods, as well as point the way to solid-state quantum computers.

Other researchers have preserved the spins of electrons while moving them the standard way using charge, and several research teams have demonstrated spin-based transistors that

could eventually yield ultralow-power processors and high-density data storage devices.

However, it would be extremely difficult to use charge to move electrons in quantum computers because quantum processors are extremely fragile and need to be insulated from their environments.

"People have suggested doing quantum computing with spins in solids, and our technique could be an important tool in moving spins around for information processing or read-in and read-out," said Sipe.

The Toronto researchers propose generating electron spin currents in semiconductors using the interference between two colors of light. The electrical currents could be controlled by adjusting the relative phase, or difference in wavelengths, of the two beams, according to the researchers. In this scheme, the interference would sort the electrons, sending those of one spin in one direction and those of the opposite spin in the opposite direction.

"Their idea is an exciting addition to the rapidly expanding collection of tools for optical manipulation of spin in solid state systems," said Jay Kikkawa, assistant professor of physics and astronomy at the University of Pennsylvania.

Sipe's research colleague was Ravi Bhat. The two published their work in the December 18, 2000 issue of *Physical Review Letters*. It was funded by the Ontario government's Photonics Research Ontario program and the Canadian government's National Sciences and Engineering Research Council.

Timeline: Unknown
Funding: Government
TRN Categories: Semiconductors, Quantum Computing
Story Type: News
Related Elements:Technical paper, "Optically Injected Spin Currents in Semiconductors," Physical Review Letters, December 18, 2000

TRN

Filters Distill Quantum Bits

By Eric Smalley, Technology Research News
March 21, 2001

To make quantum computers you need quantum bits, and to make quantum bits you need to entangle pairs of atoms or subatomic particles.

Entangling particles is old hat for physicists these days, and it can be done as simply as shining a laser on the right crystal. But entanglement is a matter of degrees, and one challenge for researchers building quantum computers and quantum cryptographic systems is getting the right amount.

"By and large... you want as much as possible," said Paul Kwiat, a physics professor at the University of Illinois.

Kwiat lead a team of researchers who developed a technique for distilling a collection of partially entangled pairs of photons down to a smaller number of more highly entangled photon pairs.

Two particles can become entangled, or linked, when they are in the quantum mechanical condition of superposition, which is a mixture of all possible states. When one of the entangled particles is measured, it collapses out of superposition into a random state and the other particle immediately collapses into the same state, regardless of the physical distance between them.

The researchers used polarization to distill the photon pairs. Because light is a type of electromagnetic radiation, it contains both electric and magnetic fields. The electric field of light vibrates in a plane perpendicular to the direction of the light wave. The electric field of unpolarized light vibrates in all directions in that plane, while the electric field of polarized light vibrates in only one direction.

The researchers sent the entangled photon pairs through partial polarizers, which partially filter light according to its polarization. "You can think of partial polarizers as a bad pair of sunglasses," said Kwiat.

However, it is inaccurate to consider a collection of entangled photon pairs as having some pairs that are more entangled than others and that the distillation process simply filters out the less entangled pairs, said Kwiat.

"They're all described by the same state, so all of them are... partially entangled," he said. "The net result [of the filtering process is] that you get less out on the other side. What does come through—what survives this filtering process—is then in a more highly entangled state," he said.

Ensuring a high degree of entanglement is crucial for some quantum cryptography proposals. "If you're trying to use entangled photons and your system gets... sufficient numbers of errors [due to partial entanglement], you could be leaking out too much information to some eavesdropper and there's no way of knowing that," said Kwiat.

The researchers are developing tools to measure the degree of entanglement, said Kwiat. "We're just now turning to the task of [using] these measures... as a sort of gauge, [an] entangle-meter," he said. "That hasn't really been implemented yet by anyone, but I think that's coming in the next year."

Practical quantum computers are at least two decades away, though quantum cryptographic systems could be developed within a decade, according to many researchers in the field.

Kwiat's research colleagues were Salvador Barraza-Lopez of the National Polytechnic Institute of Mexico, and André Stefanov and Nicolas Gisin of the University of Geneva. Kwiat and Barraza-Lopez were at the Los Alamos National Laboratory when they did the research. The researchers published the work in the February 22, 2001 issue of *Nature*. The research was funded by the National Security Agency, the Advanced Research and Development Activity (ARDA) and the European Union's Information Society Technologies (IST) Programme.

Timeline: 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Experimental entanglement distillation and 'hidden' non-locality," Nature, February 22, 2001

TRN

Rig Fires More Photon Pairs

Technology Research News, November 5/12, 2003

Many groups of researchers are working on quantum communications systems, which use attributes of individual photons to carry information.

Such systems are potentially very powerful because photons can be entangled, or connected so that attributes like polarization remain linked regardless of the distance between them.

Massachusetts Institute of Technology researchers have moved the field forward with entangled photon beams that contain specific wavelengths of light and are relatively bright.

Firing a laser into a certain type of crystal causes some single photons to become a pair of lower-energy entangled photons. The researchers generated 12,000 photon pairs per second per milliwatt of laser power by using a continuous split laser beam that hit the crystal from two directions.

The method produces relatively many entangled pairs of photons because it skips the filtering step usually required to remove unentangled photons, according to the researchers. The researchers produced entangled-photon beams at wavelengths of 795 nanometers, which is appropriate for quantum memory, and 1,600 nanometers, which be transmitted down a standard telecom fiber.

The researchers' next step is to make a brighter beam by adding an optical cavity, which amplifies light, to the device.

The project is part of a five-year program to transmit information over long distances using entanglement. The researchers presented the work at the Frontiers in Optics meeting of the Optical Society of America (OSA) in Tucson, Arizona October 5 to 9.

TRN

Laser Emits Linked Photons

By Eric Smalley, Technology Research News
November 7, 2001

The way lasers work can only be explained by quantum physics, the realm of atoms and subatomic particles. Lasers stimulate already-energized atoms, causing them to emit energy in the form of photons, the particles of light.

A team of researchers at the University of Oxford in England is taking the technology deeper into the bizarre regions of quantum physics with the development of a rudimentary laser that produces linked pairs of photons.

The work promises to make perfectly secure communications devices more practical and advance long-term efforts to build ultra-powerful quantum computers.

The device makes it easier to produce linked, or entangled, sets of two or even four photons. The researchers have demonstrated "laser-like operation" for entangled photons, said Antia Lamas-Linares, a graduate student at the University of Oxford.

When two or more quantum particles become entangled, one or more of their properties march in lockstep. For example, two photons can have their polarizations, or electric field orientations, entangled.

But when photons are entangled they exist in an unmeasurable netherworld of quantum mechanics where they are in some mixture of all possible polarizations until one of the pair is observed or otherwise comes into contact with the environment. When this happens, both photons are knocked out of entanglement and into the same definite polarization, regardless of the physical distance between them.

The usual way of producing pairs of entangled photons is shining ultraviolet laser light into a crystal, which transforms a tiny percentage of the ultraviolet photons into entangled pairs of infrared photons. The Oxford device bounces the entangled photon pairs back into the crystal while the laser is still shining on it. For each pair sent back into the crystal, four new pairs are generated.

The laser action produces more pairs of entangled photons for the same amount of power as non-lasing schemes, "and, perhaps more importantly, higher-number entangled photon states," she said.

Ordinary conversion produces about 5,000 detectable photon pairs per second, said Lamas-Linares. "Our source in its current form would produce four times more pairs, and the number would grow exponentially with the number of passes." In addition, the device entangles groups of four photons. "Current sources produce about one 4-photon state per minute, while our source will amplify this by a factor of 16, making it feasible to perform experiments on them," she said.

The Oxford device currently passes the light through the crystal only twice. Ordinary lasers use a reflective chamber, or cavity, to bounce light back and forth through a gas hundreds of times, each pass causing the gas atoms to emit more photons.

The researchers' next step is to add a reflective cavity to their device, making it more like a true laser and multiplying further the number of entangled photons it could produce.

"We are working on building a cavity system... to obtain a more conventional lasing action," said Lamas-Linares.

The goal is to produce a device that can generate useful numbers of pairs of entangled photons. "Entanglements are the main resource in quantum information," said Lamas-Linares. "One of the main problems in the field currently is to produce entanglement in a controllable and reliable way."

Current sources of entangled photons are not bright enough for some proposed quantum information processing experiments and a brighter source would make them possible, said Paul Kwiat, a professor of physics at the University of Illinois. A true entangled-photon laser "would be a very bright source of entanglement," he said.

The Oxford source of entangled photons could be used for quantum cryptography in five years and is currently being used as a tool by physicists to explore the fundamentals of quantum mechanics, said Lamas-Linares. "That is really our main interest," she said.

Lamas-Linares' research colleagues were John C. Howell and Dik Bouwmeester of the University of Oxford. They published the research in the August 30, 2001 issue of the journal *Nature*. The research was funded by the UK Engineering and Physical Sciences Research Council (EPSRC), the UK Defense Evaluation and Research Agency and the European Union (EU).

Timeline: 5 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Stimulated Emission of Polarization-Entangled Photons," Nature, August 30, 2001

TRN

Method Measures Quantum Quirk

By Eric Smalley, Technology Research News
November 13/20, 2002

Quantum entanglement, which Einstein once dismissed as impossible, is a physical resource that could transform information processing. It is key to producing phenomenally powerful quantum computers, and is the critical component of the most secure form of quantum cryptography.

Until now, however, researchers have had no way to measure entanglement directly, but have had to rely on indirect measurements or mathematical estimates.

Researchers from the Technical University of Gdansk in Poland and the University of Cambridge in England have come up with a scheme for measuring entanglement that could give scientists the means to judge the purity of the primary resource used in quantum information processing.

The scheme could mark the beginning of quantum metrology—the science of quantum measurement, said Artur Ekert, a professor of quantum physics at the University of Cambridge. "Efficient tests for quantum entanglement will be important in all applications where quantum entanglement is used," he said.

Entanglement links physical properties, such as polarization or momentum, of two or more atoms or subatomic particles. It is part of numerous schemes for secure communication, precise frequency standards, atomic clocks and clock synchronization.

When an atom or subatomic particle is isolated from its environment, it enters into the weird state of superposition, meaning it is in some mixture of all possible states. For example, a photon can be polarized in one of two opposite directions. In superposition, however, the photon is polarized in some mixture of both directions at the same time.

When two or more particles in superposition come into contact with each other, they can become entangled. A common example is photons that have their polarizations entangled. When one of the photons is knocked out of superposition to become, say, vertically polarized, the other photon leaves superposition at the same instant and also becomes vertically polarized, regardless of the distance between them.

Existing methods of checking for entanglement involve either indirect measurements, which are inefficient and leave many entangled states undetected, or a mathematical estimation, Ekert said.

The researchers' method is similar to the mathematical approach, but works on the particles directly rather than on a mathematical representation of them. "We have managed to find a physical operation that mimics the mathematical one," said Ekert.

Quantum operations alter particles that are used as quantum bits, or qubits, to represent the 1s and 0s of computing in quantum information systems. One way to carry out a quantum operation is to use a laser beam to rotate an atom held in a magnetic trap so that its orientation flips from a position representing a 1 to a position representing a 0. The basic logic of quantum computing is made up of many series of these quantum operations.

The researchers' entanglement-detection method could be included in several proposed architectures for quantum computers, including ion traps, which hold individual atoms in magnetic fields, and quantum dots, which trap individual electrons in microscopic specks of semiconductor material, according to Ekert.

The research is excellent; it is an original idea about how to detect entanglement in an efficient way, said Vlatko Vedral, a lecturer of physics at Imperial College and the University of Oxford in England. "One of the most fundamental issues in quantum information theory is whether two systems are entangled or not," he said. Scientists have had a good theoretical understanding of how to detect entanglement, but these methods are not practical in the physical world because

they involve physical impossibilities like reversing time, he said.

The researchers have come up with a practical method of testing for entanglement, said Vedral. The basic idea is to mix a bit of noise into the operation so there will always be a physically possible result, he said. "It turns out that this mixing can be performed in an efficient way," he added.

Entanglement is crucial for quantum communications, said Vedral. "Some forms of quantum cryptography depend critically on the presence of entanglement and cannot be implemented without it," he said.

It's not yet clear how useful being able to measure entanglement will be for quantum computing because researchers do not know if there is a direct link between amount of entanglement and the speed of quantum computers, Vedral said. "Everything indicates that entanglement is an important ingredient, but how much of it is enough to be clearly better than any classical computer remains an open question," he said.

The method could be used in practical applications in two to five years, said Ekert. It is likely to be used first in quantum cryptography and frequency standards, he said.

Ekert's research colleague was Pawe Horodecki of the Technical University of Gdansk in Poland. They published the research in the September 16, 2002 issue of *Physical Review Letters*. The research was funded by the Polish Committee for Scientific Research, the European Commission, Elsag SpA, the Engineering and Physical Sciences Research Council and the Royal Society of London.

Timeline: 2-5 years, 20 years
Funding: Government, Corporate
TRN Categories: Physics; Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Method for Direct Detection of Quantum Entanglement," Physical Review Letters, September 16, 2002

TRN

Self-Learning Eases Quantum Computing

By Eric Smalley, Technology Research News
July 10/17, 2002

Ordinary computers are rather simple devices, logically speaking. They cannot learn and they have to plow through large problems one step at a time.

Two largely experimental methods of computing—neural networks and quantum computing—go beyond these limitations by mimicking biological brains, and exploiting the quirks of quantum physics, respectively.

A team of researchers at Wichita State University is aiming to combine the two techniques in order to use neural networks' proven capacity for learning to help realize quantum computing's potential to solve astronomically large problems.

The researchers made a simulation of a quantum neural network and used it to show how the theoretical devices could calculate the quantum mechanical property of entanglement. Calculating entanglement was an unsolved problem in field of quantum computing, said Elizabeth Behrman, an associate professor of physics at Wichita State University.

Entanglement is one of the weirder traits of quantum physics. When a subatomic particle or atom is isolated from the environment and cannot be observed, it enters into the quantum mechanical state of superposition, meaning it is in some mixture of all possible states. For example, a particle can spin in one of two directions, up or down. In superposition, however, the particle spins in some mixture of both directions at the same time.

When two or more particles in superposition come into contact with each other, they can become entangled, meaning one or more of their properties, like spin or polarization, become linked, and move in lockstep. Two entangled photons could, for example, have linked polarizations. When one of the photons is knocked out of superposition to become vertically polarized, the other photon leaves superposition at the same instant and also becomes vertically polarized, regardless of the distance between them.

Entanglement allows quantum logic operations to work on many particles at once. A quantum computer can take advantage of entanglement to check every possible answer to a problem with one series of operations across a group of entangled particles rather than having to check each possible answer one at a time.

"Entanglement is the basis for the power of quantum computing," said Behrman. It is the reason quantum computers are theoretically able to do computations that cannot be done by even the fastest possible classical computer, she said.

Quantum computers are extremely delicate, however, and only a few simple prototypes have been built. And researchers have only come up with a few algorithms to use them with. Bringing neural networks into the picture could solve both of these problems, according to Behrman.

Artificial neural networks consist of virtual nerve cells, or neurons, linked by virtual synapses. Neurons communicate with each other through the synapses, with the output from one neuron becoming the input to another. Like biological synapses, the virtual synapses grow stronger with use and weaken with disuse. Repeated input to a neural network wears a distinct path through the neurons. In other words, neural networks learn.

"A neural network, like the one between your ears, is different from the computer on your desk in several important ways," said Behrman.

Because neural networks learn, they can handle incomplete data and scale up automatically to handle larger problems. "All three of these characteristics would be great boons to quantum computers," said Behrman.

For example, it is difficult to construct the algorithms, or software a quantum computer needs to solve a problem, she said. "A quantum neural computer... essentially constructs its own algorithm," she said.

The entanglement calculation demonstrates that quantum neural networks should be able to work for any of the many difficult problems that researchers are building quantum computers to solve, said Behrman. "We don't need to construct an algorithm for each of them if we have a quantum neural network," she said.

The ability of neural networks to handle incomplete data could be helpful because quantum computers are very sensitive to noise, said Behrman. "We're working on showing that neural computers can help with this [problem], too, but we haven't yet demonstrated it," she said.

Quantum neural networks could also help make larger quantum computers. "The advantages of scale-up are obvious," said Behrman. "At the moment, we have quantum computers that are only of the size of a few qubits."

Quantifying entanglement is a very important question in quantum information theory, said Vlatko Vedral, a lecturer of physics at Imperial College and Oxford University in England. "Entanglement is at the root of quantum teleportation, quantum cryptography and some quantum algorithms," he said.

Having a computer that learns to compute an entanglement algorithm is useful because the algorithm "involves an optimization procedure that is difficult to perform," he said.

The idea of using a quantum neural network to compute entanglement needs to be more thoroughly explored to determine if it offers any advantages, however, said Vedral. "One thing that is not convincing in the [researchers'] paper is that their method is efficient," he said.

The Wichita State University researchers are beginning a collaboration with other researchers to attempt to build a quantum neural network, said Behrman. Quantum neural networks could be used in practical applications within 10 years, she said.

Behrman's research colleagues were Vishwas Chandreshekar, Zhonghua Wang, Chaitra Belar, James Steck and Steven Skinner of Wichita State University. The research was funded by the National Science Foundation (NSF).

Timeline: <10 years
Funding: Government
TRN Categories: Quantum Computing and Communications; NeuralNetworks
Story Type: News

Related Elements: Technical paper, "A Quantum Neural Network Computes Entanglement," posted on the arXive physics archive at arXiv.org/abs/quant-ph/0202131

TRN

Tool Reads Quantum Bits

By Kimberly Patch, Technology Research News
August 1/8, 2001

The key to quantum computing is being able to use the spins of subatomic particles such as electrons to represent the ones and zeros of computing. A particle can be spin-up or spin-down in a way similar to a top spinning either clockwise or counterclockwise.

If you could reliably distinguish between spin-up and spin-down energy in large numbers of particles, the spin possibilities in each particle could serve as a quantum bit, or qubit, representing a one or a zero, and you could build a fantastically powerful computer in very little space.

The trouble is, it's difficult to measure spin. Scientists have done so by trapping isolated atoms and using lasers to measure spin states, but they are still a long way from being able to read the millions of quantum bits required to form a practical quantum computer.

Researchers at the University of California at Berkeley have taken a step towards that goal by showing that it is possible to measure the spin of a quantum state of an electron in a nickel atom embedded in a copper oxide crystal. The development has the potential to make a promising quantum computer scheme considerably more practical.

There are four major problems to be solved in making a quantum computer: its qubits must be able to represent a one or zero long enough for the computer to perform logic operations on them; the qubits must be able to interact with each other to carry out those operations; there must be some way to read the information contained in a qubit in order to see the results of the operations; and the system must contain a lot of qubits to do useful computing.

By measuring the spin of a single atom, the Berkeley researchers have found a way to read the information contained in a certain type of qubit. This type of qubit—a single atom embedded in a solid made of other atoms— has already shown potential for solving the other three problems associated with quantum computing.

A theoretical proposal by University of Maryland researcher Bruce Kane shows that qubits made from phosphorus atoms embedded in silicon could hold their spin states for a long enough time to do computing, could be placed closely enough to interact with each other, and could be made in a large quantity.

The Berkeley method addresses the key missing piece in that plan by showing that it is possible to measure the spin of

a single electron within an impurity, or atom of one material embedded in another.

The researchers used a scanning tunneling microscope (STM) to measure the spin of an electron associated with a nickel impurity embedded in copper oxide, but they had to make some modifications to do so.

Scanning tunneling microscopes use tips that resemble needles, but are so sharp that they taper to a single atom. The tip hovers over the surface of a material and maps the changes the material's electron energy makes to the electron current flowing through the tip similar to the way a seismograph maps movement.

Because spin-up and spin-down states have different energy, the researchers were able to distinguish between them. "We are trying to get an electron to jump into one of the quantum states from a nearby metal tip. The spin-down state exists at a lower energy than the spin-up state at the atom we studied, so by measuring the rate at which the electrons jump into the state as a function of their energy we can tell which is which," said Davis.

To make the scheme work, however, the researchers had to solve a pair of problems.

First, the spin energy of an electron can only be split into discernible spin-up or spin-down states under certain conditions, said Davis. "In each [impurity] atom there's a single wave function of the electron... you can split that wave function into a spin-up and spin-down state if you're in a high magnetic field at low temperatures," he said.

The amount by which the two energy levels are split is proportional to the strength of the magnetic field, so the stronger the magnetic field, the easier it is to distinguish the two levels.

Second, heat energy easily drowns out spin energy. "The amount of energy associated with the temperature has to be smaller than the splitting between the two levels [otherwise] thermal energy would just be knocking electrons up and down from the bottom [energy level] to the top one all the time," Davis said.

The researchers solved the problems by measuring electron spin in a nickel impurity embedded in a superconductor at a relatively low temperature.

Copper oxide is a high-temperature superconductor, meaning its electrons are free to travel without resistance at 85 degrees Kelvin, or -188 degrees Celsius, which, though very cold, is less cold than the temperatures of 4 degrees Kelvin, or -269 degrees Celsius required by low-temperature superconductors.

Because nickel is magnetic, it exerts a magnetic force that is very strong at distances of 10 or 20 nanometers away from the atom. "The effective field at the nickel atom is hundreds of Tesla. So we didn't need a big external magnet, we got it for free by putting a magnetic atom into the solid," said Davis.

The researchers next plan to use the same technique to measure electron spin in a phosphorus atom embedded in a silicon chip, which is the setup required in the Kane quantum computer proposal.

Because phosphorus is not magnetic, the Berkeley researchers need to generate a large magnetic field in order to measure the spins of its quantum particles. The researchers are planning to build an STM that can generate an eight Tesla field at temperatures as low as 20 millikelvin in order to carry out the measurements, said Davis.

If the researchers are able to measure spin states in phosphorus atoms, "then that's really big news because that was the really big problem of the Kane proposal," said Paul Kwiat, a physics professor at the University of Illinois at Urbana-Champaign.

"The main reason people were skeptical about [the Kane proposal] was the need for reading out single spins, which seemed like it was not going to be very easy, and it still may not be very easy. But certainly this is an experiment in the right direction," Kwiat said.

The Kane proposal is probably the most promising model so far for quantum computing, largely because it is based on silicon, Kwiat added. "If you can do something in silicon... and you get it to work, you can hand it to the silicon industry," he said.

Researchers in the quantum field generally agree that practical quantum computers are at least two decades away, if they can be built at all. "It's like asking when fusion will generate cheap energy. It's a possible but technically hard challenge," said Davis.

Davis' research colleagues were Eric W. Hudson of the University of California at Berkeley and the National Institute of Standards and Technology, Christine M. Lang and Vidya Madhavan of the University of California at Berkeley, Shuheng H. Pan of the University of California at Berkeley and Boston University, Hiroshi Eisaki from the University of Tokyo in Japan and Stanford University, and Shin-ichi Uchida of the University of Tokyo.

They published the research in the June 21, 2001 issue of the journal *Nature*. The research was funded by the Office of Naval Research (ONR) and the Department of Energy (DOE).

Timeline: > 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Interplay of Magnesium and High Tc Superconductivity at Individual Ni Impurity Atoms in Bi2Sr2CaCu2O8+ d," Nature, June 21, 2000; Additional images at the Davis group website: Socrates.Berkeley.edu/~davisgrp/stm/results/nickel/index.htm

TRN

Storage

Fiber Loop Makes Quantum Memory

By Eric Smalley, Technology Research News
April 9/16, 2003

A relatively simple device that sends individual photons cycling through a fiber-optic loop could provide the memory needed to make ultra powerful computers that use the quantum states of light as bits.

Quantum computers are potentially powerful enough to solve problems that are beyond the most powerful classical computers, including cracking the strongest secret codes and quickly searching huge databases.

Several research teams have shown that it is possible to carry out logic operations using the traits of individual photons—the fleeting particles of light—as quantum bits that represent the 1s and 0s of computing. Computers must also be able to briefly store the outcomes of logic operations.

Scientists at Johns Hopkins University have come up with a method for capturing photonic qubits for tiny fractions of a second, which enables them to briefly store information about the state of a quantum particle. The memory device consists of a storage loop and a switch that directs photons into and out of the loop.

The memory device stores a qubit by switching a photon into the loop, where it flies around at the speed of light, said James D. Franson, a physicist at Johns Hopkins University's Applied Physics Laboratory. A short time later, the state of the qubit can be read by switching the photon back out of the loop, he said.

The memory stores binary information that is based on the polarization of photons. A photon is polarized when its electric field vibrates in one of four directions: horizontal, vertical and the two diagonals. The directions are paired, and one of each pair can represent 1 and the other 0.

The researchers used a polarizing beam splitter, which is transparent to one polarization and acts like a mirror to the other, to shunt photons into and out of the loop. The beam splitter separates the two polarization components of the photon, causing one to loop in one direction and the other to loop in the opposite direction. "You can envision these components as traveling in counterpropagating directions through the device," said Franson.

It is only possible to split the polarization components of a photon when the photon is in the weird state of superposition, meaning it is in some mix of the two polarizations at the same time. Quantum particles like photons enter superposition when they are unobserved and otherwise isolated from their environments.

When the photon in the loop passes the opening, it goes through a switch. When the switch is closed, it continuously flips the values of the photon's polarization components, turning horizontal polarization to vertical and vice versa. This causes both parts of the photon to hit the mirror portion of the beam splitter, which keeps the photon inside the loop. When the switch is opened, it no longer changes the polarizations and the photon passes through the beam splitter and exits the loop in the same superposition state as when it entered.

A photon takes 13 nanoseconds, or billionths of a second, to make one round-trip through the memory device, said Franson.

Optical quantum computers are likely to employ laser pulse trains, or pulses of laser light fired at regular intervals. "These pulse trains provide a natural clock cycle for the various quantum logic operations [and] memory readouts," said Franson. The cyclical nature of the memory device fits well with this type of architecture, he said.

In principle, the researchers' device is resistant to errors caused by light-phase shifts, said Franson. As a photon makes multiple passes through the storage device, its wave can gradually stretch or compress at different rates depending on polarization. These changes are neutralized, however, because the storage device repeatedly flips the polarizations, said Franson. "These phase shifts essentially factor out of the final state and may, in some applications, not affect subsequent computations using the stored qubits," he said.

Although researchers have known for a long time that optical fibers can store photons, "this might be the first demonstration," said Eli Yablonovitch, a professor of electrical engineering at the University of California at Los Angeles.

The researchers' device "is a very cute way to provide a limited amount memory" for linear optical quantum computing, said Jonathan Dowling, a principal scientist and supervisor of the quantum computing technologies group of at NASA's Jet Propulsion Laboratory. Its potential uses are limited because "it likely cannot robustly hold the qubits for very long periods of time required for... quantum communication applications such as quantum optical repeaters," he said. Repeaters boost fading signals along communications lines.

The researchers' current prototype cannot store information long because it suffers from photon loss, said Franson. "We estimated about 19 percent loss per cycle, which means we really couldn't store the qubits for very long," he said. In principle, the loss can be overcome by a better design, custom optics and possibly new types of fiber optic components, he said.

Scientists are exploring other means of storing optical qubits, including trapping photons in special semiconductor devices and transferring quantum information from photons to groups of atoms. "Many of these techniques rely on very clever manipulations of fascinating physics," said Franson. The researchers' method is less interesting for basic physics, "but may have some technical advantages for certain applications

in the near term," he said. The devices are relatively simple and their timing corresponds to the repetition rate of commercially available lasers commonly used in optical quantum computing experiments, he said.

The researchers are now working on storing a pair of entangled qubits in a pair of synchronized cyclical memory devices, said Franson. Controlling entangled qubits is key to unleashing the power of quantum computing.

If two particles in superposition come into contact, one or more of their properties, like polarization, can become linked, or entangled. If two photons have their polarizations entangled, when one of the photons is measured and leaves superposition, the other photon leaves superposition in the same instant and assumes the opposite polarization regardless of the distance between them.

A sufficiently long string of qubits in superposition can represent every possible solution to a particular problem. Entanglement allows a quantum computer to check all possible solutions with one set of operations. Ordinary computers are much slower because they have to check answers one at a time.

The cyclical memory device could be used in practical applications in five to ten years, said Franson.

Researchers generally agree that full-scale quantum computers are 20 years away.

Franson's research colleague was Todd B. Pittman. The research appeared in the December 5, 2002 issue of *Physical Review A*. The research was funded by the Office of Naval Research (ONR), the Army Research Office (ARO), the National Security Agency (NSA), the Advanced Research Development Activity (ARDA), and the Department of Defense's Independent Research & Development (IR & D) program.

Timeline: 5-10 years
Funding: Government
TRN Categories: Physics; Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Cyclical Quantum Memory for Photonic Qubits," Physical Review A, December 5, 2002.

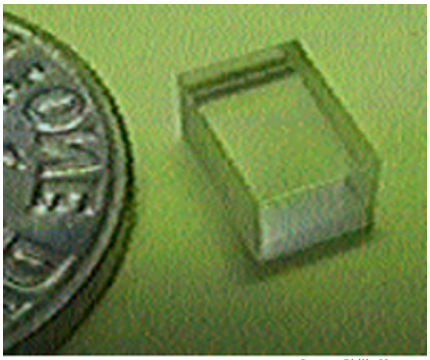
TRN

Crystal Stores Light Pulse

By Eric Smalley, Technology Research News
January 30, 2002

A year ago, two research teams independently announced that they had stored light pulses in the atoms of gases and then reconstituted the stored pulses. A third research team has accomplished the same feat using a solid material, a crystal that could eventually be used to make quantum computer memory chips.

Quantum computers would theoretically be much faster than today's classical computers in solving certain problems like cracking secret codes, but are difficult to build because quantum information is extremely fragile.



Source: Philip Hemmer

The metal atoms in this small crystal slab can hold the impression of a light pulse, effectively storing the pulse. The crystal could be a precursor to quantum computer memory chips.

Being able to store quantum information for relatively long periods of time would go a long way toward making practical quantum computers feasible. "Most quantum processors require storage," said Philip Hemmer an associate professor of physics at Texas A&M University. "For quantum storage, the advantages of the crystal [over a gas] are a much larger storage capacity, potentially much longer storage times, and the relative ease of incorporating [it] into a system," he said.

Hemmer's research team from the U.S. and South Korea was able to store light pulses in a crystal for a few tenths of a millisecond, which is comparable to what the previous experiments accomplished using gases, said Hemmer.

The researchers stored light in a yttrium silicate crystal with small amounts of the rare earth metal praseodymium added to it. Light doesn't travel through opaque matter because its photons are absorbed by the material's atoms.

The researchers fired a control laser beam into the crystal's atoms in order to overload them with photons. At the same time, they sent a weaker pulse of light of a different frequency into the crystal. The interaction between this weaker light pulse and the crystal's overloaded atoms introduced drag, which slowed the pulse to about 45 meters per second, or 100 miles per hour. Light travels through a vacuum at 186,000 miles per second.

When the researchers turned the control laser beam off, the slowed light pulse disappeared, but left an impression in the crystal's atoms. When the researchers turned the control beam back on, the pulse was reconstituted from the information stored in the atoms and it continued through the crystal.

The technique could eventually be used to store quantum information.

Quantum particles can be in one of two complementary states. For example, photons can be polarized vertically or horizontally and atoms can be spinning in one of two directions, up or down.

Using those states to represent the ones and zeros of digital information, the particles can serve as quantum bits, or qubits. The qubits that represent the output of a quantum processor could be transferred to photons that could then be sent to a quantum memory chip where the qubits could be transferred to atoms in the chip for storage.

The researchers have a ways to go before they produce a quantum memory chip. In their experiment, they stored a light pulse consisting of many photons. "The next steps will be to attempt storage of single photons, and to improve the efficiency to be close to 100 percent," said Hemmer. It could be 10 years before the light storage technique is used in practical applications, he said.

"Slow light and light storage in solids are very exciting," said David Phillips, a physicist at the Harvard-Smithsonian Center for Astrophysics. "This experimental demonstration brings us a step closer to the era of serious applications of the underlying physical concepts. While these materials still require cryogenic temperatures to show the coherence times necessary for light storage, perhaps more easily utilized materials will be developed in the future," he said.

Hemmer's research colleagues were Alexey Turukhin and Sudi Sudarshanam of the Massachusetts Institute of Technology, Selim Shahriar, now at Northwestern University, Joe Musser of Texas A&M University, Byoung Ham of the Electronics and Telecommunications Research Institute in South Korea. They published the research in the January 14, 2002 issue of the journal *Physical Review Letters*. The research was funded by the Air Force Research Laboratory, the Army Research Office, the Air Force Office of Scientific Research, and the Korean Ministry of Science and Technology.

Timeline: 10 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Observation of Ultraslow and Stored Light Pulses in a Solid," Physical Review Letters, January 14, 2002

TRN

Stored Light Altered

By Eric Smalley, Technology Research News
November 14, 2001

Controlling interactions among individual particles of light and matter could give rise to phenomenally powerful quantum computers and devices that provide perfectly secure communications.

Quantum computers will need to transfer information stored in photons, which are easy to transmit, and atoms, which is easier to use for calculations.

Researchers at the Harvard-Smithsonian Center for Astrophysics have taken their second step this year toward this goal. In January, they brought a light pulse to a halt inside a chamber of gas atoms, stored an imprint of the pulse in the atoms and then reconstituted the pulse. Now they have figured out how to alter the light information as it is stored in the group of atoms.

This is possible because the process preserves the phase of the stored light, said Phillips. "The phase of the light is transferred onto the phase of the atoms and back to the light during the light storage process," he said.

This phase information can represent the ones and zeros of computing.

The phase of a lightwave corresponds to its position in the cycle between the crest and trough. Individual photons also contain wave phase information.

An atom's phase is different. It is "related mathematically to the phases of a child's top or a gyroscope as it rotates on its axis and precesses," said Phillips. If you set a top spinning on a post, then tip the top onto its side, instead of falling off the post it will hang there sideways, rotating, or precessing, around the post. The phase of a precessing top is its position in the circle it makes as it travels around the top of the post.

The researchers found that the phase information of the light pulse remains stable and accessible when it is imprinted in the atoms: if the light pulse is in one phase when it is stored in the atoms, the pulse remains in that phase when it is restored.

This makes it possible to change the phase while the pulse information is stored. "We can apply a magnetic field to our atoms during the storage process to shift the phase of the atoms," which in turn changes that phase of the reconstituted light, said Phillips.

So far the researchers have only stored ordinary light beams using the technique. However, demonstrating control over the phase of the light opens the door for using the technique to coax the quantum properties of particles to do computing.

Being able to store and manipulate particle properties like phase paves the way for building devices that store and transmit this quantum information. Quantum repeaters, for example, could restore the quantum information in photons, which begins to destabilize after traveling 10 kilometers or so through fiber-optic communications lines. Like repeaters in conventional computer networks, quantum repeaters would make it possible to send quantum information over much longer distances. Phillips' Harvard colleague Mikhail Lukin and researchers at the University of Innsbruck in Austria have designed a quantum repeater based on the light storage technique.

Many researchers say it is likely to take decades for full-blown quantum computers to become practical. It may be possible to use quantum information for cryptography sooner, however, said Phillips. "The light storage technique could prove useful as part of a quantum repeater in such a system.

I would be surprised if the techniques involved in stored light moved out of the academic lab and into the development lab in less than five years, though," he said.

The researchers' next step is using the technique to store the quantum information from a single photon, said Phillips.

Phillips' research colleagues were Lukin, Alois Mair, Jean Hager and Ronald L. Walsworth of the Harvard-Smithsonian Center for Astrophysics. The research was funded by the National Science Foundation (NSF), the Office of Naval Research (ONR) and NASA.

Timeline: > 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Phase Coherence and Control of Stored Photonic Information," posted on the arXiv physics archive at arXiv.org/abs/quant-ph/0108046; Technical paper, "Long-Distance Quantum Communication with Atomic Ensembles and Linear Optics," posted on the arXiv physics archive at arXiv.org/abs/quant-ph/0105105

TRN

Communications

Teleportation Goes the Distance

By Eric Smalley, Technology Research News
February 12/19, 2003

You can't get from one place to another without passing through every point in between. This is true for all matter and energy, whether planets, people or quantum particles.

You can, however, do the quantum equivalent of faxing particles from one place to another, if the particles in question are photons. Teleportation makes it possible to transmit the quantum states, or structural information, of photons from one place to another.

And making photons from one location materialize at another without traveling the distance between opens the way for sending perfectly secure messages long distances.

Researchers at the University of Geneva in Switzerland and the University of Aarhus in Denmark have teleported photons from one laboratory to another lab 55 meters away, and their setup simulated a distance of two kilometers. Previous teleportation experiments have been limited to short distances within laboratories.

Quantum states, which dictate the ultimate structure of objects, can be teleported, said Nicholas Gisin, a professor of physics at the University of Geneva. The key to teleportation is that only this information is transported. "Objects can be transferred from one place to another without ever existing anywhere in between. But only the structure is teleported. The original object is destroyed and reconstructed," he said.

Teleportation relies on entanglement, a weird aspect of quantum physics. Entanglement links one or more physical properties of two or more particles, for example the polarizations, or orientations, of a pair of photons.

Particles become entangled when they are in superposition, which is a mixture of all possible quantum states. Superposition occurs when particles are isolated from their environments. A photon can be polarized in one of two opposite directions, for example, but in superposition it is polarized in some mix of both.

When a pair of particles in superposition come into contact with each other, they can become entangled. When one of the particles comes into contact with the environment and is knocked out of superposition, it is in one definite quantum state. At the same instant, regardless of the distance between them, the other particle is also knocked out of superposition and assumes the same quantum state.

Previous teleportation experiments have used photons whose polarizations are entangled. The Geneva researchers' method relied on time bins, or short time windows, said Gisin. The researchers generated photons using ultra-short laser pulses, counted time in these small increments, or bins, and timed the pulses to occur in specific bins.

Photons in superposition reside in two time bins at once, Gisin said. And photons in superposition can be entangled. The key to the researchers' teleportation experiment was entangling these photons based on time bins, because this allows them to survive transmission over fiber-optic lines better than polarization-entangled photons, he said. A pair of entangled particles can serve as transmitter and receiver to teleport a third particle.

The researchers entangled a pair of infrared photons and sent one to the second lab, then teleported a third photon by bringing it into contact with the entangled photon in the first lab. The third photon was destroyed and the entangled photon in the second lab became a replica of the third photon.

The researchers used photons of the same wavelengths used in ordinary optical communications, and they transmitted the entangled photon over a two-kilometer fiber-optic cable, proving that it is possible to teleport particles over distances.

Researchers are aiming to use teleportation to build quantum relays in order to extend the reach of quantum communications systems. Ordinary optical communications lines use repeaters to boost fading signals, but repeaters make copies of the fading photons and quantum states can't be copied without being destroyed.

Quantum relays would be a big boost for quantum cryptography, which is by far the most advanced quantum communications application, said Gisin.

Quantum cryptography allows a sender and receiver to tell for sure whether the encryption key they are using has been compromised by an eavesdropper. An encryption key is a string of numbers used to lock and unlock messages.

Last year, the Geneva researchers demonstrated a quantum cryptography system that transported a secure key over ordinary phone lines spanning 67 kilometers between Geneva and Lausanne. However, the quantum states of photons can't survive longer distances, making quantum relays necessary for long distance quantum cryptography.

The Geneva researchers are working on finding the limits for the distances between relays and determining the trade-offs between distance and performance for practical applications, said Gisin. They are also working on improving the stability of their experimental setup, he said.

Practical applications could be ready in five to ten years, said Gisin.

Gisin's research colleagues were Ivan Marcikic, Hugues de Reidmatten and Hugo Zbinden of the University of Geneva, and Wolfgang Tittel of the University of Geneva and the University of Aarhus in Denmark. They published the research in the January 30, 2003 issue of the journal *Nature*. The research was funded by the Swiss National Science Foundation and the European Community.

Timeline: 5-10 years
Funding: Government
TRN Categories: Quantum Computing and Communications
Story Type: News
Related Elements: Technical Paper, "Long-Distance Teleportation of Qubits at Telecommunication Wavelengths," Nature, January 30, 2003

TRN

Device Would Boost Quantum Messages

By Eric Smalley, Technology Research News
November 28, 2001

Quantum physics makes it possible to send perfectly secure messages, and researchers have already achieved quantum cryptography in the laboratory.

The main stumbling block to using quantum cryptography in practical systems, however, is figuring out how to send the fragile quantum states of light used in the schemes over long distances. "At the moment, quantum cryptography is restricted to several tens of kilometers," said Ignacio Cirac, a professor of physics at the University of Innsbruck in Austria.

Cirac and several colleagues have found a way to boost quantum signals that could help make quantum cryptography practical within a decade.

Signals, whether optical or electrical, fade as they travel down communications lines. Messages wouldn't get very far if it weren't for repeaters, which are simple devices that receive a weakening optical or electrical pulse and send out a stronger pulse.

Ordinary repeaters, however, don't work with quantum communications. This is because quantum signals contain photons that are in the weird quantum mechanical condition of superposition. This means the photons are in some unknown mix of all possible states. For example, a photon is both vertically and horizontally polarized when it is in superposition, and so could come out of superposition horizontally or vertically polarized.

When a photon is observed or otherwise comes into contact with its environment, it is knocked out of superposition and can no longer be used for quantum communications. The trouble with ordinary optical repeaters is they have to observe photons in order to copy them.

To get around this problem, the researchers have proposed a way of storing quantum information in small clouds of atoms and forwarding the information from one atom cloud to another using photons. The device would transfer the weakened quantum information carried by inbound photons to the atoms, correct any errors in it, and then transfer it to outbound photons to produce a stronger signal. This would take place without disturbing the quantum state of the information.

"We have found a way of building quantum repeaters using [sets of atoms]," said Cirac. "A set of several thousands or millions of atoms are used to store quantum information in a given location, correct it, and send it to the next set of atoms."

Other proposals for building quantum repeaters call for transferring quantum information between individual atoms and photons, which is difficult to do, said Cirac. The researchers' scheme has several advantages over these proposals because "we do not have to isolate atoms, no low temperature is required, and quantum gates are not required either," he said. Quantum logic gates take the quantum states of particles through a series of changes in order to perform simple mathematical calculations. This is difficult to do even in carefully controlled laboratory environments.

The researchers' proposal quantum-mechanically links, or entangles, two distant containers of gas atoms. When two or more photons are entangled, one or more of their properties stay in lockstep while the particles are in superposition. For example, researchers can entangle two photons so that when one of the photons is knocked out of superposition and becomes, for instance, horizontally polarized, the other photon also leaves superposition and becomes horizontally polarized at the same instant, regardless of the physical distance between them.

The work is an improvement over other schemes because it uses large numbers of atoms to store the information light carries in quantum communications, said Emanuel Knill, a mathematician at Los Alamos National Laboratory. Other researchers are beginning to conduct experiments that demonstrate the advantages of using these groups of atoms in quantum information processing, he said.

One advantage of the researchers' proposal is that most of the errors this scheme is likely to generate yield no photons, said Knill. In quantum communications, there are two types of errors: photons appearing when none are called for and an absence of photons when they are expected. "Some of their suggested applications intrinsically reject errors, which only results in a relatively mild — though not negligible — loss in efficiency over distance," he said.

The experimental setup needed to implement the proposal is similar to the one recently used by researchers at the University of Aarhus in Denmark to demonstrate entanglement between two samples of gas atoms, said Cirac.

"As soon as quantum cryptography is used in practical applications — this may happen in five to ten years — quantum repeaters will be needed to extend the distances," said Cirac. "Our proposal can then play a... practical role."

Cirac's research colleagues were Lu-Ming Duan of the University of Innsbruck and the University of Science and Technology of China, Mikhail D. Lukin of Harvard University and Peter Zoller of the University of Innsbruck. They published the research in the November 22, 2001 issue of the journal *Nature*. The research was funded by the Austrian Science Foundation, the European Union (EU), the European Science Foundation, the National Science Foundation (NSF) and the Chinese Science Foundation.

Timeline: 5-10 years
Funding: Government
TRN Categories: Quantum Computing; Cryptography and Security
Story Type: News
Related Elements: Technical paper, "Long-Distance Quantum Communication with Atomic Ensembles and Linear Optics," Nature, November 22, 2001

TRN

Proposal Would Marry Atom and Photon

By Eric Smalley, Technology Research News
February 7, 2001

Neither atoms nor photons are ideal for building quantum computers. Atoms are easy to store and manipulate but difficult to transport. Photons, on the other hand, are hard to manipulate and harder still to store. But they're made to move.

Some researchers are trying to figure out how to use the best of both. After all, conventional computers use both electricity and magnetism to handle bits: electricity for manipulating and moving them and magnetism for long-term storage. The goal is to build a quantum computer that uses both atoms and photons. The key is linking an atom to a photon in the quantum mechanical state of entanglement.

"Having one of each entangled means that a quantum device could readily store and manipulate the atom while sending the photon off to a distant receiver," said Michael G. Moore, a postdoctoral fellow at the Institute for Theoretical Atomic and Molecular Physics at the Harvard-Smithsonian Center for Astrophysics.

But while converting an electric bit to a magnetic bit is relatively straightforward, transferring information between a photon and an atom in an orderly fashion is a major challenge. One scheme, proposed by Moore and a colleague at the University of Arizona, calls for entangling atom-photon pairs by firing a laser into a Bose Einstein condensate.

A Bose Einstein condensate is an exotic form of matter formed by chilling atoms to near absolute zero. The atoms in a Bose Einstein condensate share the same wave function, meaning they are in the same state and orientation. This is analogous to the photons in a laser beam.

"By using a Bose Einstein condensate it should be possible to... create entangled atom-photon pairs in a highly controlled manner," said Moore.

Two particles can become entangled, or linked, when they are in the quantum mechanical condition of superposition, which is a mixture of all possible states. When one of the entangled particles is measured, it collapses out of superposition into a random state and the other particle immediately collapses into the same state, regardless of the physical distance between them.

When a photon of the right wavelength hits an atom, it bounces off rather than being absorbed. Sometimes when a photon bounces off an atom the two become entangled. However, if a second photon hits the atom it knocks the atom out of its quantum mechanical state and breaks the entanglement with the first photon.

The advantage of using a Bose Einstein condensate is that it contains large numbers of atoms—typically about one million—relative to the number of photons, said Moore. This makes it more likely that only one photon will hit each atom.

Quantum computers hold the promise of solving problems that ordinary computers cannot, such as searching massive databases and cracking powerful encryption codes, but quantum computers are likely decades away. Entangled atom-photon pairs could find use sooner, however.

The entangled pairs could be used for quantum cryptography and quantum teleportation, said Moore. Quantum cryptography and quantum teleportation have already been demonstrated using entangled photons.

Using quantum cryptography, a sender can transmit a series of individual photons to a receiver. Anyone eavesdropping on the communications would necessarily alter the state of the photons, revealing the security breach.

In quantum teleportation, the quantum state of a particle can be reproduced in another location by using a pair of particles that are entangled but separated in space as a sort of quantum fax machine.

It should be possible to demonstrate quantum cryptography or quantum teleportation with atom-photon pairs in five to ten years, said Moore.

Moore's research colleague was Pierre Meystre, a professor of physics at the University of Arizona. They published the research in the December 11, 2000 issue of *Physical Review Letters*. The research was funded by the Office of Naval Research, the National Science Foundation, the Army Research Office and the Joint Services Optics Program.

Timeline: 5-10 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Generating Entangled Atom-Photon Pairs from Bose-Einstein Condensates," Physical Review Letters, December 11, 2000

TRN

Quantum Network Withstands Noise

By Eric Smalley, Technology Research News
January 30, 2002

If practical quantum computers are ever built, chances are that someone will want to link them together. Quantum computing uses individual particles like atoms to represent the ones and zeros of digital information, and would theoretically solve certain problems that are beyond the capabilities of ordinary computers, like cracking secret codes and searching large databases.

The challenge to linking quantum computers is in building a network capable of carrying fragile quantum information across not-so-gentle fiber-optic lines, then reliably transferring the information from one quantum particle to another.

To that end, a team of researchers at the Massachusetts Institute of Technology and the U.S. Air Force Research Laboratory has proposed a scheme for transmitting and storing quantum information in a series of quantum network nodes. The researchers are aiming to space network nodes as far as 10 kilometers apart, according to Selim M. Shahriar, now an associate professor of physics at Northwestern University.

A quantum network could theoretically be used for perfectly secure communications, to transmit quantum information from one quantum computer to another, or to link logic units within quantum computers.

The researchers' quantum network scheme compensates for errors produced by weakened signals, failed handoffs between photons and atoms, and false readings by the system's detectors. "The key advantage of our scheme is that it is robust against errors," said Shahriar. Under the scheme, errors do not destroy data, but "only reduce the rate at which we can communicate. It does not affect the accuracy or fidelity of the communication process," he said.

The scheme calls for building a series of network nodes that each holds a single atom, and transferring information represented by the quantum states of photons, which can travel down fiber-optic lines, to the quantum states of these atoms. Entangling a pair of photons, sending each to a separate node in the quantum network, and transferring the photons' quantum states to the atoms causes the atoms to become entangled with each other.

Entanglement, which is one of the weirder traits of quantum physics, is the critical element in many quantum computing and communications schemes. When a subatomic particle or atom is undisturbed it enters into the quantum mechanical state of superposition, meaning it is in some mixture of all possible states. For example, particles can spin in one of two directions, up or down. In superposition, however, the particles spin in some mixture of both directions at the same time.

When two or more particles in superposition come into contact with each other, they can become entangled, meaning one or more of their properties are correlated. For example, two entangled photons could have the same polarizations. When one of the photons is knocked out of superposition and becomes, say, vertically polarized, the other photon leaves superposition at the same instant and also becomes vertically polarized, regardless of the distance between them.

Entanglement lies at the heart of quantum computers' theoretical ability to solve problems that will always remain beyond the reach of even the most powerful classical computer because it allows quantum logic operations to work on many particles at once. A quantum computer can take advantage of entanglement to check every possible answer to a problem with one series of operations rather than having to check each possible answer one at a time.

The researchers' scheme is a method for entangling distant atoms. Quantum information is transmitted between entangled particles via quantum teleportation, which is akin to faxing quantum particles. A pair of entangled atoms serve as transmitter and receiver, said Shahriar. "The atom you want to teleport is then brought close to the transmitter," he said. "A simple set of measurements is then made on the transmitter end and the observations are sent via any method, such as a phone call, to the receiver end. A simple operation on the receiver atom then turns it into a copy of the one we want to teleport."

Using quantum teleportation, qubits could be transmitted across a quantum network.

"It's an interesting idea," said Paul Kwiat, a professor of physics at the University of Illinois at Urbana-Champaign. "[But] at the moment it's not really clear what you would do with a quantum network. It might be good for hooking together quantum computers, if we had them," he said.

Quantum network nodes could eventually extend quantum cryptography, which is currently limited to point-to-point communications lines, said Kwiat. "One could imagine having quantum cryptography over a whole network," he said.

The researchers are still working on producing the entangled photons and storing single atoms, said Shahriar. "Once these are ready, we will embark on demonstrating the teleportation process itself."

The key to making useful quantum network nodes is building a chip with an array of optical cavities that each hold a single atom at its center, Shahriar said. It will be at least 10 years before a quantum network could be used for practical applications, he said.

Shahriar's research colleagues were Seth Lloyd of the Massachusetts Institute of Technology and Philip Hemmer, now at Texas A&M University. They published the research in the October 15, 2001 issue of the journal *Physical Review Letters*. The research was funded by the Army Research Office and the Air Force Office of Scientific Research.

Timeline: > 10 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Long Distance, Unconditional Teleportation of Atomic States via Complete Bell State Measurements," Physical Review Letters, October 15, 2001

TRN

Algorithms

Quantum Demo Does Tricky Computing

By Eric Smalley, Technology Research News
January 2, 2002

Quantum computers can theoretically solve problems that are beyond even the most powerful possible classical computer—like cracking secret codes—by using the bizarre properties of quantum particles to search through large numbers of possible answers at once.

Scientists from IBM Research and Stanford University have built a quantum computer out of seven atoms and used the computer to show that factoring the number 15 results in the numbers 3 and 5.

Though seven atoms doesn't sound like a lot and factoring 15 is not a big problem, the device is something of a milestone in quantum computing. Seven atoms constitute a large device by the standards of the prototype quantum computers built to date, and running a factoring algorithm on the atoms shows that they can be controlled well enough to process information.

The researchers' device is unlikely to lead directly to a practical quantum computer, but their results could make it easier to design and build quantum computers in general. "Showing that we can factor 15 with a quantum computer is akin to how researchers demonstrated early electronic computers calculating digits of the number Pi," said Isaac L. Chuang, now an associate professor at the Massachusetts Institute of Technology. "It is a milestone, but not a useful feat in and of itself."

The researchers' quantum computer consisted of five fluorine and two carbon atoms that were part of a molecule suspended in a test tube of liquid. Particles like atoms and electrons spin either up or down, similar to a top spinning clockwise or counterclockwise, and these spin directions can represent the ones and zeros of computing.

The researchers turned these atomic quantum bits on and off with a series of carefully timed radio wave pulses that reversed the spins of the atoms. This nuclear magnetic resonance (NMR) quantum computing method is based on the same technology used in MRI medical imaging machines.

What makes quantum bits, or qubits, more powerful than regular computer bits is that when quantum particles are isolated from the environment and cannot be observed, they enter the quantum mechanical state of superposition, which means they are in some mixture of both spin up and spin down. This allows a qubit to represent both one and zero at the same time, and a relatively small number of qubits to represent many numbers at once.

Particles can also be linked, or entangled. When changes are made to one entangled particle, they all change the same way regardless of the physical distance between them, as long as they remain in superposition. Using this bizarre property, quantum computers can theoretically examine every possible answer to a problem with one series of operations rather than having to check each individually, which means they could solve problems that are beyond the capabilities of the most powerful classical computer conceivable.

The way the researchers simulated, designed and operated their computer is probably more significant than what they did with it. "[That] we know how to accurately model errors occurring to large-scale, complicated quantum information processing systems will be the most useful technical component of our achievement," said Chuang.

Researchers generally agree that liquid nuclear magnetic resonance is unlikely to lead to practical quantum computers because it is probably not possible to make NMR quantum computers much bigger than seven qubits. However, the way the researchers use the spin of the atoms to compute is compatible with many quantum computer designs, including those based on semiconductor devices. "The methods we demonstrated for controlling these spins... will generally be how future quantum information processing machines are controlled and programmed," said Chuang.

The research "is an exquisite demonstration of control over complex pulse sequences combined with a growing bag of tricks for compiling quantum computing circuits," said Daniel Lidar, an assistant professor of chemistry at the University of Toronto. "There is no doubt that these techniques... will

be useful for eventual scalable solid-state quantum computing implementations."

The researchers' experiment is one of only a small number that have implemented such complex algorithms, said Emanuel Knill, a mathematician at Los Alamos National Laboratory. "The real significance is in the demonstration of techniques for the control of quantum computers. Any other comparably complex algorithm with a definite and verifiable answer can serve this purpose," he said.

Unfortunately, the researchers did not provide the scales necessary to compare their data, said Knill. "This makes it impossible to determine how well their experiment worked and how well the measured [results] compared to simulation. As a result, the value of this contribution as a demonstration of quantum control is significantly lessened," he said.

According to many researchers, it is likely to be at least 20 years before practical quantum computers can be built.

There is also a chance that practical general-purpose quantum computers will never be built, said Chuang. "Classical computing itself is growing in performance in leaps and bounds, and in terms of raw computational power, quantum computers may never be competitive," said Chuang.

Chuang's research colleagues were Lieven M. K. Vandersypen and Mathias Steffen of Stanford University and IBM Research, and Gregory Breyta, Costantino S. Yannoni and Mark H. Sherwood of IBM Research. They published the research in the December 20/27, 2001 issue of the journal *Nature*. The research was funded by IBM and the Defense Advanced Research Projects Agency (DARPA).

Timeline: 20 years
Funding: Corporate; Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance," Nature, December 20/27, 2001

TRN

Simulation Hints at Quantum Computer Power

By Eric Smalley, Technology Research News
May 2/9, 2001

Planning the best route to take for, say, running errands seems like a fairly simple problem. But the number of possibilities increases exponentially with each additional destination. For 15 destinations there are billions of possible routes.

To make matters worse, there are no known mathematical shortcuts for finding the most efficient route. Solving the problem means comparing every route. "The number of possibilities with 500 [destinations] is huge. It's more than astronomically big," said Edward Farhi, a professor of physics at the Massachusetts Institute of Technology.

"If all the computers in the world were operating since the beginning of time, they could not go through a list that long. Ordinary computers could never find an answer to that problem by blind searching," he said.

An algorithm developed by a team of researchers based at MIT, however, raises the tantalizing possibility that quantum computers will be able to solve it. Route optimization is an NP-complete problem, which is the class of problems whose solution times increase exponentially with the size of the problem, and mathematically solving one NP-complete problem solves them all.

An algorithm that solves this type of currently unsolvable problem would have a wide range of practical uses, from laying out circuit boards to scheduling flights to analyzing genes. Existing algorithms used on NP-complete problems that have large numbers of possibilities can only provide estimates.

Researchers have proved that quantum computers will be able to crack encrypted codes and search large, unstructured databases that are far beyond the abilities of even the most powerful classical computers. If researchers can prove that quantum computers will also be able to solve NP-complete problems, they will significantly broaden the range of potential uses for quantum computers.

The researchers simulated a quantum computer consisting of 20 quantum bits, or qubits, on an ordinary computer and then ran their algorithm on the simulation. They tested the algorithm with randomly generated instances of the NP-complete problem Exact Cover, which starts with a group of subsets of some number of items. The subsets have the same number of items but they can overlap each other. The problem is to find the subgroup of subsets that includes all of the items but that has no overlapping subsets.

The running time for the algorithm increased only quadratically rather than exponentially relative to the increase in the size of the problem. Quadratic time is the square of the size of the problem. Exponential time is the size of the problem to the power of three or greater. Although the time it took the algorithm to solve the problem grew as the number of possibilities increased, the quadratic growth rate didn't outstrip the theoretical ability of a quantum computer to solve large instances of the problem, according to Farhi.

The results are encouraging but far from conclusive. The researchers still need to demonstrate that classical computers require exponentially longer times to solve the same problem and that their quantum algorithm requires only quadratically longer times for larger instances of the problem than they were able to simulate. And even then, they would have only demonstrated that the algorithm outperforms classical computers for randomly generated, though difficult instances of the problem.

"What would really be convincing about the efficacy of our method would be a mathematical proof. In the absence of that, I would just say we're accumulating evidence," said Farhi.

Actually solving the problem means proving that the algorithm would work in quadratic amounts of time for every possible instance of the problem, said Farhi.

"This is very interesting work," said David Meyer, a research professor in the mathematics department at the University of California at San Diego. "It provides some hope that quantum computers may be generally useful, rather than only special interest." Researchers must demonstrate general utility in order to justify the immense resources that will be required to build quantum computers, he said.

It is possible, though not certain, that researchers will be able to determine conclusively whether quantum computers will outperform classical computers for NP-complete problems before actually building practical quantum computers, said Farhi. Practical quantum computers, which require hundreds of connected qubits, will likely take 20 years to develop, he said.

Farhi's research colleagues were Jeffrey Goldstone, Joshua Lapan, Andrew Lundgren and Daniel Preda of MIT and Sam Gutmann of Northeastern University. They published the research in the April 20, 2001 issue of the journal *Science*. The research was funded by the Department of Energy and MIT.

Timeline: 20 years
Funding: Government, University
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem," Science, April 20, 2001

TRN

Quantum Software Gets the Picture

By Eric Smalley, Technology Research News
September 4/11, 2002, 2002

When you look at a tile floor, you may think about how well the pattern goes with the rest of the room, but you won't wonder whether there is a pattern there in the first place.

A computer, on the other hand, would have a hard time simply figuring out that a black tile followed by a white tile followed by a black tile followed by a white tile constitutes a pattern.

It is clear that quantum computers, which use the quirks of quantum physics to compute, will be orders of magnitude more efficient at many tasks than ordinary, classical computers, if and when sufficiently large quantum computers can be built.

A physicist at the University of British Columbia has come up with an algorithm that proves that quantum computers would be faster at finding patterns, too. "Finding and recognizing [a linear] pattern can be accomplished much faster on a quantum computer than on a classical one," said Ralf Schützhold, a researcher at the University of British Columbia.

The algorithm would allow quantum computers to detect an 8-by-8 grid of alternating black and white squares set in an array of 640 otherwise randomly distributed squares.

This seemingly simple task takes a classical computer about 6,000 steps because it would have to compare each square to every other square, one at a time.

A quantum computer, however, can examine all of the possible solutions to a problem at the same time, in this case comparing all the squares to each other at once. The algorithm proves that this particular task can be represented mathematically in a way that a quantum computer can carry it out.

Quantum computers can check all solutions at once because they use atoms or subatomic particles to make quantum bits, or qubits. The particles have two opposite orientations that can represent the 1s and 0s of computer information.

The power of a quantum computer comes from the quirky physics of these tiny particles. When a particle is isolated from its environment it is in the weird quantum state of superposition, meaning it is in both orientations at once, and so can represent a mix of 1 and 0. This allows a string of particles in superposition to represent every combination of 1s and 0s at the same time, and a quantum computer to process all the numbers that represent possible solutions to a problem with one set of operations.

The pattern-finding algorithm is an addition to a growing set of quantum algorithms based on the quantum Fourier transform, a mathematical formula for finding order.

Other researchers have demonstrated that quantum computers would be exponentially faster than classical computers for pattern-matching tasks like finding a mug shot in a database that matches an image from a security camera. Schützhold's pattern-finding algorithm performs the first task of a pattern recognition application: finding patterns in raw data.

Pattern finding is a key component of speech, face, and handwriting recognition programs, and of software that sorts seismographs and other large sets of scientific data, said Schützhold. The exponential speed-up promised by quantum computers might enable us to attack problems that would take classical computers "longer than the age of the universe" to solve, he said.

This particular algorithm is not likely to be used in practical applications, however. "The problem I discussed is very

simple and probably not extremely important or relevant for practical applications," said Schützhold. "My main point is to demonstrate the possible exponential speed-up," he said.

The pattern-finding algorithm is also not a particularly efficient quantum algorithm, said David Meyer, a mathematics professor at the University of California at San Diego. But it is important for demonstrating that quantum computers could be used to speed up image processing tasks, he said. "There are probably other image processing problems for which quantum algorithms will be more successful," he added.

Researchers generally agree that it is likely to take at least two decades to develop practical quantum computers. Quantum computing research is now at a stage comparable to when electrical engineers began to build and combine small numbers of transistors half a century ago, said Schützhold.

Transistors are electrical switches that combine to form the basic logic circuits of computers. Today's PCs have about one billion transistors. Useful quantum computers will require at least one million qubits, the quantum equivalent of transistors. The largest prototype quantum computer built so far had seven qubits.

The research was funded by the Alexander von Humboldt Foundation in Germany and the Natural Sciences and Engineering Research Council of Canada (NSERC).

Timeline: > 20 years
Funding: Private, Government
TRN Categories: Data Structures and Algorithms; Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Pattern recognition on a quantum computer," posted on the arXive physics archive at arXiv.org/abs/quant-ph/0208063

TRN

Quantum Data Compares Faster

By Kimberly Patch, Technology Research News
January 23, 2002

Although computers that use quantum particles like atoms or electrons to represent the ones and zeros of computing are at least two decades from practical reality, researchers are finding that quantum computers can theoretically compute exponentially faster than the fastest possible electronic computer—at least for some tasks.

Researchers from Canada and the Netherlands have found a mathematical fingerprinting scheme that would allow quantum computers to compare two sets of data much more efficiently than is possible with the classical computers we use today.

This quantum fingerprinting scheme increases the list of mathematical problems that quantum computers would be able to solve much faster than classical computers. "It gives an example of a fairly natural problem where quantum communication is exponentially more efficient than classical communication," said Ronald de Wolf, who was a researcher at the Center for Mathematics and Computer Science in the Netherlands when the work was done, but is now at the University of California at Berkeley. Other examples include factoring large numbers to crack secret codes and searching large databases.

The fingerprinting scheme could eventually be used to produce efficient communications among quantum computers, and also in quantum cryptography, said de Wolf.

Quantum computers use different states of quantum particles like atoms or electrons to represent the ones and zeros of computing as quantum bits, or qubits. For example, an electron can be spin up, or spin down in a way similar to a top which spins either clockwise or counterclockwise.

The fingerprinting scheme essentially allows researchers to make a much smaller mathematical fingerprint of a set of data. It takes less computing power and communications bandwidth to work with the fingerprints rather than the full data sets to, for instance, compare them. The quantum scheme allows a mathematical fingerprint of a set of data to be more than an order of magnitude smaller than would be possible using today's classical computers.

The mathematics involves three steps. First, the data is plotted in an imaginary, many-dimensional space.

Second, the information in the many-dimensional space is boiled down, or fingerprinted, using only a small number of qubits. The number of qubits needed is equal to the logarithm of the number of dimensions involved. The logarithm of a number, which is the number of times 10 must be multiplied together to equal that number, increases very slowly relative to the size of the number. For example, the logarithm of 10 is 1 and the logarithm of 100 is 2.

Third, it is possible to test whether two given quantum states are equal, which allows two data sets plotted and fingerprinted this way to be compared. "There is no classical analog to the second or third [steps]," making it impossible for classical computers to do this,just delete" said de Wolf.

Instead, today's computers require a number of bits equal to the square root of the number of dimensions, which is a much larger number than the logarithm. For example, the square root of 10 is 3.16 and the square root of 100 is 10.

For a 1-megabyte set of data, a classical computer fingerprint would require 3,000 bits, while the quantum fingerprint would be only 25 quantum bits long. The gap widens as the data set grows. For a 1,000-gigabyte set of data, a classical fingerprint would take up 3 million bits, and the quantum scheme only 45 quantum bits. There are eight bits in one byte of data.

What makes qubits mathematically more flexible has to do with the weird quantum properties of particles. Rather than simply representing a 1 or a 0, a qubit is a superposition of both, meaning it has a certain probability of being a 0 and

a certain probability of being a 1. The two possibilities are complex numbers whose squared values add up to the total of both. "The point of quantum bits... is that their state can be partly zero and partly one at the same time. Mathematically... it's this superposition of things that would exclude each other in the classical world that matters," said de Wolf.

What the mathematics boils down to is the quantum fingerprinting scheme exponentially reduces the amount of communication required for comparing sets of data, said de Wolf.

For example, if Alice and Bob were on distance spaceships that could not communicate with each other, but could only send messages to a command center on earth, in order to compare two large sets of data from Alice and Bob, the command center would only require Alice and Bob to send the fingerprints rather than the full data set, de Wolf said.

It's exciting work, said Emanuel Knill, a mathematician at Los Alamos National Laboratory. It is "one way in which two people with large documents but limited communication can efficiently determine whether the documents or the same are not." The work establishes that quantum computing could be exponentially more efficient in this type of communications than today's computers, he added.

The researchers could implement the work in the laboratory within a few years, according to de Wolf. The quantum computers that would use the scheme, however, are further off. Most researchers agree it will be at least 20 years before practical quantum computers could be built.

De Wolf's research colleagues were Harry Berman of the University of Amsterdam and the Center for Mathematics and Computer Science (CWI) in the Netherlands, and Richard Cleve and John Watrous of the University of Calgary in Canada. They published the work in *Physical Review Letters*, September 26, 2001. The research was funded by the European Union and Natural Sciences and Engineering Research Council of Canada (NSERC).

Timeline: 3 years, > 20 years
Funding: Government
TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Quantum Fingerprinting," Physical Review Letters, September 2001, also posted in the arXiv physics archive at arXiv.org/abs/quant-ph/0102001.

TRN

Quantum Code Splits Secrets

By Eric Smalley, Technology Research News
October 10, 2001

IBM researchers have shown that tapping the weird quantum properties of particles like atoms and photons would improve on a classic technique that allows a group of people to hold pieces of a secret that can only be revealed by combining the pieces.

When a secret is too important for any one person to know, secret-sharing cryptographic protocols provide a way to break up the secret into parts held by several or even many people. The protocols keep the secret until all or most of the parts are assembled.

Adding a quantum component to this scheme would make it harder for the people holding the pieces to cheat or be coerced into revealing the secret.

The IBM scheme is a step in that direction. "We haven't done anything so sophisticated in the quantum version" as splitting a secret into many parts, said David P. DiVincenzo, a physicist at IBM Research. "We've just been investigating the simple case of splitting a secret into two."

The quantum secret-sharing scheme is similar to quantum cryptography and quantum computing because it relies on the quantum mechanical condition of entanglement.

Particles like atoms are usually either spin up or spin down, meaning that the axes they spin around point either up or down relative to the magnetic field around the atoms. But when atoms or other particles are isolated from the environment and cannot be observed, they enter the quantum mechanical state of superposition, which means they are in some mixture of both spin up and spin down.

Two or more particles in superposition can be entangled so that even if they are separated, when one of them is measured and becomes either spin up or spin down the other particle immediately leaves superposition and assumes the same spin regardless of the distance between them.

There are four possible combinations of spins for a pair of entangled particles. One combination, called a singlet, stands out from the other three, which are called triplets.

The quantum secret-sharing scheme represents a bit of information by creating a string of entangled pairs of particles. An odd number of singlets in the string represents a one, and an even number of singlets represents a zero.

Because the two particles have to be together in order to tell whether they form a singlet or a triplet, two people sharing a secret this way couldn't simply measure their halves of the string and compare notes to tell whether the bit is a one or a zero. This makes quantum versions of secret-sharing protocols more secure than classical versions.

"If the parts of the secret are actually pieces of a quantum state, then even communication—at least communication of the ordinary, classical sort—can be insufficient for them to reconstruct the secret," said DiVincenzo. "They need to do something stronger. They need some kind of additional quantum technology in order to unlock the secret," he said.

The needed quantum technology could be a quantum communications channel. If the polarization of photons were used rather than the spin of atoms, the photons could be transmitted while preserving their quantum states.

In order to carry out the scheme, however, there must be a way to store the quantum states of particles for long periods of time.

"This scheme is not something that can be realized in the immediate future, except as a demonstration," said Daniel Gottesman, a fellow at the Clay Mathematics Institute and a visiting scholar at the University of California at Berkeley. "You need to store the quantum states until it comes time to open the secret, and it will be a while until we can do that reliably."

Quantum secret sharing "would require a good quantum memory and the ability to measure qubits. Some of the rudiments of what are needed in this scheme are available today," said DiVincenzo.

Practical quantum secret sharing will also require the development of quantum repeaters in order to send quantum information over distances greater than the roughly 10 kilometers possible today. Repeaters boost signals traveling along communications lines.

Quantum repeaters could be developed in about six years but quantum memory will probably take longer, said DiVincenzo. "That gets into the cloudy future," he said.

It also remains to be seen whether the added property of requiring quantum communications makes for a more useful form of secret sharing, Gottesman said.

It should be possible to make a practical form of the quantum secret-sharing scheme before large-scale quantum computers can be built, said DiVincenzo. Large-scale quantum computers are probably more than 20 years away, according to many researchers.

DiVincenzo's research colleagues were Barbara M. Terhal and Debbie W. Leung of IBM Research. They published the research in the June 18, 2001 issue of the journal *Physical Review Letters*. The research was funded by the National Security Agency (NSA), the Army Research Office and IBM.

Timeline: Unknown
Funding: Government; Corporate
TRN Categories: Cryptography and Security; Quantum Computing
Story Type: News
Related Elements: Technical paper, "Hiding Bits in Bell States," Physical Review Letters, June 18, 2001

TRN

Sampling Ability Broadens Quantum Computing

By Eric Smalley, Technology Research News
June 28/July 5, 2000

Though quantum computers are not likely to emerge from the laboratory for a long time, the range of problems they will eventually be able to tackle is steadily expanding. Lucent Technologies' Bell Labs last month announced an algorithm that will allow quantum computers to do sampling computations, expanding their potential capabilities beyond factorization and searching.

The sampling algorithm, written by Bell Labs' researcher Lov K. Grover, enables three types of applications for quantum computing: statistical sampling, searching with sketchy information and Monte Carlo integration, which is a technique for approximating the answers to scientific problems that are too difficult to solve.

Although only simple prototypes have been built to date, quantum computers have proven to be blazingly fast. Quantum computers solve problems almost instantly because they process every possible answer simultaneously. The difficulty is in extracting the answer. At the heart of each quantum algorithm is a series of quantum mechanical operations that ensure that when the system is measured, and thus taken out of its quantum state, the answer is preserved.

Quantum computers are so fast because there are far fewer quantum mechanical operations in a quantum algorithm than steps in a comparable classical algorithm. If an algorithm on a classical computer takes 100 steps to solve a problem, a comparable quantum algorithm would take the square root of 100, or 10, steps. The advantage increases as the problem gets more complicated: only the most powerful supercomputers running for weeks can crack the Data Encryption Standard because it takes about 1018 steps. The square root of 1018 is one billion. Some of today's desktop computers can process one billion steps in one second.

Grover's quantum sampling algorithm is similar to classical algorithms that use sampling but takes advantage of the quantum speed-up. "The difference is that usually the classical problem is so complicated that no one bothers to solve it as it is," Grover said.

Grover's algorithm allows searches through large numbers of possibilities using queries that can yield more than one right answer. In these searches, the queries use multiple terms which can be weighted according to probabilities. For example, you would be able to search through a city telephone directory using information like first name and neighborhood if you were unsure of the last name of the person you were looking for. You would select possible last names and give them probabilities and the algorithm would return the closest matches based on all the information, Grover said.

The sampling algorithm is an extension of a quantum search algorithm Grover devised in 1996. That algorithm was a major breakthrough in the fledgling field of quantum computing because it gave the theoretical devices some of the capabilities of today's classical computers. The sampling algorithm could yield an even broader range of applications for quantum computers, Grover said.

Although the sampling algorithm is probably not as "novel and exciting" as Grover's original search algorithm, no one doubts the importance of sampling on quantum computers, said Daniel Lidar, a physicist researching quantum computing at the University of California at Berkeley. Lidar co-authored a paper that extended Grover's original search algorithm to support random distributions, which in turn was a precursor to Grover's sampling algorithm.

Quantum computers, and thus the sampling algorithm, are not likely to be commercially available for more than two decades, according to Grover. Funding for the project was supplied by the National Security Agency and the U.S. Army Research Office.

Timeline: >20 years
Funding: Government
TRN Categories: Quantum Computing; Data Structures and Algorithms
Story Type: News
Related Elements: "Technical paper: Rapid sampling through quantum computing" presented at the Association for Computing Machinery's Symposium on the Theory of Computing (STOC), May, 2000.

TRN

Portfolios Boost Quantum Computing

By Eric Smalley, Technology Research News
February 6, 2002

Financial advisers commonly tell investors to diversify their portfolios in order to minimize risk. This concept is also true in computing.

Just as multiple investments allow investors to better balance financial risk and reward, a mix of algorithms will work better than any single algorithm to solve computer problems that take varying amounts of time for each attempt. In computing, the potential risk is that any given attempt will require a lot of time, while the potential reward is a quick solution.

Researchers who previously proved this point for classical computing have shown that the portfolio strategy will also improve the performance of quantum computers.

In both classical and quantum computing, the advantage of using the portfolio strategy boils down to having a range of tools available in the face of the unknown.

In classical computing, these types of problems include scheduling and route-planning problems that require each possibility to be examined one at a time, and Web searches and robot navigation that exist in variable environments like the Internet or the physical world. "For an algorithm or program that has a certain probability of executing in a given time, many trials of that algorithm will [vary] in their finishing times," said Bernardo Huberman, a scientist at Hewlett-Packard Laboratories.

In their previous work, the researchers identified that variance for these hard combinatorial classical computer problems, and were able to construct a mixture of algorithms that decreased the variability and also increased performance.

Quantum algorithms by their nature are probabilistic, varying in unknown ways on different problems, said Huberman. According to the researchers' calculations, the gain in efficiency in using portfolios of quantum algorithms is equivalent to the gain in using portfolios of classical algorithms.

In quantum computing, the length of time a program runs is set beforehand and the question is whether it will succeed. The variability is in the likelihood of success. Using portfolios of algorithms will improve those chances of success.

In addition, it might be possible to use the weirdness of quantum mechanics to further increase the efficiency by combining contributions from multiple algorithms, said Huberman.

Quantum computing can in theory use the interactions of atoms and subatomic particles to solve certain problems like cracking secret codes and searching large databases much faster than the fastest classical computer possible.

Quantum particles like atoms and electrons can spin in one of two directions, up or down. These two directions can represent the ones and zeros of digital information. When a subatomic particle or atom is undisturbed it enters into the weird quantum mechanical state of superposition, meaning it is in some unknown mixture of all possible states. In superposition, the particles spin in some mixture of up and down at the same time.

In these unknown superpositions, particles have certain probabilities of being in any one state. Quantum algorithms run a certain number of operations based on these probabilities. After the algorithm goes through the given number of operations, the results are examined, which destroys the superposition. If the computer did not find the answer during these operations, the problem must be run all over again.

Quantum portfolios would allow the researchers to find the algorithm with the best chance of finding the answer for a given problem and number of operations.

Taking advantage of quantum portfolios will require practical quantum computers, which are probably decades away. "Twenty years sounds like a safe bet," said Huberman.

Huberman's research colleagues were Sebastian M. Maurer of Stanford University and Tad Hogg of Hewlett-Packard Labs. They published their research in the December 17, 2001 issue of the journal *Physical Review Letters*. The research was funded by the Fannie and John Hertz Foundation and Hewlett-Packard Company.

Timeline: 20 years
Funding: Private, Corporate

TRN Categories: Quantum Computing
Story Type: News
Related Elements: Technical paper, "Quantum portfolios," Physical Review Letters, December 17, 2001

TRN

Programming Goes Quantum

By Eric Smalley, Technology Research News
March 28/April 4, 2001

Quantum computing is in an embryonic stage of development and the field is still firmly in the hands of those who study atoms, electrons and photons for a living.

But a few computer scientists and mathematicians who also speak the language of physics are beginning to prepare for the inevitable handover to the programmers who make today's computers useful.

A group based in Italy is among the latest researchers who are attempting to bridge the chasm between traditional programming tools and the inscrutable world of quantum mechanics. The researchers are building a programming architecture for quantum computing.

The researchers are developing a C++ class library, or vocabulary for the C++ programming language, that is designed for quantum computing. The class library will contain basic building blocks for programming quantum computers, including registers, operators and instructions for manipulating quantum bits.

Registers are slots where computer processors temporarily place numbers like values and addresses as they are working on them. Operators are instructions for specific actions like addition and multiplication.

"Our goal... is an automatic tool which reads a source code in a high-level programming language and outputs a stream of quantum machine code," said Stefano Bettelli, a graduate student at Trento University in Italy.

The researchers are not developing a new programming language specifically for quantum computers, but are building an extension to a standard classical computer programming language. The researchers' architecture is a hardware abstraction layer, which attempts to shield programmers from the details of a particular type of computer hardware so they can use the same tools to write software for different types of computers.

"A reasonable analogy would be the extensions needed to ease the effective use of parallel computer architectures, or those needed to access external devices with different semantics, such as the graphics board," said Emanuel Knill, a mathematician at Los Alamos National Laboratory.

Programming languages and their extensions are either interpreted or compiled. Software written in interpreted languages goes straight from the programmer to the computer, which uses a lot of resources converting the software to a more machine-friendly form. Software written in compiled languages is processed by another tool, a compiler, which does the conversion before the software is used on a computer.

The researchers plan to make as much as possible of their quantum computing extension compiled, said Bettelli. Interpreted languages put an added burden on programmers because there is no compiler to catch code that a computer can't handle, and this is especially true for unusual hardware like quantum computers.

On the other hand, it will be difficult to create a compiler that understands the requirements of quantum computers. "The compiler won't stop if you try to do things that make no physical sense," said Bernhard Ömer, a graduate student at the Technical University of Vienna. "All these restrictions will have to be enforced solely by the implementation of the C++ class library and the discipline of the programmer."

Ömer has developed a similar programming architecture aimed at studying new ways of programming that are particular to quantum computing rather than giving programmers familiar tools for working with quantum computers.

The goal of that effort is to develop a true quantum programming language complete with quantum semantics, Ömer said. "While having a standardized [programming language extension] to numerically simulate, or at some time actually control, a quantum computer would certainly be a good thing, I don't think that a library on top of an existing classical language is an adequate paradigm for quantum programming itself," he said.

How soon anyone will need to write software for quantum computers is an open question. While researchers are producing a steadily increasing number of quantum algorithms, which are critical for demonstrating that quantum computers are worth the vast effort and expense that will be required to create them, only a handful of minuscule prototypes exist to run the algorithms.

"Our seven-qubit experiments are, in a sense, one-shot programs, and hooking them up into a general language doesn't really make sense," said Knill.

In addition to laying the groundwork for the day when quantum computers become available to programmers, the C++ library could make it easier for researchers to work with quantum computer simulations, he said. "Beyond that, it is hard to know how technology and software semantics [will] develop, and flexibility in that respect is well advised," said Knill.

It will be at least 20 years before practical quantum computers are developed, according to many researchers.

"You can try to extrapolate the growth in number of qubits to see how many qubits we might be able to control all at once in, say, 20 years," said Knill. "You'll find that using even an optimistic extrapolation based on exponential growth... it isn't that many."

"You also have to realize that the needed advancements in improving error rates per operation are hard to predict," he said. "Currently an error rate of 1 in 10 for any of the few two-qubit devices available is considered extremely good. As far as we know, this has to come down to below 1 in 10,000."

Bettelli's research colleagues were Tommaso Calarco of the Institute of Theoretical Physics at the University of Innsbruk in Austria and Luciano Serafini of the Institute for Scientific and Technological Research at the Trentino Institute of Culture in Italy. The research was funded by Italian Ministry of Research and the Italian National Institute for Nuclear Physics.

Timeline: > 20 years
Funding: Government
TRN Categories: Quantum Computing; Programming Languages and Compilers
Story Type: News
Related Elements: None

TRN

Theory

Quantum Computing Has Limits

Technology Research News, September 10/17, 2003

There are many long-term research efforts aimed at eventually producing a quantum computer, which would use the traits of atomic particles like electrons, photons and atoms to compute.

Although it is extremely difficult to use such infinitesimally small parts, the weird quantum trait of entanglement would allow calculations to be carried out all at once on a series of numbers, making quantum computers fantastically fast. In theory, they could solve large problems that could never be solved by classical computers, including breaking all security codes.

Quantum computers are not likely to ever replace classical computers for everyday use, however.

Researchers from the University of Arkansas and Texas A&M University have shown that quantum computers, while theoretically useful for very large problems, are likely to always need very large amounts of power.

According to their calculations, the statistical nature of quantum data, the practical requirements of inputting data into systems capable of carrying out entanglement, and the difficulty of error correction, or checking data, make quantum computers less efficient than classical computers for all but a few types of problems.

The work appeared in the September, 2003 issue of *Fluctuation and Noise Letters*.

TRN

Quantum Computing without Weirdness

By Eric Smalley, Technology Research News
October 18, 2000

Researchers laying the groundwork for software that will run on quantum computers could be barking up the wrong tree by assuming that one of the weirder aspects of quantum mechanics, entanglement, is a necessary ingredient.

When two or more atoms or subatomic particles are entangled, any change to one is immediately reflected by the same change in the other regardless of the physical distance between them.

Researchers have demonstrated that quantum computers have the potential to be much faster than normal computers for certain tasks like factoring and searching databases. Many researchers have argued that entanglement is the reason quantum computers will be more efficient.

But some computer scientists who are working on quantum algorithms are questioning that assumption. David A. Meyer, a research professor in the mathematics department at University of California in San Diego, has demonstrated that, contrary to appearances, a particular quantum search algorithm does not use entanglement.

"The point of that paper was to say that [interference] is really the crucial feature of how quantum algorithms work" rather than entanglement, he said.

Interference is the interaction of two or more waves. When atoms and subatomic particles are in their quantum states, they exist as waves.

"Interference is the same phenomenon you see with water waves," Meyer said. "If you start waves from two sides of a pool that make a corner, you'll get points where they reinforce so that the waves will be higher and points where they cancel out so the surface will be flat."

Atoms and particles spin in one of two directions, up or down, which can represent the ones and zeros of binary computing. A particle has a probability of spinning in either direction when it is in its quantum state. A quantum computer acts on a set of particles by influencing the probabilities of the particles' spins so that when the particles leave their quantum state the resulting spin directions represent a specific number.

Influencing the probabilities of the particles' spins is accomplished by creating specific patterns of interference among the particles' waves.

"If you're trying to get some specific outcome, what you want to do is set up the internal workings of the [quantum] computer so that the computational paths which correspond to outcomes that you don't want—the answers that are wrong—cancel out, and the computational paths which lead to the [outcome] that you do want—the correct answer—reinforce," said Meyer.

The crux of the debate is whether entanglement is the key to creating the correct interference patterns. According to Meyer, any process that controls interference should be sufficient.

The issue of whether entanglement is necessary in quantum algorithms might seem like an esoteric debate given that many researchers say that practical quantum computers are at least 20 years away. But the stakes for developing quantum algorithms are actually quite high, Meyer said.

"If we're trying convince the government and industry to fund the incredible expense and commitment of resources that's going to be necessary to get [quantum computers] built, we have to demonstrate that they're going to be able to do something useful," he said. "We really need to find more algorithms which will motivate this development. Figuring out how algorithms work and what's necessary to design them is really a crucial thing at this point in the history of quantum computing."

Consequently it's very important that researchers not get sidetracked by worrying about entanglement in their algorithms, Meyer said.

"It is a healthy thing that Meyer tries to debunk some of the claims that entanglement is the essential ingredient for quantum computation," said Wim van Dam, a computer scientist and member of the Center for Quantum Computation at the University of Oxford. "Entanglement is somewhat of a pet topic for physicists," he said. Computer scientists who are trying to come up with new quantum algorithms are less interested in this, he said.

Meyer published his work in the August 28, 2000 issue of the journal *Physical Review Letters*. The research was funded by the Army Research Office and the Advanced Research Development Agency.

Timeline: > 20 years
Funding: Government
TRN Categories: Quantum Computing; Data Structures and Algorithms
Story Type: News
Related Elements: Technical paper "Sophisticated Quantum Search Without Entanglement" in August 28, 2000 Physical Review Letters

TRN

Index

TRN's Making The Future Report is published 10 times a year by Technology Research News, LLC. Each 20- to 40-page package assesses the state of research in a field like biochips, data storage or human-computer interaction.

Single reports are $300 to $500. A one-year subscription is $1,600. To buy a report or yearly subscription, go to www.trnmag.com/email.html.

We welcome comments of any type at feedback@trnmag.com. For questions about subscriptions, email mtfsubs@trnmag.com or call (617) 325-4940.

Technology Research News is an independent publisher and news service dedicated to covering technology research developments in university, government and corporate laboratories.

Kimberly Patch
Editor
kpatch@trnmag.com

Eric Smalley
Editor
esmalley@trnmag.com

Ted Smalley Bowen
Contributing Editor
tbowen@trnmag.com

Chhavi Sachdev
Contributing Writer
csachdev@trnmag.com