TRN's
Making the Future Report
The State of an Emerging Technology and a Look at What Lies Ahead

Report Number 1 December, 2002

Quantum Cryptography: Potentially Perfect Security

Executive Summary

Quantum cryptography uses traits of individual photons to distribute random mathematical keys that can be used to encrypt and decrypt communications; this provides theoretically perfect security. Rudimentary commercial systems are available now. The first-generation systems make it possible to establish secure communications between two points in metropolitan areas.

Over the next few years the systems should gain speed, span longer distances, and eliminate the vulnerabilities that have prevented ths first generation of the technology from reaching perfect security.

Look for satellite-based quantum cryptography within five years. Quantum repeaters are needed to extend the technology to longer ditances on the ground and may be available in five to ten years. It is a thornier issue to integrate quantum cryptography into data networks like the Internet because current quantum cryptography systems depend on point-to-point connections, while the Internet has an open, many-to-many structure.

In the back-and-forth war between code makers and code breakers, code makers currently have the advantage. They are likely to hold the advantage for the foreseeable future, but it is also possible that the tide could turn. In August, a team of scientists from the Indian Institute of Technology found a method for identifying large prime numbers, which is a key step toward a mathematical code-breaking formula.

Quantum cryptography will become an outright necessity if and when quantum computers are built, but this is not likely to happen for at least two decades. Quantum computers use the quirks of particles like atoms and photons to compute and would be fast enough to easily break security codes currently in use.

What to Look For

Equipment and capabilities:

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

Implementations:

Gigabit-per-second point-to-point
Via satellite
On a network
On the Internet

Threat levels:

10-qubit quantum computer (practical quantum systems possible)
100-qubit quantum computer (large-scale within a decade)
1,000-qubit quantum computer (encryption codes compromised)

Real-world ready?

Rudimentary quantum cryptographic systems have emerged from lab and are now commercially available. The technology is very much a work in progress, however, and will remain fertile ground for improvements for years or decades to come.

Quantum cryptography taps the traits of individual photons to distribute random mathematical keys that can be used to encrypt and decrypt communications. Quantum cryptography can theoretically provide perfect security, but its current practice falls short of perfection. Closing the gap between theory and practice means speeding up the technology, lengthening its reach, and adding more quantum mechanics to reduce its vulnerabilities. There's also the question of exactly what the first generation of this technology is suited for.

This report assesses the state of quantum cryptography research and maps out the goals and strategies poised to shape the technology's future.

- The first section of the report covers the first generation of quantum cryptography systems, target applications, and research aimed at improving the performance and reliability of quantum cryptography.

- The second section examines research aimed at extending the technology from short, point-to-point connections to global networks including the Internet.

- The third section details efforts to make the theoretically perfect security more perfect by putting more quantum in quantum cryptography.

- The fourth section takes a look at the need for quantum cryptography and the factors that will eventually make it indispensable.

The first generation

Most quantum cryptography systems demonstrated to date are based on the original protocol devised by Charles Bennett of IBM Research and Gilles Brassard of the University of Montréal in 1984. (See How It Works, opposite)

The protocol calls for light sources that generate single photons, but those light sources have yet to be pe he rfected or built in forms that can be readily integrated into quantum cryptographic systems. Instead, most existing systems rely on heavily-filtered lasers, which usually generate empty pulses, sometimes generate the desired single-photon pulses, and occasionally generate two-photon pulses. Because the systems sometimes produce two-photon pulses, users have to assume that an eavesdropper could discover some transmitted bits, and so must take the extra step of distilling strings of bits into smaller strings to ensure secrecy. As a result, the early systems are not very efficient. Data transmission rates for existing quantum cryptography systems are on the order of hundreds of bits per second compared to millions of bits per second for ordinary data communications.

Improving the situation requires better single-photon sources. Ideally, quantum cryptographic systems should incorporate simple components—along the lines of light emitting diodes (LEDs) — that produce a single photon every time they receive an electric pulse, and that work at room temperature.

There are three approaches to producing reliable single-photon sources: quantum dots, nanocrystals and molecules.

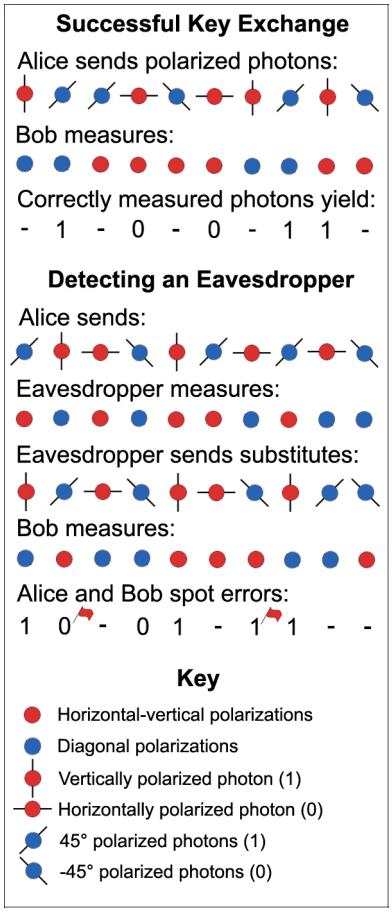
All involve coaxing individual electrons into giving up energy in the form of single photons, and all are more efficient than the attenuated, or filtered, light sources currently in use.

How It Works

Alice can send Bob perfectly secure messages using quantum key distribution because it allows them to tell for sure whether the encryption keys they are using to lock and unlock messages have been copied.

Quantum key distribution systems use single photons to represent the binary numbers, or bits, that make up encryption keys. The use of single photons is what guarantees security. If there were two or more photons per bit, eavesdropper Eve could siphon off extra photons to make a copy of a key without being detected.

The systems use polarized photons to represent bits. Photons have both electric and magnetic fields. The electric field of ordinary photons vibrates in all directions perpendicular to the photon's course. Polarized photons have electric fields that vibrate in only one of four directions: vertical, horizontal and the two diagonals.



Two pairs of polarizations, vertical and horizontal, and the two diagonals, can each be used to represent the 1s and 0s of digital information. For example, vertical could represent 1 and horizontal could represent 0.

To send an encryption key to Bob, Alice transmits a string of randomly polarized photons and records how each photon was polarized. Bob measures the photons, but because of a quirk of quantum physics—the Heisenberg uncertainty principle—he can only look for one of the two pairs of states in each photon. Bob has to choose which type of polarization to look for, and he only gets one look because the act of measuring the photon alters it.

Bob randomly chooses whether to look for vertical and horizontal or the diagonal orientations. He tells Alice, over a regular, unsecure communications

Quantum dots are infinitesimal pieces of semiconductor material that trap individual electrons. Applying a voltage to a quantum dot causes a trapped electron to give off a photon. Because they can be triggered by electricity, quantum dots have the potential to be cheaply and easily integrated into electronic devices. Most quantum dot photon sources, however, work only at temperatures several hundred degrees below zero.

Nanocrystals are microscopic specks of crystal that give off photons by fluorescence. When a laser hits a nanocrystal, the nanocrystal absorbs some of the energy from the beam, then releases the energy as a single photon. Nanocrystals work at room temperature, but are relatively inefficient and require a laser.

Certain individual molecules can also be coaxed to give off individual photons when they are excited by a laser. The molecules work at room temperature, but wear out relatively quickly.

The single-photon detectors used on the receiving end of quantum cryptography systems are also in need of improvement. The devices usually consist of pieces of semiconductor that generate a small electric current when they are hit by photons. Most of the detectors used today are slow and have high dark-count rates, meaning they register photon hits when none occur. Better prototypes have been built using superconductors, but these require cryogenic cooling.

Practical, efficient single-photon sources are likely to arrive within five years; practical, efficient single-photon detectors could take five to ten years to develop.

What it's good for

Even with less-than-ideal components, first-generation quantum cryptographic systems already make it possible to establish secure communications between two points in metropolitan areas today.

Id Quantique SA, a spinoff from the University of Geneva in Switzerland, is marketing a quantum cryptographic system that connects two PCs over a fiber-optic phone line. New York startup Magiq Technologies is readying a system that transmits cryptographic keys through the open air between two points in a line of sight. Both outfits are targeting financial services companies.

These early quantum cryptographic systems work over short distances compared to ordinary data communications. The distance record for quantum cryptography over fiber-optic lines is 41.6 miles, set by the Id Quantique system in July.

And the distance record for quantum cryptography through the open air, announced in October, is 14.5 miles. The experiment was conducted between two mountains in southern Germany by Qinetiq, plc, a research and development company spun off from the UK military. A similar experiment conducted earlier this year by researchers at Los Alamos National Laboratory spanned six miles at a lower altitude in New Mexico.

Despite the seemingly short distances, the open air systems could have a global impact. They could soon make it possible to securely distribute cryptographic keys all over the world, at least for those who own a satellite.

The distances involved in the two ground-level experiments are equivalent to sending photons up through the thin upper atmosphere channel, how he measured the photons, and she tells him which ones he chose correctly.

Alice and Bob use this common string of photon polarizations as a binary encryption key. Alice uses the key to encrypt a message, then sends the encrypted message to Bob over an open channel. Bob then uses the bit string to decrypt the message. Because the bit string was generated at random, there is no mathematical basis for decoding the message without knowing the key. And by using a new encryption key for every message, Alice and Bob can thwart code breakers who deduce keys by looking for common patterns across messages.

The quirky nature of photons makes it impossible for an eavesdropper to intercept single photons and successfully replace them. This is because, like Bob, Eve has to guess which way to measure the photons. If she chooses to measure a photon to see if it is a 1 or 0 based on the vertical and horizontal orientations but Alice encoded the bit in the diagonal orientations, Eve will get a false reading.

This means Eve could correctly measure about half of the photons she intercepts, and so half of the substitutes she sends to Bob would be polarized randomly. By chance, half of the randomly polarized photons would be correct, making about 25 percent of the substitute bits wrong.

Alice and Bob check the error rate by comparing a few of the bits Bob chose correctly. If the error rate is higher than even one percent, they can decide that the chance that Eve has intercepted their key is too high, and throw it out and transmit another.

Who to Watch

Quantum Cryptographic Systems:

Donald Bethune, IBM Research
San Jose, California
www.almaden.ibm.com/st/projects/quantum/intro/

Gerald S. Buller, Heriot Watt University
Edinburgh, Scotland
www.phy.hw.ac.uk/resrev/QUICK/index.htm

Francesco De Martini, University La Sapienza
Rome, Italy
www.infm.it/

Chip Elliott, BBN/Verizon
Cambridge, Massachusetts
www.bbn.com/networking/quantumcryptography.html

Nicolas Gisin, University of Geneva/id Quantique SA
Geneva, Switzerland
www.GAP-Optique.unige.ch/Quantum.asp
www.idquantique.com/

to reach a low-orbiting satellite. The remaining challenges to practical ground-to-satellite quantum cryptography are figuring out how to lock single-photon beams on to satellites, and miniaturizing the equipment to fit on board satellites.

Satellite-based quantum cryptography could materialize within five years.

Going the distance

Extending the distance and boosting the efficiency of quantum cryptographic systems that work over fiber-optic lines will require pushing further into the realm of quantum physics.

Ordinary communications lines use repeaters to boost fading signals. Repeaters placed at key points along communications lines replace fading light pulses with fresh ones. This process destroys any quantum information contained within the photons, however.

The solution is to transfer the quantum information, undisturbed, directly from one particle to another. This requires the weird quantum state of entanglement, which creates between two or more undisturbed particles a bond that persists regardless of how far the particles are separated from each other.

Quantum repeaters could use entanglement in one of two ways. One method is to transfer the quantum information from an incoming photon to a carefully isolated atom in the device, then transfer the information from the atom to a new photon. The other possibility is quantum teleportation, which involves entangling a pair of photons and transmitting one of the pair. Entangling a third photon with the remaining photon and measuring the two in a way that does not reveal their quantum states yields information that can be used to convert the transmitted photon of the original pair into a replica of the third photon.

Key institutions developing quantum repeaters:

- California Institute of Technology
- Harvard University
- Johns Hopkins University
- Massachusetts Institute of Technology
- Max Planck Institute in Germany
- Northwestern University
- NASA's Jet Propulsion Laboratory
- University of California at Los Angeles
- University of Innsbruck in Austria

Quantum repeaters could become practical in five to ten years, though it could take longer because controlling entanglement is particularly tricky.

Quantum networks

Ideally, quantum cryptography would be integrated into data networks, including the Internet. The guarantee of security built into the quantum cryptography protocols relies on single, point-to-point connections, however. The issue is how to adapt the protocols for networks.

Richard Hughes, Los Alamos National Laboratory
Los Alamos, New Mexico
www.lanl.gov/orgs/pa/News/UCSB032102/sld028.htm

Paul Kwiat, University of Illinois
Urbana Champaign, Illinois
www.physics.uiuc.edu/Research/QI/index.html

Hoi-Kwong Lo, Magiq Technologies
New York, New York
www.magiqtech.com/

Klaus Molmer, University of Aarhus
Århus, Denmark
www.phys.au.dk/quantop/theory.shtm

John Rarity, QinetiQ, plc
Malvern, England
www.eqcspot.org/

Jeffrey Shapiro, Massachusetts Institute of Technology
Cambridge, Massachusetts
rleweb.mit.edu/rlestaff/p-shap.htm

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

Colin Williams, NASA JPL/Quantum Confidential, Inc.
Pasadena, California/Lacanada, California
cism.jpl.nasa.gov/program/RCT/QuantCompUD.html

Horace Yuen, Northwestern University
Evanston, Illinois
www.ece.northwestern.edu/~yuen/

Anton Zeilinger, University of Vienna
Vienna, Austria
www.quantum.univie.ac.at/zeilinger/

Quantum Cryptography Theory:

Charles Bennett, IBM Research
Yorktown Heights, New York
www.research.ibm.com/people/b/bennetc/

Gilles Brassard, University of Montreal
Montreal, Canada
www.iro.umontreal.ca/labs/theorique/index.html.en

Artur Ekert, University of Oxford
Oxford, England
www.qubit.org/people/artur/index.html

Daniel Gottesman, University of California at Berkeley
Berkeley, California
www.cs.berkeley.edu/~gottesma/

Though quantum-cryptography-enabled networks are likely to use quantum repeaters, the devices are not a requirement. Solving the problem of spanning greater distances is separate from solving the problem of safely routing streams of individual photons among multiple points, and so initial implementations of multiuser quantum cryptography could arrive before usable quantum repeaters. One proposal calls for using tiny mirrors to route photons around a network without destroying quantum information.

Another possibility is the development of a quantum cryptographic scheme that gets around the one-photon limit. This would allow quantum cryptography to work over existing optical networks. Researchers at Northwestern University last month demonstrated quantum data encryption using ordinary lasers, and the researchers plan to apply their method to key distribution in the next year or two.

Key efforts to integrate quantum cryptography into networks:

- Boston University
- Harvard University
- Northwestern University
- SAIC's Telcordia Technologies
- Verizon's BBN

However successful these projects are, it will be long time before the average person can buy a quantum cryptography add-on for her computer. Even though the main trunks of the Internet and most large private networks are fiber-optic, most computers connect to the networks using twisted pair telephone wires or coaxial cable.

Gregg Jaeger, Boston University
Boston, Massachusetts
photon.bu.edu/jaeger/newhome.html

Andrew C. Yao, Princeton University
Princeton, New Jersey
www.cs.princeton.edu/~yao/

Single Photon Sources:

Philippe Grangier, Institute of Optics
Orsay Cedex, France
www.iota.u-psud.fr/~grangier/Quantum_optics.html

Ataç Imamoglu, University of California at Santa Barbara
Santa Barbara, California
www.ece.ucsb.edu/Faculty/Imamoglu/default.html

Andrew Shields, Toshiba Cambridge Research Laboratory
Cambridge, England
www.toshiba-europe.com/research/crl/index.html

Yoshihisa Yamamoto, Stanford University
Palo Alto, California
stanford.edu/group/ginzton/faculty/yamamoto.html

Making perfect perfect

The perfect in the perfectly secure communications theoretically afforded by quantum cryptography stops where theory meets implementation. Switching among the filters that polarize photons, for example, is a relatively slow process, so many quantum cryptographic systems use four separate lasers instead, each with a filter that yields a different polarization state. Though this speeds transmissions, it makes them more vulnerable. An eavesdropper could theoretically measure subtle differences in how the lasers produce photons to determine a bit string without directly observing the polarizations of the photons.

It's also difficult to come up with a process that produces a truly random string of polarizations, so there is a danger the sender could unwittingly generate his photons in a pattern that an eavesdropper could detect.

Using pairs of entangled photons circumvents these potential implementation problems. In 1990, Artur Ekert of the University of Oxford proposed a way to use entanglement forquantum key distribution.

In this approach, the sender generates pairs of entangled photons and transmits one of each pair to the receiver. The photons have no particular polarization until the receiver measures his photons, which forces them and the entangled pair-mates retained by the sender into particular polarizations.

If an eavesdropper intercepts the transmitted photons and forwards replacements to the receiver, the replacements would not be linked to the sender's photons. And when their photons don't match up, it would be obvious to the sender and receiver that something was wrong.

http://www.lanl.gov/orgs/pa/News/UCSB032102/sld028.htm

The process also provides the desired random sequence of polarizations. And because entangled photons are essentially unpolarized until they are observed, an eavesdropper has no means of distinguishing among entangled photons other than measuring them.

The main drawback to using entangled photons for quantum cryptography is the difficulty of generating the linked photon pairs. It is likely to take five to ten years for researchers to come up with practical sources of entangled photons.

What's really needed

In the back-and-forth war between code makers and code breakers, code makers currently have a decided advantage and are likely to hold that advantage for the next decade or more. The strongest encryption codes in use today are effectively invulnerable to attacks using the most powerful computers.

That invulnerability, however, rests on the assumption that the only way to break the codes is by brute force—trying every possible solution one at a time until the answer is found. It is theoretically possible, however, that someone could come up with a mathematical technique for breaking the codes. In August, a team of scientists from the Indian Institute of Technology found a method for identifying large prime numbers, a key step toward a mathematical code-breaking formula.

So for those who face potential adversaries who have deep pockets and big incentives, quantum cryptography could be the surest means of securing communications.

Quantum cryptography will become an outright necessity, however, if and when a related experimental technology, quantum computing, comes to fruition. Quantum computers use the quirks of quantum physics to check every possible answer to a problem at once. This could reduce otherwise impossible problems like factoring huge numbers by brute force to hours-long tasks. Factoring large numbers is the way to crack today's conventional encryption codes.

This makes nearly all secret communications vulnerable to the owner of the first full-scale quantum computer, but researchers generally agree that that moment is at least two decades away.

Quantum cryptography, which should be available in airtight implementations well before then, is theoretically immune to attacks by quantum computers.

It's also important to remember that secure communications require more than just a secure communications channel. Before information is encrypted for transmission and after it is decrypted on receiving end, it is only as secure as the computer systems storing it and the people using it.

Recent Key Developments

Advances in quantum cryptography systems:

- A fiber-optic distance record of 41.6 miles (Quantum secrets ride phone lines, page 7)
- A free-space distance record of 14.5 miles, announced by Qinetiq, plc in October
- An entangled-photon implementation that improves the eavesdropper detection rate announced by Los Alamos National Laboratory in July
- An implementation that automatically adjusts to changes caused by the fiber-optics, announced by IBM Research in July

Advances in single-photon sources:

- A diamond nanocrystal source implemented in a quantum cryptography system (Diamonds improve quantum crypto, page 8)
- An electronically-triggered quantum dot source (LED fires one photon at a time, page 9)
- A room temperature, quantum dot light emitting diode that could lead to a practical single-photon source (Nanoscale LED debuts, page 11)
- A quantum dot source that functions up to a relatively warm minus 73 degrees Celsius, announced by Bremen and Wurzburg universities in October

Advances in photon detectors:

- A high-speed detector based on a cryogenically-cooled superconductor (Sensitive sensor spots single photons, page 12)
- Proposals for using specially prepared gases to count individual photons offered by the University of California at Santa Barbara, and by Los Alamos National Laboratory and the University of Illinois, in October

Advances in quantum repeaters:

- An error-resistant scheme that employs single, trapped atoms (Quantum network withstands noise, page 13)
- A scheme that makes a cloud of atoms act like a single atom (Atom clouds ease quantum computing, page 14)
- A proposal for entangling distant containers of gas atoms (Device would boost quantum messages, page 15)
- Improved control over light stored in gas atoms (Stored light altered, page 16)

Advances in controlling entangled photons:

- A rudimentary entangled-photon laser (Laser emits linked photons, page 17)
- A small laser diode that coaxes entangled photons out of a crystal (Quantum crypto gear shrinks, page 18)
- A scheme for ensuring that entangled photons survive the rough-and-tumble of fiber optics (Tightening photonic bonds strengthens security, page 19)

Advances related to quantum cryptography:

- High-speed, multi-photon quantum data encryption demonstrated by Northwestern University in November
- A prototype quantum computer that can factor the number 15 (Quantum demo does tricky computing, page 20)
- A scheme for getting more than one bit of information out of each photon (Photons heft more data, page 21)
- A method that uses quantum physics to split secrets between two or more parties (Quantum code splits secrets, page 23)

Quantum Secrets Ride Phone Lines

By Eric Smalley, Technology Research News
August 7/14, 2002

The ability to safeguard secret messages using the quirks of quantum physics has been thoroughly demonstrated in the laboratory. Now field tests of quantum cryptography are showing that the technology can withstand the rigors of real-world communications.

Researchers in Switzerland have used this type of cryptography, which represents bits of information using single photons, to send theoretically perfectly secure messages between the cities of Geneva and Lausanne, which are 67 kilometers apart.

Quantum cryptography provides perfect security because it allows users to tell for sure whether the key they are using to encrypt and decrypt a message has been compromised.

Researchers at Los Alamos National Laboratory previously proved that a quantum signal could travel 50 kilometers. But that was over a spooled fiber-optic line contained in a laboratory, said Nicolas Gisin, a physics professor at the University of Geneva. "In our case the two end points were really spatially separated," he said.

More importantly, the Swiss experiment used existing fiber-optic phone lines. The fibers were "nothing special," said Gisin. They were not in commercial use during the experiment, but were part of a cable containing many fibers that were, he said.

Key encryption schemes use a unique mathematical key to mask each message. The sender and intended recipient use the key to encrypt a message, send it over unsecured channels, then decrypt it. The trick to keeping the message secret is making sure no one but the sender and receiver have access to the key.

The quantum cryptography scheme sends encryption keys over fiber-optic lines in a perfectly secure way by representing each bit with only one photon. Using two or more photons per bit makes it possible for an eavesdropper to siphon off some extra photons in order to peek at the key without being detected. Using only one photon per bit means that an eavesdropper would have to replace the photons she intercepted, but it is impossible to replicate all of the photons correctly.

This is because any given photon, or particle of light, can have one or more attributes, including polarization, which has to do with how the photon vibrates, and wave phase.

The researchers' quantum cryptography scheme generates photons in one of four states based on their wave phases. The system splits each photon, sends the halves down short pieces of fiber of slightly different lengths, and then joins the two halves. Because the halves travel different distances, their waves are out of phase, meaning the crests and troughs are out of sync by a particular amount.

The photons' four phase states come in two types: those whose waves match or are exactly opposite, and those whose waves are half way out of phase with one wave ahead of the other. Each type can be used to represent the 1s and 0s of digital information.

It is a quirk of quantum physics — the Heisenberg uncertainty principle — that makes the scheme perfectly secure: you can't look for both of the pairs of states at the same time, and you only get one look before the photon disappears. If you measure a photon to see if it is a 1 or 0 based on one pair of states, but it was generated in one of the other two states, you're out of luck. Your measuring device has absorbed the photon during your first look so you will never know whether it represented a 1 or 0.

This means an eavesdropper would only be able to correctly measure half of the photons he intercepts and would have to guess at the other half to produce substitutes. And he would only get about half the missing half right by chance, meaning one quarter of the substitute bits would be wrong.

The sender and receiver can check the error rate and so detect the eavesdropper by comparing a few bits. If the key has been compromised, they can throw it out and send another until they get an uncompromised key to encrypt their data. To form a key, the receiver measures the photons by randomly picking one of the two sets of states. Then they compare notes and the sender tells the receiver which photons he measured correctly. They then use those bits as the key.

The researchers' quantum key distribution system can only be used across relatively short distances because its performance drops off as the distance increases. At 10 kilometers the system can transmit quantum keys at 4,000 bits per second. At 20 kilometers the bit rate drops to 1,500 per second, and at 50 kilometers it drops to 100 bits per second. An ordinary modem transmits 56,000 bits per second. Once the users have an uncompromised key, however, the encrypted data can be sent over fast communications lines that include repeaters.

Today's fiber-optic communication systems compensate for diminishing signal strength — and thus span great distances — by using repeaters, which copy and retransmit fading light pulses. Repeaters can't be used to send quantum keys because they would intercept photons in the same manner as an eavesdropper.

The company id Quantique in Geneva, a spinoff from Gisin's laboratory, is marketing the quantum key distribution system. It consists of a pair of 18-inch-wide boxes that connect to personal computers via USB ports, and to each other over a fiber-optic line.

Gisin's research colleagues were Damien Stucki and Hugo Zbinden of the University of Geneva, and the Olivier Guinnard and Grégoire Ribordy of id Quantique SA. They published the research in the July 12, 2002 issue of the journal *New Journal of Physics*. The research was funded by the European Union.

Timeline: Now
Funding: Government
TRN Categories: Quantum Computing and Communications; Cryptography and Security

Story Type: News Related Elements: Technical paper, "Quantum Key distribution over 67 km with a plug & play system," *New Journal of Physics*, July 12, 2002

TRN

Diamonds Improve Quantum Crypto

By Eric Smalley, Technology Research News
September 18/25, 2002

Scientists have thoroughly demonstrated that the quirks of quantum physics can secure secret messages, and one company is already selling a commercial quantum cryptography system.

But there's still plenty of room for improvement. Prototype quantum key distribution systems are slow and only work over relatively short distances. The main challenge is coming up with a light source that reliably fires off one and only one photon per pulse.

Today's quantum cryptography prototypes use lasers that are so heavily filtered that most of the pulses contain no photons, a few contain a single photon and fewer still contain two photons. Sending a cryptographic key means waiting for enough single photon pulses to be generated, and compensating for pulses that contain too many photons or none at all.

Researchers from the French National Scientific Research Center (CNRS) and Ecole Polytechnic in France have bettered the usual weak laser pulse method with a deliberately dirtied microscopic diamond: a 40-nanometer diamond nanocrystal with a nitrogen atom embedded next to an atom-size gap in the center. A nanometer is one millionth of a millimeter, and an atom measures about one tenth of a nanometer.

The nanocrystal emits light by fluorescence. When hit by a laser, the nanocrystal absorbs energy, then gives it off in the form of a single photon.

"We have developed an efficient, stable, all solid-state, room temperature single-photon source [and] we have used this single-photon source in a quantum cryptography setup," said Alexios Beveratos, a researcher at CNRS.

When the researchers used the setup as a light source to transmit quantum encryption keys through the open air, they were able to transmit 9,000 secure bits per second over a distance of 50 meters. "The limiting factor for the distance is that we didn't have a longer corridor. We should be able to span larger distances," said Beveratos.

An encryption key is a string of numbers used to lock and unlock encrypted messages sent over unsecure communications lines.

The researchers' goal is to communicate perfectly secure keys between the Earth and satellites. Researchers at Los Alamos National Laboratory aiming for the same goal have demonstrated a quantum cryptographic system that spans

10 kilometers using weak lasers, which is roughly equivalent to sending photons up through the thinner upper atmosphere to reach satellites hundreds of kilometers above the Earth. The next challenge is being able to aim single photons precisely enough to hit satellites.

The efficiency of single-photon detectors limits the distance that quantum cryptographic systems can operate over. Detector efficiency is affected by thermal noise and so detectors are usually cooled. Noise produces false positives, or signals when no photon is present.

The researchers' diamond-based device emits a single photon about two percent of the time it is stimulated, and can deliver as many as 116,000 single-photon pulses per second. Weak lasers can also generate 116,000 single-photon pulses per second but the diamond only generates 90 two-photon pulses during that time compared to 1,300 for the weak laser, said Beveratos. Two-photon pulses compromise security, and minimizing the risk they pose lowers the efficiency of the device.

Because two-photon pulses are inevitable, quantum cryptographic schemes use privacy amplification, which reduces a string of bits that includes some that have been exposed to an eavesdropper to a smaller string of secret bits. Privacy amplification converts two or more of the original bits into a single, new bit. Even if an eavesdropper knows some of the original bits, she is highly unlikely to be able to figure out the new bit. The more two-photon pulses a light source emits, the more original bits have to be used to make one secret bit.

Quantum cryptography involves a trade-off between data rate and distance, meaning the further apart hypothetical correspondents Alice and Bob are, the fewer secure bits they can send to each other. Because it generates fewer two-photon pulses than weak lasers, the researchers' light source requires fewer pulses to make secret bits and so can span longer distances, said Beveratos.

Quantum cryptography allows users to tell for sure whether the encryption key they are using to encrypt and decrypt a message has been compromised.

Quantum cryptography schemes send encryption keys by representing each bit with only one photon. If there were two or more photons per bit, an eavesdropper could siphon off extra photons in order to copy the key without being detected. Using only one photon per bit means that an eavesdropper would have to replace the photons she intercepted, but the laws of physics make it impossible to replicate all of the photons correctly.

In the race to develop reliable single-photon light sources, several possibilities have surfaced. Certain molecules work well for a time, but "after having emitted a certain amount of photons, they photobleach, which means that they are not optically active anymore and do not emit any more photons," said Beveratos.

Quantum dots, which are microscopic specks of semiconductor that trap one or a few electrons, don't bleach, but they only emit single photons at very low temperatures, which requires cumbersome and expensive cryogenic equipment, said Beveratos.

The researchers' device, with its reduced multiple-photon rate, is the first to show a better secret bit rate than weak laser pulses, said Richard Hughes, a physicist at Los Alamos National Laboratory who has built a quantum key distribution prototype spanning 10 kilometers. "This type of light source and other similar ones will lead to improvement in the efficiency with which quantum key distribution [systems] can generate secret sharing keys," he said.

In order to reach satellites, the researchers will need to improve the device's efficiency from two percent to ten percent, said Beveratos. The researchers plan to test their system over longer distances and outdoors, he said.

Developing the quantum cryptographic systems for practical satellite communications will take at least five years, said Beveratos. The device would need to be miniaturized to fit on a satellite, he said. It will take less time to ready the device for use between two points on Earth, he said.

Beveratos' research colleagues were Rosa Brouri, André Villing, Jean-Philippe Poizat and Philippe Grangier of CNRS, and Thierry Gacoin of Ecole Polytechnique. The research was accepted for publication in the journal *Physical Review Letters*. The research was funded by the European Union.

Timeline: 5-6 years
Funding: Government
TRN Categories: Cryptography and Security; Quantum Computing and Communications
Story Type: News Related Elements: Technical paper, "Single photon quantum cryptography," European Quantum Information Processing and Communications workshop in Dublin, September, 2002

TRN

LED Fires One Photon at a Time

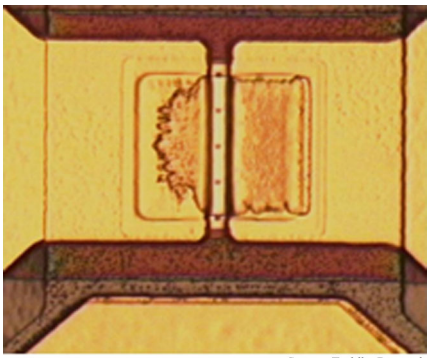
By Eric Smalley, Technology Research News
December 19, 2001

The weird nature of quantum physics makes perfectly secure communications possible. The technology has existed in the laboratory for several years — all that remains is figuring out how to make it practical.

Scientists at Toshiba Research and the University of Cambridge have taken an important step in that direction by making an electronic device that emits single photons on demand. The device could boost the transmission rates of secret communications and would be smaller and easier to use than similar light sources.

Quantum cryptography uses strings of individual photons, which are the indivisible particles of light, to make the mathematical keys that scramble secret messages. The keys are long, random numbers in the form of bits, the ones and zeros of digital communications. Ordinary communications transmits bits as light pulses, but because each light pulse contains many photons an eavesdropper could siphon some of them off to record the series of pulses to get a copy of the key without being detected.

However, when the keys' bits are encoded in the quantum states of individual photons — like how they are polarized — eavesdroppers can't escape detection. Because a photon cannot be split, an eavesdropper can't look at it without stopping it from reaching the intended receiver. And an eavesdropper can't cover his tracks by making copies of the photons he intercepts because he cannot reliably recreate their quantum states, which means the sender and receiver can compare notes to see that some of the photons have been altered.



Source: Toshiba Research

One photon at a time comes out of each of the holes aligned vertically across the top of this light emitting diode.

When a sender and receiver know they have an uncompromised key, the sender can use it to encrypt messages that only the receiver can unscramble.

Making practical quantum cryptographic systems requires light sources that produce one photon at a time. A candle flame emits about one hundred thousand trillion photons per second, many at the same time.

Even the dimmest possible ordinary light source occasionally emits two photons at once. "We can control and trigger the emission time of the photons," said Andrew Shields, a group leader at Toshiba Research Europe in Cambridge, England.

Single-photon light sources are not new, but previous devices have all been triggered by lasers. "This is a cumbersome and expensive arrangement that would be difficult to achieve outside the laboratory," said Shields. "The new device is driven by a voltage so [it] is more robust, compact and would be cheaper to manufacture."

The researchers' single-photon source, a special type of light emitting diode (LED), contains a layer of quantum dots surrounded by layers of semiconductor material. Each quantum dot, which is a speck of semiconductor material about 20 nanometers in diameter, holds a single electron when a voltage is applied to the device. When the negatively-charged electron combines with a positively-charged hole in the quantum dot, it releases the energy as a single photon. A nanometer is one millionth of a millimeter.

The diode is capped by a metal layer with a series of small openings that block all but a single quantum dot per opening. By pulsing electrical current through the device, the researchers cause the quantum dots to emit a photon per pulse.

The device can theoretically emit a photon every half a nanosecond, said Shields. A nanosecond is one billionth of a second. But in practice the researchers' diode does not emit a photon with every pulse.

"The efficiency has not been optimized in this prototype, so [it] is quite low," said Shields. "If we use a cavity structure to direct more of the light out of the device in a certain direction, we can expect efficiencies exceeding 10 percent.

Ten percent efficiency could be good enough for practical devices. A potentially bigger hurdle is the cold temperatures needed to run the diode. The researchers' prototype operates at five degrees Kelvin, or -268 degrees Celsius.

"We have already seen efficient emission from quantum dots at temperatures exceeding [-73 degrees Celsius], for which cryogen-free thermal-electric cooling can be used," said Shields. "We hope to be able to push this further to room temperature."

A single-photon source that is triggered by an electrical current would be much more practical than an optically triggered single-photon source, said Gerard Milburn, a physics professor at the University of Queensland in Australia. "The control circuits could be integrated into the device producing the photons and processing their detection."

Without single-photon sources, researchers have to use privacy amplification techniques to ensure that transmitted bits remain secret, which results in less efficient transmission rates, said Richard Hughes, a physicist at Los Alamos National Laboratory.

This new light source technology could lead to higher secret bit rates if it could be made into a practical device, he said. Making an electrically-driven device is a big step in that direction, "but it would also be important for a practical device to operate at a temperature that would not require the user to deal with cryogens."

The researchers next steps are to increase the efficiency and raise the operating temperature of the single-photon diode, said Shields. "There are technological challenges to overcome, but we think we know the solutions. We think we can make a useful device within three years," he said.

Shields' research colleagues were Zhiliang Yuan, Beata E. Kardynal and R. Mark Stevenson of Toshiba Research, Charlene J. Lobo, Ken Cooper and David A. Ritchie of the University of Cambridge, and Neil S. Beattie and Michael Pepper of both institutions. They published the research in the December 13, 2001 online issue of the journal *Science*. The research was funded by Toshiba Corporation in the

Engineering and Physical Sciences Research Council of the UK.

Timeline: < 3 years
Funding: Corporate; Government
TRN Categories: Optical Computing, Optoelectronics and Photonics;
Quantum Computing; Semiconductors
Story Type: News Related Elements: Technical paper, "Electrically captured in Single Photon Source," *Science*, online December 13, 2001

TRN

Nanoscale LED Debuts

By Kimberly Patch, Technology Research News
October 30/November 6, 2002

Because high-speed communications are carried out using light pulses, the industry is always on the lookout for small, efficient light sources. At the same time, a key need of the emerging quantum cryptography market, which promises to provide perfectly secure communications, is a light source that can reliably mete out single photons.

A group of researchers from Switzerland have found a way to make extremely small light-emitting diodes that could provide optical communications with a smaller, low-power light source. The method could eventually produce diodes so small they could be single-photon sources.

Key to producing the devices was figuring out how to construct and align such small electrical components, according to Andrea Fiore, an assistant professor at The Swiss Federal Institute of Technology at Lausanne (EPFL) and a researcher at the Italian National Research Council (CNR).

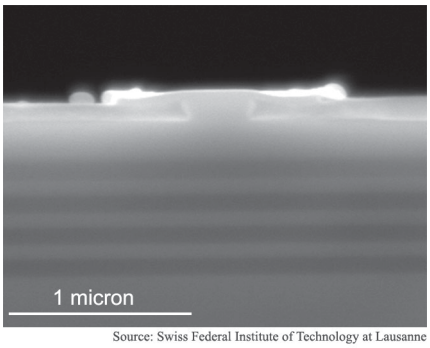
The researchers modified a method used to make a type of laser from semiconductor chip material. The method is usually used to fabricate devices with active electrical-optical areas of two or three microns, which is about half the size of a red blood cell. The researchers' modifications allowed them to produce a device with an active area of 100 nanometers, or about one 50th the size of a red blood cell. The entire device measures 600 nanometers across. A nanometer is one thousandth of a micron and one millionth of a millimeter.

The goal was to make a device that directed current to a layer containing quantum dots — 25-nanometer-wide, seven-nanometer-high bits of the semiconductor indium arsenide. Quantum dots can confine single, negatively-charged electrons. When an electric current brings a positively-charged hole to the dot, the electron and hole combine to emit a photon.

The difficult part was producing a device that efficiently guided electricity to the tiny quantum dots, said Fiore. There were two problems to solve, she said. The first was finding an efficient way to align the device's electrical contacts, and the second was finding a way to confine the electrical flow to a specific, vertical path within the device.

The researchers used optical lithography to etch mesas one or two microns in diameter into a cap of the semiconductor gallium arsenide attached to a layer of aluminum-gallium arsenide on top of the device. Then they heated the sample to 400 degrees Celsius and exposed it to water vapor, which caused the aluminum in the layer below the cap to oxidize, or combine with some of the oxygen in the water. This is the same type of reaction that causes iron to rust.

The oxidation continued underneath the gallium arsenide cap, spreading from the outside in, said Fiore. The researchers timed the oxidation process to leave a narrow channel of unoxidized material under the center of the cap. "Since the oxide is insulating, this defines a current constriction, which can be made much smaller than the original gallium arsenide mesa," said Fiore.



Source: Swiss Federal Institute of Technology at Lausanne

This electron microscope image shows a side view of a light-emitting diode that is just one tenth the size of a red blood cell.

This resulted in an automatic alignment of the contact area — the mesa. This solved the first problem: because the contact area was already lined up, less precision was required in depositing metal electrodes onto the contact. Otherwise, "having to align such small structures [would require] high-resolution fabrication tools, which are expensive and not compatible with an industrial process," Fiore said.

The researchers then attached metal contact layers above the mesa and below the base. "Because the surface is covered with insulating aluminum oxide everywhere except on the gallium arsenide mesas, current can flow only inside the [channel] in the aluminum gallium arsenide layer," Fiore said.

The researchers solved the challenge of confining the current by working with the physical design of the chip, said Fiore. In the researchers' first attempt to make the devices, the electrical current spread laterally rather than being channeled to the quantum dots, said Fiore. "In order to avoid that, we carefully redesigned the layer above the quantum dots [to make] it easier for the current to flow vertically than laterally," she said.

The researchers' quantum dots turned out to be very temperature-tolerant, meaning they continue to confine electrons even when the temperature rises to room temperature. "This holds true only as long as the energy barrier to [electron] escape is larger than the thermal energy. For most quantum dots this is not true anymore at room temperature," said Fiore.

The researchers' tiny light emitting diode produces infrared light with a wavelength of 1.3 microns, which is widely used in today's fiber-optic communications. Its small size makes the device useful as a light source for single-mode fiber, according to Fiore. Single mode fibers are 8 to 9 microns in diameter, and are used for long, high-speed links.

The devices could eventually be scaled down so that they contain single quantum dots, which would only emit one photon at a time, said Fiore. Single-quantum-dot light emitting diodes could "produce light pulses containing single photons, and this [could] be used to transmit information in a quantum-secure way," Fiore said.

Quantum cryptography, which has the potential to produce perfectly secure communications, is just emerging as a commercial product. Quantum cryptography devices use states of photons—like the way a photon is polarized—to represent the ones and zeros of computing. A series of photons representing a string of ones and zeros is used as a key to encrypt and decrypt data.

Single photon pulses cannot be observed without altering their states. Therefore, it is possible to tell for sure whether a cryptographic key represented by the quantum states of a string of single photons has been compromised. Eavesdropping on a single-photon transmission will alter the photon's state.

The quantum dot diode shows promise as a better source of single photons than the devices currently in use. Current quantum cryptography systems use heavily-filtered lasers, which mostly produce empty pulses, sometimes produce single pulses, and occasionally produce two-photon pulses. Existing quantum dot single-photon sources are relatively inefficient and work only at cryogenic temperatures.

The researchers' device is remarkably efficient, and cleverly made, said Pablo Vaccaro, a senior researcher at Adaptive Communications Research Laboratories (ATR) in Japan. The researchers "applied in a clever way the wet oxidation technique already in use," he said.

The research is novel "from the point of view that it demonstrates the fabrication of sub-micron size LEDs, each one with an active region that contains a few tens or a few hundreds of quantum he ots each," said Vaccaro. The technique could be refined to eventually produce single quantum dot devices, he added.

The current, multiple-quantum-dot design could be used in very short optical links like those within computer chips, Vaccaro said.

The researchers are working on further scaling down the diode to produce a device that emits single photons from single quantum dots at room temperature, said Fiore. The researchers are also working on making the device more efficient, she said. "We now want to further scale down the LED to a size where emission from a single quantum dot can be isolated," she said. "Another major objective is... optimizing the carrier-photon interaction to maximize the LED efficiency."

The method could produce practical, single-photon devices in two to three years, Fiore said.

Fiore's research colleagues were Jianxin X. Chen and Marc Ilegems of The Swiss Federal Institute of Technology at Lausanne. They published the research in the September 2, 2002 issue of *Applied Physics Letters*. The research was funded by the European Union and the Swiss National Science Foundation.

Timeline: 2-3 years
Funding: Government
TRN Categories: Materials Science and Engineering; Physics; Quantum
Computing and Communications
Story Type: News Related Elements: Technical paper, "Scaling Quantum-Dot Light-Emitting Diodes to Submicrometer Sizes," *Applied Physics Letters*, September 2, 2002.

TRN

Sensitive Sensor Spots Single Photons

By Chhavi Sachdev, Technology Research News
October 31, 2001

Stars and faulty transistors both emit infrared radiation, or heat, and knowing exactly how much heat distant stars and tiny transistors give off is useful. and Researchers at the Moscow State Pedagogical University the University of Rochester have developed a device that detects minuscule amounts.

The researchers' single-photon detector counts both infrared and visible light photons, whether they are emanating from cooling stars or from a misfiring transistor in your PC. It is more sensitive than current semiconductor detectors, which are prone to giving 'dark counts,' or seeing photon flashes when there aren't any, and which cannot see photons of infrared heat.

The device could spot defects in computer chips, improve communications between planets, and even enable snoop-proof secret messages.

The device consists of very narrow, ultrathin superconducting strips of niobium nitride that contain a hotspot of excited, warm electrons that switch from a superconducting to a resistive state when they encounter a photon.

"The absorber strip is... initially operating in the superconductive state, but very close to being in the resistive state. When a single photon is absorbed into the superconducting strip, it is driven into the resistive state and generates a measurable voltage that can be readily displayed on a fast oscilloscope," said Carlo Williams, a member of

the research team, now a development scientist at Corning, Inc.

The device takes 30 picoseconds, or trillionths of a second, to catch a photon and emit the resulting voltage, which translates to a speed of over 10 Gigahertz, or 10 billion distinct photons every second, said Roman Sobolewski, a professor of electrical and computer engineering at the University of Rochester.

It counts photons in the wavelength range of 0.4 to 3 microns, which covers visible light and heat down to the mid-infrared range, Sobolewski said.

The detector could be used to evaluate working integrated circuits to weed out those that leak electroluminescence, or electrical energy that is converted into light, said Williams. "This could increase the yield of manufactured integrated circuits with the minimum defects."

The photon detector is accurate even when the photon emission rate is less than 10 photons per second, said Sobolewski. A candle flame emits a hundred thousand trillion photons per second. Because the detector is so sensitive, it could be used to measure ultraweak electroluminescence from tiny nano circuits, which is hard for current photo detectors to pick up.

It could also be used in fast, free-space optical communication systems for planetary exploration and earth-orbiting missions, said Sobolewski. Light signals transmitted between earth and space are weakened by dust and particles in the atmosphere and space; the highly sensitive single-photon detector could boost the capacity of interplanetary communications.

The single-photon detector is also a prime candidate for making high-speed quantum cryptographic devices, Sobolewski said.

Quantum cryptography promises perfectly secure communications because anyone who eavesdrops on a message inevitably alters the stream of photons, leading to the detection of the snooping. A number that is sent undetected can be used as a key to encrypt a subsequent message and only the holder of the key can decrypt the message. Because the detector can sense many photons per second it would allow for high data rates, according to Sobolewski.

The device could be used in quantum cryptography as well as fundamental tests of quantum physics and quantum computation, which all work with single particles of matter, including photons, said Emanuel Knill, a mathematician at the Los Alamos National Laboratory.

There is still a lot of work to be done, however. Quantum computation requires that a single photon can be detected nearly 100% of the time, said Knill. The best photodetectors today can achieve detection probabilities above 90%, but at speeds much slower than the Moscow device. The 20% efficiency of the device shows promise given the very high repetition rates, he said.

"The high repetition rates with low dark counts are useful in quantum information processing, particularly for increasing the bit rates in quantum cryptography. If the efficiency can be substantially improved, their device could be a powerful tool for quantum information processing," said Knill.

"One of the tasks of this continuing project is to improve this number," said Williams. The device could be in practical use soon, Sobolewski said.

The researchers published their work in the journal *Applied Physics Letters*. The research was funded by Schlumberger Semiconductor Solutions; The Office of Naval Research (ONR), NATO, and The U.S. Civilian Research and Development Foundation for the Independent States of the Former Soviet Republic.

Timeline: Now
Funding: Corporate; Government
TRN Categories: Optical Computing; Optoelectronics and Photonics
Story Type: News
Related Elements: Technical papers, "Picosecond Superconducting Single-Photon Optical Detector," *Applied Physics Letters*, August 6, 2001.

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 entangles the atoms 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

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 and Communications
Story Type: News
Related Elements: Technical paper, "Dipole Blockade and Quantum Information Processing in Mesoscopic Atomic Ensembles," *Physical Review Letters*, July 16, 2001

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 and Communications; 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

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 and Communications
Story Type: News
Related Elements: Technical paper, "Phase Coherence and Control of Stored Photonic Information," posted on the arXiv physics archive at http://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 http://arXiv.org/abs/quant-ph/0105105close

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 and Communications
Story Type: News
Related Elements: Technical paper, "Stimulated Emission of Polarization-Entangled Photons," *Nature*, August 30, 2001

TRN

Quantum Crypto Gear Shrinks

By Eric Smalley, Technology Research News
October 3, 2001

Researchers around the world are closing in on realizing the centuries-old dream of being able to send secret messages that are perfectly secure against any possible code breaking attempt. Before the average computer user can protect messages using quantum cryptography, however, the bulky laboratory equipment involved must be redesigned to fit on a few computer chips.

The key to this miniaturization is figuring out how to produce pairs of entangled photons using small, low-power lasers.

Researchers from Ludwig Maximilians University in Germany have taken a step in this direction by producing entangled photons using a small laser diode. The advancement opens the way to building quantum cryptographic devices on circuit boards.

Quantum particles like photons can be entangled, or linked so that they have properties like polarization in common. Particles can remain entangled regardless of the distance between them.

Entangled photons are the main ingredient of quantum cryptography. Two people who want to secretly communicate can, in theory, split a series of entangled photon pairs. They can then measure their photons and use the results as a key to encrypt a message that can be read by the person holding the other half of the entangled photons.

Because an eavesdropper cannot look at the photons without disturbing them, any intrusion can be detected immediately and the compromised key discarded.

Photons entangled using polarization work like this: the electric field of light vibrates in a plane perpendicular to the direction the light is traveling. When light is polarized, its electric field vibrates in one of four directions on that plane: horizontal, vertical or one of the two diagonals.

Entangled photons occur in some mix of the four possible polarization orientations, but when one of the particles is measured both particles snap into one polarization, regardless of the physical distance between them.

The preferred method for producing polarization-entangled photons is shining a laser through a special crystal that can turn a single ultraviolet or blue photon into a pair of entangled infrared photons. But this process is very inefficient, said Jürgen Volz, now a graduate student at the University of Munich.

"Usually this problem is overcome by the use of intense laser beams," he said. "Only large-frame ion lasers can be used... because only these lasers are able to create an adequate power output. These lasers are quite large and need enormous amounts of electrical energy... and possibly also water cooling. This makes standard entangled-photon-pair sources very expensive," said Volz.

The researchers got around the power problem by taking advantage of a basic principle of lasers. Lasers work by stimulating the atoms of a gas, which causes the atoms to emit photons. A pair of mirrors facing each other at opposite ends of the laser's gas chamber keeps these photons bouncing back and forth through the gas. As the photons bump into the gas atoms, they stimulate the emission of more photons.

"We placed an optical resonator around the nonlinear crystal," said Volz. In this case, the photons that bounce back and forth pass through the crystal rather than hitting the atoms of a gas. "With each pass, entangled photon pairs are created. So we can use much lower laser powers," he said.

Lower laser power means the lasers can be much smaller. "We use a simple laser diode, which could be operated from a simple battery," Volz said. "That makes our source much cheaper and quite compact in contrast to those based on ion lasers."

The researchers' entangled photon source generated about 10,000 pairs of entangled photons per second. Although this is only a tiny fraction of the astronomically large number of photons generated by even low-power lasers, it is sufficient for many quantum cryptography schemes, according to Volz.

The solid-state entangled photon source could be used for quantum cryptography in a few years, said Volz. "Two to five years seems possible," he said.

Volz's research colleagues were Christian Kurtsiefer and Harald Weinfurter of Ludwig Maximilians University. They published the research in the August 6, 2001 issue of the journal *Applied Physics Letters*. The research was funded by the German Research Foundation and the European Union.

Timeline: 2-5 years
Funding: Government
TRN Categories: Quantum Computing and Communications; Optical Computing, Optoelectronics and Photonics

Story Type: News Related Elements: Technical paper, "Compact All-Solid-State Source of Polarization-Entangled Photon Pairs," *Applied Physics Letters*, August 6, 2001

TRN

Tightening Photonic Bonds Strengthens Security

By Eric Smalley, Technology Research News
May 16, 2001

The virtually perfect security afforded by quantum cryptography has been demonstrated in laboratories. But getting from the laboratory to practical applications is especially difficult for a technology that relies on the stranger aspects of quantum mechanics.

Quantum cryptography is based on manipulating and measuring the quantum states of individual photons, and keeping any particle in its quantum state means isolating it from its environment — a difficult challenge in the real world of fiber-optic cables and communications devices. A team of researchers in Austria has adapted a 5-year-old scheme for boosting quantum communications signals so they can be transmitted with relatively simple equipment, which should make it possible to build devices for transmitting secure information over long distances.

"For many protocols of quantum communication... it is necessary that two points which communicate with each other establish entanglement over long distances," said Anton Zeilinger, a professor of physics at the University of Vienna.

Two particles can become entangled, or linked, when they are in the quantum mechanical state of superposition, which is a mixture of all possible quantum states. Quantum states include particle attributes like the electron spin states spin up and spin down.

When one of the entangled particles is measured, the measurement knocks it out of superposition into a random state and the other particle immediately collapses into the same state, regardless of the physical distance between them.

Because it is impossible to observe a particle, such as a photon, in its quantum state without altering that state, anyone who eavesdrops on a message encoded in quantum particles will alter the message and reveal the security breach. If one person sends a key to another using quantum cryptography and they see that no one intercepted it, they can safely use the key to encrypt their communications.

"The problem is that if we create a pair of entangled particles in a source, the quality of the entanglement degrades with... distance," said Zeilinger. The greater the distance, the greater the amount of noise in the system.

"This noise is caused by the interaction of the particles — in our case photons — with the environment, in our case a glass fiber," he said.

Like other entanglement purification schemes, the University of Vienna proposal starts with some number of partially entangled pairs of photons and ends up with a smaller number of more highly entangled pairs. All of the pairs have the same level of entanglement to begin with and the various schemes eliminate some of the photons, which leaves the remaining ones more highly entangled.

The University of Vienna scheme sends the photons through polarization beam splitters, which filter photons based on their polarization. Photons are particles of electromagnetic energy and they have an electric field and a magnetic field. The electric field of a non polarized photon vibrates in a plane perpendicular to the direction the photon is traveling in. A polarized photon has an electric field that vibrates in only one direction of the perpendicular plane.

A sender transmits one photon from each of two entangled pairs of photons and keeps the other halves of the pairs. The sender and receiver then put their photons through a polarization beam splitter, which has two inputs and two outputs. If the photons have the same polarization, one will exit from each output.

If both sender and receiver have one photon come through each output, they both measure one photon from the same output channel of their polarization beam splitters. If the measured photons match each other, they keep the remaining photon pair, which is more highly entangled and therefore more suitable for quantum communications.

The key to the University of Vienna scheme is that it is simple enough to potentially be done outside a lab. Previous schemes have performed more complicated manipulations that require correspondingly more complicated equipment.

Combined with quantum repeaters, the method should allow for unconditionally secure quantum cryptographic key over arbitrary distances, said Zeilinger.

Quantum repeaters don't exist yet, but are theoretically possible. Classical repeaters copy a weakened signal and transmit the copy, effectively boosting the original signal. "But a classical repeater is worse than worthless for quantum states," said Daniel Gottesman, a fellow of the Clay Mathematics Institute working at the University of California at Berkeley. "Because it looks at the state, it actually creates more noise," he said.

A quantum repeater would need to be able to regenerate the state without looking at it. "That's where entanglement purification comes in," said Gottesman. "It's a way to take a number of noisy quantum states and distill out a few accurate ones. It's much harder than building a classical repeater, but perhaps this [University of Vienna] work will bring it within reach. In the context of quantum cryptography, that means you're back in business. Less noise means no foothold for an eavesdropper," he said.

Developing quantum cryptographic systems is still a difficult task; the researchers also have not addressed the key problem of how to store photons, said Seth Loyd, an associate professor of mechanical engineering at the Massachusetts Institute of Technology. "I think it's an excellent idea, but I'm not sure that it really improves the prospects for implementing quantum cryptography as much as [the researchers] claim," he said.

Practical quantum communication systems could be developed in 10 years, said Zeilinger.

Zeilinger's research colleagues were Jian-Wei Pan, Christoph Simon and Caslav Brukner of the University of Vienna. They published the research in the April 26, 2001 issue of the journal *Nature*. The research was funded by the Austrian Science Foundation, the Austrian academy of sciences and the European Union.

Timeline: 10 years
Funding: Government
TRN Categories: Quantum Computing and Communications
Story Type: News
Related Elements: Technical paper, "Entanglement purification for quantum communication," *Nature*, April 26, 2001

TRN

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 pairs a picture 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

Photons Heft More Data

By Eric Smalley, Technology Research News
July 10/17, 2002

Light doesn't weigh anything, but it does have momentum.

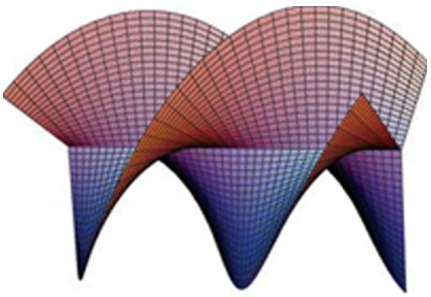
In fact, a strong light beam can move microscopic objects. A lightwave that spirals also has orbital angular momentum, which is same type of momentum the moon carries in its orbit around the earth.

Researchers from the Universities of Glasgow and Strathclyde in Scotland have found a way to measure the orbital angular momentum of individual photons, which allows them to distinguish photons that have incrementally different amounts of momentum.

The ability to measure these fine differences means the different states could be used to carry much more information than today's optical communications technologies, which generally use only the presence and absence of light pulses to represent the ones and zeros of digital information.

There are 32 unique combinations of five binary digits starting with 00000, 00001, 00010 and ending with 11111. In contrast, a single photon with 32 possible orbital angular momentum values could carry as much information as the whole group of five on/off pulses, and could therefore transmit data five times as fast.

Under the researchers' scheme, each photon "could, for example, represent a whole letter of the alphabet," said Johannes Courtial, a research fellow at the University of Glasgow in Scotland.



Source: University of Glasgow

This diagram depicts a spiral light beam moving from left to right and rotating about its axis. This type of beam can theoretically carry much more data than ordinary light beams.

The technique could further increase information capacity if it is combined with measurements of other variables of light, including its two polarization states and however many colors can be distinguished, said Courtial. Polarized light vibrates in only one of two directions rather than in all directions at once. Combining these techniques "could literally multiply the information-carrying capacity of each photon," he said.

The researchers' method could also boost the capacity of quantum communications systems and quantum computer schemes that use attributes of photons to process and transmit information, said Courtial. Quantum communications can be used to send perfectly secure messages. Quantum computers have the potential to solve certain problems faster than the fastest possible classical computer because they can theoretically process all possible answers to a problem at once rather than looking at the possibilities one by one.

The researchers measured orbital angular momentum using a series of interferometers. An interferometer splits a light beam into two beams, changes the positions of one of the beam's waves, then passes the beams through each other to create an interference pattern. When light waves meet they mix; where wave crests or troughs meet they reinforce each other, and where a crest and trough meet they cancel out.

The researchers send a light beam whose photons have a mix of orbital angular momentums into an interferometer and rotate one of the split beams 180 degrees, said Courtial. When the beams are put back together, the resulting interference pattern sorts the photons into two groups with different orbital angular momentums. "All photons with an orbital angular momentum that is an even multiple... interfere constructively in one output port of the interferometer while all those with an odd orbital angular momentum interfere constructively in the other output port," he said.

"After this first sorting stage, the photons are... passed through further interferometers," Courtial said.As more interferometers are added, more states can be distinguished, and therefore each photon can represent one of a larger range of numbers, he said.

The researchers tested the method with individual photons by transmitting so little light that most of the time no photons were transmitted, occasionally single photons were transmitted and only rarely was more than one photon transmitted at once.

To encode data in a photon, the researchers would reverse the sorting process in order to make the interferometer emit a photon with a specific orbital angular momentum, said Courtial. "At the other end, it's [orbital angular momentum] could be measured to decode the data," he said.

Using the orbital angular momentum of photons to transmit real data means getting over several hurdles. In the short term, lining up multiple interferometers has proved challenging, said Courtial.

A longer-term problem is figuring out how to preserve photons' orbital angular momentum as they traverse fiber-optic cables. "The trouble is that optical fibers — at least most fibers in use today — alter the light's" orbital angular momentum, he said. Several years ago the researchers demonstrated the problem by adding a weight to a fiber-optic cable, which causes the cable to convert light with no orbital angular momentum into light with orbital angular momentum, said Courtial. "We're currently working on fixes... for both problems," he said.

The researchers have shown that it is possible in principle to encode single photons with many different states, said Kang Wang, a professor of electrical engineering at the University of California at Los Angeles.

The principle could also be extended to other types of particles, Wang said. "For computation, the number of states of electrons could be increased using similar waves interference techniques to increase information processing volume," he said.

A lot of work needs to be done before it is possible to use orbital angular momentum to transmit data, however, said Wang. "Practical realization for commercial applications remains... daunting."

The researchers are working on making their photon sorter more compact and more stable in order to commercialize the device, said Courtial. "We are also trying out different designs," he said.

The orbital angular momentum of photons could be put to use transmitting data in five to ten years, he said.

Courtial's research colleagues were Jonathan Leach and Miles Padgett of the University of Glasgow and Stephen Barnett and Sonja Franke-Arnold of the University of Strathclyde. They published the research in the June 24, 2002 issue of the journal *Physical Review Letters*. The research was funded by Glasgow and Strathclyde universities, the

Royal Society, the Leverhulme Trust, the Royal Society of Edinburgh, the Scottish Executive Education and Lifelong Learning Department and the UK Engineering and Physical Sciences Research Counsel (EPSRC).

Timeline: 5-10 years
Funding: Government, Private
TRN Categories: Optical Computing, Optoelectronics and Photonics;
Physics; Quantum Computing and Communications; Telecommunications
Story Type: News Related Elements: Technical paper, "Measuring the Orbital Angular Momentum of a Single Photon," *Physical Review Letters*, June 24, 2002

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 spindown 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 and Communications
Story Type: News
Related Elements: Technical paper, "Hiding Bits in Bell States," *Physical Review Letters*, June 18, 2001

TRN

Index

TRN's Making The Future Report is published 12 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 $450. A one-year subscription is $1,800. 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