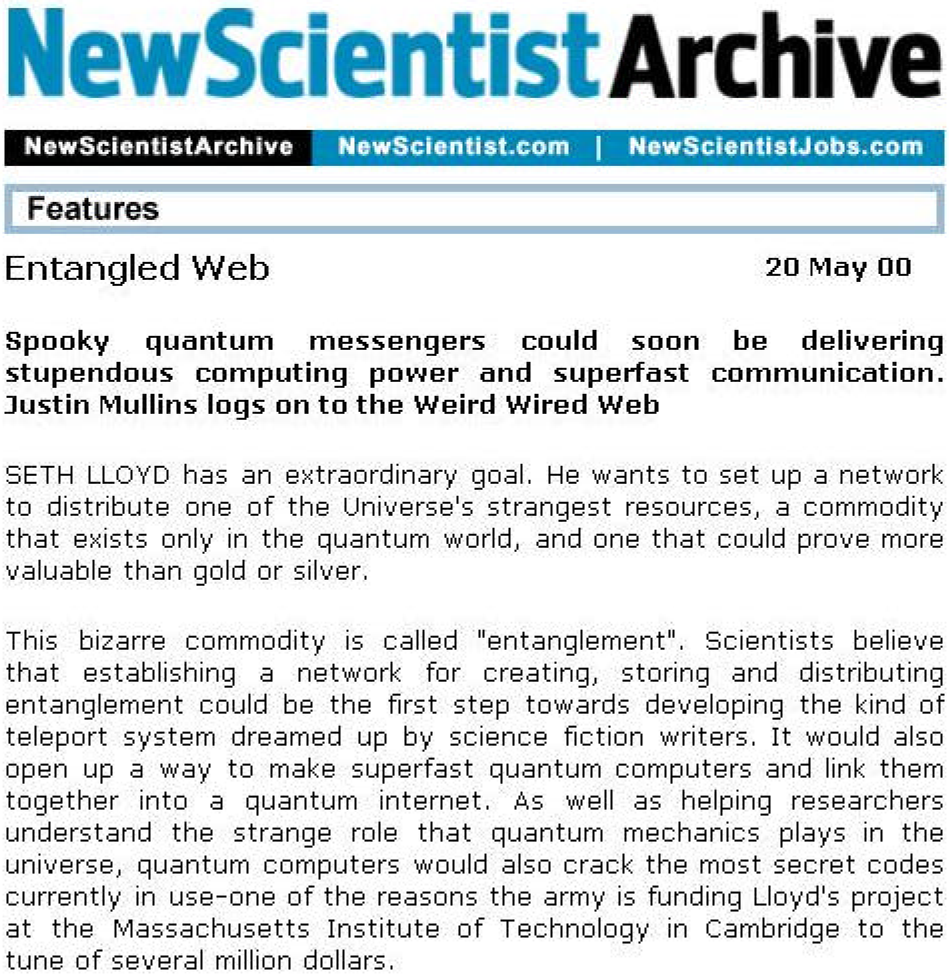
[COPY OF ARTICLE IN New Scientist REGARDING, AMONG OTHERS, OUR WORK IN QUANTUM TELEPORTATION VIA THE DARK STATE]



Entangled Web

20 May 00

Spooky quantum messengers could soon be delivering stupendous computing power and superfast communication. Justin Mullins logs on to the Weird Wired Web

SETH LLOYD has an extraordinary goal. He wants to set up a network to distribute one of the Universe's strangest resources, a commodity that exists only in the quantum world, and one that could prove more valuable than gold or silver.

This bizarre commodity is called "entanglement". Scientists believe that establishing a network for creating, storing and distributing entanglement could be the first step towards developing the kind of teleport system dreamed up by science fiction writers. It would also open up a way to make superfast quantum computers and link them together into a quantum internet. As well as helping researchers understand the strange role that quantum mechanics plays in the universe, quantum computers would also crack the most secret codes currently in use-one of the reasons the army is funding Lloyd's project at the Massachusetts Institute of Technology in Cambridge to the tune of several million dollars.

Entanglement is a ghostly, almost telepathic link between particles that have interacted at some time in the past. The connection is instantaneous and works even if the particles are on opposite sides of the Universe. Entanglement is already being used to carry out quantum cryptography and very small-scale quantum computing and **teleportation**. If entangled particles could be sent around the world through a "quantum internet", they could spark a revolution in computing, communications and our understanding of the universe.

Quantum computers would be linked up to make hugely powerful number-crunching machines. Information would wing its way around the globe at speeds far exceeding those that are even theoretically possible using today's technologies. Anyone wanting to run quantum computations would be able to download all the quantum software they needed. And physicists would be able to get their hands on "off-the-shelf" samples of quantum material. Each of these potential applications would be reason enough to build a quantum internet.

There is a problem however: quantum particles are fragile and spill their information easily. Merely looking at them can destroy it. So building a network to distribute quantum information poses some serious difficulties. But last month Lloyd and his colleagues published details of a plan to build a quantum internet, and announced that the technology to create it is available now. "All the different pieces have been done before," says Lloyd. He plans to have the first three nodes of his network set up within 3 years.

Building a quantum internet would mean rebuilding the intellectual foundations of the communications industry. Every phone call, TV broadcast and Internet connection relies crucially on the work of Claude Shannon. At Bell Labs in New Jersey, in the 1940s, Shannon laid the foundations of classical information theory. He determined the theoretical capacity of any communications channel -the maximum amount of information that can be reliably sent along it-and outlined the compression techniques that let engineers send their messages more efficiently.

Shannon also showed how to deal with noisy channels, where bits get flipped. The sender might repeat every bit three times, for example. He called his solution channel coding.

Shannon also worked out the theoretical limit of efficiency. The next generation of mobile phones will use recently developed channel codes that approach this "Shannon limit".

But Shannon's ideas apply only to classical information. The grand challenge now is to rewrite Shannon's theories for the quantum world, paving the way for the quantum internet.

Information in the quantum world is weird. A good example of classical information is a sequence of 0s and 1s, which might be encoded by varying the voltage across a wire. Above a certain level, the bit is a 1; otherwise it's a 0. But encoding a piece of information in a quantum particle such as a photon is quite different.

Photons can exist in two or more states at the same time. For example, a photon's electric field can be filtered so it oscillates in one particular plane, a phenomenon known as polarisation. Make the plane vertical, and you can call it a "0". Make it horizontal, and it's a "1".

But because of "quantum superposition", the photon can be both vertically and horizontally polarised at the same time, and so can be both 0 and 1 simultaneously. The polarisation of this photon is called a qubit-short for quantum bit (and pronounced "cue bit").

With superposition, engineers might think it possible to immediately double the capacity of communications channels using these qubits in superposition. Unfortunately, that's not the case. The strange and fragile nature of quantum information simply doesn't allow it.

The problem is not just about the amount of information that can be stored, but the amount that can be retrieved. That has to be done by taking a measurement from the photon, and in the quantum world, measurements change everything. With a single photon it is only possible to measure the polarisation in one direction. When this measurement is made, the rest of the information the photon contains is lost and cannot be retrieved. So it is only possible to extract one bit of information from a qubit. The capacity of a quantum channel for sending classical information, it would seem, cannot exceed the capacity of a classical channel.

But entanglement changes all this. The curious thing about entangled particles is that measuring one of the pair immediately determines the outcome of a measurement on the other, no matter how far apart they may be. This ability to magically connect two points in space-time means that entanglement can revolutionise communication.

In 1992, Charles Bennett of IBM's Thomas J. Watson Research Center near New York, and Stephen Wiesner of Tel Aviv University showed that entanglement has a profound effect on the capacity of a quantum channel-at the very least, it boosts it by a factor of two.

This is great news for Alice and Bob, the characters that quantum researchers use to play out their ideas. Alice spends her time sending quantum messages to Bob. So far they have been unable to communicate any faster than they could over the telephone. But what if Alice and Bob share a pair of entangled photons?

Each photon can have either a horizontal (1) or a vertical (0) polarisation, so together the pair can be in one of four states: either both vertically polarised, both horizontally polarised or either one vertically polarised and the other horizontally polarised. In binary terms this corresponds to 00, 11, 01 or 10: the decimal numbers 0 to 3. The curious thing is that Alice can determine which of these four states the whole system adopts simply by tweaking the one photon she possesses.

Alice and Bob each have one of the entangled pair, which is initially in a superposition of all four states. Alice then puts her photon through one of four very simple optics devices. And because of the strange nature of entanglement, her action also affects Bob's photon: Alice's operation simultaneously writes information onto her photon and Bob's.

Alice then sends her photon to Bob, who still knows nothing about either of the photons. When Alice's photon arrives, Bob reads the data by looking at the optical properties of the pair. This tells him which of the four operations Alice actually carried out. The extraordinary thing is that Alice has used entanglement to send two bits of information using one photon. Entanglement doubles the capacity of her channel, a phenomenon known as quantum superdense coding.

And even better things might be on the way. Physicists have recently begun to play with entangled triplets (qutrits) and entangled quads (ququarts) with more complex properties. Larger combinations are inevitable. These states might allow quantum information to streak through networks at breakneck speeds.

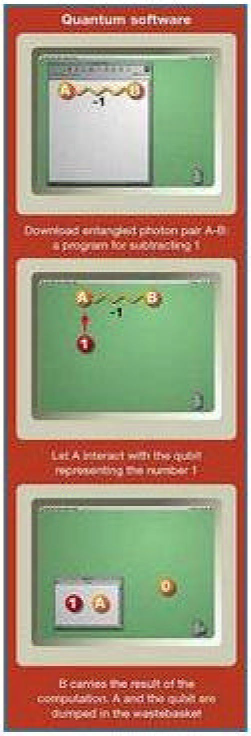
All this beautiful innovation will count for nothing, however, if physicists can't correct the errors that will inevitably arise in their quantum networks. Quantum states are so fragile that any outside influence can destroy them. Because of this, many physicists believed it would be impossible to send quantum information reliably. Last year, however, two physicists came up with a perfect solution.

Isaac Chuang at IBM Almaden in San Jose, California, and Daniel Gottesman of Microsoft Research in Redmond, Washington, have worked out a way to make software that carries out quantum computations, protects the content of quantum messages and keeps quantum bits error-free. And the crucial ingredient that makes this possible is entanglement.

Chuang and Gottesman's idea is based on quantum **teleportation**. In **teleportation**, researchers perform a measurement on the qubit to be sent, and the same measurement on one half of an entangled pair (*New Scientist*, 14 March 1998, p 26). This sends some information about the qubit to the other half of the entangled pair, allowing the original qubit to be reconstructed. But Chuang and Gottesman pointed out that this scheme allows much more than simple reconstruction.

Quantum computation is simply the result of one quantum state (called the gate) acting on another (the qubit). By preparing the state of the entangled pair in a particular way, what gets teleported can be the result of a computation performed on the original qubit (see Diagram).

Research published independently by Peter Shor of AT&T Laboratories in New Jersey and Andrew Steane of Oxford University in 1995 showed that quantum errors can be corrected simply by performing a certain series of computations on the data. So, according to Chuang and Gottesman, you could download a set of pre-fabricated "error-correcting entangled photons" from a quantum website.



High speed information transfer using quantum software

In their paper, Chuang and Gottesman predicted that the entangled pairs might one day become a commercial resource that can be bought and sold by researchers carrying out quantum computation over a quantum internet. John Preskill of Caltech agrees: if you need a gate with a really complex quantum state, he says, it would certainly be easier to download it from the quantum internet rather than make it yourself. He foresees a flourishing quantum software industry with manufacturers designing particularly valuable quantum states, creating and storing multiple copies, then allowing consumers to download them for a fee.

Such schemes could allow those with rather basic quantum computers to download extra capabilities. And the secretive nature of entangled photons-which change their state if anyone tries to look at them-could be used by a company to develop downloadable quantum software for private communications.

Most exciting of all, the quantum internet could be the ideal tool for teleporting complex molecules around the world. Currently, researchers can only teleport simple things like the quantum state of a photon; going further means using more complicated entanglements. So the quantum internet and its quantum software is just what researchers need to begin teleporting atoms, molecules and-eventually, perhaps-the components of life.

This will only work if physicists can sort out the practicalities of a quantum internet. Ignacio Cirac and Peter Zoller of Innsbruck University came up with the first plan for the quantum internet in 1997. In March this year, Lloyd and Selim Shahriar at MIT and Philip Hemmer at the Air Force Research Laboratory in Lincoln, Massachusetts brought the idea much closer to reality. Their idea is to create a pair of entangled photons and send them along two optical fibres: one to Alice and one to Bob. Alice and Bob both have laser traps containing supercooled atoms, which would absorb the photons. Lloyd and his colleagues say you can determine when an atom has absorbed a photon without disturbing it, and by checking for simultaneous absorptions Alice and Bob can find out when the atoms have absorbed an entangled pair. When this happens the atoms themselves become entangled, and Alice and Bob now share a pair of entangled particles. As the atoms have no electric charge they are immune to electric and magnetic fields, and so are easy to protect from the outside world. For the first time, entanglement would become a resource which physicists draw upon at leisure.

Alice and Bob could pull this software "off the shelf" and use it to send their messages. Physicists could use the pairs of atoms to send quantum information between quantum microcomputers-just what they need to scale up quantum computers to carry out useful calculations.

Today's quantum computers are essentially individual molecules that process quantum information but cannot share it: the most powerful is a 7-qubit machine at Los Alamos National Laboratories in New Mexico. Connecting many of these machines in parallel would allow useful quantum computations to be carried out. With a network as widespread as the Web, massive computations could be carried out on computers all over the world.

A global quantum internet might appear sooner rather than later. Lloyd hopes to have his source of entanglement running within 6 months and to be sending entanglement within 2 years. The three-node internet should come a year later.

Start investing now for the trading opportunity of the 21st century-entangled information. And there's good news for Microsoft and anyone else thinking of supplying entanglement to the world. Quantum software can be used only once: entanglement and the rules of quantum measurement mean that using it destroys it. For the first time in computing history, software pirates are set to vanish in a puff of entangled magic.

Justin Mullins

From **New Scientist magazine**, vol 166 issue 2239, 20/05/2000, page 26