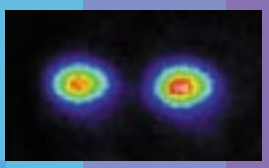
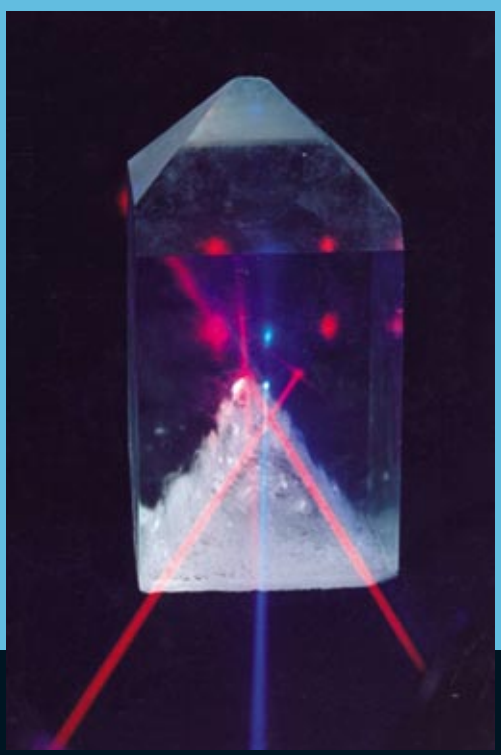
Institute of Physics

Physicists are experimenting with a new type of computing based on quantum effects that could completely revolutionise information technology

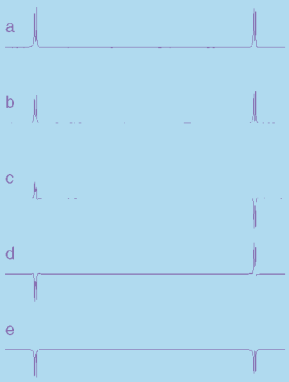


Quantum information

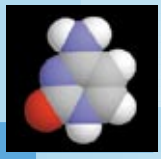


VISIONS 2
IN PHYSICS RESEARCH

Computing takes a quantum leap



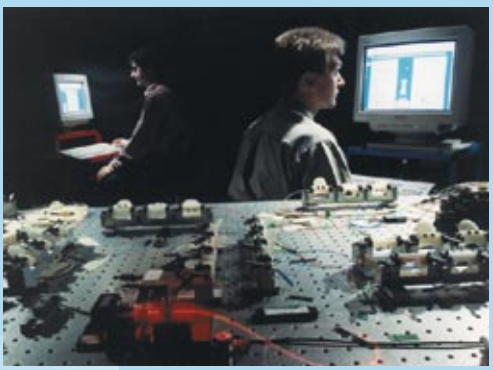
Four NMR states of the molecule cytosine (left) which is an implementation of the Grover quantum search algorithm. The bottom signal is a reference



Oxford University

All computers used today follow a classical physics approach. That is, a 'bit' of information is stored in a physical system (as a voltage, magnetic spin or light pulse) which can take two sharp values, 0 and 1. However, by harnessing quantum properties, which are quite different from classical ones, totally new types of computing processes could be developed. The crucial feature of a quantum system – for example, a photon or an atom – is that it may not exist in a sharply defined state (like an 'up' or 'down' magnetic spin) but in a so-called superposition of states (both 'up' and 'down' simultaneously). This means that a single quantum bit, called a qubit, can be in two states at the same time and thus encode two values. A two-particle system, such as a pair of interacting atoms or photons, gives a superposition of four states; a three-particle system eight states and so on. Such an approach offers extraordinary possibilities – for example, mathematical operations on multiple numbers could be performed simultaneously to create a superfast, massively parallel computer.

BT



BT's quantum cryptography system. The two computers are connected by 28 kilometres of optical fibre in the Ipswich area of BT's public network

Towards a real quantum computer

The concept of quantum computing started with theorist Richard Feynman who showed that a classical computer could not simulate quantum processes efficiently; a quantum computation was required. Later in 1985, David Deutsch, in a leap of imagination, proposed that a universal computer operating on quantum principles could simulate any physical process. Deutsch with Richard Josza then showed how a quantum computer could answer a set problem more quickly than by any classical route, giving a clear hint of its potential.

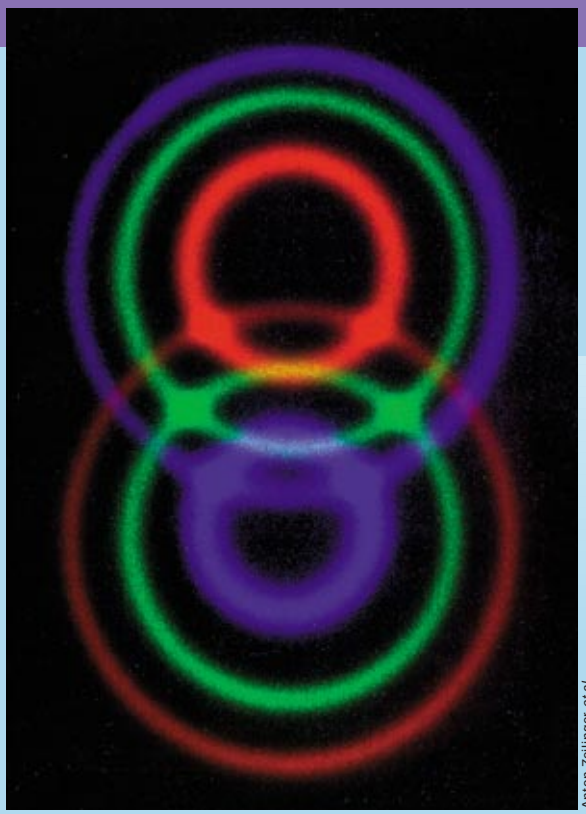
At first, quantum computing seemed to have little practical value. Then in 1994, Peter Shor at AT&T Bell Laboratories in New Jersey came up with a quantum algorithm for factorising large numbers very efficiently. It is extremely difficult to factorise such numbers by classical means; a 1000-digit number would take longer than the age of the Universe. For this reason, factorising large numbers is fundamental to the security of encoded systems in use today. However, a quantum computer could do it in a fraction of a second! More recently, Lov Grover at Bell Labs in Murray Hill, New Jersey developed an incredibly fast quantum search algorithm. Since most computer operations involve searching, such a program would speed up computing immensely.

Recognising the potential power of quantum computing, researchers worldwide are now investigating physical quantum systems in which the superposition of states could be manipulated (a quantum logic gate) so as to form the basis of a practical computer. One way to achieve a superposition of states is to shine a laser on an ion trapped in a cage of magnetic fields. A laser pulse of the right frequency and certain duration excites the ion from its ground state to an excited state (from state 0 to 1). A pulse lasting only half that time pushes the ion into a quantum superposition of both states. Researchers are currently experimenting with logic gates based on lasers and arrays of cooled ions in traps.

Another promising approach exploits nuclear magnetic resonance, in which a combination of strong magnetic and radio-frequency fields is used to control the nuclear spin states of hydrogen and carbon atoms in organic molecules. Each nucleus can either be spin-up or spin-down, thus encoding the qubit, and each molecule acts as an individual computer. Researchers at Oxford, for example, are currently experimenting with the DNA base cytosine. Other techniques involve using photons in nonlinear crystals and optical fibres, and electronic states in quantum dots.

One of the main obstacles to quantum computing is the phenomenon of decoherence. Coherent superpositions remain stable only as long as they do not interact with their environment, otherwise they collapse into one of the constituent values. While some people think that decoherence is an insurmountable problem, others such as Shor, Deutsch and Andrew Steane at

THANKS GO TO ARTUR EKERT, DAVID DEUTSCH, TONY HEY, JONATHAN JONES, PAUL TOWNSEND AND



Anton Zeilinger *et al*

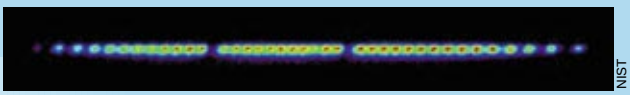
An entangled state of two photons produced by shining a laser through a nonlinear crystal (see front cover, bottom)

Oxford have been designing quantum error correction methods to compensate for decoherence. Like their classical counterparts, these methods are based on building-in redundancy, so that the same information is spread over many qubits.

Universal quantum computers may still be some way off, but one particular application – using quantum phenomena in secret communications – is nearer to commercial viability (see Box). Quantum cryptography relies on a simple one-qubit set-up which may be encoded in the polarisations or phases of a string of photons. BT has already carried out a demonstration over 28 kilometres of optical fibre looped between Martlesham and Ipswich. Another intriguing application of quantum processing is the 'teleportation' of a particle state over a large distance without physically moving the particle.

The future

At the moment researchers are designing 'toy' quantum computers with just a handful of qubits. Realistically, systems of thousands of qubits would be needed to create a useful computer. There are already plans to design larger arrays of qubits in solid-state systems that would be more compatible with current silicon and optical fibre technology. We can expect some exciting developments in the near future.



NIST

A row of mercury ions in a trap can act as a quantum computer

QUANTUM CRYPTOGRAPHY

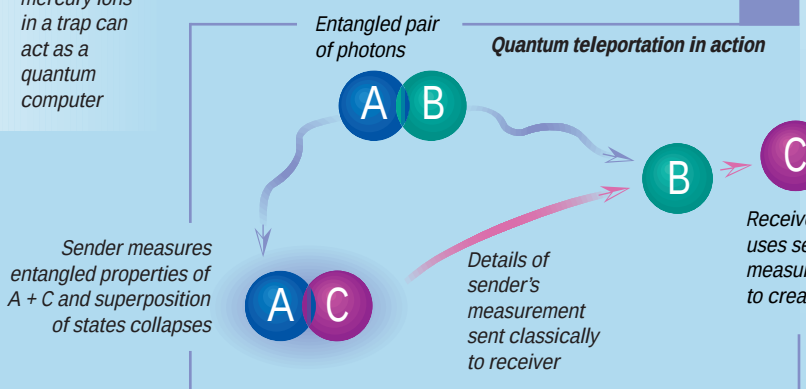
The aim of cryptography is to transmit information so that only the intended recipient receives it. Although classical cryptography employs various mathematical techniques to prevent eavesdroppers from learning the contents of encrypted messages, absolute security cannot be guaranteed. One of the main hazards in cryptography is supplying, in a secure way, a key – a series of numbers that enable the sender and receiver to encode and decode the cipher. However, by exploiting quantum principles – in particular, the Heisenberg Uncertainty Principle and a phenomenon called quantum entanglement – the information is protected by the laws of physics. The concept is called quantum cryptography, and enables two parties to exchange an enciphering key over a private channel in complete security.

An example of a cryptosystem is as follows. A sequence of correlated, or 'entangled' pairs of particles is prepared. Entangled pairs have the peculiar quantum property that when the state of one particle is measured it automatically defines the state of the other no matter how far apart they are. They might be pairs of photons with opposite polarisation states generated by certain nonlinear processes. One member of each photon pair is sent to each communicating party, and since measuring the state of one photon gives the state of the other, a key can be prepared without direct communication. Furthermore, an eavesdropper would have to detect a particle to read the signal, and then retransmit it to avoid being discovered. However, the act of detecting one particle of a pair destroys its quantum correlation with the other, and the two parties can easily verify whether this has happened by communication over an open channel, without revealing the results of their own measurements.

QUANTUM TELEPORTATION

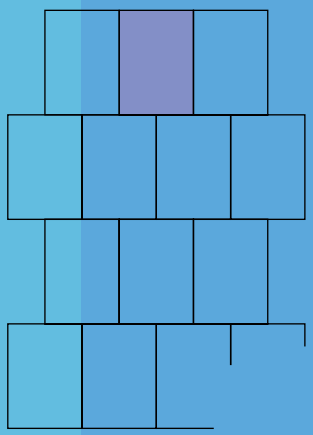
The notion of teleportation may seem like a science fiction device but researchers have actually carried out teleportation experiments on particles. Again, the key to quantum teleportation is to create a pair of entangled particles. An entangled pair A and B can serve as a vehicle to teleport the state of a third particle C from the sender to the receiver. A is sent to the sender and B to the receiver. The sender then makes a combined quantum measurement of the A and C which also 'primes' the state of B. If the sender gives the receiver the results of the combined measurement he or she can use it to recreate particle C's state from particle B (see diagram). Note that this is true teleportation in that the initial state C is destroyed; copying quantum states is forbidden!

Quantum teleportation in action



TIM SPILLER FOR THEIR HELP WITH THIS PAPER

Visions is a series of papers which highlight exciting new areas of research in physics, and their theoretical and technological implications.



AVAILABLE VISION PAPERS:

High intensity lasers

FORTHCOMING VISION PAPERS:

Novel uses of nuclear physics
Physics and finance
Spintronics

ABOUT THE INSTITUTE OF PHYSICS

The Institute of Physics is an international learned society and professional body for physicists. The Institute has more than 22,000 individual members.

FOR FURTHER INFORMATION CONTACT:

Department of Higher Education and Research
The Institute of Physics
76 Portland Place
London W1N 3DH
UK

e-mail: visions@iop.org
Institute website: http://www.iop.org/

Editor: Nina Hall. Design: Pete Hodkinson