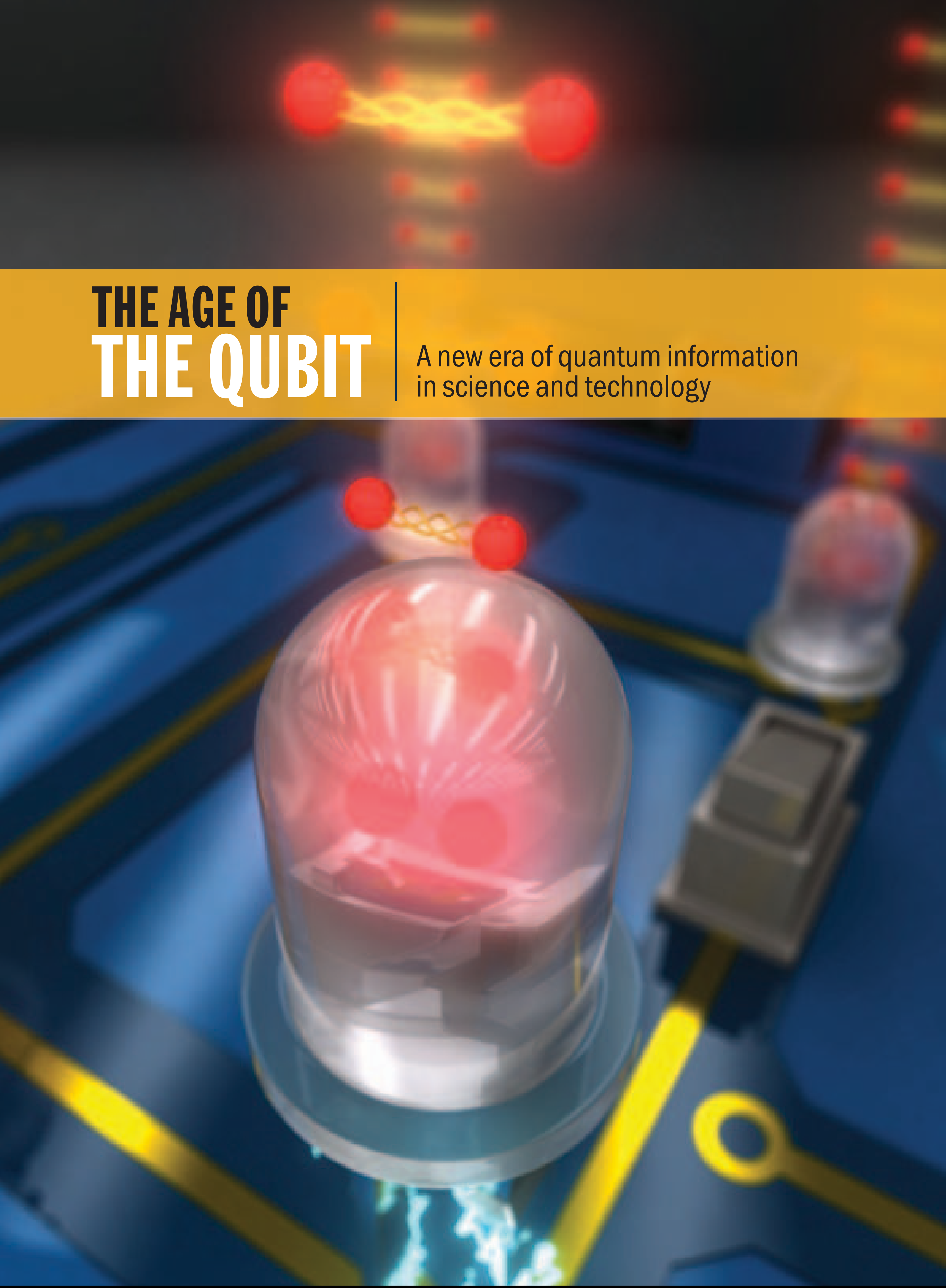
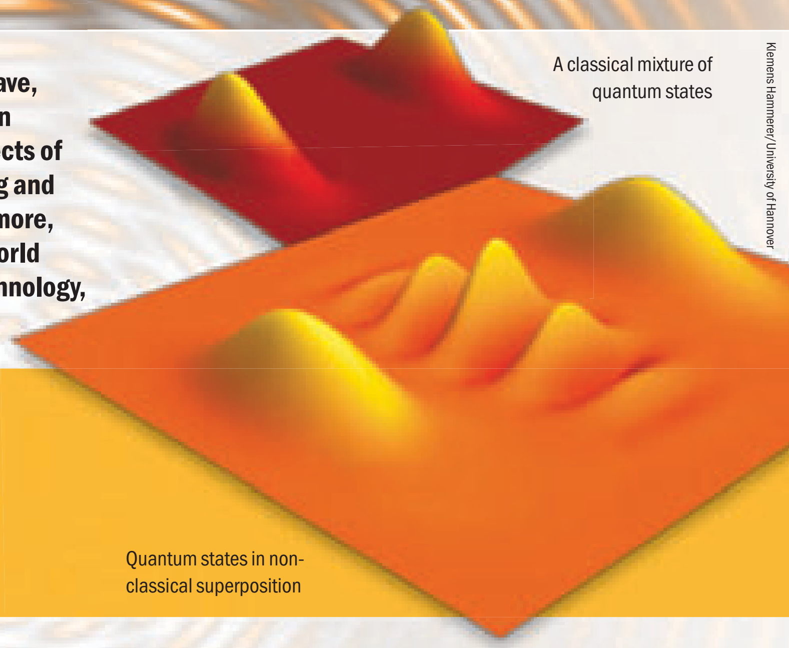
THE AGE OF THE QUBIT

A new era of quantum information in science and technology



IOP Institute of Physics

Quantum mechanics describes how physical systems behave, usually at the smallest scales. Physicists and information scientists are now studying and harnessing the deepest aspects of that behaviour to create radically new ways of communicating and processing information that are extremely powerful. Furthermore, the investigations are leading to insights into the quantum world that promise to stimulate major advances in science and technology, and could ultimately influence how we perceive reality.



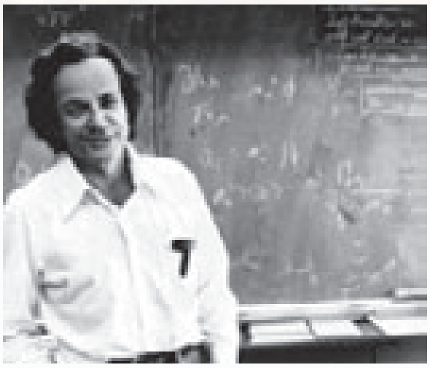
A classical mixture of quantum states

Quantum states in non-classical superposition

Klemens Hammerer/University of Hannover

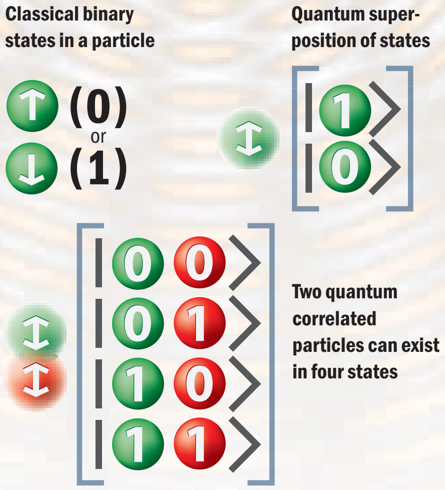
EXPLOITING THE QUANTUM REALM

It is now hard to imagine day-to-day living without information technology, which offers instant communication and access to data that can then be manipulated as needed. Such digital information is encoded as clearly separate values of 1 or 0, for example, in a two-state system such as a voltage (on or off state) in an electronic device, magnetic orientation of particles (up or down) in a memory, or a light pulse in an optical fibre. These binary "bits" are the basis of today's computers and communication systems.



Thirty years ago, physicist Richard Feynman proposed exploiting quantum interactions to create a more powerful type of computing

Such systems are said to obey the familiar laws of classical mechanics. However, in the early 1980s, the US physicist Richard Feynman suggested that the strange, "non-classical" properties of systems obeying the laws of quantum mechanics could offer a new way of processing information; a full-scale **quantum computer**, for example, would be unbelievably powerful. The concept of quantum information processing (QIP) was born.


Classical binary states in a particle
(0)
or
(1)
Quantum superposition of states
|1⟩
|0⟩
|00⟩
|01⟩
|10⟩
|11⟩
Two quantum correlated particles can exist in four states

Quantum superposition allows more information to be processed

WHY IS QUANTUM INFORMATION PROCESSING DIFFERENT?

Quantum systems such as electrons or photons (light quanta) are bizarrely different from classical systems: they behave like **particles** and also **waves**. The wave-like behaviour manifests itself in interference phenomena (wave patterns superposed to create a new, combined wave pattern); it summarises the **probabilities** of particles existing in particular quantum states. This results in apparently undetermined, fuzzy behaviour, which takes on a distinct value only when an **external measurement** is made.

The electron, for example, has the quantum property of spin, which can take two values, up and down. If isolated, the electron spin states exist with equal probability in what is called a "**coherent superposition**". In information terms, the electron spin therefore encodes simultaneously two values, 0 and 1, instead of just one, as in classical systems. Taking this concept further, the two-spin states of two particles, if combined in superposition due to wave-like interference between them, can hold four values (00, 01, 10 and 11). Similarly, three such "**correlated**" particles can encode eight values and so on, so that *N* particles can hold 2^N bits of information simultaneously. These information carriers are known as "**qubits**". In theory at least, this (2^N) exponential relationship not only allows huge amounts of information to be processed in parallel but also enables new types of computation to be carried out that are not possible with classical systems.

THE CENTRAL ROLE OF QUANTUM ENTANGLEMENT

The key to this new, burgeoning field lies in one fundamental quantum property that is furthest from classical reality: **entanglement. Certain kinds of quantum superpositions in correlated particles remain inextricably linked: an operation or measurement on one particle determines the state of the other, even when the particles are far apart.**

The first application in which quantum entanglement was specifically exploited was in **cryptographic communication** (p4). This was first developed in the UK in the early 1990s. Since then, **entanglement has become a core resource in the development of QIP**. In fact, QIP is providing *the* conduit for the birth of a new scientific field: the **physics of quantum entanglement**.

LEADING UK RESEARCH

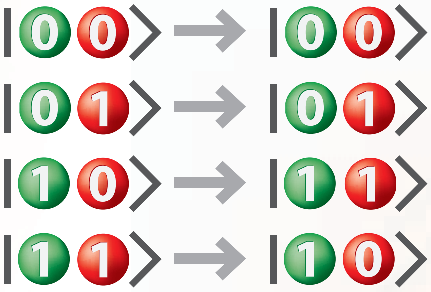
In the past two decades, the field of QIP has exploded on all fronts – trying to build a quantum computer is only one of several research threads; there are other highly significant applications. The UK is playing a major role in virtually all areas of research, as the following pages will show.

IBM

Quantum algorithms power up the speed of information processing
IBM's Blue Gene supercomputer would take millions of years to factor a 256-bit binary number, whereas a quantum computer working at the same clock speed could do it in a few seconds. (This is because if a classical computer factors a number in a certain time, it would need that time squared to factor a digit number twice as big, but a quantum computer could do it in just twice the time.)

EARLY HISTORY

Not long after Feynman's proposal, the UK quantum physicist David Deutsch laid down theoretical foundations for QIP by proving that a quantum computer could, indeed, simulate any physical process.



How a controlled-NOT gate for QIP works
Two correlated qubits are required – a control qubit (green) and the target qubit (red) that acts as the logic gate. Only when the control qubit is 1, does the target qubit change from 0 to 1 or vice versa

First quantum algorithms

The advantages of quantum computing became clear when **Peter Shor** at AT&T Bell Laboratories in the US devised a **quantum algorithm that could factorise large numbers** in a time exponentially faster than a classical algorithm. It could easily break keys used in today's encrypted communications (p4), which are based on the multiplication of two prime numbers. Later, **Lov Grover** at the same company, invented a **quantum search algorithm** that could speed up the search through an unsorted list of entries in a database, searching one million items in just a thousand steps. Many computer operations involve searching. Both algorithms are now used to demonstrate quantum-computing implementations (p6).

Elements of a quantum processor

The basic building block of any processor is a **logic gate**, which carries out a logical operation on a set of inputs to give an output. In QIP, a standard gate would be the **controlled-NOT (CNOT) gate**. This acts on two **correlated qubits**, a control qubit and a target qubit. The quantum state of the control qubit determines the operation to be carried out on the target qubit. When the control bit has a value of 0, the value of the target qubit stays the same; but when it has a value of 1, the value of the target qubit is flipped.

The first CNOT gates were built in the 1990s, in the US and Europe including the UK, using ions, which were held in traps created by electric and magnetic fields, and excited into a superposition of electronic states using laser pulses. Another model system, experimented with at the University of Oxford, as well as in the US, involved controlling the spin states of **atomic nuclei** in organic molecules, with strong magnetic and radio-frequency fields (nuclear magnetic resonance, NMR). It was used to execute Grover's search algorithm for the first time.

Practicalities

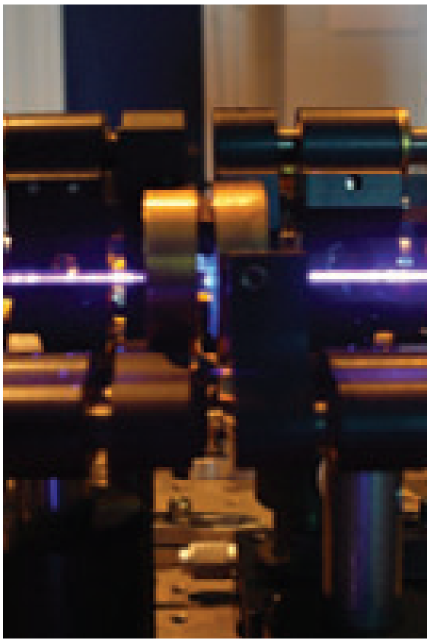
At first, it was not clear that QIP was a practical proposition – a quantum computer is still a long way off. Qubits are fragile entities that collapse when they interact with their environment – a phenomenon called **decoherence**. Then, Andrew Steane at Oxford and Peter Shor developed the first **quantum error-correction** scheme that could compensate by spreading the information over many qubits (p11). This was seen as a crucial step in developing the concept of quantum computing. Since then, researchers have also been exploring ways of increasing the qubits' **coherence times**, long enough to carry out a logic-gate operation.

Other important aspects include **scalability** and **communication.** A practical quantum computer requires many thousands of interacting qubits, which need to be controlled. Data may also need to be passed from one processing system to another, which may involve preserving quantum coherences transferred between different kinds of qubits, and over long distances.

The first practical demonstrations of QIP have been in communications, in particular in sending secure, encrypted messages – cryptography.

COMMUNICATING IN SECRET

The principle of teleportation involves transporting a qubit A$^+$ using a pair of separated entangled states, B$^-$ and B$^+$, which are in different locations. The quantum state of A$^+$ is first entangled with B$^-$, so that B$^-$ is then "primed" with A$^+$'s information, and is then measured. B$^+$'s state is transformed to that of A$^+$, while the original state of A$^+$ is destroyed – so, in effect, moving qubit A$^+$ from one location to another without moving the original particle carrying it


Marcin Kacprowicz

Entangled states of photons are the key to quantum communications

Cryptography relies on distributing a **secret key** – a series of numbers that enable the sender and receiver to encode and decode a secret message. Secure keys are essential for today's computerised financial transactions. Quantum systems provide an ideal vehicle, not least because the central tenet of quantum mechanics, the Uncertainty Principle, says that a quantum system cannot be measured without disturbing it, nor can an arbitrary quantum state be copied exactly (the "no-cloning principle"). This means that eavesdropping on a quantum-encrypted communication can be detected.

CRYPTOGRAPHIC SCHEMES

In quantum cryptographic schemes, the information is encoded as qubits of light having one or two types of polarisations: vertically and horizontally, or right and left diagonally, to represent a string of 1s and 0s. The simplest protocol, developed by Charles Bennett at IBM and Giles Brassard at the University of Montreal (the BB84 scheme), involved sending a key as a string of photons randomly polarised in one of the two settings. The receiver makes measurements randomly using two analysers that detect either the horizontal/vertical or the diagonal polarisations. The receiver never knows which polarisation setting the sender used to encode each 1 or 0 (and neither does an eavesdropper), and quantum uncertainty ensures that the right answer is obtained half of the time. Only after the information has been sent, does the sender divulge which were the correct analyser settings, and this allows the receiver to pick out the key from the results (and detect whether there was an eavesdropper).

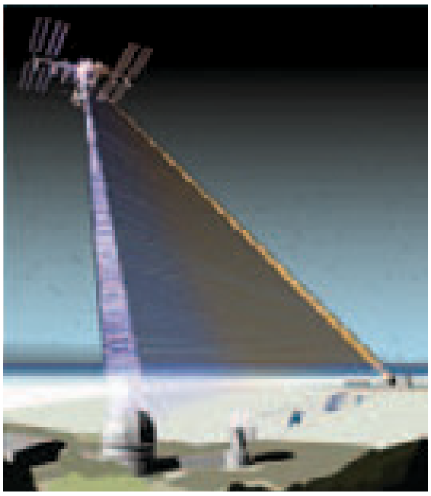
ID Quantique (Geneva)/Senetas Corporation (Australia)

Quantum cryptography was used at the FIFA World Cup in South Africa

QUANTUM KEYS ON YOUR MOBILE

Quantum cryptography could be on the high-street soon, if Tim Spiller at the University of Leeds can realise an idea developed when he worked at the Hewlett Packard Laboratories in Bristol. He envisages that quantum keys could be distributed between handheld devices and high-street cash-points through a free-space signal, to provide a rolling weekly pin number for authenticating bank transactions.

An important variation of the scheme proposed by Artur Ekert, when at the University of Oxford (now at the University of Cambridge), uses **entangled pairs of photons** with one photon from each pair supplied to the sender and receiver. The entangled photons can be prepared such that they have exactly opposite polarisations, and measuring one photon will automatically determine the polarisation state of the other. Any detection by an eavesdropper would automatically destroy this correlation.



ESA

Distribution of pairs of entangled photons across free space using the International Space Station

EXPERIMENTAL DEMONSTRATIONS

One of the first demonstrations of quantum cryptography was carried out in the 1990s by Paul Townsend and a team at BT Laboratories using a 28 km fibre over BT's public network around Ipswich. Now at the Tyndall Institute in Cork, he is working with Gerald Buller at Heriot-Watt University on constructing a practical robust system compatible with optical networks.

In 2000, a leading research group at the University of Vienna carried out the first full implementation of a quantum cryptography system using entangled states over a 360 m fibre link to transmit an image securely. Four years later, a team led by Andrew Shields at Toshiba Research Europe in Cambridge showed that quantum keys could be distributed securely over 122 km. The researchers have since been improving the reliability, taking part in European and Japanese trials that have achieved a sustained bit-rate of 1 megabit per second over 50 km of optical fibre – fast enough for video conferencing.

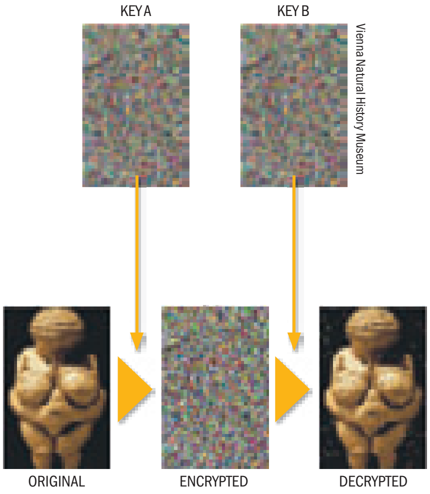
Quantum states have also been transmitted over free space, as was demonstrated in 2007 when entangled photons were distributed over a distance of 144 km between the islands of La Palma and Tenerife in the Canaries.

TELEPORTATION

Another important issue in quantum communication is relaying quantum states over long distances without degradation. Devices called **quantum repeaters** (p13) are needed to "refresh" the entangled state before forwarding it along the fibre network. This involves "**teleporting**" the state, through entanglement, to a distant device. Moving qubits around in this way will be an essential feature in a quantum communication network.

The first teleportation experiments were successfully carried out in the 1990s by teams at the universities of Innsbruck and Rome. The longest teleportation distance so far, of 16 km over free space, was recently announced by Chinese scientists, achieving an average accuracy of 89%.

Communication satellites could provide an alternative to a quantum repeater for long-distance quantum key distribution.

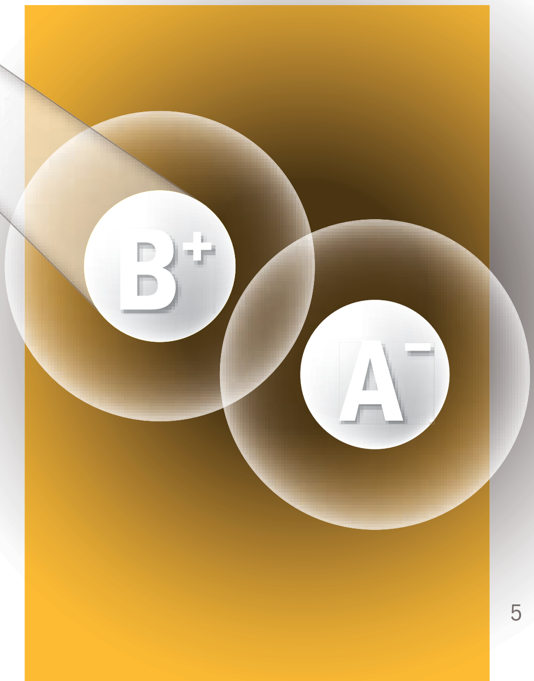


Vienna Natural History Museum

Researchers at the University of Vienna realised the first quantum cryptographic implementation, securely transmitting an image of the Venus von Willendorf statuette, with few errors

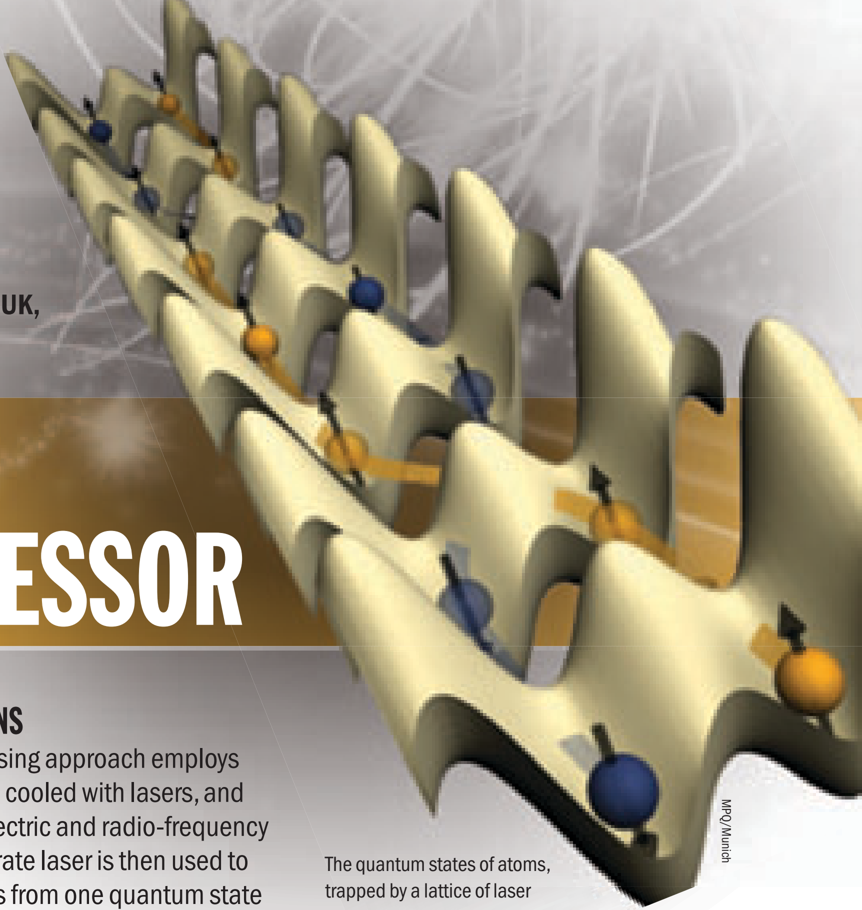
QUANTUM DIGITAL SIGNATURES

The Heriot-Watt researchers are also working on how to "sign" a document sent securely, using a **quantum digital signature**, so that its authenticity can be checked (the equivalent of a signature on a cheque that can be verified by the bank when the recipient pays it in). It uses a complex optical interference scheme, which ensures that the quantum key held by the recipient and that held by the bank agree.



Researchers around the world, including many in the UK, are exploring various candidate qubit systems.

TOWARDS A QUANTUM PROCESSOR



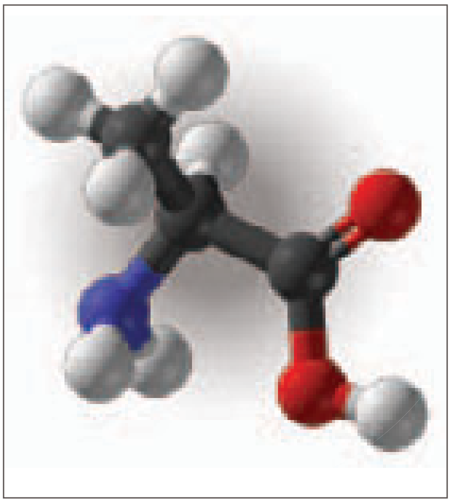
The quantum states of atoms, trapped by a lattice of laser beams, can be manipulated to create a quantum processor

MPQ/Munich

Just about any system that demonstrates quantum behaviour – from photons to molecules and superconducting devices – is being considered for QIP, and is generating a better understanding of quantum behaviour and nanoscale technologies.

NMR QUBITS

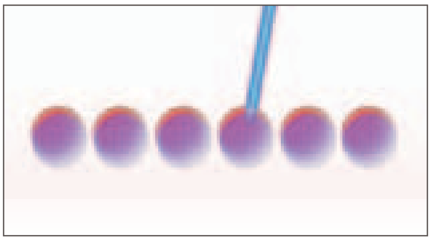
The first "toy-model" quantum computer was demonstrated in 1998 in Oxford by Jonathan Jones and colleagues, and was based on the principle of NMR (p3). The qubits were the correlated spin states of hydrogen nuclei in organic molecules dissolved in solution. Although such quantum computers have been effective in testing quantum algorithms, and a seven-qubit NMR system has been prepared, it is unlikely they could be scaled up any further.



Organic molecules such as alanine have been used to implement NMR quantum computing

TRAPPED IONS

A more promising approach employs arrays of ions, cooled with lasers, and trapped by electric and radio-frequency fields. A separate laser is then used to excite the ions from one quantum state to another. The cold ions are coaxed into entanglement with the laser, which causes them to jostle back and forth in concert so that they couple. This kind of coupling has enabled researchers to build CNOT gates (p3) using pairs of ions, and entangle eight or nine ions in a linear-shaped trap. In Oxford, Andrew Steane and David Lucas have been exploring the use of ions of a particular calcium isotope that features very sharp quantum states, which can be entangled by the above method.

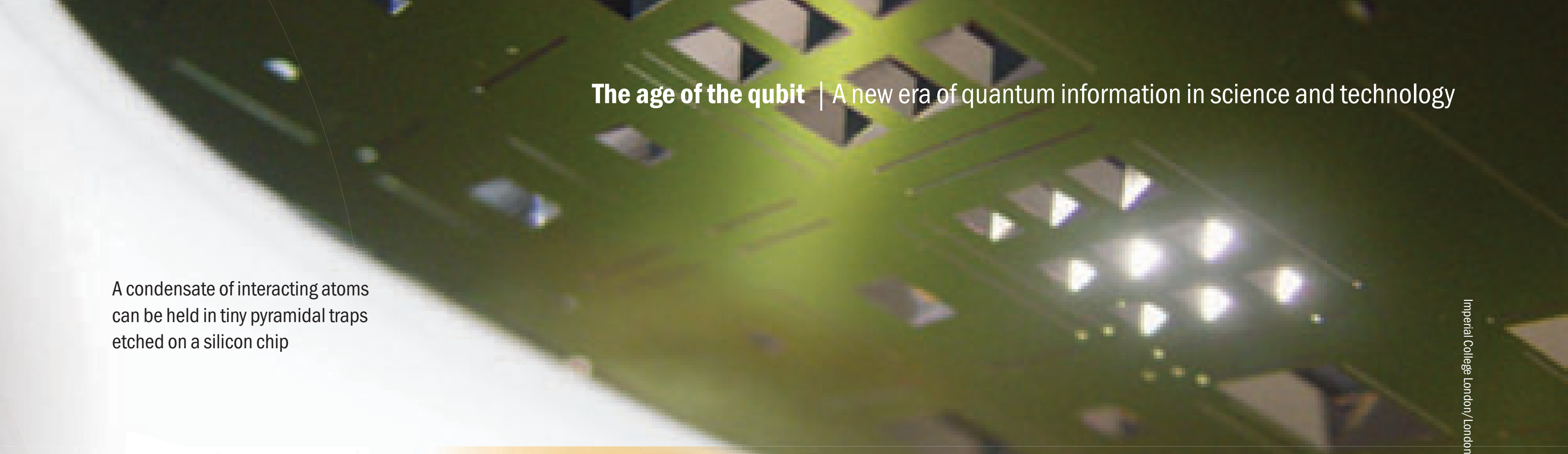


NIST/Bill Pietsch, Astronaut 3 Media Group

Trapped ions are pushed into entanglement by a laser

Building a computer would require large numbers of correlated ions. This might be best achieved using arrays of "micro-traps" made via standard microfabrication techniques. Richard Thompson and Danny Segal at Imperial College London have been working with a type of trap based on static electric and magnetic fields that could be suitable. Patrick Gill and Alastair Sinclair at the National Physical Laboratory (NPL) are building linear traps on a standard silicon wafer using gold electrodes, while Winfried Hensinger at the University of Sussex has developed a chip design that could be scaled to house a million ions, each in separate micrometre-sized traps consisting of microfabricated cantilever electrodes. The idea is to carry out quantum computing by shuttling the entangled ions around from one trapping zone to another. Information is read out, using optical fibres, via the fluorescence (photons) emitted by the ions.

Another important goal is to transfer entanglement between ions and photons, which would be essential for a quantum communication network. One of the standard ways is to capture the photons emitted by the ions between two mirrors forming an **optical cavity**. The photon bounces back and forth in the cavity, which increases the interaction with the ion, transferring the quantum states between the two qubits with high fidelity. Wolfgang Lange and Matthias Keller, also at Sussex, are building microcavities by using the ends of the communicating optical fibres as mirrors, which are integrated into the trap electrodes.



A condensate of interacting atoms can be held in tiny pyramidal traps etched on a silicon chip

Imperial College London/London Centre for Nanotechnology

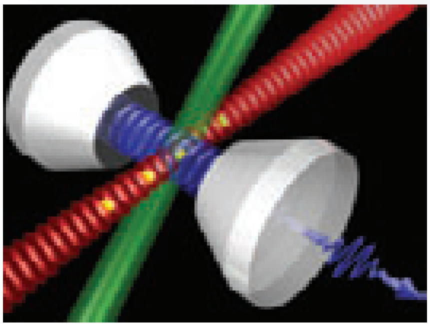
ATOMS

Trapped atoms

Stefan Kuhr at the University of Strathclyde is using an **optical lattice** comprised of interfering laser beams to prepare a "crystalline" array of ultra-cold atoms. He is able to control the quantum state of each atom using a tightly focused laser and microwaves, and is hoping to create a scalable quantum processor of several hundred atoms. Axel Kuhn at Oxford envisages confining a large array of individually controlled atoms using a matrix of **micro-mechanically operated mirrors**, and eventually coupling these atoms to multiple fibre-tip cavities to realise a hybrid network of atoms and photons.

Atom chips

A cooled cloud of atoms sharing a communal quantum state called a **Bose-Einstein condensate** could be combined with chip technology. Ed Hinds at Imperial College London prepares "atom chips" in which condensates of rubidium atoms are captured magnetically in microcavities on a chip surface. The atom qubits then interact with photons introduced via optical fibres or integrated waveguides.

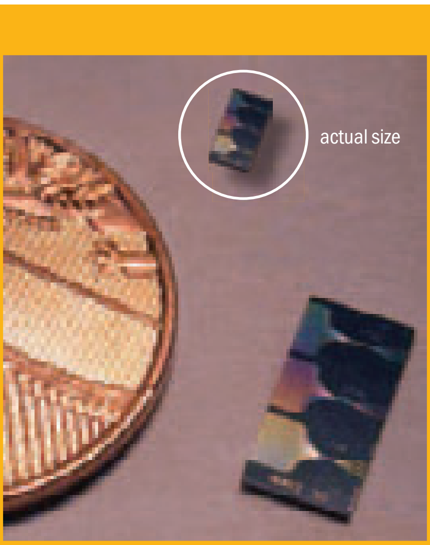


The motion of atoms slowed down and held in an optical trap of mirrors and laser beams can be controlled quantum mechanically

Max Planck Institute of Quantum Optics

PHOTONS – FLYING QUBITS

Entangled photons with opposite polarisations will clearly be important as "flying qubits" for transferring quantum information. They are robust and operations can be carried out on them with high fidelity. The standard way of generating an entangled pair of photons has been via a so-called **nonlinear process**, whereby a photon is split into two entangled photons of lower energy when it passes through a certain type of crystal. However, single photons from separate sources do not interact, as would be needed for a logic gate. Nevertheless, photons can be made to "coalesce", by sending them through a beamsplitter, which causes them to interfere in a way that results in the generation of two identical photons – a **linear process**. In 2001, Australian and North American physicists showed that this simple way of interacting photon states opened up the possibility of building a scalable, all-optical quantum computer from conventional optical elements such as phase-shifters, beamsplitters and polarisers – **linear optical computing**.



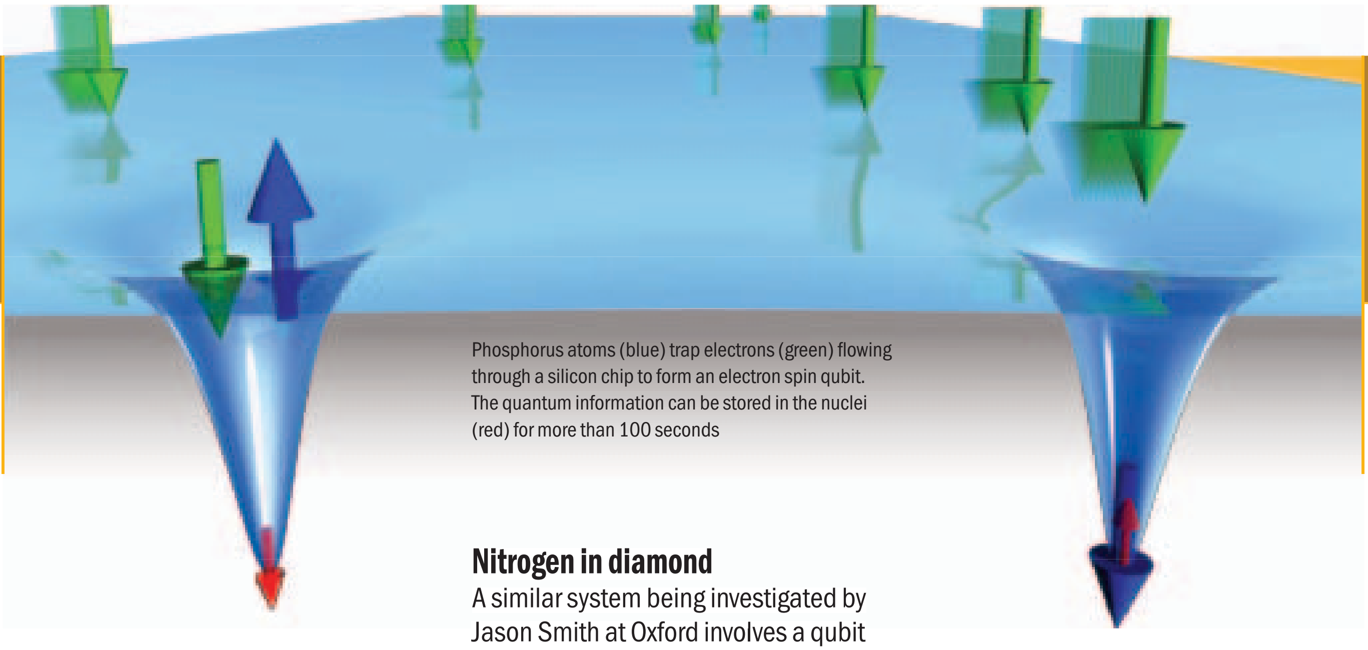
An all-optical chip developed at the University of Bristol for optical quantum computing

Jasmin Meinecke

Jeremy O'Brien at the University of Bristol leads a large team that is exploiting this breakthrough. The team is building precision optical chips with integrated waveguides and optical elements etched into them, to create a miniaturised all-optical CNOT gate, which was tested with Shor's factoring algorithm (p3). Using silicon oxynitride as a substrate, the team has coupled large numbers of photons in complex interference patterns potentially suitable for a new type of QIP called **cluster-state computing** (p11). Brian Smith's group at Oxford has also demonstrated controllable quantum interference on such chips, in collaboration with researchers in the Optoelectronics Research Centre at the University of Southampton. Ed Hinds places **organic molecules**, which emit photons when excited, in the chips' waveguides. The coupling between the molecule's quantum states and photons can be quite strong, allowing each molecule, through its optical nonlinearity, to induce interactions between photons that provide a basis for gate operations.

SPIN QUBITS IN THE SOLID STATE

A number of research groups are working on related systems that involve qubits of single atoms, ions or molecules embedded in a solid matrix, in which the quantum states are the spins of atomic electrons or nuclei. Again, such systems should lend themselves to microfabrication and be scalable. However, readout of the state of single-spin qubits has been achieved only recently.

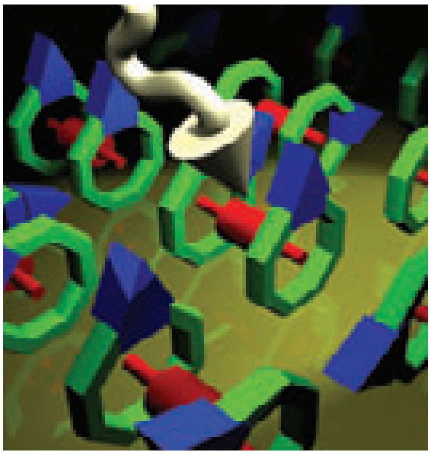


Phosphorus atoms (blue) trap electrons (green) flowing through a silicon chip to form an electron spin qubit. The quantum information can be stored in the nuclei (red) for more than 100 seconds

Gavin Morley/University College London

Phosphorus in silicon

One of the first solid-state qubits suggested was the nuclear spin of a phosphorus atom sitting in a silicon matrix. Each atom possesses a nuclear spin and an electron spin that can be controlled with radio waves and microwaves, while the qubits are coupled and measured using nearby electrodes. John Morton and colleagues at Oxford have worked on this system, recently demonstrating that large ensembles of phosphorus spin pairs can become entangled, as required for quantum computing.



Magnetically coupled metallic molecular wheels could act as qubits

Department of Chemistry/University of Manchester

Nitrogen in diamond

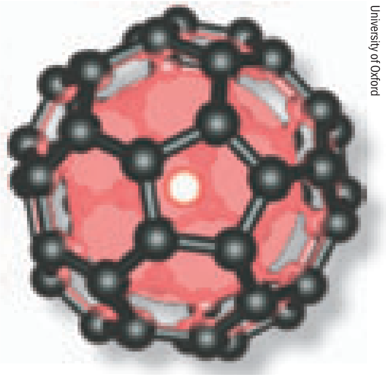
A similar system being investigated by Jason Smith at Oxford involves a qubit consisting of an impurity in diamond (a rigid lattice of carbon atoms). A single nitrogen atom sits next to a vacancy in the diamond lattice where a carbon atom would normally be, which traps a single electron (called an NV$^-$ centre). The system's electron spin state is stable for milliseconds at room temperature, and can be manipulated with radio-frequency waves and optical lasers. The NV$^-$ qubit emits single photons that can then be entangled via interference (see box, p7). Similar defect-based systems such as chromium in aluminium oxide are also being investigated.

Molecules

Teams at Oxford and the London Centre for Nanotechnology (LCN) are exploring molecular systems with electronic spins that can be manipulated and transferred. For example, John Morton is working on trapping metal ions in carbon cages called **fullerenes**, which might even be connected in chains, while others are investigating more complex, electronically active molecular configurations, as well as molecular clusters of metal atoms that can encode several magnetic states (**single-molecule magnets**).

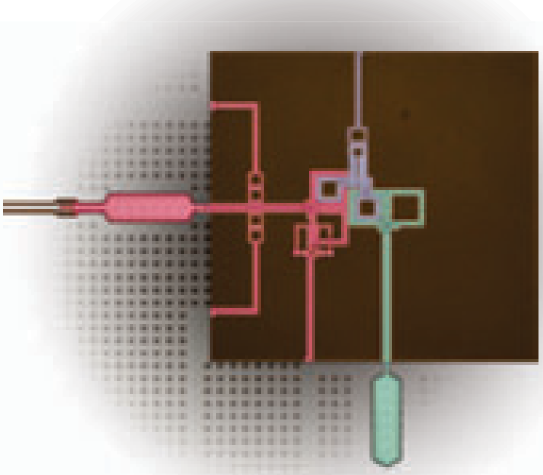
Quantum dots

An obvious solid-state candidate for quantum computing is the **quantum dot** – a nanometre-sized semiconductor structure that confines single electrons in a host semiconductor substrate. This "artificial atom" can be controlled with a voltage and a laser, and configured to emit single photons or entangled photon pairs. Maurice Skolnick and his group at the University of Sheffield have demonstrated how single electron spins can be controlled at ultrafast speeds using optical pulses, one of the requirements to achieve a high number of quantum operations before loss of coherence.



Spherical fullerene molecules with caged atoms are also possible qubit candidates

University of Oxford

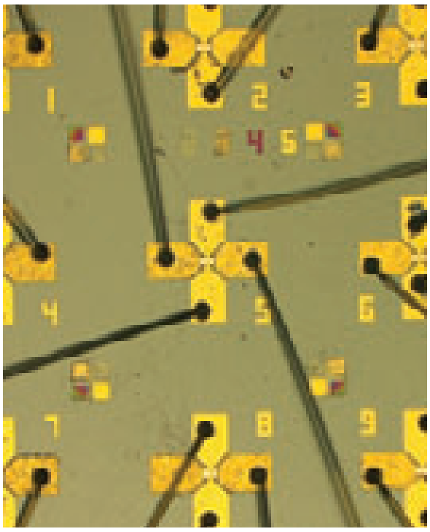


M S Allman/NIST

A superconducting circuit used in quantum computing research at the US National Institute of Standards and Technology

SUPERCONDUCTING QUBITS

Another type of artificial atom can be made from a tiny **superconducting circuit** in which correlated pairs of electrons undergo quantised oscillations. Superconducting qubits have been entangled to act as a quantum processor. They can be engineered to be compatible with standard chip technology and coupled with photons. Two drawbacks have been their short coherence times and the low temperatures required for superconductivity to occur. However, devices using **high-temperature superconductors** have been made and coherence times increased. The UK has not yet done much work on superconducting qubits, but several groups are now starting research programmes.



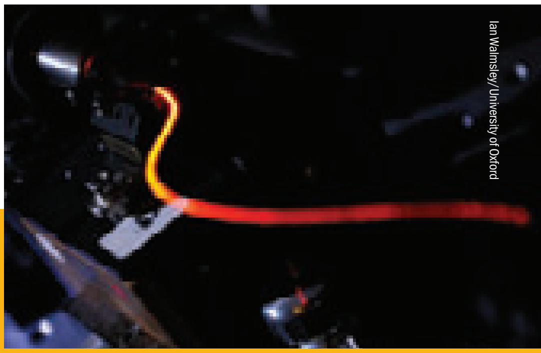
Toshiba's single-photon source is based on a quantum-dot device

SINGLE-PHOTON SOURCES AND DETECTORS

A key challenge for both quantum cryptography and computing is preparing the required single or entangled photons and then detecting them. The generation of more than one photon at a time could result in an eavesdropper collecting information without being detected.

Developing such **photon sources** is a major activity in the UK. John Rarity at the University of Bristol has built a single-photon source from a micro-structured optical fibre, while Ian Walmsley's group at the University of Oxford has developed various single-photon sources, using both nonlinear crystals and optical fibres, holding the world record for the highest-purity single photon. Wolfgang Lange and Matthias Keller at the University of Sussex have generated single photons from single ions, which is important for transferring quantum information between different carriers. Alastair Sinclair and his team at NPL are also researching single and entangled-photon sources with a view to determining standards for performance.

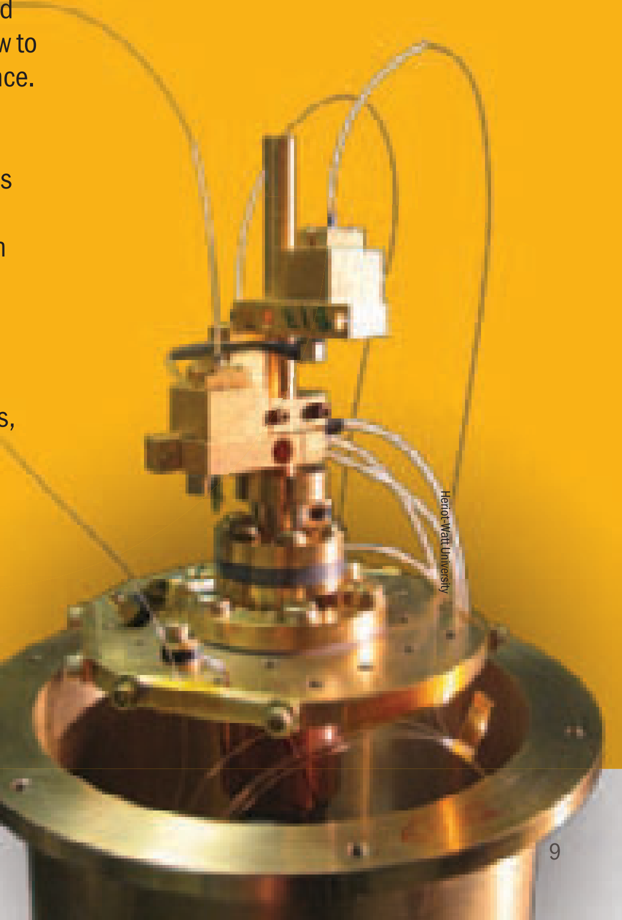
Together with the University of Cambridge and Imperial College London, Toshiba Research Europe has created a scalable semiconductor device based on quantum dots grown in an optical cavity that emits single photons at a wavelength suitable for optical-fibre transmission. One advantage of quantum dots is that they emit single or entangled photons, in response to an electrical pulse, on demand – unlike nonlinear crystals largely used to create entangled photon pairs, which emit photons probabilistically. Inexpensive chips hosting millions of such devices, each addressed by an electrical control signal, could be used in linear optical computing schemes (p7).



Ian Walmsley/University of Oxford

A single-photon source based on an optical fibre

Photon-counting detectors are also essential. UK groups, including those at Oxford, Heriot-Watt and Toshiba, have pioneered approaches to such detectors, which are particularly robust. Toshiba has developed a semiconductor photodiode that rapidly amplifies the faint signal from a photon and can detect up to 500 million photons a second. Heriot-Watt researchers are working on novel detectors based on various semiconductor materials and superconducting nanowires, particularly for single-photon detection in the near-infrared and infrared spectral regions.



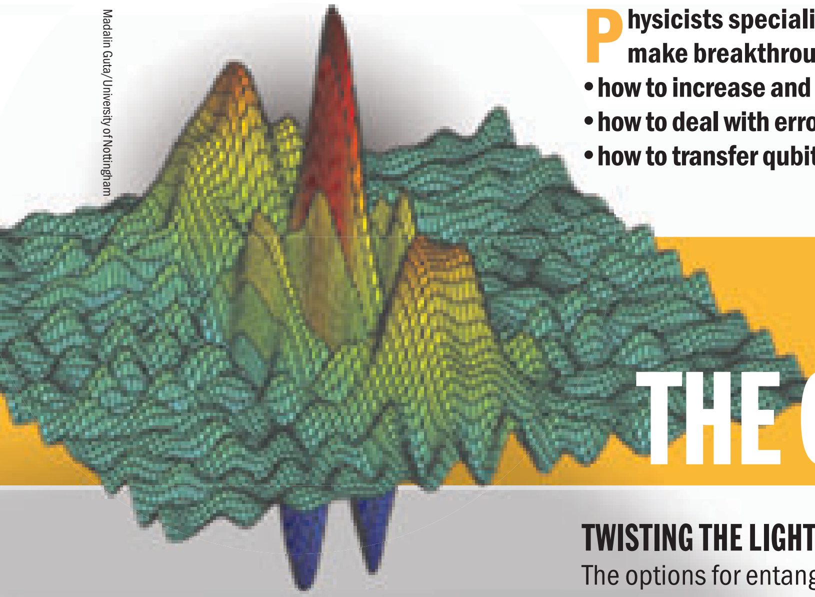
Heriot-Watt University

A single-photon detector based on a superconducting nanowire

Physicists specialising in quantum information theory are continuing to make breakthroughs that are helping to solve the major issues in QIP:

- **how to increase and manipulate entanglement – needed for large-scale qubit systems;**
- **how to deal with errors resulting from decoherence;**
- **how to transfer qubits efficiently.**

INFORMATION IN THE QUANTUM WORLD



Madalin Guta/University of Nottingham

UNDERSTANDING ENTANGLEMENT

To harness the full power of entanglement, physicists must be able to identify the different types of entanglement, which depend on what quantum states are available within a given system (in terms of energy, position or phase). They then need to measure the degree and distribution of entanglement, and follow how it evolves in time and space during quantum processing. Theorists, Vlatko Vedral at Oxford, Sir Peter Knight at Imperial College, Martin Plenio, now at the University of Ulm, and Sougato Bose at University College London (UCL), are among those who investigate how entanglement is distributed and exchanged in multi-particle systems.

Mauro Paternostro, a theorist at Queen's University Belfast working with experimentalists in Vienna, has been exploring the feasibility of transferring non-classical entangled states to a medium-scale, normally classical mechanical system. Laser light can be tuned to damp down and thus "cool" the vibrating mirror of an optical cavity via the radiation pressure that the photons exert. The mirror's vibrations can then couple to photon qubits. He has also shown how these quantum-controlled mechanical vibrations can then interact coherently with atoms in a Bose-Einstein condensate (p7) trapped in the cavity.

TWISTING THE LIGHT AWAY

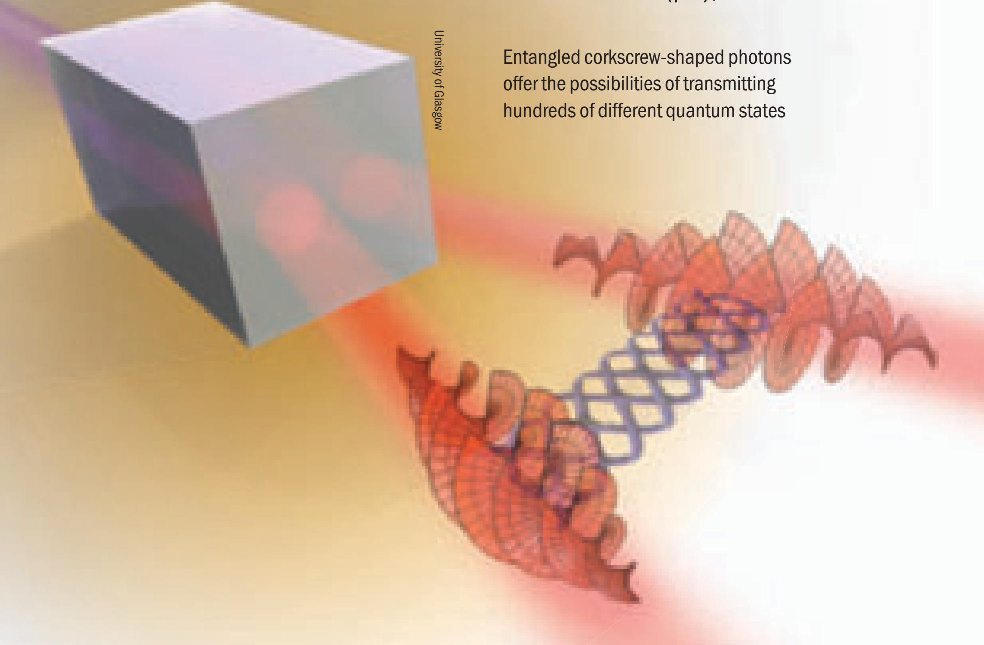
The options for entangling photons could be dramatically increased by manipulating a structural feature of light called **orbital angular momentum** (OAM). So far, photon qubits measured have been oppositely polarised quantum states. OAM can be visualised as a corkscrew-shaped pattern (see below) in the phase of the light beam, which can have any whole-number value, allowing possibly hundreds of states to be exploited in quantum communication (p4). They are not easy to measure, but using a sophisticated interference scheme akin to holographic imaging, Stephen Barnett at the University of Strathclyde and Miles Padgett at the University of Glasgow have been able to pick out and measure OAM entangled states.

GHOST IMAGING

The researchers have extended the technique to **imaging** by reflecting a stream of photons, each one part of an entangled pair, on an object. Because of entanglement, a second light beam composed of the photon partners that have never "seen" the object, also carries the imaging information, so that when combined with the first beam, a much clearer, so-called "ghost" image is generated.

DEALING WITH FAULTS

Because qubits are relatively short-lived, developing strategies for limiting errors to manageable levels is crucial. Although it is not possible to make back-up copies of quantum systems, as happens in classical computing, ingenious error-correcting methods continue to be developed. The simplest way, as first proposed by Andrew Steane and Peter Shor (p3), is to encode a bit



University of Glasgow

Entangled corkscrew-shaped photons offer the possibilities of transmitting hundreds of different quantum states

Fiona Burnell and Steve Simon/University of Oxford

Certain kinds of composite or fractional quantum particles could interact in a complex way to produce very robust qubits

of information into three entangled qubits. If one qubit randomly "flips" from, say, 1 to 0, one of the other two qubits can be used to spot the error and the third qubit can then process the information. The simplest quantum code that can correct an arbitrary qubit error requires five qubits. Often, the information is encoded in a large array of correlated qubits.

Methods are also being developed for extracting pure entangled states from a group of mixed states, as happens in linear optical systems (p7), leading to more reliable quantum computing. Increasingly, researchers are devising multi-component systems in which quantum information is shuttled into a more robust type of qubit and kept until required (p12).

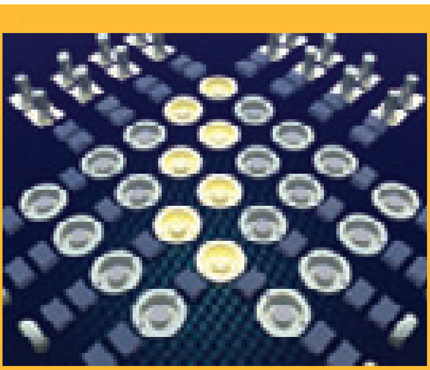
Another intriguing approach is to use highly entangled quantum systems that are **innately robust**. In certain materials, electrons interact very strongly to create a highly correlated system in which new quantum entities, "quasiparticles", emerge. Jiannis Pachos and his group at the University of Leeds are exploring unusual quasiparticles called non-Abelian anyons. Although meaningfully described only in terms of abstract mathematics, they have the property that they become entangled by weaving around each other to create so-called topological (braid-like) qubits; these are naturally resilient to decoherence, and could cope with high error rates. **Topological quantum computing** is still largely a theoretical idea, but certain 2D systems in which electrons have split into fractionally charged quasiparticles might be eventual candidates, or even materials such as graphene films. Furthermore, Sean Barrett at Imperial College is working on quantum error-correcting codes that are inspired by topological quantum-computing schemes. It turns out that these codes are highly robust to errors.

MAKING THE MOST OF ENTANGLEMENT

Describing entanglement mathematically is challenging but research has led to completely novel methodologies, in particular, measurement-based quantum computing – sometimes referred to as one-way or cluster-state computing – and ancilla-driven computing.

Measurement-based computing

The first ideas developed for quantum computing envisaged a set-up that was analogous to classical computing in which physical logic gates in a circuit process the information. Researchers at the University of Munich have proposed a new scheme that has entanglement at its heart. A cluster or grid of qubits is prepared in which each qubit is entangled with its nearest neighbour. Single qubits are then measured in a way that imprints the logic operations on this cluster state to implement the computer program. As the computation progresses, the measurements gradually use up the entanglement, so the process is one-way only. Experimentalists are excited by the idea of measurement-based, one-way computing because it is easier to implement than the reversible circuit-based system, although the initial highly entangled state cannot yet be created in many quantum systems.



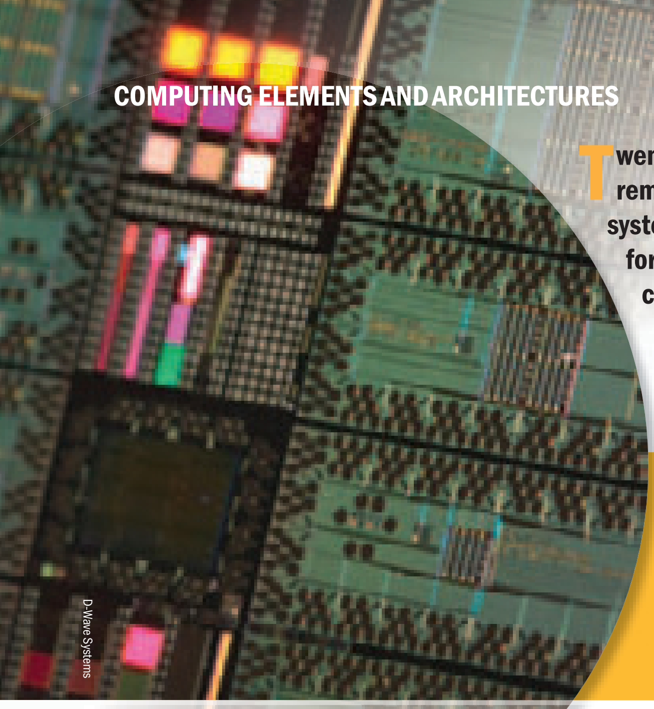
P.J. Blythe and B.T.H. Varcoe/University of Sussex

A quantum processor consisting of an array of tiny microwave cavities coupled to single atoms could be used for cluster-state computing, which is scalable and re-configurable

Dan Browne at UCL and Terry Rudolph at Imperial College have developed a scheme for applying cluster state measurements to linear optical computing (p7), while Sean Barrett and Pieter Kok, who is now at Sheffield, have shown how a cluster state could be created in a solid-state system, such as a quantum-dot array or atoms in cavities, using the optical system to mediate the entanglement. The team of Wolfgang Lange and Matthias Keller at Sussex is also implementing such a scheme with a string of ions in a cavity.

Ancilla-driven computing

Physicists at UCL, Heriot-Watt University and the universities of Strathclyde and Edinburgh have pioneered yet another approach, which is a hybrid of circuit-based and measurement-based computing. A single "flying" qubit that can be easily manipulated – an ancilla qubit – is moved across a cluster of long-lived qubits. Sequential entangling interactions between the flying qubit and individual cluster qubits steer the computation. Ancilla-driven computing could be applied to arrays of entangled atoms and ions or superconducting qubits.



D-Wave Systems

There has been considerable progress in quantum computing . One Canadian company, D-Wave, is aiming to build a useful quantum processor based on superconducting qubits

Twenty years ago, the prospect of realising a quantum computer seemed remote, but huge progress has been made. Coherence times in various systems have risen, reaching a few seconds in trapped ions and atoms, for example. New, faster algorithms to control gate speeds, and error-correction codes that can deal with large error rates have meant that quantum computation is starting to be regarded as a practical reality. There has been remarkable progress in increasing the ratio of the qubit coherence time to the gate-operation time.

A PRACTICAL QUANTUM COMPUTER

Furthermore, novel approaches that exploit the unique properties of quantum superposition and entanglement have opened up a new frontier in QIP. At the moment, it is not clear which types of qubits will form the basis of quantum computers, but most probably they will encompass a variety of optical fibre/chip-based systems that are compatible with current technologies.

Any quantum computer has several requirements:

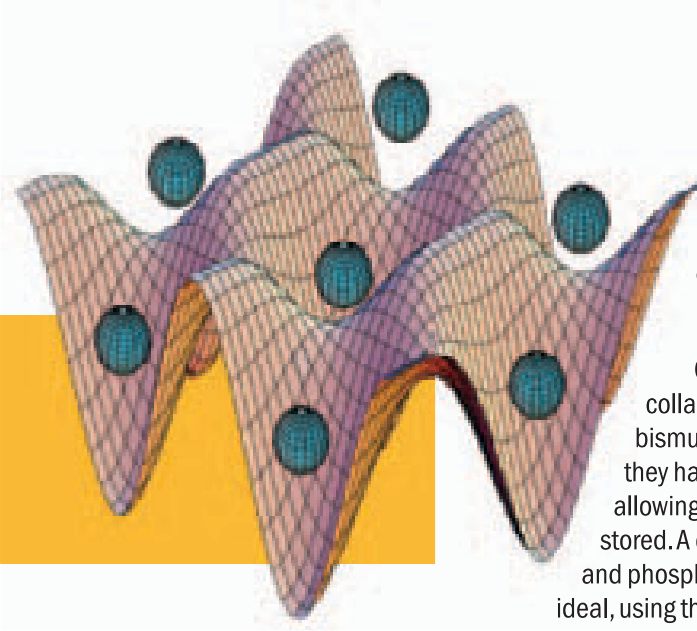
- Qubits with coherence times long enough to carry out a logic operation, preferably working at room temperature.
- An adequate error-correction strategy to maintain a practicable level of fidelity.
- Qubits that can be entangled in a scalable, controllable way, and are well characterised and easy to measure.
- Different species of qubits that can interact strongly and precisely, so that information can be communicated between systems – via light pulses, voltages or even tiny mechanical vibrations – and then stored.

A useful quantum computer would involve millions of qubits, and researchers are already considering what kind of architecture it might have. It is likely to be a hybrid network in which essential functions such as information processing, storage and communication are carried out by different qubit types. Researchers working with ion and optical chips (p6-7), for example, are already thinking about how to manipulate entangled qubit interactions across a large system. This means that information has to be reversibly mapped between light- and matter-based systems, which requires strong coupling between the different qubits. Many research groups are studying different modes of coupling.

DISTRIBUTED COMPUTING

Entangling very large numbers of qubits would be challenging. One approach that might be practical, and would work for measurement-based quantum computing (p11), is to construct a **scalable network of small groups of entangled qubits** such as trapped ions or quantum dots. The entanglements could be translated between groups, and also measured, via emitted/absorbed photons using optical cavities and fibres as described on p8. Inevitably, noise-based errors would creep in, especially in systems using electron spins. However, Simon Benjamin at Oxford proposes such a system using NV^- (nitrogen-induced vacancy in diamond) qubits (p8) in which errors could be controlled. Atoms of the carbon-13 isotope, naturally occurring in the diamond substrate, have a nuclear spin that can be entangled with a nearby NV^- electron spin. The nuclear spins would hold onto the information for a relatively long time (“**client qubits**”) while the electron spins (“**broker qubits**”) pass on the information across the network via photon emission. Even if the transaction fails several times before success, the information will have been kept for the duration.

Researchers at the University of Oxford test the coupling of photons with diamond-based qubits



Clouds of trapped atoms with stable quantum states could be the nodes for storing quantum information

CURRENT COHERENCE TIMES OF QUBITS

Photon (infrared photon in optical fibre)	0.1 ms
Trapped ion	15 s
Trapped neutral atom	10 s
NMR molecule nuclear spin	2 s
Quantum dot	3 μs
Phosphorus in silicon	10 s
Silicon nuclear spin	25 s
Superconducting qubit	4 μs

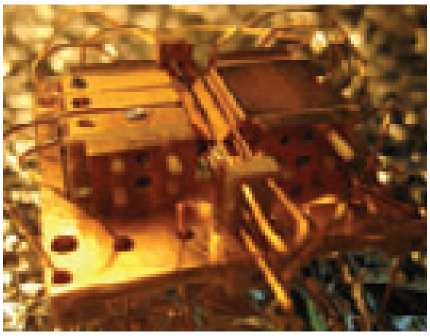
QUANTUM MEMORIES AND REPEATERS

Essential parts of any computer are random access memory and information storage. While photons are excellent for communication, matter qubits such as electron or nuclear spins are more suitable for holding information. **Nuclear spins** can have coherence lifetimes of more than a second, so are suitable for memory qubits. Their quantum states can be transferred via electronic coupling as described above. John Morton has been investigating a **solid-state quantum memory** stored in phosphorus-31 nuclei in pure silicon-28 (p8). The coherence lifetime is almost 2 seconds and the overall store-to-readout fidelity is about 90%.

Gavin Morley at LCN and collaborators have shown that bismuth atoms are also suitable; they have a large nuclear spin, allowing more information to be stored. A combination of bismuth and phosphorus nuclei might be ideal, using the former nucleus to store information and the latter to control it.

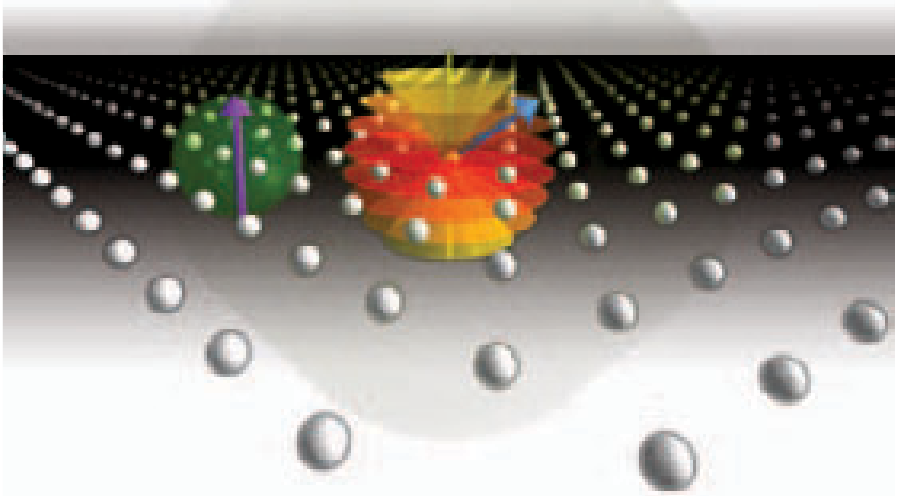
Another type of matter-light coupling being investigated for quantum memories is that between laser beams and ensembles of atoms. **Clouds of atoms** are candidates for quantum repeaters needed in optical communication and cryptography (p5), as well as distributed computer networks, to store information for a few microseconds before forwarding it onwards. Various configurations of carefully tuned lasers and atomic ensembles are being studied to map photon qubits onto the atoms' quantum states and then retrieve the information remotely.

Ian Walmsley, Dieter Jaksch and collaborators at Oxford are developing such **optical memories** using a phenomenon called Raman scattering to inscribe the information on **room-temperature atom clouds**, combined with a control laser that turns the interaction on and off, in order to "map" the quantum state of the input light beam onto the long-lived internal states of the atoms. The system works at bandwidths near those used in current telecommunications. Another method being studied by Axel Kuhn's team at Oxford is to store and retrieve information by a recently discovered quantum effect, known as "**slow light**", in which photons are controllably "trapped" in the internal states of the atoms. A further potential approach is to use a single atom for photon storage, with the atom confined between two opposing mirrors that form a resonant cavity, substantially increasing the atom-photon coupling strength.



Hensiger group/ University of Sussex

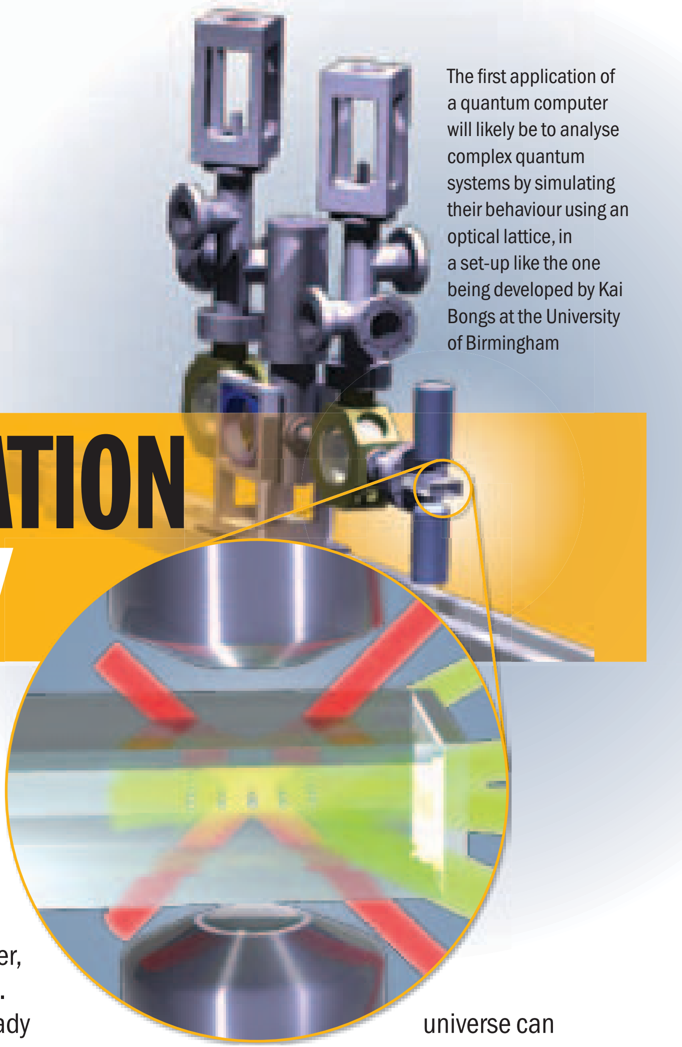
A chip design that could eventually trap and manipulate millions of entangled ions



Manuel Vögtli/LCN

A quantum memory could be based on the nuclear spin of bismuth (blue arrow), which can tilt in 10 different directions. Its electron spin (purple arrow) couples with the nuclear spin, and so transfers information to and from the system

To carry out a quantum computation that could not easily be performed on a classical computer would require a minimum of 50 entangled qubits, which has not yet been achieved. However, the QIP community believes that such systems could be available in a few years' time. While we are not likely to see a fully scalable quantum computer on our desktops for possibly another 20 years, other important applications are much closer.



The first application of a quantum computer will likely be to analyse complex quantum systems by simulating their behaviour using an optical lattice, in a set-up like the one being developed by Kai Bongs at the University of Birmingham

QUANTUM INFORMATION PROCESSING TODAY

PRECISION MEASUREMENT

One of the first applications of QIP will exploit the properties of quantum entanglement in a small number of qubits to make accurate measurements.

NIST

An atomic clock based on quantum logic has been developed by physicists at the US National Institute of Standards and Technology

A better time standard

Cooled, trapped atoms or ions are already used as clocks to provide standards for **time and frequency measurements**. A laser tuned to cycle cold caesium atoms between two quantum states that are separated by a microwave frequency interval provides a measurement that is accurate to better than 1 second in 30 million years. However, using entanglement between two dissimilar ions in a linear trap allows even more precise measurements to be made. Patrick Gill at NPL is planning to construct an atomic clock that exploits quantum logic to read out the result of probing quantum states separated by a much larger, optical frequency interval. US researchers have already shown that a **quantum logic clock** is accurate to 1 second in 3.7 billion years. This could eventually be used in **GPS satellite systems and telecommunications**.

Magnetic field sensors

Because entangled states are easily perturbed by their environment, they can be used as **sensors**. For example, Oxford researchers have prepared a 10-qubit multi-entangled state of nuclear spins in a star-shaped molecule that shows enhanced sensitivity to magnetic fields. The coupling of nuclear and electron spins in NV$^-$ qubits (p8) or qubits consisting of magnetic molecules could also be the basis of nano-probes to **analyse biological molecules**.

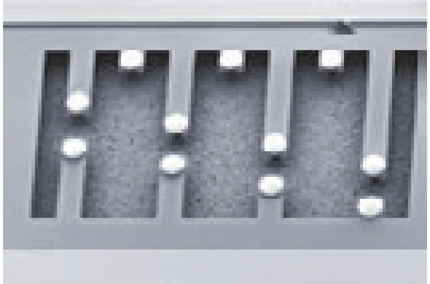
Measuring position

The most accurate way of measuring position and distance is **interferometry**, whereby the relative distances travelled by two laser beams from a beamsplitter are determined from interference fringes produced when their light is combined. Interferometry experiments attempting to detect **gravitational waves** from violent cosmic explosions across the universe can measure distances as small as the size of an atomic nucleus. They depend on measuring tiny displacements in massive suspended mirrors. By optomechanically controlling the mirrors at the quantum scale (p7), even more precise measurements can be obtained than would be achievable classically. Similar quantum optomechanical coupling could lead to new **high-efficiency transducers**.

Quantum entanglement may play a role in photosynthesis

Imaging and lithography

Non-classical entanglement of photons is also being exploited to overcome the natural resolution (diffraction) limit of classical optical systems, which depends on the wavelength of the light being used. The aim is to develop **improved microscopy** (particularly for biomedical studies) and **lithography** (for carving finer features on electronic devices). Pieter Kok, together with Samuel Braunstein, then both at Bangor University (Braunstein is now at the University of York), and researchers at NASA's Jet Propulsion Laboratory made the first proposal for using entanglement to beat the diffraction limit.



Keith Schwab group/CALTECH

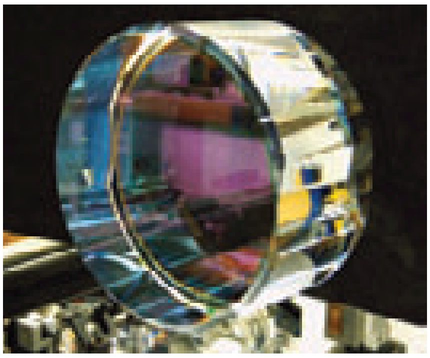
Tiny mechanical levers that are controlled quantum mechanically by light

ROUTE TO NEW TECHNOLOGIES

Researchers are already developing an analogue form of quantum computation – **quantum simulation** – to simulate and thus understand very complicated quantum systems of technological importance such as high-temperature superconductors. Micheal Köhl at the University of Cambridge and Christopher Foot at Oxford are using a 2D array of cold atoms trapped in an optical lattice to mimic solid-state quantum systems by observing each atom and determining its quantum state. Ed Hinds is leading a major new collaboration between Imperial College and Durham University to develop quantum simulators using cold molecules.

WIDER IMPLICATIONS

Studies of QIP have had a huge effect on the development of physics in the past decades. It has brought together disparate areas of physics and deepened physicists' understanding of the quantum world. Theoretical advances have provided new descriptive tools, and a conceptual language that will accelerate advances in other fields such as electronics and optics, where research is now at the nanoscale. QIP is also stimulating **new developments in mathematics and information theory**. In addition, some researchers think that the QIP approach might offer an easier way to **teach students** the basics of quantum mechanics.



Albert Einstein Institute, Hannover

Advanced gravitational-wave detectors will use mirrors that work with quantum-controlled precision

QUANTUM BIOLOGY

One of the most intriguing developments is the application of QIP ideas to **biology**. There has been much discussion about the role of quantum correlations in biological systems. For example, recent experiments indicate that entanglement could play a role in the surprisingly fast transfer of energy in the biomolecular systems that mediate **photosynthesis** in plants. Susana Huelga, when at the University of Hertfordshire, and Martin Plenio, both now at the University of Ulm, discovered that there is a subtle interplay between environmental noise and quantum coherence that optimises the transport efficiency in photosynthesis. Alexandra Olaya-Castro at UCL is also working in this new area. Harnessing such quantum coherence might be the key to more efficient **solar-energy devices**.

Even **bird navigation** could depend on quantum coherence. Birds' eyes are thought to contain a molecular "magnetic quantum compass". The molecule contains a pair of correlated electron spins whose coherence is affected by orientation to the Earth's magnetic field, so providing a direction. Indeed, experiments demonstrated that a weak, interfering oscillating field destroyed the birds' sense of direction. Simon Benjamin has been studying theoretically how the coherence is maintained (if it exists) and whether a similar system could be applied in quantum computing.

THE UK POSITION

In the earliest days, some of the seminal breakthroughs in the field were made by audacious researchers in a few UK physics departments. QIP was then a niche area. Since then, many other university physics departments and research laboratories have developed strong research activities in areas associated with QIP. This new, expanding field has invigorated and re-focused various areas of physics, attracting the brightest and most creative researchers, including those from other countries who have set up research groups at UK universities. With good investment, the UK will remain a front-runner in quantum information science and technology research, and so benefit from the potential economic and societal rewards.

Studies on the European robin indicate that it may rely on an entanglement-based compass to navigate

EUROPEAN COLLABORATIONS

A series of quantum information processing and communication networks have been set up under the EU Framework programmes.

QUIE2T (Quantum Information Entanglement-Enabled Technologies) http://qurope.eu/quie2t
This is an EU FP7 Coordination Action project aiming to coordinate European research in Quantum Information Processing and Communication (QIPC). Funding is €650 000 over three years. The QUIE2T architecture is structured around a set of four Virtual Institutes. Ian Walmsley (University of Oxford) is director of the Virtual Institute for Quantum Technologies.

Q-ESSENCE (Quantum Interfaces, Sensors, and Communication based on Entanglement) http://qurope.eu/projects/qessence
This is an Integrating Project to explore quantum entanglement, both theoretically and experimentally. It has a budget of €4.7 million over three years. The UK partner is the University of Oxford (Ian Walmsley).

AQUTE (Atomic Quantum Technologies) http://qurope.eu/projects/aqute
This Integrating Project aims at developing quantum technologies based on atomic, molecular and optical systems, developing novel hybrid systems, for example. The UK partner is Imperial College London (Ed Hinds and Sir Peter Knight).

Some key research papers in quantum information processing:

1. D. Deutsch, “Quantum Theory, the Church-Turing principle and the universal quantum computer”, *Proc. R. Soc. Lond. A*, **400**, 97 (1985).

2. L. K. Grover, “A fast quantum mechanical algorithm for database search”, http://arxiv.org/pdf/quant-ph/9605043v3.

3. P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, http://arxiv.org/pdf/quant-ph/9508027.

4. D. P. DiVincenzo and P. W. Shor, “Fault tolerant error correction with efficient quantum codes”, *Phys. Rev. Lett.*, **77**, 3260 (1996).

5. A. M. Steane, “Efficient fault-tolerant quantum computing”, http://arxiv.org/pdf/quant-ph/9809054.

6. A. K. Ekert, J. G. Rarity, P. R. Tapster and G. M. Palma, “Practical quantum cryptography based on two-photon interferometry”, *Phys. Rev. Lett.*, **69**, 1293 (1992).

7. J. I. Cirac and P. Zoller, “Quantum computation with cold trapped ions”, *Phys. Rev. Lett.*, **74**, 4091 (1995).

9. B. Kane, “A silicon-based nuclear spin quantum computer”, *Nature*, **393**, 133 (1998).

10. E. Knill, R. Laflamme, and G. J. Milburn, “A scheme for efficient quantum computation with linear optics”, *Nature*, **409**, 46, (2001).

11. R. Raussendorf and H. J. Briegel, “A one-way quantum computer”, *Phys. Rev. Lett.*, **86**, 5188 (2001).

For further information, contact:

Tajinder Panesor
IOP Institute of Physics
76 Portland Place
London W1B 1NT
Tel +44 (0)20 7470 4800
Fax +44 (0)20 7470 4848
E-mail tajinder.panesor@iop.org
www.iop.org
Registered charity no. 293851

The Institute of Physics is a scientific charity devoted to increasing the practice, understanding and application of physics. It has a worldwide membership of around 40 000 and is a leading communicator of physics-related science to all audiences, from specialists through to government and the general public. Its publishing company, IOP Publishing, is a world leader in scientific publishing and the electronic dissemination of physics.

This document is also available to download as a PDF from our website. The RNIB clear print guidelines have been considered in the production of this document. Clear print is a design approach that considers the needs of people with sight problems. For more information, visit www.rnib.org.uk.

Front cover image
Researchers at Toshiba UK have created the first electrically-driven source of entangled photon pairs by embedding a quantum dot in a semiconductor LED structure. It could realise the goal of scalable quantum computing

Writer: **Nina Hall** Design: **h2o-creative**