

Quantum information processing with atoms and photons

C. Monroe

FOCUS Center and Department of Physics, University of Michigan, Ann Arbor, Michigan 48109-1120, USA (e-mail: crmonroe@umich.edu)

Quantum information processors exploit the quantum features of superposition and entanglement for applications not possible in classical devices, offering the potential for significant improvements in the communication and processing of information. Experimental realization of large-scale quantum information processors remains a long-term vision, as the required nearly pure quantum behaviour is observed only in exotic hardware such as individual laser-cooled atoms and isolated photons. But recent theoretical and experimental advances suggest that cold atoms and individual photons may lead the way towards bigger and better quantum information processors, effectively building mesoscopic versions of ‘Schrödinger’s cat’ from the bottom up.

In 1948, Claude Shannon discovered how to quantify information¹ — a result so fundamental and revolutionary that in hindsight it is surprising it had not been formulated earlier. Shannon’s bit, or binary digit, became the fundamental unit of information, providing a metric for comparing forms of information and optimizing the amount of resources needed to faithfully convey a given amount of information, even in the presence of noise.

Shannon’s pioneering work not uncoincidentally prefigured the information age. Bits were found in nature, from unwieldy vacuum tubes in the 1940s to the modern semiconductor transistors of less than 10^{-5} cm in size. Under this impressive progression of technology, we have enjoyed an exponential growth in computing power and information processing speed given by the familiar ‘Moore’s Law’, where computer chips have doubled in density every year or two. Unfortunately, the days (or years) of Moore’s Law are numbered. As bits continually shrink in size, they will eventually approach the size of individual molecules — by the year 2020 if the current growth continues. At these nanometre-length scales, the laws of quantum mechanics begin to hold sway. In fact, classical bits can still be stored and manipulated here, as verified by the ground-breaking theoretical work of Paul Benioff^{2,3} and Richard Feynman⁴ in the early 1980s, and foreseen in Feynman’s remarkable 1959 charge towards nanotechnology, *There’s Plenty of Room at the Bottom*⁵. But even if we could somehow reach the bottom, where quantum states of every atom in a computer chip host classical bits, there would be no more room for further gains without splitting the atom.

Quantum rules

If we instead focus on the pure quantum features of a collection of atom-sized bits, we indeed find more room. For an isolated quantum system, the fundamental unit of information is the quantum bit or ‘qubit’. Qubits are just quantum two-level systems such as the spin of an electron or the polarization of a photon, and can be prepared in a coherent superposition state of 0 and 1:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

Here, α and β are the complex amplitudes of qubit states $|0\rangle$ and $|1\rangle$, and the superposition is resolved into either

definite state $|0\rangle$ or $|1\rangle$ upon measurement with respective probabilities $|\alpha|^2$ and $|\beta|^2 = 1 - |\alpha|^2$. In one sense, this is just a single bit of information. But in another sense, the continuous amplitudes α and β carry an infinite amount of information, similar to analogue information carriers such as the continuous voltage stored on capacitors. However, analogue systems are known to suffer from the cumulative build-up of noise, as opposed to digital standards like transistor–transistor logic that latch to their high or low levels through constant measurement and feedback. Quantum bits are similarly vulnerable to analogue noise⁶, but they can offer much more in return: quantum entanglement. In a classical analogue system, we need N capacitors to store N continuous voltages. But with N qubits, the most general state is specified by 2^N independent amplitudes $\gamma_0, \dots, \gamma_{2^N-1}$

$$|\Psi\rangle = \gamma_0|0_1 0_2 0_3 \dots 0_N\rangle + \gamma_1|0_1 0_2 0_3 \dots 1_N\rangle + \dots + \gamma_{2^N-1}|1_1 1_2 1_3 \dots 1_N\rangle \quad (2)$$

A collection of qubits therefore has the potential for storing exponentially more information than a comparable collection of classical information carriers. (Of course, the trick is extracting this information following a measurement, as discussed in the below applications.) The above state is entangled, as it is not generally separable into a product of individual qubit states. The implicit interconnects from entanglement give a quantum information processor its power (ref. 7; and see Box 1).

Atoms and photons: good quantum hardware

The chief hardware requirements for a quantum information processor are⁸:

1. The quantum system (that is, a collection of qubits) must be initialized in a well-defined state such as $|0_1 0_2 0_3 \dots 0_N\rangle$.
2. Arbitrary unitary operators must be available and controlled to launch the initial state to an arbitrary entangled state (equation (2)).
3. Measurements of the qubits must be performed with high quantum efficiency.

The first two requirements demand that the qubits are well isolated from the environment to ensure pure initial quantum states and to preserve their superposition character, but they must also interact strongly between one another in order to become entangled. On the other hand,

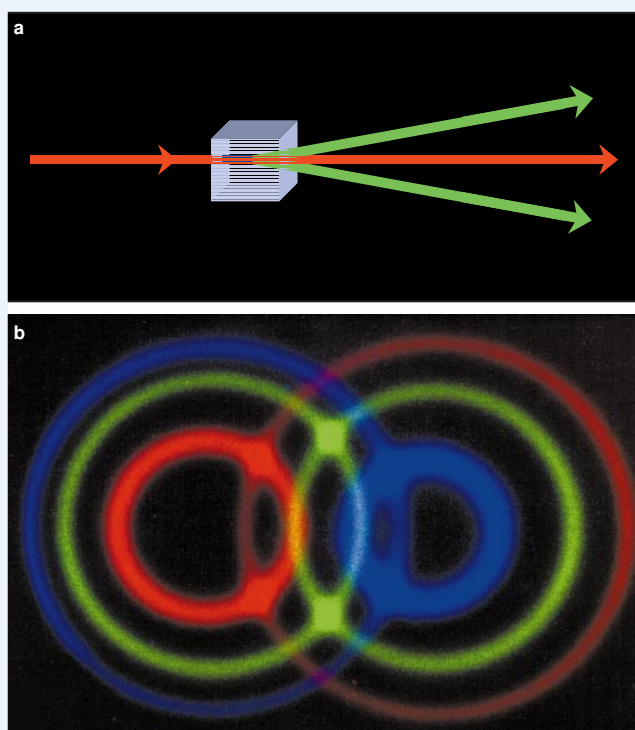


Figure 1 Optical parametric down-conversion. **a**, An ultraviolet photon incident on a nonlinear crystal can sometimes split spontaneously into two daughter photons. These photons are emitted on opposite sides of the pump beam, along two cones, one of which has horizontal polarization, the other of which has vertical polarization. **b**, Along the optical axis, several cone pairs can be seen. Photon pairs emitted along the intersections of the cones are entangled in polarization. (Image courtesy of A. Zeilinger, University of Vienna.)

the last stipulation requires the strongest possible interaction with the environment to be switched on at will.

These stringent hardware requirements unfortunately rule out most known physical systems. Conventional solid-state architectures such as silicon are ideal for classical information for the same reason they are unsuitable for quantum information; as discussed above, their stability is given by the latching of logic levels, or continuous monitoring by the environment⁶. The most attractive candidates for quantum information processors currently come from the area of atomic physics and quantum optics⁹. Here, individual atoms and photons are manipulated in a controlled environment with well-understood couplings, offering environmental isolation that is unsurpassed in other physical systems.

Complex entangled states such as equation (2) can be generated by sequentially applying quantum logic-gate primitives to smaller numbers of qubits, similar to the use of sequences of universal logic gates such as NAND ('not-and') in classical computation. In fact, it has been shown that arbitrary entangled states can be generated from sequences of simple qubit logic gates acting on any one or two qubits at a time^{10,11}. This sequential model of quantum computing fits naturally with quantum optical and atomic systems, where interactions are generally weak and typically involve at most two qubits.

Quantum information processing requires qubits to behave as quantum memories for long-term storage and for many applications to behave as quantum transmitters for long-distance communication. Cold and localized individual atoms are the natural choice for qubit memories and sources of local entanglement for quantum information processing. The stability of quantum states in cold atoms is unrivalled, evidenced by the fact that such quantum systems currently host the world's best frequency standards (see review in this issue by Udem, Holzwarth and Hänsch, pages 233–237). Individual

Box 1

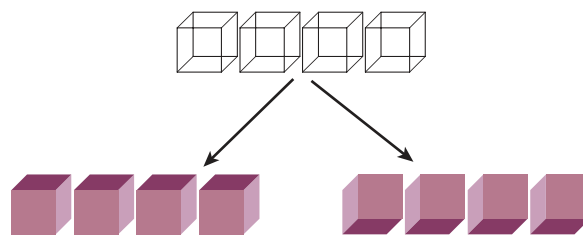
Entanglement, Schrödinger's cat and decoherence

Multiple quantum bits can be prepared in entangled states that are not able to be factored into a product of individual qubit states. An interesting class of entangled states is the 'Schrödinger-cat' states of N quantum bits, written as

$$|\Psi\rangle_{\text{cat}} = |0_1 0_2 0_3 \dots 0_N\rangle + |1_1 1_2 1_3 \dots 1_N\rangle \approx |\text{'live cat'}\rangle + |\text{'dead cat'}\rangle$$

This state is known as a mesoscopic Schrödinger-cat state, as the constituents of the superposition are as far apart as possible, analogous to the live and dead feline. As Schrödinger himself noted, describing a macroscopic object such as a cat with quantum terms is of course ridiculous, but for mesoscopic systems where N is not too large, the above state is useful in grasping large-scale entanglement.

The qubits in a Schrödinger-cat state are perfectly correlated, yet each qubit is entirely random when considered alone. This hidden wiring of entanglement, responsible for gains in quantum information processing, can be roughly visualized in the following analogy⁸⁹. Consider $N = 4$ adjacent three-dimensional cubes drawn with ambiguous perspective.



After a brief moment, your mind typically locks onto one of the two perspectives, and you will almost certainly see all cubes emerge with the same perspective. This is roughly analogous to a measurement of an entangled superposition.

The Schrödinger-cat state also highlights the difficulty in maintaining complex entangled quantum superpositions. If just one of the N qubits gets measured by the environment, every qubit loses its coherence. Decoherence makes it more difficult to engineer large entangled states, with the coherence survival probability decaying exponentially with the number of qubits⁹⁰. Extrapolating to $N \sim 10^{28}$ qubits in a real Schrödinger's cat, we find that the superposition of live and dead would almost instantaneously collapse into one or the other.

photons, on the other hand, are the natural source for the communication of quantum information, as they can traverse large distances through the atmosphere or optical fibres with minimal disturbance.

Quantum communication

Imagine two distant parties, Alice and Bob, share two entangled qubits analogous to an Einstein–Podolsky–Rosen (EPR) state¹²

$$|\Psi_{AB}\rangle = |0_A 0_B\rangle + |1_A 1_B\rangle \quad (3)$$

What can Alice and Bob do with their entangled pair? At first glance, they might try to exploit the strong correlations in their entangled states for direct (and superluminal) communication. A measurement by Alice or Bob immediately conveys the state of the other's qubit, but such measurements would yield only a sequence of perfectly random (yet correlated) bits, which carry no information according to Shannon. On the other hand, correlated random strings

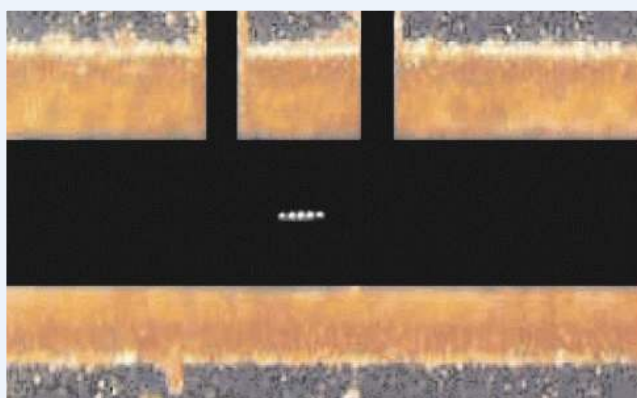


Figure 2 A crystal of five atomic beryllium ions (small white dots at centre) confined in a radio-frequency ion trap. The ions balance their mutual Coulomb repulsion with the confining force of electric fields generated from the surrounding electrodes (brown). The ions strongly fluoresce under the application of appropriate laser radiation near 313 nm. The horizontal electrode gap is about 0.2 mm and the ion-ion spacing is ~ 5 μm . (Image courtesy of NIST, Boulder.)

are extremely useful for cryptographic key distribution, as in the classic 'one-time pad'¹³.

Quantum cryptographic key distribution

Charles Bennett and Gilles Brassard developed the first protocols for quantum cryptographic key distribution (QKD) in 1984 (ref. 14), following earlier ideas of Steven Wiesner¹⁵. This scheme used the transmission of non-orthogonal states of single-photon qubits¹⁶, with security derived from the impossibility of an eavesdropper distinguishing the two states without being detected (on average). Several groups have implemented these protocols over tens of kilometres in underground fibres¹⁷⁻²⁰. Instead of idealized single-photon sources, these experiments used highly attenuated laser sources, which have a finite probability of emitting multiple photons per pulse. This gives rise to a trade-off between bit communication rate and security, resulting from the potential for eavesdropping on the surplus photons.

The use of entangled qubits can eliminate this trade-off and dramatically improve QKD. For example, by encoding qubits in orthogonal states of photon polarization in the form of equation (3), the measured presence of one photon at Alice indicates that Bob has

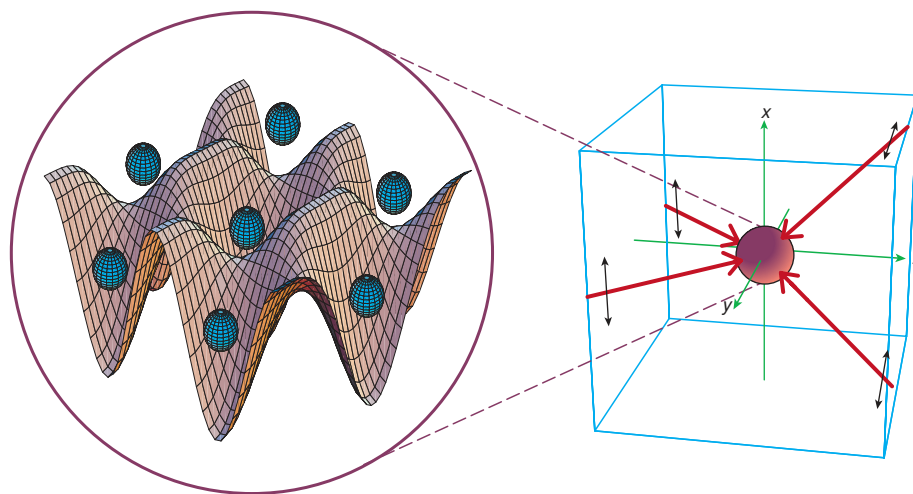
exactly one photon, which can be used to improve the security of the above single-qubit QKD scheme. Entangled qubits also offer an alternative QKD protocol, first pointed out by Artur Ekert in 1991 (ref. 21), and implemented recently by groups at Vienna University²², Los Alamos National Laboratory²³ and the University of Geneva²⁴. Here, the security is derived from the fact that a potential eavesdropper disturbs the entanglement shared by Alice and Bob.

These experiments used nonlinear optical parametric down-conversion (PDC) as their source of EPR-like entangled pairs. Ultraviolet pump photons are directed into a nonlinear crystal that gives rise to a small probability of down-conversion into pairs of visible or infrared daughter photons, as depicted in Fig. 1. These daughter photons always appear simultaneously, and can be entangled in their polarization degrees of freedom with appropriate phase-matching and mode selection. Unfortunately, PDC photon sources have several drawbacks in quantum information applications. Similar to the case of a highly attenuated laser source, there is a small probability of emitting pairs of down-converted photons that again offers an avenue for potential eavesdropping. Furthermore, PDC suffers from poor efficiency, as the probability of down-conversion per pump photon is typically below 10^{-10} (ref. 25). The presence of an entangled pair can be inferred only after a measurement (post-selection), so such states cannot be cascaded for subsequent processing to produce large-scale entangled photon states. Nevertheless, PDC sources are very useful for demonstrating rudimentary quantum communication protocols such as QKD.

Quantum teleportation

How can qubits be transmitted between remote locations? One method is to simply move the qubits through space, similar to the transmission of classical bits with electrical currents. However, this can be very difficult in practice, especially over long distances, as it must be done without disturbing or measuring the qubit state. Quantum teleportation, discovered by Bennett in 1993 (ref. 26), offers an alternative method of transmission without physical contact²⁷, as described in Box 2. The drawback is that the sender and receiver must already possess entangled qubits, a situation that may be as difficult as physically moving qubits from A to B in the first place, as entanglement always originates between nearby qubits. The real power of quantum teleportation is that it allows quantum information to be conveyed over a channel that may be unsuitable for direct physical transmission at the time of communication, or a channel that cannot reliably host the form of qubit stored at each end. For example, teleportation might allow quantum states in

Figure 3 Schematic of an optical lattice. A pattern of crossed laser beams (right) creates an array of potential wells that can confine individual laser-cooled cold atoms (left). The atom-atom separation is of the order of the optical wavelength. (Image courtesy of S. Rolston, NIST.)



atoms to be communicated between remote locations that possess previously entangled photons.

Groups from the universities of Innsbruck²⁸ and Rome²⁹ were the first to demonstrate certain critical aspects of quantum teleportation in 1997. In these experiments, polarization qubits of single photons were teleported between spatially separated locations using PDC. The low efficiency of these sources precluded the teleportation of larger numbers of qubits or the recycling of qubits^{30,31}. Shortly thereafter, a team at the California Institute of Technology (CalTech) efficiently teleported the continuous quantum state of a single-mode optical field³², relying on the deterministic entanglement of a pair of field modes, demonstrating a net fidelity of 58% without the need for post-selection.

Will we ever be able to teleport objects with more than just a single quantum degree of freedom? The answer is yes, as long as the three quantum hardware requirements are satisfied. But what about teleporting truly macroscopic objects with perhaps 10²⁸ effective qubits? This prospect, about as likely as preparing a real Schrödinger's cat both alive and dead, is clearly "ridiculous" as Schrödinger himself said³³. Instead, it is more fruitful to consider what we can do with a more modest system of perhaps 300 qubits, where the ~10⁹⁰ available quantum states are still more than the number of particles in the Universe.

Quantum computing

In 1985, David Deutsch showed how quantum superposition and entanglement could be harnessed to process information more efficiently than any classical machine³⁴. Deutsch's 'quantum parallelism' allows an *N*-qubit quantum computer to operate on quantum superposition states of all 2^{*N*} inputs. Extraction of information in a quantum computer is nontrivial, because simply measuring a quantum state such as equation (2) with an exponential number of nonzero amplitudes will yield a highly random result. In certain algorithms, however, appropriate quantum logic gates cause the amplitudes to interfere so that only a few amplitudes survive in the end. Following a measurement (or a limited number of repeated measurements on identical runs), the result (or distribution of results) can depend on a global property of all 2^{*N*} inputs.

The best-known example of this procedure is Peter Shor's 1994 factoring algorithm³⁵, where a quantum computer would be able to factor large numbers exponentially faster than any known classical computer algorithm. Fast quantum number factoring has profound implications in cryptanalysis, as many popular encryption algorithms such as RSA (Rivest–Shamir–Adleman)³⁶ rely on the inability to factor large numbers. In 1996, Lov Grover discovered a quantum algorithm that would search an unsorted database of *M* elements in a time that scales roughly *M*^{1/2} faster than any possible classical search algorithm³⁷. These discoveries have ushered a flurry of theoretical activity searching for further useful quantum computer applications.

A key development in 1995 was quantum error correction^{38,39}, an extension of Shannon's famous 1948 noisy coding theorem¹ to the quantum realm. Quantum error correction detects and corrects slight quantum gate errors or weak interactions with the environment through redundant encoding of qubits. This means that experiments need not be perfect; they require only that noise levels be below a certain threshold, with a trade-off between the amount of extra qubits required and the error threshold level. According to some models⁴⁰, arbitrary-length quantum computation can proceed error-free with only a polynomial overhead in time and space, so long as the error probability per fundamental operation is kept below about 10⁻⁵. What follows is a review of the most promising quantum computer architectures that may someday reach this level of fidelity.

Ion traps

Laser-cooled and trapped atomic ions represent one of the most attractive candidates for a large-scale quantum computer⁴¹⁻⁴⁴. Here, electromagnetic fields confine individual atoms in free space in a

Box 2

Quantum teleportation

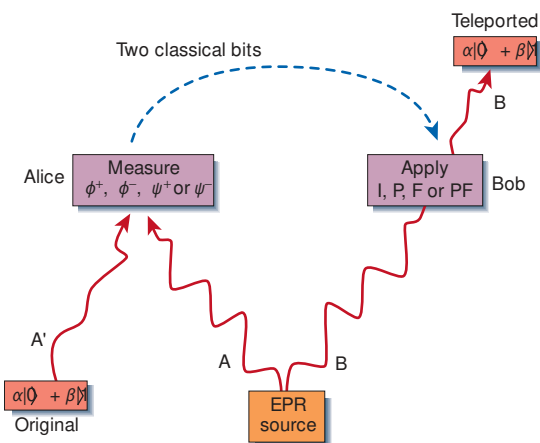
Quantum teleportation, the 'disembodied transport' of a quantum state from one site to another⁹¹, is conceptually simple, as outlined in the figure below. Imagine that Alice and Bob each already possess one of two qubits prepared in an entangled state such as equation (3). If Alice prepares another qubit *A'* in the arbitrary state $\alpha|0\rangle_{A'} + \beta|1\rangle_{A'}$, the overall state of the three qubits is

$$\begin{aligned} |\Psi\rangle &= (\alpha|0\rangle_{A'} + \beta|1\rangle_{A'}) (|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle) \\ &= |\phi^+\rangle_{A'A} (\alpha|0\rangle_B + \beta|1\rangle_B) + |\phi^-\rangle_{A'A} (\alpha|0\rangle_B - \beta|1\rangle_B) \\ &\quad + |\psi^+\rangle_{A'A} (\alpha|1\rangle_B + \beta|0\rangle_B) + |\psi^-\rangle_{A'A} (\alpha|1\rangle_B - \beta|0\rangle_B) \end{aligned} \quad (5)$$

where the four 'Bell' states of the Alice's qubits are defined as

$$\begin{aligned} |\phi^\pm\rangle &\equiv |0_A 0_A\rangle \pm |1_A 1_A\rangle \\ |\psi^\pm\rangle &\equiv |0_A 1_A\rangle \pm |1_A 0_A\rangle \end{aligned} \quad (6)$$

To pass the quantum information of Alice's qubit (the amplitudes α and β) to Bob, Alice makes a perfect projection measurement of her qubit pair onto this complete basis of Bell states. This can be done with simple operations of quantum logic gates on qubits *A* and *A'* along with an efficient measurement of both qubits, as depicted in the figure. This measurement immediately projects Bob's lone qubit onto one of the four states correlated with the state measured by Alice given in equation (5), resulting in his qubit now carrying the quantum information α and β . After Alice communicates which Bell state she measured to Bob using classical means (for example, a phone call), Bob performs a prescribed local qubit manipulation on his one qubit to replicate the initial state $\alpha|0\rangle + \beta|1\rangle$ in his qubit. For example, if Alice reports a measurement of $|\phi^+\rangle$, then Bob does nothing to his qubit (operation I). If Alice instead reports a measurement of $|\psi^-\rangle$, then Bob flips his qubit (operation F) and additionally adds a π -phase shift (operation P). In this way, the qubit $\alpha|0\rangle + \beta|1\rangle$ is 'teleported' from Alice to Bob without disturbing or measuring the qubit.



vacuum chamber, and when multiple ions are confined and laser-cooled, they form simple stationary crystal structures given by the balance of the external confining force of the trap with the mutual repulsion of the atoms (Fig. 2). Qubits are stored in internal electronic states of the atoms, typically the same long-lived hyperfine states that are used in atomic clocks. When appropriate laser radiation is directed to the atomic ions, qubit states can be mapped coherently onto the quantum state of collective motion of the atoms and subsequently mapped to other atoms. A single normal mode of collective

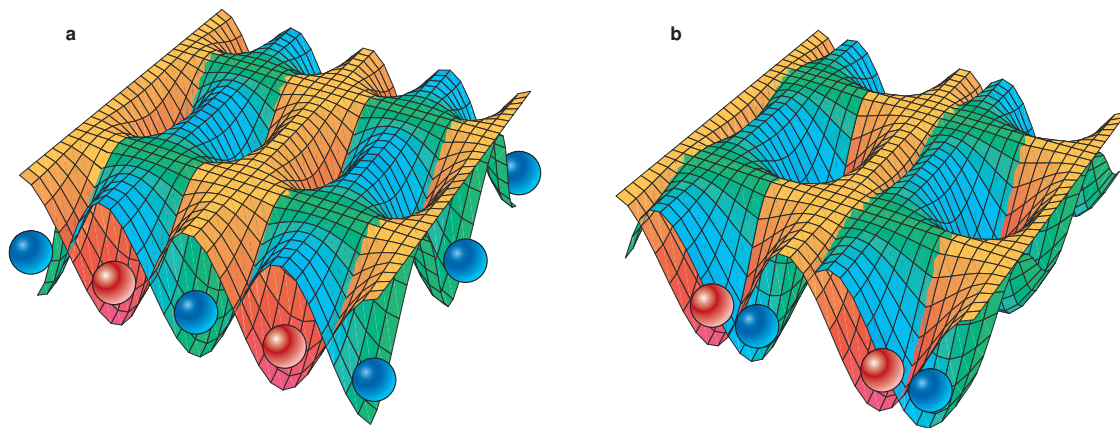


Figure 4 Optical lattice potentials. **a**, Optical lattice potentials can depend on the internal state (red or blue) of the confined atom qubits. **b**, These complementary lattice potentials can be controlled by varying the polarization of one of the lattice light fields,

shifting the interference pattern and bringing atoms together in pairs for quantum logic gates. (Image courtesy of I. Deutsch, University of New Mexico.)

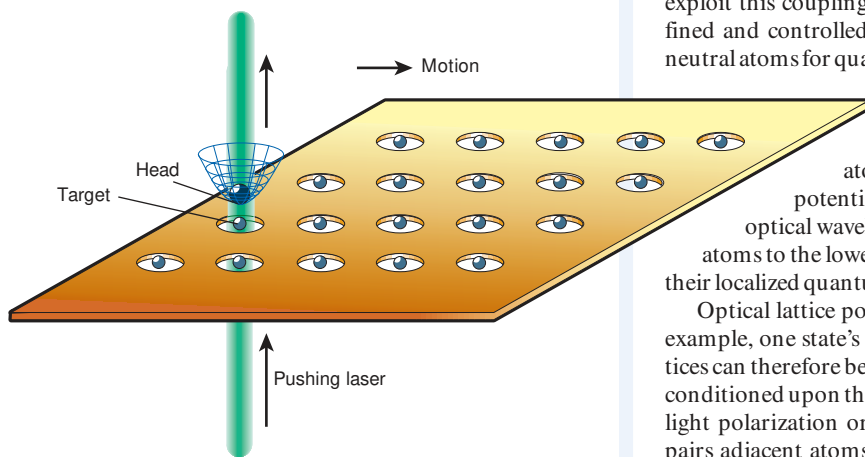
crystal motion thus behaves as a quantum data-bus, allowing quantum information to be shared and entangled between remote atomic qubits in the crystal. Finally, the internal states of individual trapped ions can be measured with nearly 100% quantum efficiency⁴⁵ by applying appropriate laser radiation and collecting fluorescence — one qubit state is bright and the other is dark.

Quantum logic gates have been demonstrated with up to four trapped atomic ion qubits at the National Institute of Standards and Technology (NIST) at Boulder, Colorado^{46,47}. Although this scheme is in principle scalable to arbitrarily large numbers of qubits, the main problems deal with the collective motion of the atoms. The quantum gate speed is limited to the frequency of motion, typically in the sub-megahertz range. As more qubits are added to the collection, the density of motional states balloons, and isolation of a single mode of motion (for example, the centre-of-mass) becomes even more slow and difficult. Moreover, external noisy electric fields tend

to compromise the motional coherence of large numbers of trapped atomic ions⁴⁸.

A promising approach that attacks both problems is the quantum charged-coupled device (CCD), where individual atomic ions are entangled as above, but only among a small collection (under 10) of atomic ions in an ‘accumulator’⁴³. Scaling to larger numbers is accomplished by physically swapping individual atoms between the accumulator and a ‘memory’ reservoir of trapped atom qubits. This can be done quickly with externally applied electric fields in elaborate ion-trap electrode geometries. The key features of the quantum CCD are that the ion shuttling can be done without perturbing the internal qubits, and the motional quantum state of the ions factors from the internal qubit states following quantum gate operation. In order to quench the motional energy from rapid shuttling and allow subsequent logic gates, ancillary ions in the accumulator can be laser-cooled between gate operations. The qubit ions are thereby sympathetically cooled⁴⁹ through their strong Coulomb interaction with these extra refrigerator ions. Sympathetic cooling can also eliminate motional decoherence during logic gate operation^{43,50,51}.

Figure 5 Scheme for a scalable ion trap and optical-lattice quantum computer. An array of independent (memory) ion traps is coupled through interaction with a roving (head) ion trap. A strong optical-lattice laser field entangles the head ion with a given memory or target ion. (Image courtesy of P. Zoller, University of Innsbruck.)



Cold atoms and dipoles in optical lattices

Neutral atom qubits enjoy a weak coupling to the environment, at the expense of a weak dipole–dipole coupling between each other. To exploit this coupling for entanglement, atoms must be tightly confined and controlled to sub-micron dimensions. A natural host of neutral atoms for quantum information purposes is the optical lattice — an array of cold atoms confined in free space by a pattern of crossed laser beams⁵².

The dipole force between the polarizable atoms and the field results in a regular pattern of potential wells, the spacing of which is of the order of an optical wavelength (Fig. 3). Several groups have laser-cooled atoms to the lowest bound state in lattice wells^{53–55} and controlled their localized quantum wavepacket states^{56,57}.

Optical lattice potentials generally depend upon qubit level (for example, one state’s valley can be another state’s hill). Atoms in lattices can therefore be shifted to nearly overlap with their neighbours, conditioned upon their internal qubit state, by modulating the lattice light polarization or intensity, as shown in Fig. 4. One proposal⁵⁸ pairs adjacent atoms together with one of the atoms prepared in a short-lived excited state. The resultant resonant dipole–dipole interaction, mediated by the shared excitation, allows pair-wise

entanglement. The speed of this quantum gate must be faster than the excited-state decay time, meaning the atoms must be localized and overlapped to well under an optical wavelength. A related proposal would transiently bring adjacent atoms together depending on their internal qubit levels, but instead rely on ‘cold collisions’ for entangling logic gates⁵⁹. If the atoms are sufficiently cold, then such *s*-wave collisions will result in a conditional phase shift of their quantum states, or a quantum phase gate.

Another approach exploits the large electric dipole moments of Rydberg atoms⁶⁰ or even simple heteronuclear molecules⁶¹ in an externally applied electric field. For instance, selected atoms held in an optical lattice can be entangled by promoting them to Rydberg states and relying on their mutual dipole–dipole interaction. The interaction strengths over micrometre distances can be in the gigahertz regime, implying very fast quantum gate operation.

One significant drawback to the use of optical lattices in quantum information is that the lattice sites are typically not uniformly packed. However, the same statistical properties of bosons responsible for Bose–Einstein condensation (see review in this issue by Anglin and Ketterle, pages 211–218) can be exploited for better control of atom number in optical lattices. A subtle interplay between a repulsive *s*-wave scattering interaction between bosonic atoms and the tunnelling of atoms between lattice sites can smooth out the atom-number statistics between wells, a phenomenon known as a Mott-insulator phase transition^{62,63}. Signatures of this behaviour have been observed in an optical lattice loaded with a Bose–Einstein condensate. Researchers at Yale University⁶⁴ measured fluctuations in the number N of atoms per lattice site by coherently combining atoms in adjacent sites in an atom interferometer, and reported a spread in atom number that is a factor of about 40 below the standard $N^{1/2}$ shot-noise level. A group at the Max Planck Institute for Quantum Optics (MPQ) in Garching, near Munich, has recently observed signatures of the small N limit to such ‘number-squeezed’ states, where exactly one atom resides in each site⁶⁵. This sets the stage for future progress in quantum gate operations using optical lattices.

A further proposal combines the features of optical lattices and ion traps, where individual ions are entangled through a common interaction with a pulsed, high-strength optical lattice⁶⁶. The lattice jerks two ions such that the internal qubit states of each ion are mapped to displaced spatial positions, smearing out their charge distributions⁶⁷. The interaction between these ‘engineered’ dipoles then allows entangling quantum logic gates that can be much faster than the ion–trap frequency. Moreover, pure quantum states of motion are not necessary, so long as the ions are confined to much less than the ion–ion separation. Finally, the ions need not be close together or even in the same trap, providing a convenient method for scaling to arbitrary numbers of qubits in an array of separate ion traps (Fig. 5).

Quantum networks

As more complex quantum communication protocols are demonstrated, there will be a pressing need to store quantum information in long-term memories. To construct reliable quantum networks of both quantum transmitters and quantum memories, small quantum computers will be needed at the nodes, acting as routers, repeaters and switches.

Degradation of quantum information will be unavoidable when qubits are sent over large distances or over noisy channels. This will require quantum ‘repeaters’ to be placed periodically along the channel so that qubit errors can be corrected. These repeaters can take the form of error-correcting quantum computers, or stations that share several imperfect entangled qubit pairs with adjacent sites⁶⁸. Here, quantum computer operations at the nodes ‘purify’ the entangled states so that states can effectively be teleported over remote distances. Remarkably, some of these protocols require local operation fidelities of only 98% for successful transmission⁶⁹.

A key component of such a quantum network is the faithful and coherent conversion of quantum information between different

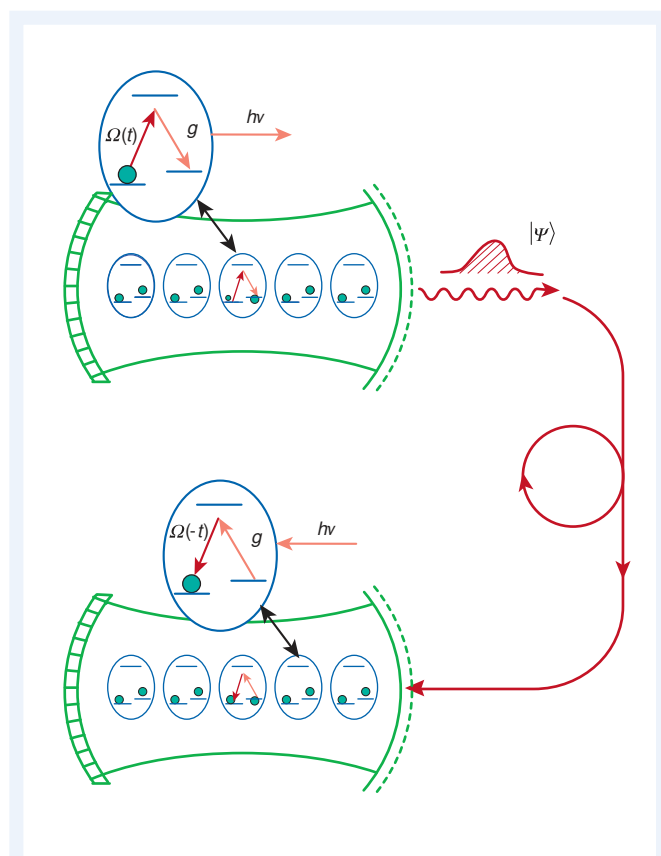


Figure 6 Atom–photon quantum network. A selected atom inside the top optical cavity coherently transfers its internal qubit onto a single-photon qubit in the cavity through the application of a classical laser pulse represented by the coupling $\Omega(t)$. The coupling g is between the single-photon field in the cavity and the atom. The single photon leaks out of the top cavity, only to be caught in the lower cavity by a time-reversed and synchronized classical laser pulse $\Omega(-t)$. (Image courtesy of H. J. Kimble, CalTech.)

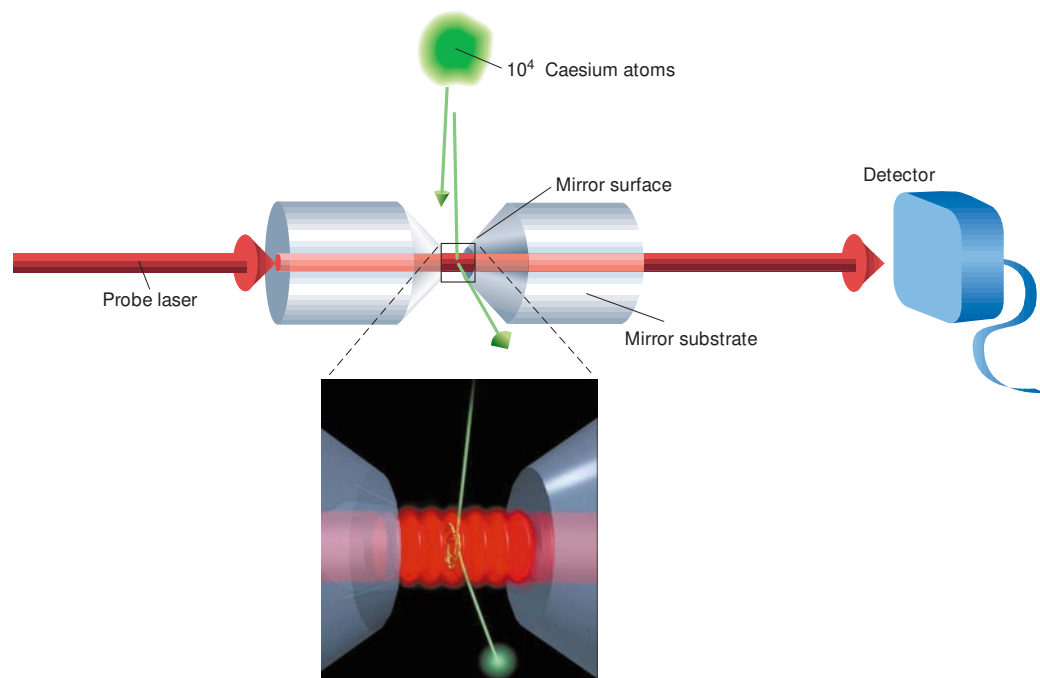
systems. Of particular interest is the reversible mapping of qubits from photon states to atomic states. This might allow the implementation of photonic quantum repeaters and also the teleportation of qubits from remotely located atoms through common EPR pairs of photons.

Cavity quantum electrodynamics and cold atoms

An elegant proposal to marry atomic and photonic quantum bits in optical cavity quantum electrodynamics (QED) was developed in 1997 (ref. 70). In this scheme, a small number of cold atoms are confined to the antinodes of a single-photon standing-wave field in a high-finesse Fabry–Perot optical cavity. Qubit states stored in the internal states of the atoms can be mapped to the qubit spanned by the number of photons (0 or 1) in the cavity through application of an appropriate laser pulse from the side. The photon can be made to leak out of the cavity within a pre-set time window, resulting in an ideal single-photon source for use in quantum communication⁷¹. Moreover, after the photon leaks out of the cavity, it can be deterministically ‘caught’ in a second cavity by the application of another laser pulse, whose envelope is time reversed with respect to the first pulse, as depicted in Fig. 6. Generalizations involving more than one atom in each cavity can distribute entanglement to many nodes while also featuring fault-tolerant error correction⁷².

Applying cavity-QED techniques to quantum information requires a single-atom/single-photon coupling that overwhelms any loss or decoherence rate, including atomic spontaneous emission and photon leakage through the mirrors. This leads to cavities of small

Figure 7 Single-atom cavity-QED experiment. Cold caesium atoms are dropped into a high-finesse optical cavity of axial spacing $\sim 10\ \mu\text{m}$. The trajectory of a single atom traversing the cavity is reconstructed (inset) by monitoring the field that leaks out of the cavity. (Image courtesy of H. J. Kimble, CalTech)



volume (for a high single-photon intensity) and extremely high mirror reflectivity (to keep the photon in the cavity). Groups from CalTech^{73,74} and MPQ⁷⁵ are beginning to master this difficult technology by trapping individually laser-cooled atoms inside miniature high-finesse cavities (Fig. 7). The atoms evolve in the requisite ‘strong-coupling’ limit, where even single photons in the cavity can significantly influence the dynamics of atomic motion⁷⁶. However, the atomic trajectories are still extended when compared to the optical wavelength, which effectively randomizes the atom–photon coupling and leads to decoherence. A second MPQ group is progressing on a complementary system, where individual atomic ions have been tightly bound within a larger optical cavity so that the atomic trajectory is well under an optical wavelength⁷⁷. But here the atom–photon system is not strongly coupled, because the insulating surfaces of a smaller cavity could interfere with the ion-trapping fields. These experiments, along with approaches from several other groups, point the way towards an ultimate goal in quantum information networking—that of coherently exchanging single atoms and single photons.

‘Stopping’ light

Several recent experiments from the universities of Harvard^{78,79} and Berkeley⁸⁰ have reported slowing and even ‘stopping’ light using the techniques of electromagnetically induced transparency⁸¹ in an atomic vapour. The stopping of light might seem trivial at first glance—it can be easily accomplished by putting an opaque black screen in front of a light source. Instead of irreversibly destroying the photons, however, these experiments offer the potential for mapping quantum states of photons onto collective quantum states of the atomic vapour⁸². For example, single-photon qubits can be mapped onto a single qubit spanning all N spins in a vapour:

$$[\alpha|0\rangle_{\gamma} + \beta|1\rangle_{\gamma}]|0_{\text{exc}}\rangle \rightarrow |0\rangle_{\gamma}[\alpha|0_{\text{exc}}\rangle + \beta|1_{\text{exc}}\rangle] \quad (4)$$

where $|1\rangle_{\gamma}$ and $|0\rangle_{\gamma}$ represent the presence or absence of the photon, respectively, and $|0_{\text{exc}}\rangle = |\downarrow_1\downarrow_2\downarrow_3\dots\downarrow_N\rangle$ and $|1_{\text{exc}}\rangle = [|\uparrow_1\downarrow_2\downarrow_3\dots\downarrow_N\rangle +$

$|\downarrow_1\uparrow_2\downarrow_3\dots\downarrow_N\rangle + \dots + |\downarrow_1\downarrow_2\downarrow_3\dots\uparrow_N\rangle]/N^{1/2}$ are the symmetric states of zero and one excitation, respectively. Recent work from Harvard has demonstrated classical coherence in this process⁸³, although quantum coherence involving small numbers of photons has not yet been observed.

A drawback in this mapping is the requirement of quantum number states of photons in the first place, which may ultimately require the cold atom and cavity-QED systems mentioned above. One way around this requirement is to exploit interactions between the atoms in the vapour to generate quantum states of excitation. If a classical laser pulse excites atoms to Rydberg states for instance, then a strong resonant dipole–dipole interaction can inhibit (shift spectroscopically) further excitations, leaving the state $|1_{\text{exc}}\rangle$, or exactly one excited Rydberg atom in the collection, a phenomenon called the ‘dipole blockade’⁸⁴.

An alternative quantum network might map the continuous degrees of freedom of a light field (for example, polarization or electric-field quadratures) onto a collection of atoms. In this way, atoms can be entangled in symmetric (‘spin-squeezed’) states with many excitations, an extension of states like $|1_{\text{exc}}\rangle$ above^{85,86}. A group at the University of Aarhus has recently entangled spatially separated collections of atoms through common interaction with a light field that traverses both collections (ref. 87; and see Fig. 8). In this case, a macroscopic number of atoms is made to behave as a single quantum degree of freedom, and such a system has promise for teleporting states between remotely located quantum memories⁸⁸. These experiments can be remarkably simple, requiring only trivial optical equipment and thermal samples of atoms in vapour cells.

Conclusions

Quantum information technology is likely to have an important role in information processing after the demise of Moore’s Law. The extent of this role is unknown, as quantum information processors currently have only a limited number of known applications, such as number factoring, database searches and enhanced communication

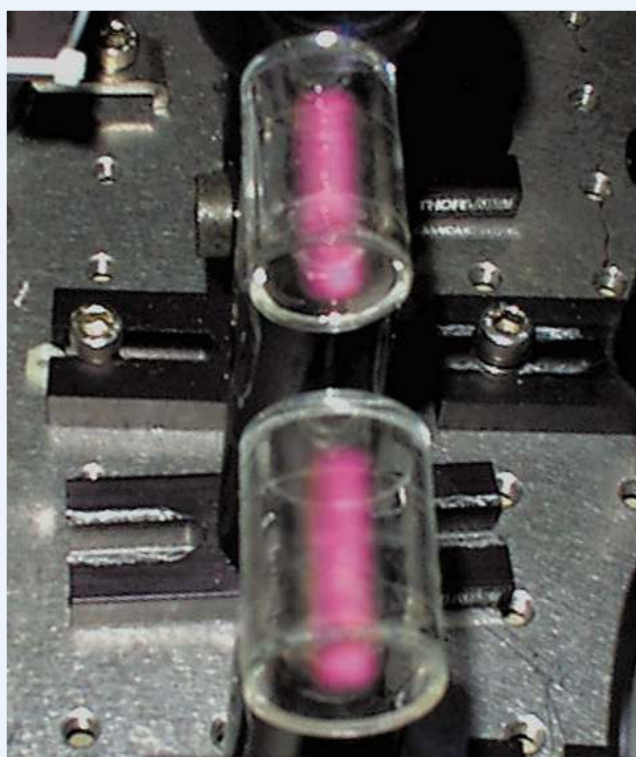


Figure 8 Pair of rubidium vapour cells used for storage and entanglement. A common laser beam traverses both cells, resulting in the purple fluorescence glow. Particular measurements of the polarization of the output light projects the atom collections in a ‘spin-squeezed’ state where the collective magnetization of the two macroscopic samples is weakly entangled. (Image courtesy of E. Polzik, University of Aarhus.)

protocols. Moreover, it may take decades to learn how to build large-scale quantum hardware, as this revolutionary form of information processing demands that revolutionary and exotic devices be engineered. Current devices come primarily from the areas of quantum optics and atomic physics, usually involving laser-cooled and trapped atoms. But perhaps the most exciting feature of this field is that the first large-scale quantum computer will probably be built from a physical system that is not currently known.

To quote Richard Feynman: “I think it is safe to say that nobody understands quantum mechanics.” Current experiments that control individual atoms and photons will continue to lead the bizarre features of quantum-mechanical foundations to the forefront. After all, the systems currently under study are exactly the thought experiments envisioned by Einstein, Bohr and the other founding fathers of quantum physics. With the new language of quantum information, we might hope to gain more insight in the underlying quantum-physical principles, exactly as Shannon’s theory of classical information ushered advances in physics responsible for the current digital age. □

- Shannon, C. E. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423; 623–656 (1948).
- Benioff, P. The computer as a physical system: a microscopic quantum mechanical model of computers as represented by Turing machines. *J. Stat. Phys.* **22**, 563–591 (1980).
- Benioff, P. Quantum mechanical Hamiltonian models of Turing machines that dissipate no energy. *Phys. Rev. Lett.* **48**, 1581–1585 (1982).
- Feynman, R. Simulating physics with computers. *J. Theor. Phys.* **21**, 467–488 (1982).
- Feynman, R. P. There’s plenty of room at the bottom. *Eng. Sci.* February 1960 issue (produced by the CalTech Office of Public Relations) (1960); also available at <<http://www.zyvx.com/nanotech/feynman.html>>.
- Landauer, R. in *Proc. Drexel-4 Symp. Quantum Nonintegrability* (eds Feng, D. H. & Hu, B.-L.) 44–53 (International Press, Boston, 1997).
- Jozsa, R. in *The Geometric Universe* (ed. Huggett, S. et al.) 369–379 (Oxford Univ. Press, Oxford, 1998); preprint quant-ph/9707034 (Entanglement and quantum computation) at <http://xxx.lanl.gov> (1997).
- DiVincenzo, D. The physical implementation of quantum computation. *Fortschr. Phys.* **48**, 771–783 (2000).

- Special issue on experimental proposals for quantum computation. *Fortschr. Phys.* **48** (2000).
- DiVincenzo, D. Two-bit gates are universal for quantum computation. *Phys. Rev. A* **51**, 1015–1022 (1995).
- Lloyd, S. Almost any quantum logic gate is universal. *Phys. Rev. Lett.* **75**, 346–349 (1995).
- Einstein, A. Podolsky, B. & Rosen, N. Can quantum-mechanical description of reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).
- Kahn, D. *The Codebreakers: The Story of Secret Writing* (Macmillan, New York, 1967).
- Bennett, C. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE Int. Conf. Comp. Syst. Signal Proc.* **11**, 175–179 (1984).
- Wiesner, S. Conjugate coding. *Sigact News* **15**, 78–88 (1983).
- Bennett, C. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124 (1992).
- Franson, J. & Ilves, H. Quantum cryptography using optical fibers. *Appl. Opt.* **33**, 2949–2954 (1994).
- Marand, C. & Townsend, P. Quantum key distribution over distances as long as 30 km. *Opt. Lett.* **20**, 1695–1697 (1995).
- Müller, A., Zbinden, H. & Gisin, N. Quantum cryptography over 23 km in installed under-lake telecom fiber. *Europhys. Lett.* **33**, 335–339 (1996).
- Hughes, R. J., Morgan, G. L. & Peterson, C. G. Quantum key distribution over a 48 km optical fibre network. *J. Mod. Opt.* **47**, 533–547 (2000).
- Ekert, A. K. Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
- Jennewein, T., Simon, C., Weihs, G., Weinfurter, H. & Zeilinger, A. Quantum cryptography with entangled photons. *Phys. Rev. Lett.* **84**, 4729–4732 (2000).
- Naik, D. S., Peterson, C. G., White, A. G., Berglund, A. J. & Kwiat, P. G. Entangled state quantum cryptography: eavesdropping on the Ekert protocol. *Phys. Rev. Lett.* **84**, 4733–4736 (2000).
- Tittel, W., Brendel, J., Zbinden, H. & Gisin, N. Quantum cryptography using entangled photons in energy-time Bell states. *Phys. Rev. Lett.* **84**, 4737–4740 (2000).
- Kwiat, P. G., Waks, E., White, A. G., Appelbaum, I. & Eberhard, P. H. Ultrabright source of polarization-entangled photons. *Phys. Rev. A* **60**, 773–776 (1999).
- Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
- Braunstein, S. L. A fun talk on teleportation. <www.informatics.bangor.ac.uk/~schmue/tpopt.html> (5 February 1995).
- Bouwmeester, D. et al. Experimental quantum teleportation. *Nature* **390**, 575–579 (1997).
- Boschi, D., Branca, S., De Martini, F., Hardy, L. & Popescu, S. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **80**, 1121–1125 (1998).
- Braunstein, S. L. & Kimble, H. J. A posteriori teleportation. *Nature* **394**, 840–841 (1998).
- Bouwmeester, D. et al. Reply to ‘A posteriori teleportation’ by S. L. Braunstein and H. J. Kimble. *Nature* **394**, 841 (1998).
- Furusawa, A. et al. Unconditional quantum teleportation. *Science* **282**, 706–709 (1998).
- Schrödinger, E. The present situation in quantum mechanics. *Naturwissenschaften* **23**, 807–812; 823–828; 844–849 (1935).
- Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A* **400**, 97–117 (1985).
- Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.* **26**, 1484–1509 (1997).
- Rivest, R., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. Assoc. Comput. Mach.* **21**, 120–126 (1978).
- Grover, L. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325–328 (1997).
- Shor, P. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, 2493–2496 (1995).
- Stane, A. Error correcting codes in quantum theory. *Phys. Rev. Lett.* **77**, 793–797 (1996).
- Preskill, J. Battling decoherence: the fault-tolerant quantum computer. *Phys. Today* **52**, 24–30 (1999).
- Cirac, I. & Zoller, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.* **74**, 4091–4094 (1995).
- Stane, A. The ion trap quantum information processor. *Appl. Phys. B* **64**, 623–642 (1997).
- Wineland, D. et al. Experimental issues in coherent quantum manipulation of trapped atomic ions. *J. Res. Natl. Inst. Stand. Tech.* **103**, 259–328 (1998).
- Sørensen, A. & Mølmer, K. Quantum computation with ions in thermal motion. *Phys. Rev. Lett.* **82**, 1971–1975 (1999).
- Blatt, R. & Zoller, P. Quantum jumps in atomic systems. *Eur. J. Phys.* **9**, 250 (1988).
- Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M. & Wineland, D. J. Demonstration of a universal quantum logic gate. *Phys. Rev. Lett.* **75**, 4714–4717 (1995).
- Sackett, C. et al. Experimental entanglement of four particles. *Nature* **404**, 256–259 (2000).
- Turchette, Q. A. et al. Heating of trapped ions from the quantum ground state. *Phys. Rev. A* **61**, 063418-1–063418-8 (2000).
- Larson, D. J. et al. Sympathetic cooling of trapped ions: a laser-cooled two-species nonneutral ion plasma. *Phys. Rev. Lett.* **57**, 70 (1986).
- Kielpinski, D. et al. Sympathetic cooling of trapped ions for quantum logic. *Phys. Rev. A* **61**, 032310-1–032310-8 (2000).
- Morigi, G. & Walther, H. Two-species Coulomb chains for quantum information. *Eur. Phys. J. D* **13**, 261–269 (2001).
- Jessen, P. & Deutsch, I. Optical lattices. *Adv. At. Mol. Opt. Phys.* **37**, 95–138 (1996).
- Hamann, S. et al. Resolved-sideband Raman cooling to the ground state of an optical lattice. *Phys. Rev. Lett.* **80**, 4149–4152 (1998).
- Vuletic, V., Chin, C., Kerman, A. J. & Chu, S. Raman sideband cooling of trapped cesium atoms at very high densities. *Phys. Rev. Lett.* **81**, 5768–5771 (1998).
- Perrin, H., Kuhn, A., Bouchoule, I. & Salomon, C. Sideband cooling of neutral atoms in a far-detuned optical lattice. *Europhys. Lett.* **42**, 395–400 (1998).
- Raihel, G., Phillips, W. D. & Rolston, S. L. Coherence decay of wave-packets in optical lattices. *Phys. Rev. Lett.* **81**, 3615 (1998).
- Haycock, D. L., Alsing, P. M., Grondalski, J., Deutsch, I. H. & Jessen, P. S. Mesoscopic quantum coherence in an optical lattice. *Phys. Rev. Lett.* **85**, 3365 (2000).
- Brennen, G., Caves, C., Jessen, P. & Deutsch, I. Quantum logic gates in optical lattices. *Phys. Rev. Lett.* **82**, 1060–1063 (1999).

59. Jaksch, D., Briegel, H. J., Cirac, J. I., Gardiner, C. W. & Zoller, P. Entanglement of atoms via cold controlled collisions. *Phys. Rev. Lett.* **82**, 1975–1978 (1999).
60. Jaksch, D. *et al.* Fast quantum gates for neutral atoms. *Phys. Rev. Lett.* **85**, 2208–2211 (2000).
61. DeMille, D. Quantum computation with trapped polar molecules. Preprint quant-ph/0109083 at <http://xxx.lanl.gov> (2001).
62. Jaksch, D., Bruder, C., Cirac, J. I., Gardiner, C. W. & Zoller, P. Cold bosonic atoms in optical lattices. *Phys. Rev. Lett.* **81**, 3108–3111 (1998).
63. Spekkens, R. W. & Sipe, J. E. Spatial fragmentation of a Bose-Einstein condensate in a double-well potential. *Phys. Rev. A* **59**, 3868–3877 (1999).
64. Orzel, C., Tuchman, A. K., Fenselau, M. L., Yasuda, M. & Kasevich, M. A. Squeezed states in a Bose-Einstein condensate. *Science* **291**, 2386–2389 (2001).
65. Greiner, M., Mandel, O., Esslinger, T., Hansch, T. W. & Bloch, I. Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms. *Nature* **415**, 39–44 (2002).
66. Cirac, I. & Zoller, P. A scalable quantum computer with ions in an array of microtraps. *Nature* **404**, 579–581 (2000).
67. Monroe, C., Meekhof, D. M., King, B. E. & Wineland, D. J. A Schrödinger cat superposition state of an atom. *Science* **272**, 1131–1136 (1996).
68. Bennett, C. H. *et al.* Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722–725 (1996).
69. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
70. Cirac, I., Zoller, P., Kimble, H. & Mabuchi, H. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.* **78**, 3221–3224 (1997).
71. Law, C. & Kimble, H. Deterministic generation of a bit-stream of single-photon pulses. *J. Mod. Opt.* **44**, 2067–2074 (1997).
72. van Enk, S., Cirac, I. & Zoller, P. Ideal quantum communication over noisy channels, a quantum optical implementation. *Phys. Rev. Lett.* **78**, 4293–4296 (1997).
73. Ye, J., Vernooij, D. W. & Kimble, H. J. Trapping of single atoms in cavity QED. *Phys. Rev. Lett.* **83**, 4987–4990 (1999).
74. Hood, C. J., Lynn, T. W., Doherty, A. C., Parkins, A. S. & Kimble, H. J. The atom-cavity microscope: single atoms bound in orbit by single photons. *Science* **287**, 1447–1453 (2000).
75. Pinske, P., Fischer, T., Maunz, P. & Rempe, G. Trapping an atom with single photons. *Nature* **404**, 365–368 (2000).
76. Doherty, A., Lynn, T. W., Hood, C. J. & Kimble, H. J. Trapping of single atoms with single photons in cavity QED. *Phys. Rev. A* **63**, 013401–1–013401–24 (2001).
77. Guthöhrlein, G. R., Keller, M., Hayasaka, K., Lange, W. & Walther, H. A single ion as a nanoscopic probe of an optical field. *Nature* **414**, 49–51 (2001).
78. Liu, C., Dutton, Z., Behroozi, C. H. & Hau, L. V. Observation of coherent optical information storage in an atomic medium using halted light pulses. *Nature* **409**, 490–493 (2001).
79. Phillips, D. F., Fleischhauer, A., Mair, A., Walsworth, R. L. & Lukin, M. D. Storage of light in atomic vapor. *Phys. Rev. Lett.* **86**, 783–786 (2001).
80. Budker, D., Kimball, D. F., Rochester, S. M. & Yashchuk, V. V. Nonlinear magneto-optics and reduced group velocity of light in atomic vapor with slow ground state relaxation. *Phys. Rev. Lett.* **83**, 1767–1770 (1999).
81. Lukin, M. & Imamoglu, A. Controlling photons using electromagnetically induced transparency. *Nature* **413**, 273–276 (2001).
82. Fleischhauer, M. & Lukin, M. Dark-state polaritons in electromagnetically induced transparency. *Phys. Rev. Lett.* **84**, 5094–5097 (2000).
83. Mair, A., Hager, J., Phillips, D. F., Walsworth, R. L. & Lukin, M. D. Phase coherence and control of stored photonic information. Preprint quant-ph/0108046 at <http://xxx.lanl.gov> (2001).
84. Lukin, M. *et al.* Dipole blockade and quantum information processing in mesoscopic atomic ensembles. *Phys. Rev. Lett.* **87**, 037901–1–037901–4 (2001).
85. Hald, J., Sørensen, J. L., Schori, C. & Polzik, E. S. Spin squeezed atoms: a macroscopic entangled ensemble created by light. *Phys. Rev. Lett.* **83**, 1319–1322 (1999).
86. Kuzmich, A., Mandel, L. & Bigelow, N. Generation of spin squeezing via continuous quantum nondemolition measurement. *Phys. Rev. Lett.* **85**, 1594–1597 (2000).
87. Julsgaard, B., Kozhokin, A. & Polzik, E. Experimental long-lived entanglement of two macroscopic objects. *Nature* **413**, 400–403 (2001).
88. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001).
89. Wolf, F. A. *Taking the Quantum Leap* (Harper and Row, San Francisco, 1981).
90. Zurek, W. H. Decoherence and the transition from quantum to classical. *Phys. Today* **44**, 34–44 (1991).
91. Braunstein, S. L., D’Ariano, G. M., Milburn, G. J. & Sacchi, M. F. Universal teleportation with a twist. *Phys. Rev. Lett.* **84**, 3486–3489 (2000).

Acknowledgements

This work is supported by the US National Security Agency and Advanced Research and Development Activity under an Army Research Office contract, and by the National Science Foundation ITR programme.