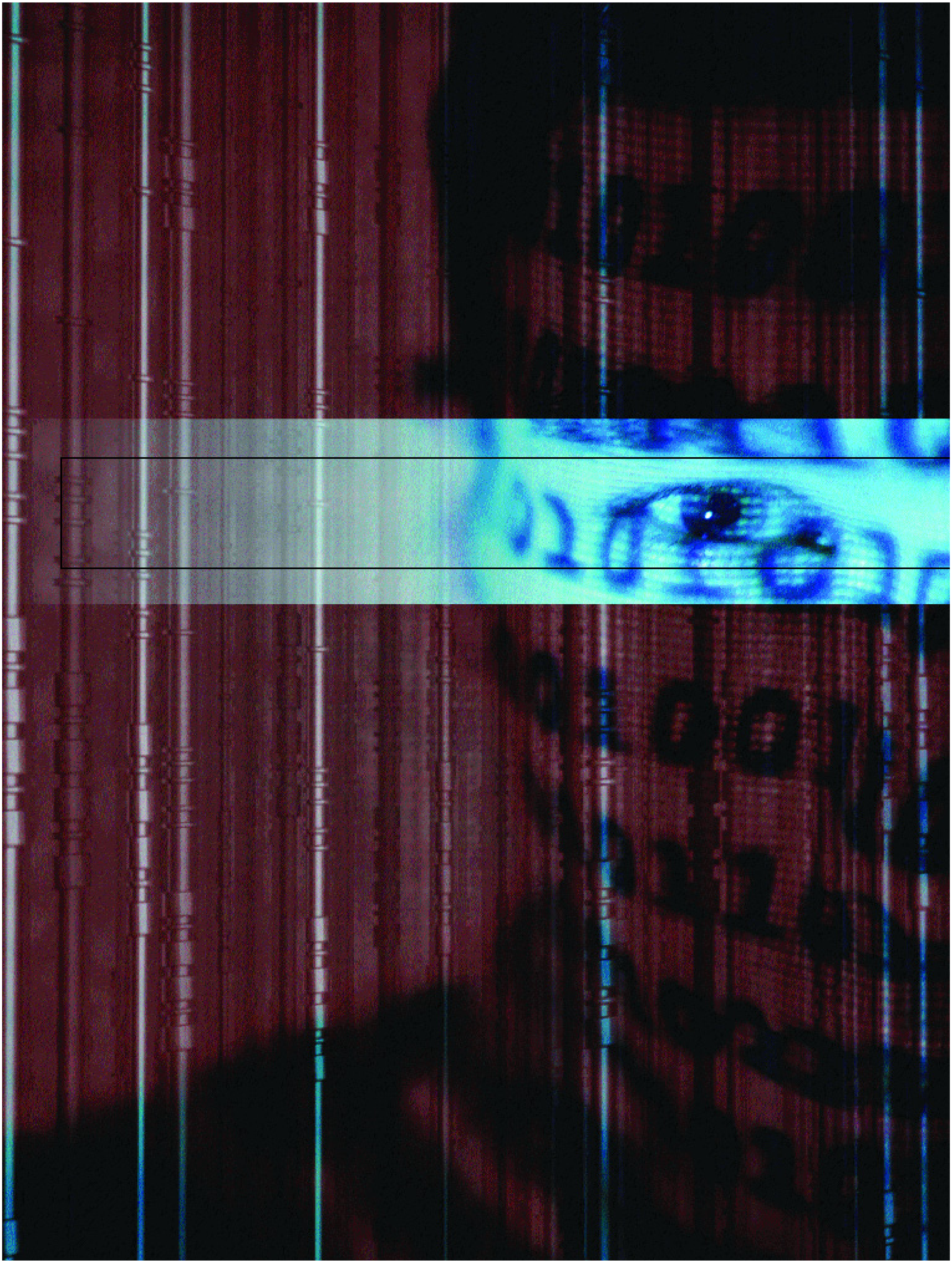
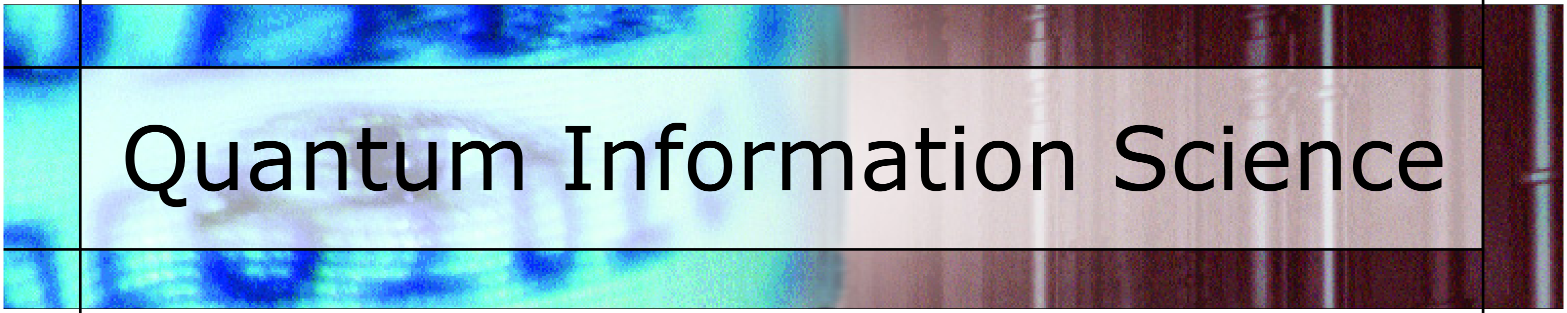


Quantum technology has made great strides in recent years. While quantum computers offer many benefits, we are far from seeing them implemented on a mass scale. Here we review the basic building blocks of quantum information processing, identify the advantages of quantum physics over classical physics, explain how quantum communication protocols work and identify the challenges we need to overcome to realize a quantum computer.

Ian Walmsley and Peter Knight



Quantum Information Science

IBM's Rolf Landauer has said that all information is physical. This phrase encapsulates a line of thinking that has led to some remarkable changes in recent years in the way we view communications, computing and cryptography. Through the use of quantum physics, several objectives once thought impossible have now been achieved. Quantum communications links are impossible to eavesdrop, for example. Already, the early versions of quantum computers can turn algorithms, euphemistically described as "difficult" for a Pentium computer to perform, into "easy" calculations.

The details of what constitutes "difficult" and "easy" are the subjects of mathematical complexity theory, but the following example serves to illustrate the potential impact on our lives of quantum information processing. The security of many forms of encryption is predicated on the difficulty of factoring large numbers. On a computer designed according to the laws of classical physics, finding the factors of a 1024-digit number would take a period of time longer than the lifetime of our universe. A quantum computer could find the answer in the blink of an eye. On the condition, of course, that we can build a quantum computer… that is the challenge! Yet it's well worth the chase, because as we shall see, a quantum computer with a modest-size register could outperform any classical machine.

Quantum information processing offers a qualitatively different way in which to think about manipulating information. Moore's law states that the number of transistors per chip increases exponentially with time, as shown in Fig. 1. The implication is that there will be about one electron per transistor by the year 2016. This lone electron will be confined to a region so small that it will act as a quantum mechanical particle, not as a charged billiard ball, as in classical physics. For this reason we are fortunate that quantum physics has become more important in the design of classical computers and has also offered up an entirely new field, quantum computing.

1047-6938/02/11/0042/8-$0015.00 © Optical Society of America

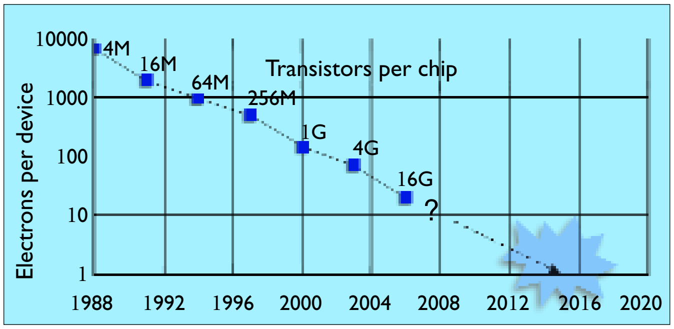


Figure 1. Quantum consequences of Moore's law: by 2015, a transistor in a computer will have only a single electron confined to such a small volume that it will behave quantum mechanically.

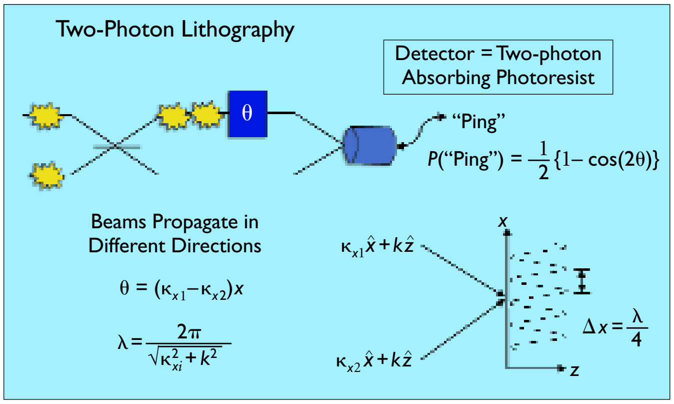
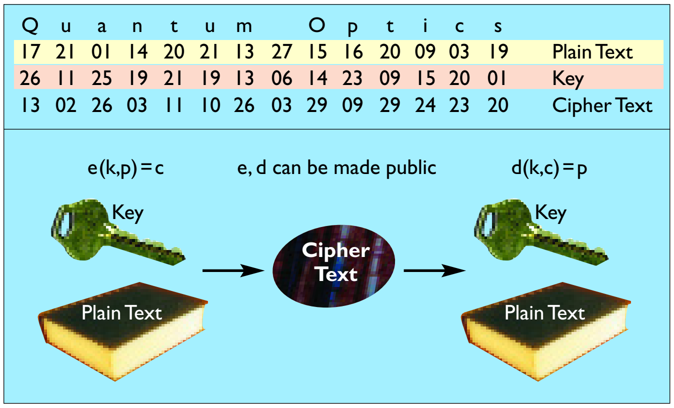

Two-Photon Lithography
Detector = Two-photon Absorbing Photoresist
θ
"Ping"
P("Ping") = ½{1− cos(2θ)}
Beams Propagate in Different Directions
θ = (κ_x1−κ_x2)x
λ = 2π/√(κ_xi² + k²)
κ_x1 x̂ + k ẑ
κ_x2 x̂ + k ẑ
x
z
Δx = λ/4

Figure 2. Entanglement provides a resource that allows higher resolution in an optical system at a given wavelength. Quantum lithography exploits this resource to generate finer patterns on a two-photon absorbing photoresist than can be obtained from illuminating the same material with classical light.



Q	u	a	n	t	u	m		O	p	t	i	c	s	
17	21	01	14	20	21	13	27	15	16	20	09	03	19	Plain Text
26	11	25	19	21	19	13	06	14	23	09	15	20	01	Key
13	02	26	03	11	10	26	03	29	09	29	24	23	20	Cipher Text

Figure 3. Completely secure communication between two parties (the proverbial Alice and Bob) is possible using single photons or entangled photon pairs. An eavesdropper can neither replicate nor measure the transmitted photon without modifying the information encoded in it in a way that is detectable by the sender and receiver.

The entanglement advantage

What features of quantum physics make it different from classical physics for the purposes of information processing? The essential characteristic is entanglement. This is the name given to the correlation between different quantum systems, a correlation that is stronger than any that is possible in classical physics. To understand entanglement, one needs to understand another important feature of quantum mechanics: interference.

In quantum mechanics, a system's state is specified by its wave function $\psi(x)=\langle x|\psi\rangle$. The square of this entity represents the probability density function that you would find the system located at x if you measured its position. Quantum interference arises when the state of the system is described by a superposition of two wave functions $\psi(x)+\theta(x)$. The probability density for finding the system at position x is then not simply the sum of the probability distributions $|\psi(x)|^2$ and $|\theta(x)|^2$, as it would be for a system obeying the laws of classical physics, but is modulated by an interference term that may exclude the system completely from being at particular locations. The notion that something heavy, like a neutron, could, when passed through a pair of slits, fail to appear at certain places where it would be allowed if one of the slits were closed contains, in Feynman's words, "the only mystery" of quantum physics.[1]

Quantum systems, like classical systems, may be correlated. A correlation between two systems is simply the statement that if a measurement of one system yields the result A, then a measurement of the second system will yield with some probability the result B. Perfect correlation occurs when the second result is certain. So the state $\psi(x_1,x_2)=\delta(X-x_1-x_2)$ of two particles, *1* and *2*, is perfectly position-correlated, because if a measurement of the position of the first system gives the result $x_1=Y$, then one may infer with certainty that the position of the second system is $x_2=X-Y$. If the wave function can be written as the product of two wave functions of the subsystems, then the system is said to be in an uncorrelated state. The state $\psi(x_1,x_2)=\delta(X-x_1)\delta(Y-x_2)$ is uncorrelated since the result of the measurement of the position of either system is independent of the result of the measurement of the other system.

Let's say that there is a second state of the pair of systems $\theta(x_1,x_2)$. Then the superposition state $\psi(x_1,x_2)+\theta(x_1,x_2)$ is entangled if it gives correlated results of measurements of the positions of the two systems. Interestingly, to give some degree of correlation to the system as a whole, it is not necessary that either of the states $\psi(x_1,x_2)$ or $\theta(x_1,x_2)$ be correlated themselves.

More generally, entanglement is the superposition of states of two or more quantum systems that yield correlated outcomes of measurements. The strong correlations possessed by entangled state are important in several quantum technologies.

Quantum-enhanced precision measurement

How can this potential be harnessed? The key is to be able to count the number of particles in the system. We can illustrate this point by considering the problem of quantum-enhanced phase measurement. Let's say one wishes to determine the phase shift induced on a beam by a specific optical element. One way to do this is to put the element into one arm of an interferometer and illuminate the interferometer input. A measurement of the difference photocurrent of two detectors looking at the output ports of the interferometer will exhibit a sinusoidal fringe pattern as the

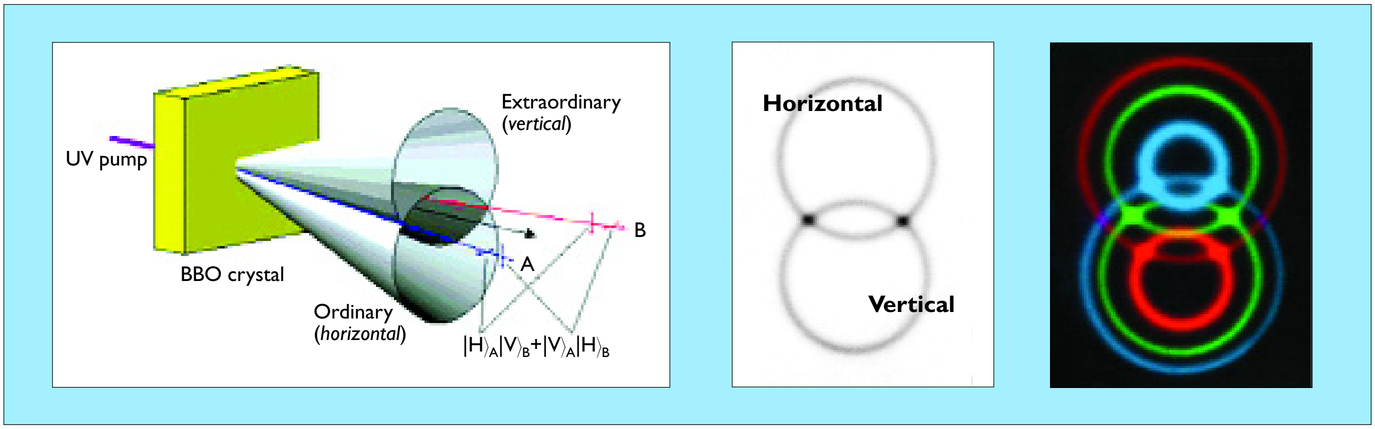


Figure 4. (a) Polarization-entangled photon pairs can be generated by parametric downconversion. In this process, a strong pump beam on a nonlinear medium spontaneously generates pairs of photons (the signal and the idler) at roughly half the frequency of the pump wave. These photon pairs are emitted into "cones" in the forward direction. (b) In Type-II phase matching, the cones intersect at two points. In these directions, photons have indeterminate polarization, although the polarization of each photon is highly correlated with its sibling: they are polarization-entangled pairs. (Institut für Experimentalphysik, Universität Wien.)

phase is changed. A particular phase can be measured by comparing the difference photocurrent to the known maximum and minimum photocurrents. The accuracy of this phase measurement will be determined by the photocurrent fluctuations. If the input light is classical, the fluctuations will be at the shot-noise limit. That is, if the input radiation has a mean photon number N, the accuracy of the phase measurement will be $\Delta\theta/\theta=1/\sqrt{N}$.

The accuracy can be improved if nonclassical light is used to illuminate the interferometer. Consider the case in which exactly one photon is put into each of the input ports a and b of the interferometer. The state of the system at the input can be denoted $|1\rangle_a|1\rangle_b$. When these photons are incident on the beam splitter, they can be scattered into either output port. But because they are bosons, they prefer to stick together, and they both exit from the same output, either up or down, with equal probability. After the beam splitter, the system is therefore in an entangled state, $1/\sqrt{2}(|0\rangle_a|2\rangle_b+|2\rangle_a|0\rangle_b)$. If the phase shifter is in the a-arm of the interferometer, then just before the second beam splitter, the state is $1/\sqrt{2}(|0\rangle_a|2\rangle_b+e^{i2\theta}|2\rangle_a|0\rangle_b)$, and after the beam splitter it is $(1/\sqrt{2}(1+e^{i2\theta})1\rangle_a|1\rangle_b-i/2\sqrt{2}(1-e^{i2\theta})0\rangle_a|2\rangle_b+i/2\sqrt{2}(1-e^{i2\theta})2\rangle_a|0\rangle_b)$.

The rate of coincidence photon counts from the detectors is proportional to the square of the probability amplitude that there is simultaneously a photon in output port a and one in port b. The coefficient of this state in the output gives for the count rate $R_c(\theta)=1/2(1+\cos2\theta)$. At this point it is easy to show that the phase accuracy is $\Delta\theta/\theta=1/2$, an improvement of $\sqrt{2}$ over what could be obtained classically using the same average input power. This concept can be extended to input states containing $N/2$ photons per port, with a resulting increase in accuracy to $\Delta\theta/\theta=1/N$. This is called the Heisenberg limit of measurement, and is the tightest known quantum limit on interferometry accuracy.[2] Attaining this limit, however, requires detectors that can discriminate between N and $N+1$ photons, or N-fold coincidence detection. Both are technically difficult, and the Heisenberg limit has only been reached in experiments with small numbers of photons.[3]

Because frequency measurement is akin to phase measurement, the same idea can be applied to enhance the accuracy of atomic clocks.[4] It has proven possible to make a clock based on entangled trapped ions, where up to five particles can be measured together. This promises to make clocks with small numbers of atoms or ions more accurate.

Accuracy enhancement by use of entanglement was described in a recent paper on quantum lithography,[5] in which a pattern can be written with the precision of a fraction of a wavelength: if there are N photons of wavelength λ input to the apparatus, then one can write features with size λ/N. The setup for such a scheme is shown in Fig. 2. Again, only two photons are put into the interferometer. After the beam splitter, the two beams are directed at an angle onto a nonlinear photoresist that can absorb two photons with high probability but single photons with low probability. The spatial distribution of the absorption in this photoresist, which will yield a pattern when etched, is $P(x)=1/2(1+\cos4\pi x/\lambda)$. In a classical system, the best that can be achieved with such a photoresist is $P(x)=1/4(1+2\cos2\pi x/\lambda+\cos4\pi x/\lambda)$. The modulation depth of the resist is greater than that of classical lithography, and the feature size is thus twice as fine as that which can be achieved in a classical system. Of course, one might always use a linear photoresist, simply halve the wavelength of the illumination, and do just as well. But it is clear that this approach will not scale to higher order, because there are technical difficulties in handling very short wavelengths in precision imaging optics. Whether further improvements in resolution can be made with enhanced photoresists remains to be seen, but this area of research points the way to a potentially important technology.

Quantum cryptography

The strong correlations inherent in an entangled state can also be used in cryptography, the business of sending messages from one place to another in secret, coded so that they cannot be read by anyone who might be listening in on the communication. A very secure way of doing this is to use a form of encryption called a "one-time pad," shown in Fig. 3. In this scheme, both sender and receiver have the same random string of bits, consisting of "0"s and "1"s. This random string of bits is called the key.

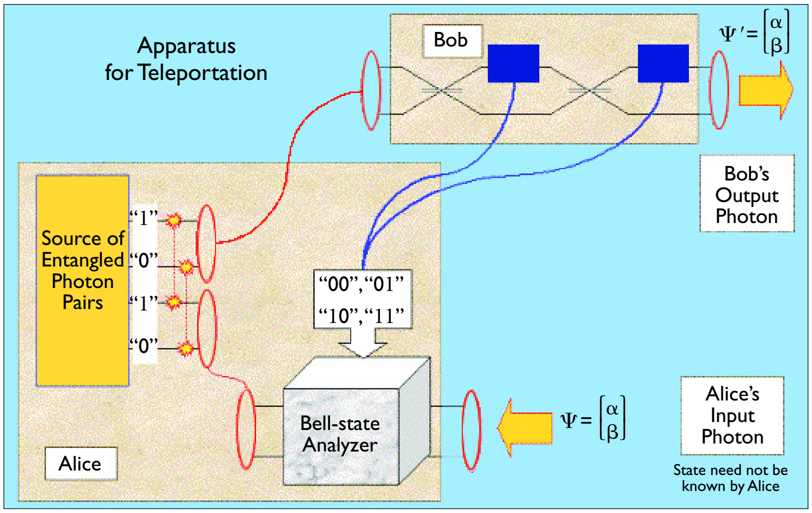

Apparatus
for Teleportation
Bob
$\Psi' = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$
Bob's Output Photon
Source of Entangled Photon Pairs
"1"
"0"
"1"
"0"
"00","01"
"10","11"
Bell-state Analyzer
$\Psi = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$
Alice's Input Photon
State need not be known by Alice
Alice

Figure 5. An application of entangled photons in quantum communications. Alice distributes one half of an entangled pair of photons to Bob and keeps one herself. She can use this to "teleport" the unknown state *f* of her own photon to Bob. To do this, Alice first combines her entangled photon with the unknown one and makes a measurement of the pair. The result of this measurement is one of four outcomes, represented by two bits of data. She communicates the result of the measurement to Bob via a classical channel (blue lines). Bob can then appropriately manipulate his photon to prepare it in the same state as the input photon *f*. This set of acts completely erases any information in the input photon, so the no-cloning theorem is not violated. The number of bits of information Alice must communicate to Bob over the classical channels is dramatically fewer than what would be needed for a complete specification of the state of her original particle.

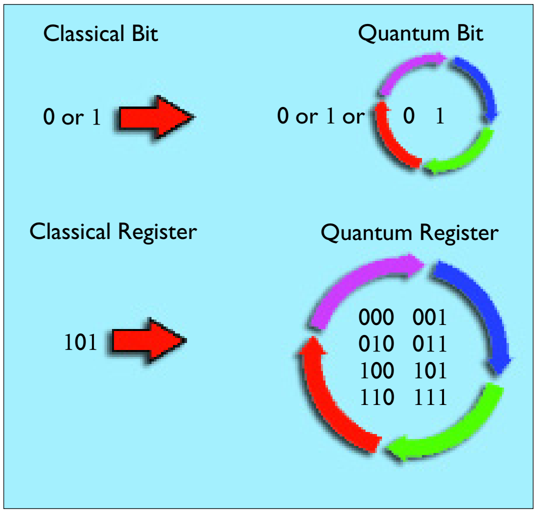


Figure 6. Comparison of processor registers of classical bits and qubits. The former can represent one of 2^N numbers. The latter can represent arbitrary superpositions of all 2^N at once. The manipulation of this superposition accounts for all the dramatically increased computational power of the quantum information processor.

When the sender (the eponymous Alice) wishes to communicate with the receiver (Bob) she encodes her message as a binary string, and adds the key modulo 2. This yields a bit string—the cipher text—which she then sends over a public channel to Bob. He adds his key to the cipher text modulo 2 and recovers the plain text of Alice's message. The eavesdropper (Eve) cannot recover the message unless she possesses the same key as Alice and Bob. Of course, the key can only be used once, otherwise Eve could intercept two messages and determine the key. So the problem is how to get Bob the key without Eve also getting it. Although entangled pairs of photons can help in establishing a secure communications link,[6] it is useful to consider the earliest protocol that uses single photons. This protocol illustrates two other critical features of quantum mechanics: the properties of detectors and the impossibility of making exact copies of quantum systems.

The "no-cloning" property

In the communications scheme proposed by Bennett and Brassard,[7] the so-called BB84 protocol, quantum mechanics helps in two ways. First, there is a minimum level of noise in any photodetector. An avalanche photodiode, for example, can "see" one photon or more. But it gives no signal without at least one photon being present (notwithstanding inevitable technical noise which, in this case, gives a small dark background count). Thus, if the key is sent from Alice to Bob, encoded in individual photons one bit at a time, and if Eve removes one of these photons to examine it, Bob will not receive it. It will not form part of the key. Of course, Eve is very clever. She picks off a photon, duplicates it, retains one copy and sends the other to Bob. Now both of them have the key. Here the second feature of quantum physics comes into play—the so-called "no cloning" property.[8] This means that you cannot make an exact copy of a single quantum system unless you know its state beforehand. Thus, Eve would need to know how the information was coded into the photon *before* she tried to duplicate it, in which case she would have no need to do so. Quantum mechanics catches her in the paradox that in order to learn the secret key she must already know it.

There are several ways to generate secret keys in this way, and all of them use the idea that there is no information encoded in a quantum system unless it is read out. In the BB84 cryptography protocol, Alice establishes the key by choosing at random whether to code "0"s and "1"s into her photon by giving it 0° or 45° linear polarization (logical "0") or 90° or –45° linear polarization (logical "1"). Bob then measures the photon received from Alice by randomly selecting the orientation of his polarizing beam splitter at 0° or 45° and then recording out of which port the photon comes. Bob and Alice then can establish the key by communicating in public about their choice of polarizer angles, keeping secret the actual results of the measurement. When they both choose the same angles, they can establish in perfect secrecy bits of the key known only to them. They can, moreover, check that Eve has not tapped the line by checking certain sections of the key with each other. If they find that their checked sections are not correlated, they know that Eve has manipulated the photons and they can discard the link.

This is one of the most advanced areas of quantum information science.[9] Functioning cryptographic links have already been established in several locations around the world: a free space version in Los Alamos,[10] a fiber version under Lake Geneva,[11] commercial telecommunications fiber in the U.K.,[12] as well as in many laboratories. A detailed review of this area, including a discussion of the experimental aspects, has recently been published in this magazine.[13]

Quantum communications

Another branch of quantum communications involves the knotty problem of sending someone (Bob again) a quantum system in an unknown state. Since the sender (Alice) has only a single copy of the system, she cannot determine its state and then send a design specification to Bob using the usual channels (the BBC interplanetary service, FedEx, etc.) For this reason, she uses entanglement. Alice and Bob arrange to share an entangled pair of ancillary systems, perhaps photons, as in Fig. 4. Alice first compares her unknown system with her component of the ancilla. If her system can be in any superposition of two states, and her ancilla has the same property, her comparison will yield at most one of 2 x 2 = 4 outcomes. In doing this she naturally alters her system so much that no record of its original state remains.

She tells Bob, via a broadcast channel for example, the result of her comparison. Bob is then able to manipulate his component of the ancilla in a specific way, without even looking at it. This turns his system into a replica of Alice's original unknown system. Since Alice has no way to get any information about her original system except from Bob, this procedure does not violate the no-cloning theorem. This protocol, invoking an image of the transporter technology in Star Trek, is called quantum teleportation.[14] It is illustrated schematically for photons in Fig. 5. A number of groups around the world have reported experimental demonstrations of teleportation.[15]

Why does Alice not just send her quantum system to Bob? Assuming she could use the special Speed O'Light FedEx service, Bob would end up with the input photon as before without having to dabble in quantum magic. In a sense, it's only a question of money. By sharing the entangled systems prior to when they are needed, Alice does not have to worry about whether there is a traffic jam on the highway and FedEx cannot get through.

It is exactly this reasoning that makes quantum dense coding a possible way to send more information more cheaply.[16] In this protocol, Alice again sends Bob one of her entangled systems, and again keeps the other half. When Bob is ready to send a message to Alice, he manipulates his system and sends it back to her. Alice now compares the two parts of the entangled system and gets one of four results from her comparison. This yields the two bits of information that have effectively been communicated by Bob to Alice, even though he sent her only one particle. Of course, he had to have received the particle from Alice over the same channel beforehand, so although it may be one particle, it requires two uses of the channel. But one of these can be done at a time when the cost of that channel is small, so Bob's total cost of sending two bits of information is lower than if he had to send them both at the peak rate of the communications link.[17]

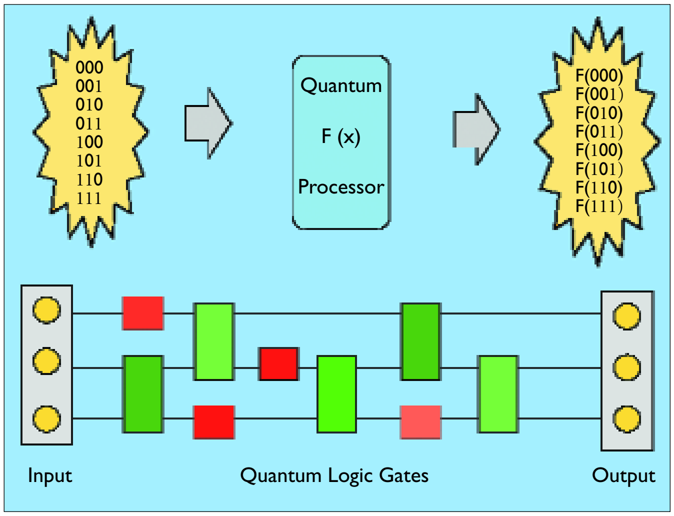


Figure 7. A quantum computer is a network of controlled interactions (the logic gates) between two qubits (green boxes), such as the Q-CNOT gate, and manipulations of individual qubits (red boxes). The sequential action of a number of two-qubit interactions generates entangled states in the register.

Control In	Target In	Control Out	Target Out
$\vert“0”\rangle$	$\vert“0”\rangle$	$\vert“0”\rangle$	$\vert“0”\rangle$
$\vert“0”\rangle$	$\vert“1”\rangle$	$\vert“0”\rangle$	$\vert“1”\rangle$
$\vert“1”\rangle$	$\vert“0”\rangle$	$\vert“1”\rangle$	$\vert“1”\rangle$
$\vert“1”\rangle$	$\vert“1”\rangle$	$\vert“1”\rangle$	$\vert“0”\rangle$

Table 1. Logical state truth table for the quantum CNOT gate.

Quantum computation

A major goal of quantum technology research is the realization of a quantum computer, a general-purpose information-processing machine with the ability to run quantum algorithms. Quantum algorithms are recipes for performing tasks that make use of quantum hardware in such a way that there are advantages of scale or speed over what can be achieved by known algorithms using classical computing machinery. The best known of these algorithms are for searching a database[18] and for finding the prime factors of a large number.[19] These problems are considered hard ones for classical computers to solve because the time taken to obtain the answer scales exponentially with the "size" of the input information (say, the number of records in the database or the number of digits in the prime number being factored). Running quantum algorithms on quantum computers would make it possible to get to the answer in a time that scaled only polynomially with the input size.

The algorithms work by harnessing the entanglement between the quantum systems in the register. The standard model of a quantum computer consists of the register, which is acted on by the processor, and read out to reveal the result of the computation.[20] In a regular classical computer, the register consists of logical bits that can be strung together to represent a binary number. What sort of data is stored in a register of N bits in a classical computer? At a minimum, each logical bit of the register is encoded in one physical particle. If the particle can be in one of two states, (say, spin up or spin down) and represent a logical "0" or "1," then the register of a classical computer contains a single N-bit string that represents in binary one of 2^N numbers.

In a quantum computer, the register consists of a set of "qubits"—quantum bits—whose logical states are represented by particular physical states of the system. Because these are quantum rather than classical states, we'll denote them as $|\text{“0”}\rangle$ and $|\text{“1”}\rangle$. Now, each of these qubits can be in a superposition state $1/\sqrt{2}(|\text{“0”}\rangle+|\text{“1”}\rangle)$, and therefore the register of our quantum computer can be in a superposition state of all 2^N binary numbers that can be encoded in N qubits *at once*, as shown in Fig. 6. Of course, a measurement of the register will collapse it into only one of these states, but the power of a quantum processor arises because all of the 2^N numbers can be manipulated together, rather than individually, as would happen in a classical machine. It is this parallelism of manipulation that gives quantum computing its awesome potential. Because the action of the processor will inevitably generate superpositions of correlated states between different bits of the register, information processing in a quantum computer necessarily involves entanglement—on the condition of course that you want it to do more than is possible with a classical computer.

How does the processor engender entanglement? The network model of a quantum computer uses a sequence of quantum "gates" to couple two particles together. This notion is illustrated schematically in Fig. 7. From this two-qubit gate operation, and a small set of one-particle operations that are used to generate superpositions of the state of each particle individually, one can build up a "universal" computer, one that can be programmed to execute any quantum algorithm.

The basic element of quantum logic is the quantum CNOT gate.[21] The truth table for this gate is the same as that of a classical CNOT gate for reversible computation, and is shown in Table 1. The two input bits, labeled the control and target bits, interact in such a way that the state of the target bit is changed from logical "0" to logical "1," or *vice versa*, if the state of the control bit is logical "1." It turns out that this gate can generate entanglement between the target and control qubits. When the input state of the control and target is the uncorrelated state $1/\sqrt{2}(|\text{“0”}\rangle+|\text{“1”}\rangle)_c|\text{“0”}\rangle_t$, then the output state is the entangled state $1/\sqrt{2}(|\text{“0”}\rangle_c|\text{“1”}\rangle_t+|\text{“1”}\rangle_c|\text{“1”}\rangle_t)$. Imagine this gate applied many times to pairs of qubits in the register as the algorithm is executed, and it is clear that the register is very likely to be in a highly entangled state at some point in the calculation.

The sort of interactions that can be used to make a quantum CNOT gate are many and varied (see partial list, sidebar on facing page). But all share the feature that the interaction of one qubit with another depends on the state of the qubits. For example, if an atom in an optical lattice trap is brought close to a second atom in an adjacent well of the lattice, then the energy levels of the valence electrons in each of the atoms are shifted because of the fluctuations of the dipole moment of the other atom. The shifts are greater for higher levels. Thus, an electron in an excited state picks up phase more slowly than one in the ground state. This conditional phase shift (i.e., the amount of phase which depends on the state of the control electron) forms the basis of the conditional state change performed by a quantum CNOT gate.

The atoms must be controlled very carefully, however. It turns out that the fidelity of gate operation must be about one part in a thousand or better before a quantum computer is realistic. This is but one of the hurdles to harnessing quantum weirdness.[22]

Quantum delicacy

Quantum interference is fragile. It is very difficult to maintain superposition states of many particles in which each particle is physically separated from all the others. Entanglement also is delicate. The reason for this is that all systems, quantum or classical, are not isolated. They interact with everything around them: local fluctuating electromagnetic fields, the presence of impurity ions, coupling to unobserved degrees of freedom of the system containing the qubit and so forth. These fluctuations destroy quantum interference. A simple analogy is the interference of optical waves in Young's double-slit experiment. In that apparatus, waves from two spatially separated portions of a beam are brought together. If the two parts of the beam have the same phase, then the fringe pattern remains stable. But if the phase of one part of the beam is drifting with respect to the other, then the fringe pattern will be washed out. And the more slits you have in the screen, the lower the visibility for the same amount of phase randomization per pair of slits.

It might appear that the situation is hopeless: worse than trying to balance several pencils on their tips on the deck of a ship in a storm. But, amazingly, quantum mechanics provides a way to solve this problem, through even higher levels of entanglement. In classical information processing, inevitable environmental noise is dealt with by error correction. In its simplest form, this involves repeating the message transmission or calculation until a majority result is obtained. But there are more efficient ways: use of a parity check on a block of bits, for example. It turns out that a similar notion can be applied to a quantum register.[23] There is, however, one difficulty: you are not allowed to measure the register, because then you would destroy the superposition state

Platforms for quantum computers

The essence of a qubit is the availability of a two-state quantum system, together with a way to manipulate the qubit and to measure its state. What this means is that one must be able to generate arbitrary superpositions of the qubit's two states and have the qubit interact strongly with at least one other qubit in the register. A reliable readout method is necessary. The qubit should also have some immunity to environmental disturbances. The challenge is to find qubits with strong coupling to each other and to the readout device, but weak coupling to everything else.

Physical System	Qubit States	One-Qubit Gate	Two-Qubit Gate	Decoherence Mechanism
Atoms/Lattices	Electron energy	Optical	Controlled collisions	Collisions/ Spontaneous emission
Ions	Electron energy	Optical	Vibrations	Trap fields
Doped solids	Impurity nuclei spin	Magnetic	Electric/Spin	Local fields
Quantum dots	Electron energy	Optical	Coulomb	Local fields
Quantum dots	Spin	Magnetic (ESR)	Spin-spin interaction	Off-resonant Raman spin-flip/ Spin-orbit coupling
Superconductors	Trapped flux	External magnetic flux	Inductive coupling	Local flux or current fluctuations
Superconductors	Charge	RF	Inductive or capacitive coupling	Local charge or voltage fluctuations
Atoms/CQED (Cavity Quantum Electrodynamics)	Electron energy/ Presence or absence of photon	Optical/ Millimeter wave	Cavity-enhanced atom-atom coupling	Spontaneous emission/ Photon scattering
Photons	Polarization	Linear dielectrics	Photodetection	Coupling to other degrees of freedom or scattering to other modes

Table 2. A number of candidate systems exist across many different areas of physics. The most promising are shown here.

encoded in it. So how do we determine what might be wrong with the register qubits without looking at them? Simple. Entangle them with an ancillary register, and measure the ancilla! Because the two registers are correlated, the results of the measurement of the ancilla will tell you how to fix the errors in the processing register, without destroying any coherent superpositions in the processing register itself.

Another way to prevent your register coherence falling apart is to know a little about the sort of noise that is acting upon it.[24] If the noise has some very slow components (or some with very long wavelengths), then it is sometimes possible to find certain combinations of qubit states for which the noise on one qubit exactly cancels the noise on another. These qubit states live in a "decoherence free subspace," or DFS.[25] If you can use only computational states that lie in this DFS, then your computer will be immune to environmental perturbations.

It is the possibility of combining these tools to combat noise that leads researchers to believe that a quantum computer can be built even though decoherence lurks around every corner.

The quantum future?

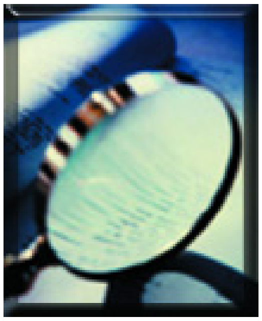
Quantum information science offers a qualitatively different way to look at information processing. It brings not only the promise of a new technology, but also new insights into quantum physics itself. And it requires interdisciplinary thinking of the broadest and deepest kind: from computer science, information theory, atomic physics and optics to many-body chemistry and solid-state physics and engineering. We have only been able to touch the surface of the immense amount of work in this area, and the interested reader is referred to a number of books and review articles for further information.[26]

Several viable technologies have already sprung from this well. Quantum cryptography is on the verge of being a commercial venture. Quantum-enhanced metrology will have important applications in fields in which precision is critical. But all of these will make use of a small number of particles, with consequently limited amounts of entanglement. The goal of a true quantum computer with 1000-qubit registers is still a long way off. Nevertheless, the payoff for making such a machine is substantial, and the new scientific insight and spin-off technologies along the way make it a worthwhile endeavor.

References

Please see OPN Feature Article References, page 56.

Ian Walmsley is at the University of Oxford, U.K. His e-mail address is walmsley@physics.ox.ac.uk. Peter Knight is with the Imperial College in London, U.K. His e-mail address is p.knight@ic.ac.uk.



References

Note: References in *Optics & Photonics News* feature articles are published exactly as submitted by the authors.

MEMS: Some Self-Assembly Required 20

Uthara Srinivasan, Michael A. Helmbrecht, Richard S. Muller and Roger T. Howe

1. J. Benyus, Biomimicry: Innovation Inspired by Nature, William Morrow and Company, New York, 1997.
2. G. M. Whitesides and B. Grzybowski, "Self-Assembly at All Scales," Science 295, 29 March 2002, 2418-2421.
3. J. S. Smith, "High Density, Low Parasitic Direct Integration by Fluidic Self-Assembly (FSA)," International Electron Devices Meeting, 2000.
4. K. F. Böhringer, K. Goldberg, M. B. Cohn, R. T. Howe, and A. P. Pisano, "Parallel Microassembly with Electrostatic Force Fields," Proc. 1998 IEEE Conf. on Robotics and Automation, Leuven, Belgium, May 1998, pp. 1204-11.
5. T. Nakakubo and I. Shimoyama, "Three-Dimensional Micro Self-Assembly Using Bridging Flocculation," Proc. 1997 International Conf. on Solid-State Sensors and Actuators, Sendai, Japan, June 7-10, 1999, pp. 1166-9.
6. Y. Murakami, K. Idegami, H. Nagai, T. Kikuchi, Y. Morita, A. Yamamura, K. Yokoyama and E. Tamiya, "Application of Micromachine Techniques to Biotechnological Research," Materials Science and Engineering C 12, 2000, pp. 67-70.
7. S. C. Esener and D. Hartmann, "DNA Assisted Microassembly: A Heterogeneous Integration Technology for Optoelectronics," SPIE Critical Reviews of Optical Science and Technology, 1998, pp. 13-40.
8. A. Terfort, N. Bowden, and G. M. Whitesides, "Three-Dimensional Self-Assembly of Millimetre-Scale Components," Nature 386, pp. 162-4 (1997).
9. U. Srinivasan, R. T. Howe, and D. Liepmann, "Microstructure to Substrate Self-Assembly Using Capillary Forces," Journal of Microelectromechanical Systems 10 (1), March 2001, pp. 17-24.
10. U. Srinivasan, M. A. Helmbrecht, C. Rembe, R. S. Muller and R. T. Howe, "Fluidic Self-Assembly of Micromirrors onto Microactuators Using Capillary Forces," Journal of Selected Topics in Quantum Electronics, Jan 2002.

Biomedical Applications of Fluorescence Lifetime Imaging 26

Dan Elson, Stephen Webb, Jan Siegel, Klaus Suhling, Dan Davis, John Lever, David Phillips, Andrew Wallace and Paul French

1. Medical Diagnostic System Based on Simultaneous Multispectral Fluorescence Imaging, S. Andersson-Engels, J. Johansson and S. Svanberg, Appl. Opt. 33, 8022-8029 (1994)
2. Fluorescence lifetime system for microscopy and multi-well plate imaging using a blue picosecond diode laser, D. S. Elson, J. Siegel, S. E. D. Webb, S. Lévêque-Fort, M. J. Lever, P. M. W. French, K. Lauritsen, M. Wahl, R. Erdmann, Opt Lett, 27, 1409-1411 (2002)
3. Imaging the environment of green fluorescent protein, K. Suhling, J. Siegel, D. Phillips, P. M. W. French, S. Lévêque-Fort, S. E. D. Webb and D. M. Davis, To be published in the Biophysical Journal
4. Unpublished work, K. Suhling, J. Siegel, D. Phillips, P. M. W. French, S. Lévêque-Fort, S. E. D. Webb and D. M. Davis
5. Energy transfer: a spectroscopic ruler, L. Stryer and RP Haugland, Proc Natl Acad Sci USA; 58, 719-726 (1967)
6. Imaging FRET between spectrally similar GFP molecules in single cells, AG Harpur, FS Wouters and PI Bastiaens. Nat Biotechnol., 19, 167-169 (2001)
7. Time-resolved fluorescence and photon migration studies in biomedical and model random media, B. B. Das, F. Liu and R. R. Alfano, Reports on Progress in Physics 60 227-292 (1997)
8. Time correlated single photon counting, D.V. O'-Connor and D. Phillips, Academic Press, London 1984
9. Simultaneous confocal lifetime imaging of multiple fluorophores using the intensity-modulated multiple-wavelength scanning (IMS) technique, K. Carlsson and A. Liljeborg, Journal of Microscopy 191, 119-127 (1998)
10. Time-resolved fluorescence microscopy using two photon excitation, P.T. C So, T. French; W. M. Yu; K Berland, C.Y. Dong and E. Gratton, Bioimaging 3, 49-63 (1995)
11. Application of the stretched exponential function to fluorescence lifetime imaging, K. C. B. Lee, J. Siegel, S. E. D. Webb, S. Lévêque-Fort, M. J. Cole, R. Jones, K. Dowling, M. J. Lever, and P. M. W. French, Biophysical Journal 81, 1265 (2001)
12. Fluorescence lifetime imaging with picosecond resolution for biomedical applications, K. Dowling, M. J. Dayel, M. J. Lever, P. M. W. French, J. D. Hares, and A. K. L. Dymoke-Bradshaw, Optics Letters 23, 810 (1998).
13. Fluorescence lifetime imaging using a diode-pumped all-solid-state laser system, R. Jones, K. Dowling, M. J. Cole, D. Parsons-Karavassilis, M. J. Lever, P. M. W. French, J. D. Hares, and A. K. L. Dymoke-Bradshaw. Electronics Letters 35, 256-257, (1999)
14. Model LDH 400 from PicoQuant GmbH
15. Model HRI from Kentech Instruments Ltd
16. Fluorescence lifetime imaging microscopy (FLIM) - spatial resolution of structures on the nanosecond timescale, T. W. J. Gadella, T. M. Jovin, and R. M. Clegg, Biophysical Chemistry 48, 221-239 (1993).
17. Whole-field 5-D fluorescence microscopy combining lifetime and spectral resolution with optical sectioning, J. Siegel, D. S. Elson, S. E. D. Webb, D. Parsons-Karavassilis, S. Lévêque-Fort, M. J. Cole, M. J. Lever, P. M. W. French., M. A. A. Neil, R. Jusˇkaitis, L. O. Sucharov and T. Wilson, Optics Letters 26, 1338-1340 (2001)
18. Model MSMI-02V from Optical Insights, Inc
19. Wide-field time-resolved fluorescence anisotropy imaging (TR-FAIM) – Imaging the mobility of a fluorophore, J. Siegel, K. Suhling, S. Lévêque-Fort, S.E.D. Webb, D.M. Davis, D. Phillips, P.M.W. French and Y. Sabharwal, To be published in the Review of Scientific instruments
20. Real-time confocal scanning optical microscope, G. Q. Xiao, T. R. Corle and G. S. Kino, Appl. Phys Lett., 53: 716-718 (1988).
21. Multifocal multiphoton microscopy, J. Bewersdorf, R. Pick & S.W. Hell, Optics Letters 23, 655-657 (1998)
22. Method of obtaining optical sectioning by using structured light in a conventional microscope, M. A. A. Neil, R. Jusˇkaitis and T. Wilson, Optics Letters 22, 1905-1907 (1997)
23. Time-domain whole-field fluorescence lifetime imaging with optical sectioning, M. J. Cole, J. Siegel, S. E. D. Webb, R. Jones, K. Dowling, M. J. Dayel, D. Parsons-Karavassilis, P. M. W. French, M. J. Lever, L. O. Sucharov, M. A. A. Neil, R. Jusˇkaitis and T. Wilson, Journal of Microscopy 203 246-257 (2001)
24. Unpublished work, S E.D. Webb, K Suhling, J Siegel, S Lévêque- Fort, D Phillips and D M. Davis, P M.W. French, M. A. A. Neil, R. Jusˇkaitis and T. Wilson
25. Studying biological tissue with fluorescence lifetime imaging: microscopy, endoscopy and complex decay profiles, J. Siegel, D. S. Elson, S. E. D. Webb, K. C. Benny Lee, A. Vlandas, G. L. Gambaruto, S. Lévêque-Fort, M. J. Lever, P. J. Tadrous, G. W. H. Stamp, A. L. Wallace, P. M. W. French and F. Alvarez, Submitted to Applied Optics.

Polymer Optical Interference Filters 34

Roger Strharsky and John Wheatley

1. J. Menendez, et al., OPN August 1999, 28-29, (1999).
2. M. Weber, et al., Science 287 (5462), 2451-2456, (2000).
3. R. Assam & N. Bashara, Ellipsometry and Polarized Light, North-Holland (1988).
4. A. Thelen, Design of Optical Interference Coatings, MacGraw-Hill (1989).
5. E. Lorenz, et al., Proceedings of ICRC 2001, 912-914 (2001).
6. Gilles Bogaert, GLAST Review October 16, 2001 (2001).
7. B. J. Pichler, et al, IEEE Transactions on Nuclear Science, 47, 1391-1396. (2001).
8. Anonymous, Research Disclosure 439, Article 439052, 1930-1931, (2000)

FEATURE ARTICLE REFERENCES

Quantum Information Science 42

Ian Walmsley and Peter Knight

1. R. P. Feynman in Lectures on Physics, vol. III, p.1-1 (Addison-Wesley, Reading, MA, 1963)
2. M. J. Holland and K. Burnett, Phys. Rev. Lett., 71, 1355 (1993)
3. A. Kuzmich and L. Mandel, Quant. Semi. Opt., 10, 493 (1998)
4. D. J. Wineland, J. J. Bollinger, W. M. Itano, F. L. Moore, D. J. Heinzen, Phys. Rev. A, 46, R6797 (1992): S. F. Huelga, C. Macchiavello, T. Pellizari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, Phys. Rev. Lett., 79, 3865 (1997)
5. A. N. Boto, P. Kok, D. S. Abrams, S. L. Braunstein, C. P. Williams and J. P. Dowling, Phys. Rev. Lett., 85, 2733 (2000)
6. A. K. Ekert, Phys. Rev. Lett., (1993)
7. C. H. Bennett and G. Brassard, in Proc of IEEE Conference on Computers, Systems and Signal Processing, (IEEE Press, New York, 1984); C. H. Bennett. F. Besette, G. Brassard, L. Salvail and J. Smolin, J. Cryptol., 5, 3 (1992)
8. W. K. Wootters and W. H. Zurek, Nature, 200, 802 (1982)
9. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys., 74, 145 (2002)
10. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson and C. M. Simmons, LANL preprint server, quant-ph/9805071
11. G. Ribordy, J.-D.Gautier, N. Gisin, O. Guinnard and H. Zbinden, Elec. Lett., 34, 2116 (1998)
12. P. D. Townsend, Electron. Lett.,33,188 (1997)
13. [Ref: Risk and Bethune, OPN, July 2002]
14. C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett., 70, 1895 (1993)
15. For a discussion, see The Physics of Quantum Information, eds. D. Bouwmeester, A. K. Ekert and A. Zeilinger (Springer, Berlin, 2000)
16. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett., 69, 2881 (1992)
17. K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, Phys. Rev. Lett., 76, 4656 (1996)
18. L. K. Grover, Phys. Rev. Lett., 79, 325 (1997)
19. P. Shor, in Proceedings of the Symposium on the Foundations of Computer Science, 1994, Los Alamitos, California (IEEE Computer Society Press, New York, 1994) p.124
20. D. Deutsch, Proc. Roy. Soc. London A, 425, 73 (1989)
21. D. Deutsch, Proc. Roy. Soc. London A, 400, 97 (1985) (CNOT)
22. J. Preskill, Proc. Roy. Soc. London A, 454, 385 (1998); A. M. Steane, Nature, 399, 124 (1999)
23. A. Calderbank and P. Shor, Phys. Rev. A, 52, R2493 (1995); ibid, 54, 1098 (1996); A. M. Steane, Phys. Rev. Lett., 77, 793 (1995)
24. G. M. Palma, K.-A. Suominen and A. K. Ekert, Proc. Roy. Soc. London, A 452, 567 (1996)
25. D. Lidar, I. L. Chuang and B. Whaley, Phys. Rev. Lett., 81, 2594 (1998)
26. See, for example, the text by M. Nielsen and I. L Chuang, Quantum Information and Quantum Computation, (Cambridge University Press, 2001), and Ref.[14]. There are also numerous review articles in journals, such as Fortschritte der Physik, 48 (9) (2000); Special Focus Issue on Experimental Proposals for Quantum Computation, eds. S. L. Braunstein and H.-K. Lo. A journal is now devoted to this subject area: Quantum Information & Computation, Rinton Press, Princeton, NJ.

A Multiport Cross-Connect Switch Using VLIMOEMS Mirror Arrays 50

Dmitry V. Bakin and Janusz Bryzek

1. Selected papers on optical MEMS/ Victor M.Bright, editor. - (SPIE milestone series; v. MS 153), 628 pages. 1999. Published by SPIE, P.O.Box 10, Bellingham, Washington 98227-0010 USA
2. Rai-Choudhury, P. MEMS & MOEMS: technology and applications/ Prosenjit Rai-Choudhury - (SPIE Press monograph; volume PM85), 520 pages. 2001. Published by SPIE, P.O.Box 10, Bellingham, Washington 98227-0010 USA
3. Ramaswami, Rajiv. Optical networks: a practical perspective/ Rajiv Ramaswami, Kumar N. Sivarajan, 632 pages. 1998. Academic Press, San Diego, CA, USA
4. Yariv, Amnon. Introduction to optical electronics, 552 pages. 1985. Published by CBS College Publishing, New York, NY, USA