Quantum Information Processing: Cryptography, Computation, and Teleportation

TIMOTHY P. SPILLER

Present information technology is based on the laws of classical physics. However, advances in quantum physics have stimulated interest in its potential impact on such technology. This article is a reasonably introductory review of three aspects of quantum information processing, cryptography, computation, and teleportation. In order to give a level of self-containment, I serve up hors d'oeuvres *on the relevant parts of quantum physics and the sorts of quantum systems which might form the building blocks for quantum processors.*

Quantum cryptography utilizes states of individual quantum systems for the transfer of conventional classical bits of information. The impossibility of measuring quantum systems without disturbing them guarantees the detection of eavesdropping and hence secure information transfer is possible. In a sense, teleportation is the inverse of cryptography, using more robust classical bits to faithfully transfer a quantum state through a noisy environment. Quantum computation utilizes the evolving quantum state of a complex system, which consists of many interacting individuals. If such a machine could be built, it would be capable of solving some problems which are intractable on any conventional computer; I illustrate this with Shor's quantum factoring algorithm.

I give some details of the current experimental achievements, proposals, and prospects for the future and of the patents granted to date.

I. Introduction

Quantum mechanics [1]–[8] was developed originally as a theory to explain the behavior of large numbers (ensembles) of microscopic objects, such as atoms or electrons. However, over the last decade or so, considerable interest has developed in the application of quantum theory to *individual* systems and to physically larger (mesoscopic or even macroscopic) systems where a small number of *collective* degrees of freedom show genuine quantum behavior. In part, this interest has been stimulated by the tremendous advances which have occurred in experimental physics and the relevant engineering. For example, it is now possible to fabricate very sophisticated semiconducting or superconducting devices in which quantum effects play the dominant role. The behavior of some of these devices is governed by the motion of single electrons or single quanta of magnetic flux [9]–[11]. In addition, considerable progress has been made in atomic and laser physics [12]. *Single* atoms or ions can be trapped and probed with electromagnetic fields. Correspondingly, single photons (quantized excitations of the electromagnetic field) can be produced trapped in cavities or as traveling quanta.

One exciting aspect of this developing fundamental research is its technological potential. It could spawn what might be termed *quantum information technology*. In such a scenario, machines would process and exchange information according to the laws of quantum physics, in contrast to the workings of conventional information technology, where all this is done classically. Information processing now plays a significant role in all of our lives. We communicate, for example, by telephone and over the Internet. We carry and use an increasing number of cards containing magnetically stored data. Many household and workplace appliances contain processing power, from simple microprocessors through to powerful computers. It is obvious that quantum physics is not going to make significant inroads into this huge technology spectrum in the foreseeable future. Nevertheless, even if quantum machines could outperform their classical counterparts (or, better still, open up completely new avenues) in just a few useful applications, there would be real excitement. Quantum engineering would begin to evolve.

Although the fundamental research is still in its infancy, interesting and promising ideas for applications of quantum information processing [13] have started to develop. I discuss three of them in this article.

- *Quantum cryptography*: Here the exchange of individual quantum systems between two correspondents enables them to establish a shared random bit (binary digit) string, or key, which can then be used for the encryption of a secret message. The use of quantum states by the correspondents, who have become known in the literature as Alice and Bob, means that they can be sure as to whether or not an eavesdropper, Eve, has been listening. No such guarantee exists if Alice and Bob exchange their key classically because classical information can be read without disturbing it in any way.

Manuscript received February 27, 1996; revised September 10, 1996.

The author is with the Mathematics Group, Hewlett–Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, United Kingdom (e-mail: ts@hplb.hpl.hp.com).

Publisher Item Identifier S 0018-9219(96)08870-6.

- *Quantum computation*: A classical computer processes its input according to its program to produce the output. Any classical system is always in one of a defined set of states. For example, a perfect classical bit is actually *in* state *zero* or state *one* at any time; the two possibilities are mutually exclusive. However, as will be seen, a quantum system can exist in what might be termed a schizophrenic state, known as a *superposition state*. At all times during its existence, such a quantum state possesses components corresponding to each of (or at least some of) the different classical possibilities. For example, a superposition state of a quantum bit (qubit), would contain a component corresponding to the value *zero and* a component corresponding to *one at the same time*. The state is neither wholly *zero* nor wholly *one*, as must apply for a classical bit. This superposition phenomenon means that if a computer is built which evolves according to quantum rules, it could be prepared in a superposition of the possible classical input states. In a sense it then processes the different inputs in parallel, to produce a superposition of outputs. It is known already that this parallelism would enable a quantum computer to attack some problems which are intractable on any classical machine.
- *Quantum teleportation*: Quantum states are often extremely fragile; interactions with other systems disrupt and eventually destroy their subtle superposition properties. On the other hand, classical bits are more robust and can easily be checked for errors, which must involve an interaction with some other system, in a nondisruptive way. Quantum teleportation effects the faithful transfer of an *unknown* quantum state through a potentially hostile environment by using classical bits. If quantum computers become a reality, there could be a real demand for such a facility, as outputs from some machines might be needed as input for others.

I devote a section to each of the above. In each case I will give the basic idea and discuss some of the practical problems which have to be addressed to turn the theory into experiment, the first step toward the technological goal. I describe the current status of experiments; actual, preliminary, or proposed. As will be seen, quantum information processing is not simply a theoretician's dream. Working prototype quantum cryptosystems actually exist and practical quantum gates which could form the building blocks for a quantum computer are just about with us. The bibliography contains a broad spectrum of references, from articles at a similar level to this one through to the full-blown technical research papers. Additional references, articles, and information can be accessed at the following World Wide Web (WWW) sites:

- http://vesta.physics.ucla.edu/~smolin/index.html
- http://eve.physics.ox.ac.uk/QChome.html
- http://feynman.stanford.edu/qcomp/
- http://xxx.lanl.gov/archive/quant-ph

(The quant-ph/numbers given for some of the references locate them at the Los Alamos e-print server, the fourth of these addresses.) The closing section of this article is devoted to comments on the future prospects for and potential value of quantum information processing. It is hard to draw any firm conclusions about a fast developing subject; however, this does not matter. My aim, indeed the aim of the whole paper, is to promote thought, interaction, and discussion.

Before turning to the main subject of this report and in an attempt to make it somewhat self-contained, I give two other sections. The first discusses some of the important features of quantum mechanics, those which are essential for understanding the later sections. The second discusses various simple quantum systems which could be deemed to be candidate building blocks for more complex quantum machines. As will be seen, there is a consensus that photons are probably best for transporting quantum information. However, there is no clear favorite when it comes to building quantum gates for manipulating the information. There are a few possibilities which warrant consideration, along with their good and bad features.

There are a few footnotes in this paper and an appendix. These contain items which may be slightly off the main theme or raise technical points which deserve a bit more than a mere reference. They can be ignored at first reading.

II. Quantum Mechanics

A. *Quantum Systems and States*

The motion of a classical object such as a billiard ball or a planet is described by giving the trajectory, the position as a function of time, of its center of mass. It is known empirically that such a trajectory can be observed with insignificant disturbance to or modification of the motion. Similarly, the value of a classical bit can be read without changing its value. It is therefore natural to assume that classical objects follow their trajectories whether or not they are observed. Of course, interactions with other systems (collectively called *the environment*) can be made so severe that the motion of the object of interest is disrupted. However, *in principle*, within classical physics this disruption can be reduced arbitrarily. For the case of quantum systems, things are rather different. All of this breaks down. In general, it is impossible *even in principle* to observe a quantum system without irreversibly disturbing it. Correspondingly, it is incorrect to assume that a quantum system follows something akin to a classical trajectory, essentially independent of its environment. What a quantum system does depends dramatically on how you choose to interact with it. Worse than this, at the *individual* level, what you see as a result of this interaction does not enable you to infer what the system was doing before you looked. The interaction is irreversible.

The behavior of a quantum system is described by giving its quantum state, often denoted by $|\psi\rangle$, as a function of time. Mathematically speaking, $|\psi\rangle$ is a vector in an abstract Hilbert space of possible states for the system. However, in order to discuss and perform calculations for a quantum system, it is often convenient to choose a particular (and more familiar) *representation* of its state. For example, in the case of a single qubit, the state *one* (denoted generally by $|1\rangle$) could be represented by the column vector $\binom{1}{0}$ and the state *zero* (denoted generally by $|0\rangle$) by $\binom{0}{1}$. Observables, properties of a quantum system which may be observed, are given by operators. These act on the quantum state to give the value of the observable for the system in that state. For example, with the qubit states represented by the vectors, the "bit value operator" (i.e., B) is represented by the matrix $\left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$. In the general notation

$$\begin{aligned} B|1\rangle &= 1|1\rangle \\ B|0\rangle &= 0|0\rangle \end{aligned} \tag{1}$$

so the operation of B on the state yields the bit value. These results drop out simply in the vector and matrix representation.

The states $|1\rangle$ and $|0\rangle$ are *eigenstates* of the operator B. A system in an eigenstate has a definite bit value known as the *eigenvalue*; these are obviously one and zero, respectively, for the qubit example. In quantum mechanics, the set of all possible eigenstates of an operator such as B form a *basis*. The qubit basis contains just two states. *Any* state of a quantum system may be expanded as a linear combination, a *superposition*, of a set of basis states. For example, an arbitrary qubit state $|\psi\rangle$ can be expanded as

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{2}$$

for some coefficients a and b. In vector form this would read $\binom{b}{a}$. Such expansions are analogous to the decomposition of a musical note, created, for example, by a plucked guitar string. Here the basis consists of the vibrational state of the string at its fundamental frequency, along with those at all the higher harmonics. *Any* note may be expanded as a linear combination of the basis notes with appropriate coefficients. It is well known that the relative *phases* between the harmonics must be given, in addition to the *magnitudes* of the harmonics present, to completely specify a note. Exactly the same holds true in quantum mechanics. To achieve this, the coefficients in a superposition, a and b in (2) for example, are generally *complex* numbers, so they carry a magnitude and a phase. The complex coefficients in a superposition state are often called the *amplitudes* for the basis states to which they pertain.

The precise meaning of the quantum state of a system is still a debating point today, 70 years after the birth of the theory! However, one thing that is certainly true, the minimum statement that can be made about the physical meaning of $|\psi\rangle$, is that the state of a quantum system just before its interaction with (classical) measurement apparatus can be used to predict the *probabilities* of the possible results that the apparatus will record. This is the orthodox interpretation of $|\psi\rangle$. It is also often called the Copenhagen interpretation because its foremost advocate was Neils Bohr. In a nutshell, Bohr's view was that since quantum systems only express themselves through the results recorded by measurement apparatus—there is no other way to *see* them—this was all that the theory, quantum mechanics, had to predict. The fact that the predictions are only probabilistic simply had to be accepted as a property of nature. Albert Einstein never accepted this essentially pragmatic viewpoint and he and Bohr discussed it over many years. For an excellent account, see [8].

The outcome of any individual measurement is a truly random process, with a distribution set by $|\psi\rangle$. The *probabilities* of the measurement results for an observable are given by the squared moduli of the amplitudes of the basis states for that observable, when $|\psi\rangle$ is expanded in that basis. For example, a measurement of the bit value B for a qubit in the state (2) would yield one with probability $|b|^2 = b^*b$ (* denotes complex conjugation) and zero with probability $|a|^2$. In the general notation these probabilities can be respectively written as $|\langle 1|\psi\rangle|^2$ and $|\langle 0|\psi\rangle|^2$, where $\langle\chi|\psi\rangle$ denotes the *inner product* between the two Hilbert space states. In the vector representation, a state $\langle\chi|$ is found from its counterpart $|\chi\rangle$ by transpose and complex conjugation; the two operations together are known as Hermitian conjugation and are denoted by $\dagger$. Thus $\langle\psi|$ for the qubit state (2) is represented by the row vector $(b^*\ a^*)$. The inner product is then simply a familiar dot (or scalar) product between the vectors.

Given the probability interpretation for $|\psi\rangle$, quantum states are normalized to $\langle\psi|\psi\rangle = 1$ so all the probabilities sum to unity. This yields the constraint $(b^*\ a^*)\cdot\binom{b}{a} = |b|^2 + |a|^2 = 1$ on the amplitudes for the qubit, and an analogous condition for the amplitudes of any quantum system. The basis states corresponding to any operator are (or can be constructed to be) mutually orthogonal, so any pair have zero inner product. They are also normalized. (It is easy to see from the vector representation that $\langle 1|1\rangle = \langle 0|0\rangle = 1$ and $\langle 1|0\rangle = \langle 0|1\rangle = 0$ for the qubit.)

Although individual measurements of a qubit value will *always* yield one or zero, one of the *eigenvalues* of B, it is clear that (apart from the special cases when $|\psi\rangle$ is actually equal to an eigenstate of B) the *average* bit value for a large number of measurements will lie somewhere between zero and one. This average, known in quantum mechanics as the *expectation value* of B, is given by $\langle\psi|B|\psi\rangle$. For the simple qubit example (2), it is easy to show that this is $|b|^2$. Operators corresponding to observables in quantum mechanics are equal to their Hermitian conjugate, so $B^\dagger = B$. This ensures that all the eigenvalues of such operators (the outcomes of individual measurements) and the expectation value (the average over many identical measurements) for *any* state of the system are *real numbers*, as they must be if they are to correspond to actual measured results.

The point which quantum folk still debate is the physical interpretation of $|\psi\rangle$ above and beyond that of giving the statistical behavior of ensembles of quantum systems, of giving the probability distributions of measurement results and the expectation values [5]–[8], [14, ch. 20], [15]. The minimal pragmatic viewpoint is certainly not wrong; the question is as to whether or not it can be bettered by something more illuminating and precise. It is probably fair to say that the recent advances in experimental physics which now give access to individual quantum systems have heightened this debate. The Copenhagen interpretation is now being squeezed.

B. The Two Vital Points

There are two important aspects to the time evolution of a quantum state $|\psi\rangle$. These embody the famous wave-particle duality associated with quantum systems. Basically, when a quantum system evolves unhindered it exhibits smooth wave-like properties. On the other hand, when a it interacts with some form of environment or apparatus, so it is prepared (emitted) or measured (detected), it exhibits discrete particle-like properties. For example, this is where the well-known "collapse" of quantum states comes into play. Both of these aspects of the evolution play important roles in the field of quantum information processing.

- *Reversible wavelike behavior.* When it is isolated from its environment, including measurement apparatus, the state of a quantum system evolves *coherently* and reversibly according to the Schrödinger equation

$$H|\psi\rangle = i\hbar\frac{\partial|\psi\rangle}{\partial t}. \tag{3}$$

  H is the Hamiltonian operator of the system, which represents its energy. The vital point here is that if $|\psi_1\rangle$ and $|\psi_2\rangle$ are each solutions to (3), then it is clear that $c_1|\psi_1\rangle + c_2|\psi_2\rangle$ is also a solution, for arbitrary coefficients c_1 and c_2. Thus *superposition states* are preserved in time.[1] This property is crucial for quantum computation.
- *Irreversible particle-like behavior.* When it is coupled to an environment the evolution of a quantum state is modified. Such coupling could be deliberate; it could be to an apparatus designed to measure some property of the quantum system. However, it could be inadvertent; for example there could be a frictional (energy removing) force acting on the system. In either situation the state evolves irreversibly. Fragile but often desirable superposition states get destroyed or at least partially scrambled as time goes on; they *decohere*. Often this can be viewed as some sort of localization of the state; the interaction with the environment causes the quantum system to resemble more closely a classical system localized in a definite state. Such irreversible behavior is vital in two respects. Firstly, in the case of cryptography, any eavesdropper who measures a quantum system to try and determine its state cannot avoid changing this state, which is the key to the whole approach. Secondly and more generally, irreversibility may mean trouble. Any aspect of quantum information processing which relies on the reversible Schrödinger evolution of some quantum state must be protected from any environmental disruption. Practical realizations of quantum machines have to address this crucial issue.

The terms *reversible* and *irreversible* used here do carry their usual statistical mechanical connotation. The conventional and most widely used approach for discussing irreversibility in quantum physics is the density operator formalism, which describes a large number, an ensemble, of quantum systems in direct statistical terms [3], [15]–[17]. An excellent account of quantum measurement viewed this way is given in [18]. The entropy [19] of an ensemble of quantum systems is defined in terms of its density operator. This entropy is preserved for reversible Schrödinger evolution but changes when the environment acts to introduce irreversibility. (A more detailed discussion of density operators and irreversibility is given in the Appendix.)

The recent interest in *individual* quantum systems has lead to new approaches for putting irreversibility into quantum mechanics. These can describe the behavior of the state of a *single* quantum system as it interacts with an environment, as well as producing the usual statistical results [15], [20]–[22]. In such models superposition states are typically destroyed; a state can evolve into a localized classical one through the effect of the environment. Given the importance of individual systems for quantum information processing, I choose to talk deliberately in terms of the irreversible evolution of the states of single systems, rather than in terms of density operators.

C. An Example—Photon Polarization

A simple example, which will also be useful later on, should help to clarify some of this formalism. One way of characterizing a photon, a quantum of light, is by its linear polarization. Rotating a polarizer by 180° has no effect as far as the light is concerned. (Of course, your sunglasses will no longer fit on your nose or hook behind your ears, but photons do not care about this!) Specifying the plane of polarization somewhere between 0° and 180° covers the full range of possibilities and so it is customary to denote the polarization state of a photon by a double-headed arrow which defines this plane.

The superposition principle is demonstrated by the state $|\text{⤢}\rangle$. This can be decomposed into vertical ($|\updownarrow\rangle$) and horizontal ($|\leftrightarrow\rangle$) polarization states as

$$|\text{⤢}\rangle = 2^{-1/2}(|\updownarrow\rangle + |\leftrightarrow\rangle). \tag{4}$$

Provided that there is insignificant coupling to any sort of environment, this superposition state is preserved as the photons evolve, whether this is through free space or down a perfect optical fiber. The original polarization state $|\text{⤢}\rangle$ is preserved.

[1] This follows from the linearity of (3). Formally, the solution may be written as $|\psi(t)\rangle = U|\psi(0)\rangle$ where U is the *unitary* evolution operator $U = \exp\left[-(i/\hbar)\int_0^t dt' H\right]$, so it is clear that superpositions are preserved as U applies linearly term by term. A unitary operator is one whose Hermitian conjugate is its inverse, $U^\dagger U = UU^\dagger = I$ where I is the identity operator; in a matrix representation I would simply be the appropriate dimension identity matrix. The evolution operator U is unitary because the Hamiltonian, being an observable corresponding to the energy, is Hermitian, so $H^\dagger = H$. Reversible time evolution as generated by (3) is often called *unitary evolution*.

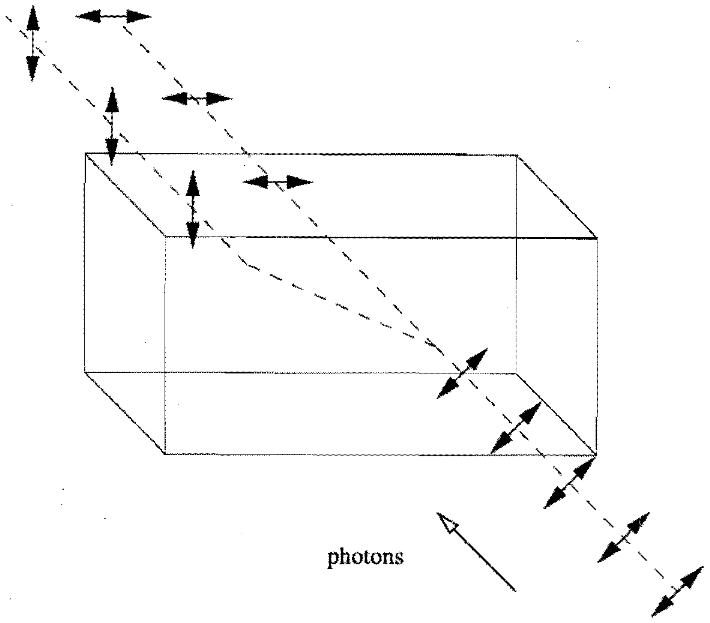

Fig. 1. A schematic illustration of the behavior of a calcite crystal. Independent of the incident polarization, when detected, the emergent photons are found to be in state $|\leftrightarrow\rangle$ in the undisplaced beam, or state $|\updownarrow\rangle$ in the displaced beam. The relative weights in these two beams follow from the squared moduli of their amplitudes in the incident state. With this given by (4), there is an equal split.

An example of an unwanted and unavoidable environment effect might arise if the photons propagate down an imperfect optical fiber. Any real fiber will interact with photons to some extent. Consider a model example where an interaction modifies the amplitudes in the superposition introducing a relative phase ϕ between them, so that the state becomes

$$|\psi\rangle = 2^{-1/2}(\exp(i\phi)|\updownarrow\rangle + |\leftrightarrow\rangle). \quad (5)$$

Such a phase difference could arise if the two rectilinear polarizations $\updownarrow$ and $\leftrightarrow$ travel with different speeds in the fiber, an effect known as birefringence. This in itself is *not* an irreversible interaction. Clearly, although the state has changed, the original one could be recovered by introducing another change of $-\phi$ or a further shift to make the total a multiple of (2π), perhaps by using another piece of fiber. However, if the environment contains *fluctuations*, with the result that ϕ ends up with a *random* component, then the interaction is *irreversible*. If the propagation distance is sufficient for the (root mean square) random piece of ϕ to be of the order of 2π, then the final plane of polarization will be random *in whichever basis it is measured.* For example, using (4) and the relationship $|\searrow\rangle = 2^{-1/2}(|\leftrightarrow\rangle - |\updownarrow\rangle)$, the state (5) can be rewritten as

$$|\psi\rangle = \exp(i\phi/2)(\cos(\phi/2)|\nearrow\rangle - i\sin(\phi/2)|\searrow\rangle). \quad (6)$$

Measuring the diagonal polarization would thus yield $\nearrow$ with probability $\cos^2(\phi/2)$ and $\searrow$ with probability $\sin^2(\phi/2)$. For random ϕ these both average to 1/2, in sharp contrast to the initial state (4) which would yield $\nearrow$ with unit probability. The final random state contains no memory of the initial state $|\nearrow\rangle$; it could equally well have been $|\searrow\rangle$. Such an interaction with the environment is therefore irreversible. (See the Appendix for more details.) It cannot be unwound by another piece of fiber, or by any other means. (However, as will be mentioned later, it is possible to fight against irreversibility by building redundancy into states of more complex quantum systems.)

A similar dramatic effect occurs if the polarization of the photons is *measured*; this also serves to illustrate the somewhat strange and counterintuitive nature of superposition states. Although (some) sunglasses act as polarizers, they are not very good for making measurements as they *absorb* one plane of polarization. A calcite crystal is much better [23], [24] as it distinguishes between two orthogonal polarization states without absorbing either of them. For a suitable orientation, the birefringent crystal permits photons in state $|\leftrightarrow\rangle$ to pass straight through, while photons in state $|\updownarrow\rangle$ emerge displaced. This is illustrated in Fig. 1. Putting photon detectors in both of the emergent paths means that the polarization of each photon that comes in can be measured. I must emphasize that the production of genuine single photon states is now an experimental reality [12], [25], [26]. Such measurements really can be done. So what happens if photons in state $|\nearrow\rangle$, given by (4), are sent one by one into an apparatus aligned to measure vertical and horizontal polarizations (henceforth called the rectilinear basis)? The answer is that event by event one *or* other of the detectors fires.

Conventional quantum mechanics simply predicts the statistical results averaged over many events. The probabilities can be read off as the squared (moduli) of the amplitudes in the incoming superposition state (4). As these are both 1/2, the average detector count rates will be equal.

However, if you wish to say something about the individual events, and I certainly do, then the interpretation is that in each event a photon is projected at random from $|\nearrow\rangle$ to $|\updownarrow\rangle$ or $|\leftrightarrow\rangle$ by the measurement process. Note that you *cannot* shrug this off as due to half of the photons *being* in state $|\updownarrow\rangle$ and the other half *being* in state $|\leftrightarrow\rangle$ *before* entering the crystal. This is not the correct interpretation of a state such as (4). Any state decomposition, such as in (4), is a mathematical one. You can please yourself as to whether or not you make it, or make some different one instead. The point is that the decomposition into a basis defined by some observable enables you to read off the probabilities for the results should you choose to measure *that observable* for the photons. However, each individual photon in the ensemble is capable of generating any of the possible outcomes, any of the eigenvalues of the observable, according to these probabilities. Thus the different amplitudes in a superposition exist for *each* photon and cannot be put down to a lack of classical knowledge about the initial ensemble. This latter case is described by a mixture and not a superposition; this is illustrated in the Appendix. A very striking example of superposition states applying to individuals one by one has been provided by neutron interference experiments [27], [28]. An interference pattern, which relies crucially on amplitudes for different paths in a superposition state, can be built up over a period of time with neutrons from a reactor. The beam intensity can be so low that, on average, one neutron has been detected well before the next one has left the reactor pile!

It is also important to appreciate that the result of an *individual* measurement does not tell you the state of that photon *before* it entered your apparatus. If you register $|\updownarrow\rangle$, the state could have been $|\updownarrow\rangle$. However, it could also have been $|\nearrow\rangle$ which happened to project to $|\updownarrow\rangle$. You can be confident that it was not $|\leftrightarrow\rangle$ but that is all, until you measure other identically prepared photons and build up some statistics. This uncertainty regarding an individual incoming state is the key to quantum cryptography, where individual quantum systems are used to carry bits of information.

The photon detectors are an integral part of the measurement apparatus. If they are removed, the beams from the calcite crystal could be recombined to form the original state. A difference in optical path length for the two routes would produce a different final state, controllable by the path difference. This is, of course, an example of interference. Although interference is also a familiar classical wave phenomenon, the point is that it can occur for quantum systems even when they are sent through the apparatus one at a time. There is thus no problem in spatially separating the components of a superposition state such as (4). Separation alone does not destroy the superposition; this happens only when some irreversible interaction occurs, like a detection of one of the components.

D. Entangled States

Possibly the most counterintuitive aspect of quantum mechanics is that of entangled states. These play a part in some areas of quantum information processing, but not all. They are used in some cryptography schemes, but are not essential for an understanding of the basic idea. However, they are essential for teleportation and do crop up in the field of computation.

Two quantum systems together can be regarded as one combined system; mathematically this is described by a state in a larger Hilbert space which is the *tensor product* of the Hilbert spaces of the individual systems. If the two quantum systems have had no past interaction, simply declaring them to be a combined system cannot have any significant implications. The combined state is just a single (tensor) product of their individual states. For example, if you have two qubits (labeled one and two) with qubit one in state $|1\rangle_1$ and qubit two in state $|0\rangle_2$, the combined state $|\chi\rangle_{12}$ is denoted by

$$|\chi\rangle_{12} = |1\rangle_1 |0\rangle_2. \qquad (7)$$

Operators also need to carry a subscript indicating the subspace in which they operate. They only operate on the piece(s) of the combined state which carry the same label. For example, the bit value operator B_1 only operates on the $|1\rangle_1$ part of $|\chi\rangle_{12}$ and similarly for B_2. The total bit value for the system is given by $B_t = B_1 + B_2$. $|\chi\rangle_{12}$ is an eigenstate of B_t with eigenvalue one. There are three other eigenstates which make up the two-qubit basis: $|1\rangle_1|1\rangle_2$, $|0\rangle_1|1\rangle_2$, and $|0\rangle_1|0\rangle_2$. Four basis states are required; this is the product of two for qubit one and two for qubit two. A two-qubit state could therefore be represented a column vector containing *four* amplitudes, one for each basis state. Correspondingly, operators would be 4×4 matrices. I will stick to the general notation. (Going further, a system of n qubits has a basis of 2^n states and an analogous vector and matrix representation.) In the general state and operator description, inner products and expectation values are evaluated by matching up subscripts. It is customary to drop repeated ones so $\langle\chi|_{12} B_1 |\chi\rangle_{12}$ is denoted by $\langle\chi|B_1|\chi\rangle_{12}$. Evaluating this expectation value gives

$$\langle\chi|B_1|\chi\rangle_{12} = \langle 1|B_1|1\rangle_1 \langle 0|0\rangle_2 = 1. \qquad (8)$$

Note that in a single product state such as $|\chi\rangle_{12}$, the expectation value of B_1 is independent of the state of qubit two. $|0\rangle_2$ could be replaced by an arbitrary state with no effect on qubit one. Each qubit can be deemed as being in a well defined state independent of its partner when the combined state is a single product.

Things get stranger (some say spooky) if the combined state is a superposition of two or more of the basis states, each of which is a single product. For example, consider the combined state of two photons given by

$$|\psi\rangle_{12} = 2^{-1/2}(|\updownarrow\rangle_1|\updownarrow\rangle_2 + |\leftrightarrow\rangle_1|\leftrightarrow\rangle_2). \qquad (9)$$

I have switched to the concrete example of photon polarizations because such states *really* can be prepared in a laboratory; however, there is an obvious correspondence between photons and qubits as individually both have two-state bases. States such as (9) *cannot* be rewritten as a single product of a state for photon one with a state for photon two [analogous to the two qubit state (7)], for *any* crafty choice of states. Thus neither photon can be said to be "in some definite state" independent from its partner! The two form a single entangled system. The spooky aspect of such states is that the two subsystems may well be far apart. Indeed, to prepare photons in a state such as (9) they must have a common origin and, once prepared, they clearly then fly apart at the speed of light. Despite such separation, the two subsystems in a state like (9) can retain their intimate entanglement until some irreversible interaction occurs. One consequence of entanglement is perfect correlation between the results of measurements made on the subsystems using the same basis. For example, if you measure the polarization of photon one in the rectilinear basis and find $\updownarrow$, then you can be sure that a similar measurement made on photon two will have yielded the same result. The outcomes $\leftrightarrow$ correlate in the same way.

Einstein was one of the first to worry about the effective lack of identity of either subsystem in an entangled state and raised the problem in a famous paper with Boris Podolsky and Nathan Rosen [29], [8]. States like (8) are therefore often referred to as EPR pairs. Almost 30 years later, John Bell developed the ideas of EPR and proved a remarkable result [30], [31], [14], [8], [6], [32], [33]. Basically, Bell proved that quantum mechanics, as a theory, is nonlocal. The correlations between the results of measurements made on the two subsystems of an EPR pair simply cannot be mimicked by *any* scheme which assumes that the behavior of one subsystem is determined only by things local to it. There really is an intimate *nonlocal* connection to its distant partner. Bell's result has been investigated in some equally remarkable experiments by Alain Aspect and his group [32], [34]–[36]. Their results confirm the predictions of quantum mechanics and thus demonstrate that nonlocality actually exists *in nature*.

The perfect correlations between photon polarizations measured using the same basis do not in fact demonstrate a disagreement between the predictions of quantum mechanics and results constrained by locality. There is *no* disagreement for this case; this develops only when the polarization detector bases for photons one and two have a relative angle between them, reaching its maximum for an angle of 22.5° [6], [32], [33]. (Bell is reputed to have remarked that only an Irishman would have looked for maximum quantum correlations at an angle of 22.5°!) I will not go into the details of Bell's theorem here. However, it is worth noting that the state (9) can be rewritten in the diagonal basis using (4) and the relationship $|\searrow\rangle = 2^{-1/2}(|\leftrightarrow\rangle - |\updownarrow\rangle)$ to give

$$|\psi\rangle_{12} = 2^{-1/2}(|\nearrow\rangle_1|\nearrow\rangle_2 + |\searrow\rangle_1|\searrow\rangle_2). \qquad (10)$$

Perfect correlations between the photon polarizations also occur when they are both measured in the diagonal basis, or indeed any other one. The fact that the perfect correlations occur for *any* basis indicates that there is rather more to the correlations in an entangled state, compared to the classical ones present between, for example, two halves of a torn bank note. Classically, the tear has to be made at the outset in order to separate the two systems. In the quantum case it is as if the bank note is stretched out. The tear is only made when the first measurement is performed and it is made in a direction across the note determined by this measurement!

It should also be stressed that the nonlocal connections embodied in EPR pairs *cannot* be used to send messages arbitrarily fast. This would be in conflict with Einstein's theory of special relativity. The irreversible and random nature of individual quantum measurements prevents such faster than light signaling. Although perfect correlations exist between the results recorded by two well separated observers (using the same basis), it is impossible for either of them to twist the arm of any individual EPR pair and *enforce* a chosen outcome. If this could be achieved, essentially instantaneous signaling would be possible. The idea fails because the individual outcomes occur at random. Nevertheless, entangled states do possess spooky nonlocal connections and these can be utilized for aspects of quantum information processing.

III. Candidate Quantum Systems

This section considers different quantum systems which might be usable as components of quantum information processors. Classical data is usually stored, processed, and transmitted digitally, in terms of bits. The quantum scenarios considered to date also possess this digital aspect and so therefore need systems with a *discrete* basis of states. Qubits, two-state basis quantum systems, are the most obvious choice and research to date has concentrated on these systems. I have therefore focused on these and will continue to do so. However, simple quantum systems with larger discrete bases do exist and these may prove useful in the future. It is also worth emphasising that even with a "digital" basis, a nonclassical "analog" aspect rears its head for quantum systems. Superpositions of discrete basis states, such as the qubit state (2), contain *continuously variable* amplitudes.

A single discrete basis is inadequate for cryptography. To keep Eve guessing, an alternative must exist like in the case of rectilinear and diagonal polarizations for photons. Measurements made in the alternative bases do not *commute*; the order in which they are made matters. (The operators corresponding to the observables, A and B say, are such that $AB \neq BA$.) Quantum systems used for any form of communication must also propagate well and hold their quantum coherence for the time elapsed during transmission. Alice and Bob must be able to send and receive them easily, which suggests using fundamental microscopic systems rather than anything bigger or fabricated. Entangled states are not a must, but they can be used.

One discrete basis will do for computation. The important point here is that a number of systems must be able to *interact* in a *specified manner*, while maintaining the quantum coherence of the *whole* coupled system.

Teleportation needs entangled states. As the idea is to be able to transport on demand an unknown quantum state across a hostile environment, the underlying assumption is that the EPR pairs used are spatially separated beforehand. The communication aspect requires ease of propagation. However, in addition, it must be possible to *store* the EPR pairs in some way which preserves the entanglement. This is certainly a nontrivial requirement.

In all these cases, there will be assorted (classical) hardware to support the quantum systems in the execution of their tasks. For example, the systems may need careful positioning and subjection to well-timed and well-shaped external electromagnetic pulses, in order to follow the desired quantum evolution. One potential problem is that, even if the whole coupled system evolves in a reversible quantum fashion, according to the Schrödinger equation (3), it may not perform the *desired* evolution because of imperfections. These can be thought of as errors in the full system Hamiltonian H which determines the Schrödinger evolution; the experimental H may not be exactly what it is supposed to be. This problem is clearly worse for more complex systems; more than likely it will be a real headache for quantum computation.

The classical hardware, what might be termed the "local" environment of the full quantum system, may also introduce unwanted irreversibility, so the evolution is not even Schrödinger in nature. Some irreversibility will be deliberate, *measurements* are bound to be made at certain times. However, unwanted irreversibilty means that superposition states will also get destroyed between such times, instead of persisting and evolving as they should. In addition and unfortunately, there are also bound to be other facets to the environment such as noise from further afield. The irreversibility introduced by the *total* environment seen by the full quantum system has to be kept small. This problem of decoherence is also worse for more complex systems, so it forms a second huge barrier against the realization of quantum computation.

Basically, then, quantum information processing in general needs discrete quantum states which are somewhat robust. Five possibilities are introduced here; their actual or potential use in the appropriate cases is discussed later in the relevant sections.

A. Photons

As seen in Section II-C, photons have discrete polarization states and alternative bases. Phase angle can be used instead of polarization. There is a direct analogy but the physical implementation is different. Interferometers are used to separate different states, rather than calcite crystals. Single photon states can be created, as can entangled states. In fact, a popular method for producing genuine single photon states [25], [26] is to use one half of an EPR pair. The perfect correlations in such pairs means that a measurement on the retained partner can be used to infer a property of the propagating one, thus preparing a single photon in a known state. In the original Aspect experiments [32], [34]–[36] such pairs were produced by the cascade decay of calcium-40 atoms. However, these days parametric down-conversion [37]–[39], [25], [26] has taken over. A laser beam is fed into a nonlinear crystal such as potassium dihydrogen phosphate. Single beam photons get converted into entangled pairs, the partners heading off in different directions. Obviously traveling photon states propagate well, through the vacuum or down optical fibers. This is due to the weakness of their interactions with other systems. Such photons, propagating down fibers, are thus good—almost certainly the best—candidates for use in cryptography. However, their weakness of interaction renders them as poor candidates for interacting computational qubits.

Photons can also be trapped in high-Q cavities [12]. High-Q (quality factor) means low dissipation, so coherence times can be as long as a hundredth or a tenth of a second. The coherence time t_c of an oscillator such as a cavity relates to the resonant frequency ω_{res} through the dimensionless quality factor, so $t_c \sim Q/\omega_{\text{res}}$. For superconducting microwave cavities with $\omega_{\text{res}} \sim$ 10–100 GHz, quality factors can be as high as $10^9 - 10^{10}$ [40]. In a cavity the discrete basis used is not the photon polarization, but the actual *number* of photons present. Clearly such photons do not propagate, but they can interact with other quantum systems in a coherent fashion, so are good candidates for use in computation.

B. Atoms or Ions

Individual atoms, ions or molecules can be trapped in electromagnetic fields, or controlled in beams [12], [41]. A single atom has discrete (quantized) energy levels, but no alternative discrete basis. However, these states can be coupled to trapped photons (see Section III-A) and with coherence times of sufficient length to demonstrate reversible quantum interactions [12], [41]–[44] which could be used for computation. As the trapped photons usually have microwave frequencies, highly excited (almost ionized) atoms, often called Rydberg atoms, are used to achieve comparable energy level difference frequencies. Optical photons and much higher energy atomic transitions are another possibility [12], [45]; the important factor is the frequency matching.

A number of ions placed together symmetrically in a trap [46], [47] could be thought of as a very small crystal, with discrete vibrational excitations called phonons. The ions in such a system can be probed with lasers and the coherence time of the whole crystal may long enough to perform many reversible quantum interactions [48]. Such crystals might be very useful for computation [49], [50].

C. Quantum Dots

Progress in techniques such as epitaxy and lithography have lead to the fabrication of sophisticated microscopic (at the $\sim 10^{-8}$ m scale) structures whose quantum behavior is determined by one or a few fundamental charges. These are electrons in metals, electrons and holes in semiconductors and electron pairs in superconductors. In superconductors the electrons bind into pairs which then condense into a macroscopic quantum state. A good textbook on this is [51]; it also contains an extensive list of references. The simplest fabricated structure might be a single confining box, but channels, coupled boxes and even arrays are possible [9]–[11]. Various terms are used in the literature; quantum dots, boxes, wires and wells, ultrasmall capacitance devices, nanostructures, and mesoscopic systems, for example. There are two ways to achieve discrete quantum states in such systems. A single charge in a box can occupy different energy eigenstates (rather as if it is in an artificial atom), or the discrete number of charges in the box can be varied.[2] Clearly, fabricated systems are not easily transportable; they generally need very low temperatures to operate and so are surrounded by cryogenic equipment. However, they can be fabricated close enough together to interact electrostatically and they can be coupled to external electromagnetic fields. Although dissipative irreversible effects do come into play, such coupled systems can remain coherent for long enough to exhibit interesting quantum phenomena [9]–[11]. They are thus good candidates for use in computation [54].

D. Magnetic Moments or Spins

Fundamental particles such as electrons, neutrons, or, at a slightly larger scale, atomic nuclei or whole atoms, possess an intrinsic spin angular momentum, which gives rise to a magnetic moment. This spin in a defined direction has a discrete basis and alternative bases can be generated by rotating the direction, rather like the photon polarization example. There is a real analogy between the two-state bases of photon polarization states and spin-1/2 particles like electrons. (For example, many discussions of EPR pairs and Bell's theorem use spin-1/2 language even though the experiments use entangled photons.) Beams of particles with spin can be made [41], these can be polarized with magnetic fields and, in principle, EPR pairs of spins can also be made. Such systems might be usable for communications. However, in comparison to photons, they are rather more sensitive to scattering and electromagnetic noise. Shielded vacuum tubes would be needed for their propagation, instead of optical fibers, so photons look to be a better bet.

Trapped magnetic moments (due to nuclear or perhaps atomic spins) in close proximity would interact magnetically in a similar fashion to the electrostatic interactions between charges in adjacent quantum dots. Such systems are thus candidates for use in computation [55]. Trapped spins can certainly exhibit coherent quantum behavior, so it is known that the decoherence from the trapping aspect of their environment can be made small. Consideration must be given to the level of irreversible spin relaxation introduced by the additional environment that would be needed to implement useful computational interactions, but such systems are certainly decent candidates for quantum computation.

E. Superconducting Rings

It is well known that the magnetic flux threading a closed superconducting ring is quantized. Its allowed values are integer multiples of $h/2e$. This follows from matching the superconducting state around the orbit of the ring, rather in the way that matching an electron state around an atomic orbit leads to discrete states of the atom [51, ch. 6]. To hold quantized flux, a ring must be everywhere thick compared to the magnetic penetration depth for superconductors (around 10^{-7} m [51]). Rings are thus typically much larger than microscopic quantum dots and somewhat larger than so-called mesoscopic systems, where a whole device is at the $\sim 10^{-6}$ m scale. Hence the terminology of macroscopic quantum phenomena, frequently used in connection with such superconducting ring systems and circuits. Unfortunately, to date the discrete quantized flux states of a superconducting ring have not been shown to be genuine quantum states. Experiments designed to demonstrate *superpositions* of such states—the true test—have yet to show success [56]–[59].[3] However, some evidence has been seen [53], [60]–[62] for discrete energy eigenstates of superconducting rings containing Josephson junctions [52], [51]. These states seem to have good stability against irreversible environment effects and they do couple to external magnetic fields. Experimental work on the quantum behavior of coupled ring systems is probably not as advanced as that for quantum dots. As with dots, these systems are not really transportable and they need cryogenic cooling. While more fundamental research is needed, such superconducting systems could have potential for use in quantum computation.

High temperature superconductors—so-called because they only need dunking in liquid nitrogen to work, rather than the liquid helium needed for traditional superconducting metals and alloys—have yet to make any real research inroads in macroscopic quantum phenomena. However, this could change if the quality, fabricability, and transition temperatures continue to improve, so such materials could be useful in the future. Clearly, an emergence of usable room temperature superconductivity would impact broadly on technology in general, not just on quantum information technology.

IV. Quantum Cryptography

A. The Idea

Cryptography in general has developed to satisfy a number of basic needs. Examples are the enabling of two entities to exchange confidential information, the provision of authentication (so users can assure one another of

[2] In this latter case, alternative discrete bases could be established. Two adjacent boxes can be thought of as a tiny capacitor. If charges can tunnel between the boxes in a reversible manner (first considered by Brian Josephson for the superconducting case [52], [51]) then it is possible to arrange for the discrete charge and energy states each to decompose into superpositions of the other [53], just like the photon polarizations of Section II-C.

[3] If such experiments succeed, they will demonstrate the existence of alternative discrete bases, flux and energy states in this case. The experiments aim to observe oscillations of flux for an energy state superposition; this would demonstrate that flux and energy form alternative bases like the rectilinear and diagonal photon polarizations.

their identity) and the guarantee that a nonconfidential message has not been altered in transit. The usual example discussed for quantum cryptography, which I will adopt here, is confidential communication between two people, Alice and Bob. However, data exchange between two computers belonging to banks, companies or governments often requires secrecy and many other examples spring to mind. Here, information or data means conventional classical information, a string of bits in definite states. The problem with such information is that in principle it can be read by an eavesdropper, Eve, without any disturbance whatsoever. Alice and Bob cannot be sure whether or not Eve has read their private message. Hence the need for encryption, to make the message incomprehensible to Eve even if she intercepts it. However, is the incomprehensible message indecipherable? Can Eve crack the code and determine the true message? (She may have the use of a very powerful computer.) The answer depends on the encryption technique. One very desirable feature of a modern cipher is the ability to communicate secretly from scratch, initiated by public exchange of details about the encryption procedure. (Such ciphers are called public key cryptosystems.) Alice and Bob may not know each other. They may not have met, nor even have communicated before. Increasingly many mail, business, and financial transactions are being carried out electronically between people who have little or no anticipation of the need for secret communication. Public key cryptosystems are very suitable for such situations. The most well known system is RSA, named after its inventors Ronald Rivest, Adi Shamir, and Leonard Adleman. It is based on the difficulty of factorizing large composite integers [63], [64]. The trouble is that public key cryptosystems have not been *proven* to be secure! Mathematically speaking, cracking such a cryptosystem with a classical algorithm is a very hard problem, but it has not been proven to be impossible.

One system which is *known* to be secure is the Vernam cipher (after Gilbert Vernam) [24]. It is also called a one-time pad because it requires a key as long as the message that Alice sends to Bob; the key is used only once and then carefully destroyed. This system is secure in the sense that Eve cannot crack the code provided that she has no information about the key. However, this has really just shifted the problem. If Alice and Bob share the key as classical information, they cannot be sure that Eve did not intercept and read it. This is where quantum mechanics is put to use. If the key is distributed using individual quantum systems, the irreversibility of quantum measurements ensures that Eve *cannot* determine the key without leaving behind some evidence of her tampering. This, then, is the basis for quantum cryptography. Physically secure quantum key distribution is combined with the mathematical security of the Vernam cipher to produce a fully secure system.

As a theoretical subject, quantum cryptography was established in the early 1980's by Bennett and Brassard [65]–[67] with some notable input by Wiesner [68]. A very complete account of the subject is given in [69] and a useful and more recent collection of papers in [70]. Some notable popular articles are [24], [71], [72]. (A more extensive bibliography can be found via the WWW addresses given in the introduction.)

As in [24], I shall use the linear photon polarizations introduced in Section II-C to explain the key distribution technique. However, one of these bases could be replaced by a left/right circular polarization basis [69], or both could be replaced by phase angle bases [26]; the principle is unchanged. (The methods used in the real experiments will be specified in Section IV-C.) The assumption is that Alice and Bob have access to two channels, one quantum and one public. Individual polarized photons are sent down the quantum channel; these are what Eve may try to intercept. On the other hand, Eve hears everything that Alice and Bob declare publicly, but cannot corrupt these messages. If Eve could interfere with the *public* messages, she could impersonate Bob to Alice and vice versa, and so trick them into sharing their key information with her instead of each other [73].

The key is distributed in the following way. Alice sends photons one by one, in states which she chooses at random from $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|⤢\rangle$, and $|⤡\rangle$. Bob randomly chooses to measure the polarization in either the rectilinear basis or the diagonal basis. He records his results and keeps them secret. He then announces publicly the list of bases he used for the measurements, but *not* the results. (He also declares the events for which there was a clear malfunction and he got no count, or both of his detectors fired. Alice discards these data without further ado.) Alice then tells Bob which data to keep, which are those for which he used the rectilinear basis when she sent $|\updownarrow\rangle$ or $|\leftrightarrow\rangle$ and those for which he used the diagonal basis when she sent $|⤢\rangle$ or $|⤡\rangle$. They agree a protocol for converting the retained data into bits, which could be $|\updownarrow\rangle = |1\rangle$, $|\leftrightarrow\rangle = |0\rangle$, $|⤢\rangle = |1\rangle$, and $|⤡\rangle = |0\rangle$. They now have a shared random bit string, which is often called the *raw quantum transmission* (RQT).

B. Errors and Eavesdropping

The problem with the RQT is that it will contain errors, from two sources. First, errors always occur in any real system. These can be viewed as due to unwanted aspects of the system environment which cannot be decoupled any further. Even with no eavesdropping and when Bob chooses the correct basis, his apparatus may on occasion register a $|\leftrightarrow\rangle$ when Alice sent a $|\updownarrow\rangle$, for example. Some of the shared bits will therefore disagree because of these system errors. Second, Eve cannot listen in without causing errors. All she can do is the same as Bob and guess the basis in which to measure, event by event.[4] To learn anything about the key, Eve must make quantum measurements and the irreversibility of such measurements means that she cannot tell what the incoming state was; all she can do is record a result and then send an identical photon on to Bob, who is waiting for one. So, for half (on average) of the data which Alice and

[4] This oversimplifies the situation a little. In fact, Eve can try more subtle forms of intercepting measurements even in this single photon case [69], such as measuring in some intermediate basis, partway between rectilinear and diagonal. However, her actions are always detectable.

Bob choose to keep, Eve will have guessed wrong and sent on an alternative basis photon to Bob. Out of these, he will project half back to the original polarization sent by Alice and half to the wrong one. (Remember, this is for events where Alice and Bob are using the same basis.) Eve therefore corrupts one quarter of the RQT that she intercepts.

Alice and Bob now have two problems. Firstly, they must somehow find and remove the errors in the RQT if it is to be used as a cryptographic key. Second, if in the light of this they believe that some eavesdropping has occurred, they have to face the fact that Eve will know the values of some of the *correct* bits. Alice and Bob can deal with both of these problems, but at the expense of reducing the RQT. Nevertheless, it is worth it because after they have done so the result will be certifiably secret. Eve's expected information about the final key can be reduced to an exponentially small fraction of one bit [69]. I outline the so-called *key distillation* procedure; details can be found in [69], [74].

From laboratory tests on the equipment, Alice and Bob should have some idea of the expected system errors. They can estimate the errors in the RQT by public comparison of a small amount of it (which is then discarded). If these errors exceed their expectations, it is likely that Eve has been at work. If there is an error rate of about 25%, she has probably read the whole RQT. Alice and Bob therefore have to bin it and try again. However, at least they *know* that this must be done. (Note that any realistic cryptosystem must have a no-eavesdropping system error rate well below one quarter to be of any use.) This is why it is best to establish a key with the quantum channel, rather than send the actual message. With the former approach, if eavesdropping is occurring then Alice and Bob can find out *before* they release the message. With an error rate well under 25%, Alice and Bob have a usable RQT and can proceed to isolate and eliminate the errors. This they do [69] by randomly permuting the RQT (to randomize error positions) and then block dividing. Bisective parity checks on the blocks can isolate the bits in error. The parity of a string of bits can be defined as its sum, modulo two. It is therefore zero if the string contains an even number of 1's and one if it contains an odd number. A block of size $\sim 2^k$ requires the disclosure of $\sim k$ parities for such a bisective check. Publicly chosen *random* string parities can be compared to check that all the errors have all been found. The probability of a remaining error showing up through a comparison of a random string parity is 1/2. If one does, Alice and Bob do another bisective search. Throughout the distillation procedure, for *every* bit of information (parity value) revealed publicly, Alice and Bob discard one bit of the string used to create it, so as to avoid increasing Eve's information.

Having removed all the errors, Alice and Bob can then decrease Eve's knowledge of the remaining correct RQT. This process is called *privacy amplification* [74]. From the initial RQT error rate, Eve's information on the corrected RQT, the number of its bits she knows, can be estimated. If Alice and Bob agree on a random subset of bit positions in the corrected RQT, then it is clear that Eve will only know the *parity* of that subset if she knows the values of *all* the bits it contains, which is extremely unlikely. Thus Alice and Bob can use this parity as the first bit of a new, almost totally secret, final key. Indeed, by choosing a number of independent subsets approximately equal to the corrected RQT size *minus* the number of its bits that they estimate Eve knows, Alice and Bob obtain a corresponding number of shared bits, the final almost perfectly secret key. Privacy amplification mixes up what Eve does know with what she does not, effectively diluting her knowledge.

To give you a feel for the numbers [69], with 4% RQT errors (taken to be dominated by eavesdropping) Alice and Bob could distill 2000 bits down to 754, about which Eve could be expected to know less than 10^{-6} of one bit. With a higher RQT error rate of 8%, 2000 bits distil down to 105, with an even better secrecy.

C. Practical Considerations and Experiments

One important practical issue is that at present most of the experiments use very weak light pulses, rather than single photons. Although on average these pulses only contain about 1/10 of a photon, this does mean that they give a small probability for finding two or more photons.[5] This opens up another eavesdropping possibility. Eve could use a beam-splitter (a half-silvered angled mirror) to take some of the light pulse, while the remainder propagates on to Bob. This cannot be done for genuine single photon states as then only she *or* Bob could detect, but not both of them. The reason such weak pulses of light are employed in the transmission is that this keeps the probability of successful beam-splitting small. At this level it can be dealt with comfortably as part of the key distillation process [69]. Note that if much stronger light pulses are used, these can be split easily; in such a case the transmitted information is then classical rather than quantum.

Weak light pulses are currently preferred to photons because they are easy to produce and transmit. A laser or light emitting diode simply has to be filtered down to the appropriate level. A detailed discussion of the relative merits of the two approaches and problems common to both of them is given in [39].

The main comparison points to note are that with current detectors the throughput (which limits the bit rate) of single photon systems is less than 10% of that for weak light pulse systems. Worse, on top of this, photon systems have fiber launch losses of approximately 80%. These arise in attempting to propagate the photons produced in a nonlinear crystal down an optical fiber; no such losses occur with

[5] An example state is a coherent state $|\updownarrow, c\rangle_{\text{coh}} = \Sigma_{n=0}^{\infty} c^n (n!)^{-1/2} \exp(-|c|^2/2) |\updownarrow, n\rangle$. This is a *superposition* of states containing different *numbers* (n) of photons each with the same polarization, in this case $\updownarrow$. c is the small and experimentally controllable parameter that governs the average number of photons present, the expectation value of the photon number. The probability of measuring a light pulse in state $|\updownarrow, c\rangle_{\text{coh}}$ and finding one photon is the squared modulus of the one photon amplitude in the coherent state, $p_1 = |\langle \updownarrow, 1 | \updownarrow, c\rangle_{\text{coh}}|^2 \approx |c|^2$ and it is this which is fixed at about 1/10 in the experiments. The probability of two or more photons is $p_{n \geq 2} = \Sigma_{n=2}^{\infty} p_n \approx p_1^2/2$; this is much less than p_1 when p_1 is much less than unity.

weak light pulses because for them the full systems can be in fiber. (A nonlinear fiber section which effects parametric down conversion of photons would help overcome launch losses.) On the plus side, though, photons do offer better security; no eavesdropping by beam-splitting is possible. This advantage is heightened if EPR pairs of photons are used [76]–[78]. It is also worth noting that if EPR pairs entangled in polarization (or in phase) are used, the randomness of basis can be generated *passively* with beam splitters; these make the random selection of basis to be measured [75]. If Alice generates EPR pairs, measures one passively and sends the other to Bob who does the same, then neither of them needs to choose randomly between the polarization (or phase) measurement bases; this can be arranged to occur as part of the measurement process. This could be important in the future as the lack of active basis switching might permit considerable increases in bit rate. However, the present state of things is that weak light pulses win out over photons.

Problems common to both approaches are those of transmission and detection, which have an unfortunate link at the moment. Optical fibers, the obvious way to send photons with decent but not perfect environmental protection, work pretty well at wavelengths of 1.55 μm, with losses less than 0.2 dB km^{-1}. The losses are 0.3 dB km^{-1} at 1.3 μm; both of these are standard telecommunication wavelengths. The losses climb to 2 dB km^{-1} at 600–900 nm. The trouble is that photon detectors work best at these latter wavelengths. (Silicon avalanche diodes can give subnanosecond time resolution and better than 70% quantum efficiency.) The lack of good photon detectors at the longer wavelengths where fibers work well is probably the dominant practical problem at this time [75].

Despite all the problems, experimenters in the field have made good progress. This list is not exhaustive, but cites the first success and some recent experiments.

- The first successful prototype ran in 1989 [79], [24], [69]. Subsequent improved versions were run, but the apparatus was designed merely to demonstrate the principle. Weak polarized light pulses were transmitted over a quantum channel length ~30 cm, at a very slow bit rate and with about 4% system errors. However, error elimination and privacy amplification protocols were implemented to show that secret keys could be distilled.
- These experiments ran an all fiber system built using only commercially available components [80]. Weak polarized light pulses at 800 nm were used, so a good detector could be employed. However, this meant tolerating increased fiber problems in comparison to those which occur at the longer standard telecommunication wavelengths. A raw data rate ~10 kbit/s^{-1} was achieved, with system errors of 0.35% for 300 m of fiber and 0.54% for 1100 m. The authors discuss three separate fiber environment problems:
  - — Topological phase: When the wave vector (or $\boldsymbol{k}$-vector) of a photon, which defines its direction of propagation and its wavelength, is transported around a topologically nontrivial circuit this gives rise to a geometric, or Berry, phase [81]–[83]. Fibers must therefore be fixed; fluctuations in the *orientation* of a cable could translate into photon phase fluctuations.
  - — Polarization mode dispersion: Dispersion is the spread of a pulse due to its different frequency components having different speeds; this can cause a pulse to lose coherence. For polarization modes propagating down standard fibers this can be ~0.1–1 ps km$^{-1/2}$. The total coherence loss down the fiber must be kept less than the coherence time of the laser providing the pulses and the latter can now be as long as a few nanoseconds [80]. Dispersion is thus not the main problem at current operational distances.
  - — Intrinsic birefringence: Birefringence means that the two different modes of polarization have different speeds, which introduces a relative phase between the modes like in the model example of Section II-C. A fixed birefringence can be compensated for; the problems of irreversibility arise when it *fluctuates* and makes the polarization of a pulse unstable. Such fluctuations occur due to changes in thermal or mechanical stresses. At present tens of km of fiber can be stabilized for ~ 20 min against such fluctuations [80].

- Birefringence is identified as the dominant problem. The experiments employed manual polarization compensators to adjust for the nonfluctuating parts of these environment effects.

  Recent experiments by the same research group [84] have demonstrated the principle of quantum cryptography under Lake Geneva. Polarization states of weak light pulses (with average photon number 0.12) were transmitted down 23 km of standard installed Swiss Telecom PTT fiber, most of which is buried under Lake Geneva. System errors of less than 3.4% were obtained working at the standard telecom wavelength of 1300 nm. (Similar results were found using 26 km of coiled fiber in the laboratory.) Good polarization stability over periods up to ~1 h was achieved. However, the authors note that at certain times high instability occurred which they believe could have been due to nearby civil engineering works. This illustrates the sort of problems which will need careful consideration for systems operating in the outside world, rather than under laboratory test conditions.
- These experiments used weak polarized light pulses at 633 nm, with a low data rate of 1 bit/s $^{-1}$ and system errors of less than 0.5% for 10 m of fiber. However, the interesting feature is that polarization compensation was performed electronically, rather than manually. The authors state that they plan to use longer wave-

lengths in the future and that a system with a raw data rate of 100 kbit/s^{-1} (also to include error removal and privacy compensation) is under construction [85].

- These experiments ran a system based on standard optical communication fiber and components. Rather than polarization, phase states of weak light pulses at $1.3\ \mu\mathrm{m}$ were employed, with system errors of 5% for 10 km of fiber. Sequences of $\sim$ 150 bits were sent in 0.002 s long bursts; this would equate to a raw data rate of about 75 kbit/s^{-1} if continuous transmission is achieved [86].
- Reference [75], cited earlier for a number of practical considerations, is predominantly a review paper. However, in addition the authors discuss preliminary EPR pair phase interferometry experiments. High visibility nonlocal interference fringes were seen with interferometers separated by 4.3 km of standard communication fiber. The EPR pairs were produced by downconversion of a laser in a nonlinear crystal. This produces two photons (of different wavelength) entangled in phase rather than polarization. (However, the form of the state is still that of (9), simply with a change of label.) The photon wavelength relates to its angle from the initial laser beam, so the two different photons can be selected according to their direction of propagation. The short wavelength 820 nm photons were measured local to production (by Alice) and their longer wavelength $1.3\ \mu\mathrm{m}$ partners, which propagate better, were sent down the fiber (to Bob). The fact that good fringes were seen corresponds to a verification of the perfect correlations present in an entangled state, *both* photons in state $|\updownarrow\rangle$ or *both* in $|\leftrightarrow\rangle$ in the language of (9). These perfect correlations alone do not imply a violation of Bell's locality constraint; see Section II-D. However, they are strongly suggestive of entanglement and they are the necessary ingredient for use in cryptography. All this therefore bodes well for future EPR pair cryptosystems.

D. Patents

Three patents have been granted in this area and others may well be pending.

- With respect to current experimental systems, this is the main patent. The implementation described uses phase bases of weak coherent light pulses and interferometers. The examination of the RQT for eavesdropping, the error elimination technique and privacy amplification are mentioned [87].
- This patent is concerned with a different eavesdropping detection technique. Although Alice and Bob do not use data taken with *different* bases in the RQT, they can examine these data for evidence of eavesdropping [89], rather than use some of the RQT. The implementation described uses polarization bases of single photons [88].
- This patent covers the use of the nonlocal correlations between EPR pairs for key transmission. The implementation described uses phase bases of entangled photon pairs and interferometers. Polarization bases of weak pulses of light are mentioned as an alternative realization [90].

V. Quantum Computation

A. The Idea

There are two significant aspects of classical computation which feed into the idea of quantum computation, the Church–Turing hypothesis [91], [92] and the concept of reversible computation [93], [94].

The first is embodied in Turing's proposal of a simple model computer (the Universal Turing Machine) which could be programmed to perform any operation that might be regarded as computable. The machine consists of a potentially *infinite tape* on which resides a sequence of bits and a *head* which executes the computation. The head processes the bit value at its location together with the finite state of its internal memory, following some specified logical operation. According to the results, it resets the tape bit (to one or zero), resets its internal memory and hops one bit to the left or right on the tape, or stays where it is. (All this is repeated. The sequence may or may not terminate; this depends on the computation.) According to the Church–Turing hypothesis, such a machine can execute any algorithm and so is able to model any classical computer. In this mathematical sense, all existing computers are equivalent. Of course, this says nothing about speed, memory capacity, fancy graphics capabilities and suchlike, which are the quantities that continue to improve and thus sell new machines.

The idea of reversible computation was introduced mathematically by Yves Lecerf [93] in 1963 and placed on a more physical footing by Charles Bennett [94] in 1973. Conventional operations like AND or OR are irreversible. They must be because with two inputs and one output, the inputs cannot be inferred uniquely from the output. Even at the classical level this irreversibility cannot be ignored. Any *physical* realizations of such processes will cost. They will dissipate energy somewhere; the Second Law of Thermodynamics cannot be beaten. The entropy change associated with the erasure of a bit is $\Delta S = k \ln 2$ (see the Appendix). At a temperature T, this costs an energy $\Delta E = T\Delta S = kT \ln 2$ [95].

To avoid this dissipation, reversible operations must have the same number of outputs as inputs. Since throwing away your garbage costs, you have to keep it [95]. An example of a reversible operation is the controlled-NOT, or exclusive-OR (XOR), denoted by C_{12}. This has two inputs and outputs; bit one (with value ϵ_1) is the *control* and bit two (with value ϵ_2) is the *target*. The operation negates ϵ_2 if $\epsilon_1 = 1$ and leaves it alone if $\epsilon_1 = 0$. Expressed in state notation (ready for the quantum case), this operation is

$$C_{12}|\epsilon_1\rangle_1|\epsilon_2\rangle_2 = |\epsilon_1\rangle_1|(\epsilon_1 + \epsilon_2) \bmod 2\rangle_2. \qquad (11)$$

For classical computation, when the bits are classical and thus exist in definite states (zero or one), there are four possible inputs each of which has a unique output. (For example, $C_{12}|1\rangle_1|0\rangle_2 = |1\rangle_1|1\rangle_2$.) The point about elementary gates such as classical XOR is that many of them can be combined to perform *reversible* classical computations; they can be used to construct a reversible Turing machine [96], [97].

Suppose that such a machine is employed to calculate a function of a variable x, which ranges $0 \rightarrow 2^{m-1}$. This function, $f(x)$, ranges $0 \rightarrow 2^{n-1}$, so the computer needs a register of size $(m+n)$ bits to hold all the data. (It will almost certainly need some additional bits for processing.) As far as the calculation is concerned m bits can be deemed the input register (i) and n bits the output (o). However, as far as the physical evolution is concerned, the whole register is updated reversibly to its new set of values. The function calculation, denoted by the operator F applied to the decomposed register state, is represented by

$$F|x\rangle_i|0\rangle_o = |x\rangle_i|f(x)\rangle_o. \tag{12}$$

In this symbolic reversible classical computation *one* of the 2^m possible inputs $|x\rangle_i$ is prepared and F generates the corresponding output, $f(x)$, putting this in the output part of the register which was set initially to zero. In this example the input value x has been kept in its register. This is not always necessary to ensure reversibility. If $f(x)$ is a simple monatonic function of x (for the range of interest), there is then a one-to-one relationship between $f(x)$ and x and there is no need to keep x. However, if there is no such one-to-one relationship and the definition of the inverse of f is ambiguous, it is necessary to keep a record of x to ensure reversibility. Shor's quantum factoring algorithm utilizes a *periodic* function $f(x)$. Anticipating this, I have kept the input x in (12).

The subject of quantum computation began its development about 15 years ago. Notable contributions came from Paul Benioff [98], Richard Feynman [99], [100], David Albert [101], and David Deutsch [102]. Good discussions are given at an introductory level in [13], [55], [95], [103], [104] and at a higher level in [105]–[107]. (Further work can be accessed via the WWW addresses given in the introduction.)

In his work, Deutsch basically modified the Church–Turing hypothesis to allow for physics [102]. This is, of course, an eminently reasonable thing to do since *any* computer which is ever built will be made out of stuff which obeys the laws of physics. Deutsch's version of the Church–Turing hypothesis is [102]:

> Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means.

Here, in cases when the physical system demonstrates some intrinsically quantum mechanical property, such as superposition of states, the Universal Turing Machine (UTM) cannot perform the simulation since it is based on the classical tenet of systems being in definite states. A generalization, the Universal Quantum Computer (UQC) [102], is needed. In the same sense that any classical computer is equivalent to the UTM, it is thought that any possible quantum computer will be equivalent to the UQC. However, this is not known; it is still an open problem [106].

Analogous to the construction of classical computers from a number of elementary classical logic gates, the idea is that quantum computers could be constructed from elementary reversible quantum logic gates [108]–[112]. This is why reversible classical gates are of such interest, for it is quantum versions of *these* which form the potential building blocks for quantum machines. (There is clearly no point in trying to construct a quantum version of a process which by its definition is irreversible even at the classical level.) The quantum XOR operation forms a very important elementary quantum gate [13], [105]. *Superposition of states* is the key phenomenon exhibitable by qubits but not by classical bits. The quantum XOR process can utilize this in a highly nontrivial fashion. It therefore forms a good centerpiece for a discussion of quantum computation.

In the classical case, the input to XOR must be one of four possible combinations of bit one and bit two values. In the quantum case, the superposition property makes this range of choice *infinite*. For instance, bit one alone can be in an arbitrary superposition of $|0\rangle_1$ and $|1\rangle_1$, as in (2). This is the crucial point because it enables XOR to turn *single product* states of the two qubits into *entanglements*; for example

$$C_{12}2^{-1/2}(|0\rangle_1 + |1\rangle_1)|0\rangle_2 = 2^{-1/2}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2). \tag{13}$$

(Note that there is no change in the operation defined by (11), it is just that now it must be applied term by term to the quantum states.) As will be seen, it is the ability to produce entangled final states which gives quantum computers their crucial advantage over classical ones. The reversibility of XOR also means that it can be used for disentangling states:

$$C_{12}2^{-1/2}(|0\rangle_1|0\rangle_2 \pm |1\rangle_1|1\rangle_2) = 2^{-1/2}(|0\rangle_1 \pm |1\rangle_1)|0\rangle_2 \tag{14}$$

$$C_{12}2^{-1/2}(|0\rangle_1|1\rangle_2 \pm |1\rangle_1|0\rangle_2) = 2^{-1/2}(|0\rangle_1 \pm |1\rangle_1)|1\rangle_2. \tag{15}$$

A pictorial representation of the XOR gate is given in Fig. 2. State swapping is also possible [105]. Three XOR operations yield

$$C_{12}C_{21}C_{12}|\psi\rangle_1|\phi\rangle_2 = |\phi\rangle_1|\psi\rangle_2 \tag{16}$$

for arbitrary states $|\psi\rangle$ and $|\phi\rangle$. I reiterate that the qubits in these examples must be quantum systems, so they can be placed in superpositions or entanglements *and* that the operation of XOR must be a reversible quantum evolution according to the Schrödinger equation (3); C_{12} must be realized by the Hamiltonian of the physical XOR gate. The irreversible effects of the gate environment, including any measurement apparatus, must be negligible during the operation.

However, this is not all. To construct a quantum computer from such reversible quantum logic gates [108], [111]

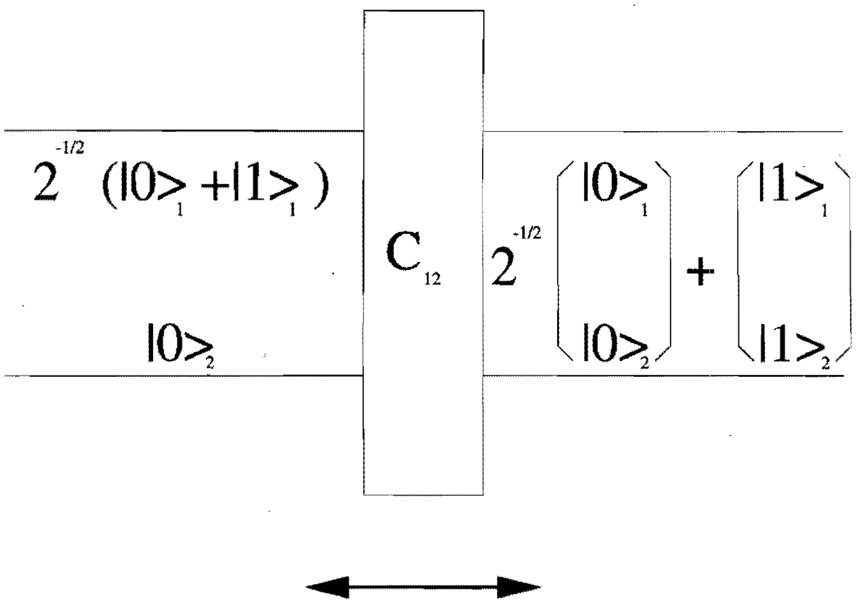

Fig. 2. The XOR gate applied to two qubits. The right hand state is entangled; it is not possible to associate a definite state with one qubit independent of the other one, as is the case for the left hand side. The *reversibility* of the gate means that it can be run left to right *or* right to left.

and to utilize the superposition principle, the effects of the environment must be small enough so that the *whole* computer evolves in reversible Schrödinger fashion, as dictated by the Hamiltonian of the complete machine. Furthermore, this must be the correct Hamiltonian; it must not contain imperfections which generate the wrong reversible evolution. These are both extremely tough requirements and they are considered in Section V-C. For the moment, assuming that they can be met, consider the example of a *quantum* calculation of $f(x)$ [analogous to the classical version of (12)]. Suppose that this is performed with the initial state of the m-qubit part (the calculation input) of the $(m+n)$-qubit register prepared as a *superposition of all possible classical inputs*

$$|\psi\rangle_i = 2^{-m/2} \sum_{x=0}^{2^m-1} |x\rangle_i. \tag{17}$$

The $2^{-m/2}$ is for normalization; there are 2^m terms in the sum. This preparation is not as daunting as it might appear. If each of the m qubits is simply prepared in the superposition state $2^{-1/2}(|0\rangle + |1\rangle)$, the single product of all these contains the 2^m states $|x\rangle_i$ with equal amplitude $2^{-m/2}$, as required. The calculation of f gives

$$F|\psi\rangle_i|0\rangle_o = 2^{-m/2} \sum_{x=0}^{2^m-1} (|x\rangle_i|f(x)\rangle_o). \tag{18}$$

The final state is an entanglement of the so-called input and output parts of the $(m+n)$-qubit register. It looks as if the computation has evaluated all 2^m possible values of $f(x)$ in one run!

B. Possible Uses

In fact, computing functions is an example for which quantum machines do no better than classical ones. Despite the final entangled state in (18), you cannot access all the different values of $f(x)$. The only way to get information out of the quantum computer is to perform a *measurement*, of f in this case. For example, if all the 2^m values of f are different, a measurement of f will yield *one* of these at random, each with a probability of $1/2^m$ for the state (18). At the same time the state will be projected to the single term in the superposition corresponding to this outcome. The irreversibility of the measurement process destroys the information about all the other values of $f(x)$.

In a sense, simply quantum computing a function is a challenge to classical machines on their own patch. However, quantum computation has the potential to expand this patch and give access to solutions of some problems which are intractable with classical machines. A difficult problem is deemed classically tractable if the time taken to solve it scales only as a polynomial function of the size of the input. It is deemed classically intractable if this scaling is given by an exponential function. This is where quantum machines can come into their own. Examples of such problems might be the evaluation of some property of f, or the verification of a statement about f. For either problem, all the (2^m for the case above) individual values of f do not form part of the answer. Nevertheless, the classical approach involves calculating all (or possibly most) of them one by one in order to distil the actual answer required. On the other hand, the superposition state (18) of the quantum computer contains amplitudes for all the f values. If this can be manipulated in some way so that some chosen measurement on the new final state will answer the problem posed, then clearly the solution can be found much more quickly via the quantum route. The manipulation followed by the irreversible measurement will certainly destroy the information on all the f values, but this does not matter as they are not the answers required. Another way of viewing this exponential speeding up of the calculation is to regard the 2^m calculations as running in parallel, producing the solution through quantum interference [13], [106].

1) Period Finding: One very useful problem which can be solved this way is finding the period of $f(x)$ when it is a periodic function of its argument x [105]–[107]. To achieve this, three further stages of manipulation must be applied to the state (18) of the quantum register: 1) an irreversible measurement (of f), followed by 2) a reversible quantum operation (a Fourier transform), followed by 3) a final irreversible measurement. The periodicity means that a measurement of f must leave the *calculational input* part of the register state as a superposition of $|x\rangle_i$ states where the x values are spaced out by r, the period being sought. A discrete quantum Fourier transform then takes this state into a new basis in the space of possible (reciprocal) periods and in this basis the amplitude of the state peaks sharply around multiples of $1/r$. This is analogous to the Fourier decomposition of a (time-dependent) musical note in the frequency, or reciprocal period, domain. When analyzed in the latter domain, the note exhibits peaks around its fundamental frequency (reciprocal period) and the higher harmonics, which are multiples of this. The final problem solving measurement on the quantum register is done in the reciprocal period basis. From this result (or, more correctly, the results of a few runs), the period r may be determined.

Here is a simplified outline, based on the assumption that r divides the input register range 2^m ($\equiv q$) exactly [105]–[107].

1) A measurement of f applied to the state (18) removes the entanglement. It gives some result f_0 and projects the state of the register to a *single product* of an input and an output state. The output part of the register state is $|f_0\rangle_o$ and the input part is a superposition of all the states $|x\rangle_i$ whose x-value satisfies $f(x) = f_0$. This can be written as

$$|\phi\rangle_i = \sum_{x=0}^{q-1} g(x)|x\rangle_i \tag{19}$$

where the coefficient $g(x)$ is simply defined to pick out the (q/r) values of x for which $f(x) = f_0$. This can be expressed mathematically as

$$g(x) = (r/q)^{1/2} \sum_{j=0}^{(q/r)-1} \delta_{x,jr+l} \tag{20}$$

where l is some unknown offset and $\delta_{a,b}$ is *zero* if $a \neq b$ and *unity* if $a = b$. As the entanglement has gone and no further interaction occurs with the output part of the register, this can now be ignored.

2) The next stage is a (discrete) Fourier transform, which effects a change of basis from the q states $|x\rangle_i$ to the q new ones $|k\rangle_i$. These relate to each other by

$$\begin{aligned}|x\rangle_i &= q^{-1/2} \sum_{k=0}^{q-1} \exp{(2\pi ikx/q)}|k\rangle_i \\ |k\rangle_i &= q^{-1/2} \sum_{x=0}^{q-1} \exp{(-2\pi ikx/q)}|x\rangle_i. \end{aligned} \tag{21}$$

Physically, this requires reversible quantum operations to be applied to the m qubits of the i-register so that the final q ($= 2^m$) binary register possibilities correspond to the q different states $|k\rangle_i$ in the same way that the initial ones corresponded to the $|x\rangle_i$. It is worth noting that this transform can be applied to the register through a series of simple one- and two-qubit operations [113]. A good approximation to it is also possible, with a significant reduction in the required number of simple operations [113]. If the qubit operations to effect the transform are made when the register state is $|\phi\rangle_i$ of (19), this will end up expanded in the $|k\rangle_i$ basis (denoted by a tilde) as $|\tilde{\phi}\rangle_i = \Sigma_{k=0}^{q-1} \tilde{g}(k)|k\rangle_i$ where the amplitude $\tilde{g}(k)$ is

$$\tilde{g}(k) = q^{-1/2} \sum_{x=0}^{q-1} \exp{(2\pi ikx/q)} g(x). \tag{22}$$

Given the form (20) of $g(x)$, it follows that $\tilde{g}(k) = r^{-1/2} \exp{(2\pi ilk/q)}$ if $k = \lambda(q/r)$ for the r possible values of $\lambda = 0, 1, \cdots r-1$, and zero otherwise.

3) The final "problem solving" measurement of k will therefore yield one of the $\lambda(q/r)$, a multiple of (q/r), each one occurring randomly with a probability $1/r$. Note that the unknown offset l has no effect on this. Given that q ($= 2^m$) is known, the desired period r can be found from q and a few values of $\lambda(q/r)$.

2) Factorization: Being able to find the period of a function is a very handy facility to have because other problems can be reduced to this one. The most spectacular use for a quantum computer which has been proposed to date is based on such a reduction. There is no known efficient classical algorithm for factorizing large composite integers. However, Peter Shor has shown how a quantum computer could potentially perform such a task [114], [13], [105], [106]. The quantum part involves finding a period as outlined above; the rest is number theory, with these calculations being tractable on a conventional classical computer. If the (large) number to be factorized is N, another number y, coprime with N, is chosen at random. The periodic function is defined by

$$f_N(x) = y^x \bmod N. \tag{23}$$

This means evaluate y^x modulo N, so f only takes values between zero and $N-1$. The way to check the coprime condition is to verify that the greatest common divisor of y and N is unity, $\gcd{(y, N)} = 1$. This can be done easily with Euclid's algorithm for finding gcd of two numbers [106]. Of course, if, having chosen a y at random, you find that $\gcd{(y, N)} \neq 1$, this is not a problem as you will have found a factor of N anyway. Choosing y coprime with N guarantees that f is periodic; otherwise it may not be.

A nontrivial factor of N can be deduced from r, the period of $f_N(x)$. Here is a sketch of the argument [105]–[107]. If y is coprime with N it is possible to define an exponent r so that $y^r \bmod N = 1$. From the form of (23) it is then clear that $f_N(x+r) = f_N(x)$, so r is the desired period. Setting $z = y^{r/2}$ (which requires an even r) means that finding r, the result of the quantum computation, finds solutions to $z^2 \bmod N = 1$. These might be trivially given by $z \bmod N = 1, N-1$; if so they are no use. However, if the solutions are *nontrivial* and so take the form $z \bmod N = c, N-c$ with $c > 1$, they can be used to find factors of N. In this case it is certainly true that $c-1 \neq 0$ and $c+1 \neq N$, but that $(c+1)(c-1) \bmod N = 0$. Thus $(c+1)(c-1)$ is a multiple of N, although neither $(c+1)$ nor $(c-1)$ are on their own. The greatest common divisor of N and $(c \pm 1)$ therefore cannot be N; instead it will be a nontrivial factor of N. So, finding r (by quantum computation) gives z which gives c which gives factors of N from $\gcd(c \pm 1, N)$. Clearly, the method fails if r is odd or if c turns out to be one or $N-1$. In such a case a different random y must be chosen. However, the probability of failure is small for random y [106].

A simple example should help. To factorize $N = 15$, not exactly a difficult task, a coprime y is needed so $\gcd(y, 15) = 1$. This means that y can be picked from the set $\{2, 4, 7, 8, 11, 13, 14\}$. Take $y = 8$. The values of $8^x \bmod 15$ for $x = 1,2,3,4,5,6,7\cdots$ are $8,4,2,1,8,4,2\cdots$, so the period is $r = 4$. This is what the quantum computer would find; for a useful calculation using a very large N the period would also be very large. Here, $y^{r/2}$ gives $z = 64$ and thus $c = z \bmod N = 4$. In this case $c \pm 1$ *are* the two factors of 15. Alternatively, $y = 11$ yields $c = 11$ and the factors follow from simple calculations of $\gcd(10, 15)$ and $\gcd(12, 15)$. The only choice of y which fails is 14, illustrating the good chance of the method being successful.

It should be noted that the quantum manipulations needed for this period finding are not simply assumed to be implementable. As well as those for the discrete Fourier transform, the elementary quantum gate layouts and operations for the modular exponentiation have actually been worked out, so, in effect, the blueprint for a quantum factoring machine exists [115], [55], [116], [113], [117]. The factorization of large integers is clearly a very important issue. RSA, the most popular public key cryptosystem [63], [64], is based on this being a very hard problem. The construction of a quantum computer capable of rendering such factorization tractable would ruin RSA as a cryptosystem. This might even generate a market for quantum cryptosystems!

Since the central manoeuvre in the quantum period finding procedure is a Fourier transform, it is interesting to ponder on the possibility of performing this transform by *classical* wave means, or by a *simulation* of such an approach. Is a quantum machine really needed? In fact it is, because to solve a realistic problem, to factorize a *large* composite number, the period sought will be exponentially large. This can only be handled in some internal abstract Hilbert space of a quantum machine; to deal with such a period in the physical space of a classical wave experiment, or a simulation thereof, is totally implausible [13].

The discrete logarithm problem—for integers y, N, and a, find x such that $y^x \bmod N = a$—can be reduced to a period finding problem [13] in a similar fashion to the factorization problem, and so forms another example amenable to quantum computation. Further suggestions and discussion can be found in [102], [103], and [118], for example. However, probably the most important point to note is that, despite the early days, such suggestions are being made. It seems likely that more will follow.

C. Practicalities and Possible Realizations

Hypothetically, there is no problem in putting together elementary quantum components, or gates, to form a computer [108], [109]. On paper, it should be possible to devise complex systems, or networks, whose total Hamiltonian gives a Schrödinger evolution [see (3)] which will perform a desired quantum computation. As already mentioned, this has been done for the quantum factoring case. However, the *physical construction* of these systems is a different matter. This should not be regarded as a very difficult but definitely tractable problem. Theoreticians should not sit around with their feet up drinking coffee simply waiting for the experimenters and engineers to crack this one, and many do not.

In this context, the physical nature of *all* information processors and indeed the physical nature of information itself, has long been stressed by Rolf Landauer. (For a recent paper, see [119], which cites some of his earlier work and many other useful references.) With respect to quantum computation, there are two main problems, mentioned at the start of Section III and now considered in a bit more detail in the next two subsubsections.

1) Incorrect Reversible Evolution: The continuously variable and numerous amplitudes in complex quantum states (i.e., of a system containing many qubits), while giving great power to computers based on quantum parallelism, may also be a reason for them never being built. In a sense, the continuous amplitudes give quantum computation the same problem [120] as analog computation: more power, but more susceptibility to imperfections. An unwanted piece in the system Hamiltonian will generate an unwanted "error" piece in the evolved state.

A trivial example of this is the fixed birefringence for a photon; if ϕ is a small ($\ll 1$) nonrandom phase in (5) the error piece is approximately $2^{-1/2} i\phi|\updownarrow\rangle$. Here it is obvious that such an error can be removed. Quantum cryptography experiments can deal with a fixed birefringence. However, while these experiments may deal with a large number of photons, these are *independent* qubits; they do not interact. In a complex system like a computer, containing many *interacting* qubits, the error problem is greatly amplified.

There are many more starting points for such errors.[6] As well as effects like fixed birefringence, which could be deemed as due to errors in the construction of the system, external electromagnetic pulses applied to the system could be incorrectly shaped or timed. These errors build and interact in time. In an extreme case, such errors can actually conspire to cause a *reversal* of the intended evolution [119]; dramatic erroneous quantum interference occurs.

2) Decoherence: In general, the bigger a system gets, the harder it becomes to keep the environment at bay. Large and complex quantum systems can usually only keep their coherence for short times. Then their evolution becomes irreversible and superposition states are destroyed. This is, of course, why the macroscopic world looks classical rather than quantum. One obviously important example of a decohering environment is a heat bath, or reservoir; for discussions in the context of quantum computation see [106], [121], [122]. The state of a quantum system coupled to such an environment gets scrambled and the system acquires a finite entropy as it reaches thermal equilibrium. (See the appendix.) To avoid (or at least to minimize) such irreversibility, thermal decoupling is necessary.

If the time taken for a system to perform some typical simple reversible quantum process [such as the XOR operation given by (13)–(15)] is t_c, and the time taken for the environment to mess up the quantum state is t_d, then the bottom line is that $t_d \gg t_c$ must hold for the process to be able to occur. The *decoherence time* must be long compared to the *clock time*; this is true for quantum processes in general and a quantum computation would be no exception [106], [107], [121]–[124].

This condition can certainly hold true for the candidate quantum systems given in Section III, as they execute a *single* logic operation; indeed, this is why they made the list. (Detailed discussion, including numerical estimates of t_d and t_c for certain candidates, is given in [123], for example.) However, the problem is that for complex systems containing many elementary quantum gates, t_c increases and t_d decreases. The former is due to the facts that many gates are required to carry out a number of logic operations [117] and that the time for a single operation will generally increase for a gate which is part of a larger system [124]. For the latter, simple theoretical models [122], [125] suggest that t_d for n coupled systems is n times smaller than that for one. This is all a big worry. Will it be possible to make quantum machines for which t_d is still in excess of the t_c value for any useful task, such as factorizing a large composite number? This is a question currently under debate [121], [124], [126]. While no clear cut answer exists, I think it is fair to say that achieving practical success will be extremely difficult in the near future. For example, the clock time for the factoring of an L-bit number could scale like L^6 up to L^8 (dependent upon the precise realization of device considered) [124]; this would compete fiercely with the decoherence time of the device as L is increased.

A point on which there is some consensus is that a real thorn could be the spontaneous emission of photons—in fact *one* could be enough—from any quantum computer which utilizes excited states of elementary systems [124], [126], [127]. While other environment effects may be down directly to the skill of the quantum engineers, *fundamental* decohering effects like spontaneous emission are rather harder to control.

Problems may also arise if what could be termed *intrinsic* state collapse or localization exists. State collapse might possibly occur in nature as a *fundamental process*. If so, reversible quantum theory is only ever an approximation to what happens in the irreversible real world, good when the irreversibility is very small. Intrinsic collapse could be regarded as an essentially uncontrollable decohering effect on a quantum computer [128].

3) Error Correction: One interesting idea, which might assist a quantum computation by staving off the effects of errors and decoherence, is the possibility of error correction. The concept is the same as in classical error correction, or the operation of a refrigerator. As the *system of interest* suffers an unwanted increase in entropy (see the Appendix), this is extracted, but at the expense of increasing the entropy somewhere else. It is clear that for quantum systems this must be a tricky procedure, unlike typical error correction applied to classical data. In the case of quantum cryptography, Eve has already found to her cost that it is impossible to simply inspect a qubit without irreversibly changing it. Nevertheless, this does not preclude all forms of tinkering.

The "Zeno" or "watchdog" effect, where repeated measurements keep projecting a system state back into some chosen basis, might be usable as a technique for eliminating small errors as they creep into a quantum state [121]. The "Zeno" effect is a statistical one; on average, repeated measurements could be arranged to retard the unwanted evolution of a system away from its intended state. In terms of the behavior of *individual* systems [129], this means that the actual state would irreversibly project onto the intended one with a probability close to unity. Occasionally, though, the projection would be to a totally unwanted orthogonal one. In such cases the attempted correction completely ruins the computation! However, on average the procedure would be beneficial.

Another possibility is to build in redundancy, in the same spirit as is done in classical error correcting theory. The extra qubits, along with judiciously chosen interactions and measurements, can then be used to stabilize the "important" qubit states against errors. Many papers have appeared recently on this subject; some examples are [130]–[135] and many more can be found at the WWW addresses given in the introduction. Here are some interesting points.

- If decoherence simply acts to dephase the amplitudes in a qubit state, like in the example of (5) with a *random* phase ϕ, this error can be corrected if the state is encoded into a state of three qubits [134]. Loosely speaking, this is because a phase error looks

[6] The general form of a single one, due to a small error term H_e in the Hamiltonian, follows from footnote one. If $H = H_c + H_e$, where H_c is what H is supposed to be, the evolved state is approximately $|\psi(t)\rangle \approx |\psi_c(t)\rangle - (i/\hbar)U_c \int_0^t dt' H_e|\psi(0)\rangle$. The first term is the intended state and U_c is the intended evolution operator. The second term is the unwanted "error" amplitude.

like an amplitude error in a rotated basis, the diagonal decomposition of (6). (The extreme case is a phase error of π in the rectilinear basis; this gives a complete amplitude error in the diagonal basis as it flips the qubit from $|\swarrow\!\!\!\!\!\nearrow\rangle$ to $|\nwarrow\!\!\!\!\!\searrow\rangle$.) Three qubits is the minimum number required to correct such an error [134].

- A general decoherence error in a qubit state can be thought of as a random phase error *and* a random amplitude error *in the same basis*. Two extra qubits are needed to cope with each of these, so the minimum encoding of a single qubit against an *arbitrary* decoherence error needs five qubits [135].
- Provided that the error correction procedures do not themselves introduce too much additional decoherence, it seems possible that an exponential decrease in decoherence can be achieved with only a polynomial increase in resources, at least in certain model systems [132].
- When a qubit state is encoded into a number of qubits, these are also *all* assumed to decohere in a similar fashion. (It would be unrealistic to assume anything less and it would perhaps be more realistic to assume even more.) Any correction ideas, even for encoding much more complicated states with some redundancy, have to confront the additional decohering onslaught and win out.

Most of the work on quantum error correction to date has focused on preserving the state of a number of qubits. This may well be all that is needed to make use of error correction for "memory" qubits in a quantum computer, or to extend transmission distances for states being used in quantum cryptography. Correction of evolving and interacting "processor" qubits in a computer is clearly going to be rather more tricky, if at all possible. People have begun work in this direction, considering logical operations applied to encoded qubits [136] and correction applied to entangled qubits [137]. However, it is not clear that the current error correction approaches can deal with incorrect reversible evolution of a complex quantum computer [119]. Indeed, they could make it worse because a lot more qubits (for redundancy) and hardware (to support them) introduced to correct errors due to decoherence could introduce more Hamiltonian imperfections. Quantum errors and their correction are very interesting and active areas of debate and research.

4) Experimental Possibilities: The construction of an experimental prototype, even just a simple one, to examine the viability of useful quantum computation, is still some way off. The current state of play is that proposals for physical realizations of individual quantum gates have been and are being made. Many fundamental experiments on these systems have been done, many more are underway and there are reports of a successful implementation of a single two-bit logic gate [127]. The coupling together of a number of such gates is the next experimental challenge; theoretical work on this is already in progress. This is why the example of the factorization of 15, given earlier, is not quite as daft as it might seem! The first quantum machines are likely to consist of a nontrivial but not large number (perhaps 20 $\sim$ 30) of qubits, so will only be capable of this level of task. Similarly, the simulation of such a machine on a *classical* computer, including physically realistic decohering effects and measurements, will be limited to this sort of scale.

I will outline some proposals for quantum gates and give references where more detail can be found. Section III identified that candidates for gates should have discrete quantum states which are somewhat robust against their environment. In the light of the Section V-A consideration of a model quantum gate (the XOR), another requirement can be added. The systems must be able to exhibit conditional and controllable dynamics. The behavior of the target qubit must *follow* from the control qubit.

- *Atoms and Photons* [12], [41]–[45], [105], [106]. To make an XOR gate, the target qubit states are two relevant Rydberg atom states (Section III-B) and the control qubit is a mode in a cavity (Section III-A) whose photon number is zero or one. The atom interacts with the photon as it passes through the cavity. This interaction is purely dispersive and generates a phase shift for the overall quantum state. The additional application of classical microwave pulses either side of this can fix it so that the atomic state flips or is unchanged dependent upon the photon number and without changing this number, as must happen for the control bit.

  A schematic illustration goes as follows. The microwave pulses, $M_{\pi/2}$, are so-called $\pi/2$-pulses which partially rotate the atom states into each other: $M_{\pi/2}|0\rangle_2 = 2^{-1/2}(|0\rangle_2 + |1\rangle_2)$ and $M_{\pi/2}|1\rangle_2 = 2^{-1/2}(|1\rangle_2 - |0\rangle_2)$. (Two consecutive $\pi/2$-pulses form a π-pulse, which completely flips the state; $M_\pi|0\rangle_2 = |1\rangle_2$ and $M_\pi|1\rangle_2 = -|0\rangle_2$.) The dispersive atom-photon interaction in the cavity simply performs a phase shift P: $P|0\rangle_1|1\rangle_2 = -|0\rangle_1|1\rangle_2$ with all other combinations unchanged. Sandwiching P between two $\pi/2$-pulses implements an XOR process; $C_{12} \sim M_{\pi/2}PM_{\pi/2}$. (There are a couple of sign changes compared to the earlier definition of C_{12}, but these do not affect the basic idea.)

  In effect, the phase shift enables the second microwave pulse to *undo* the first when the control bit is zero, otherwise the two pulses *combine* to produce a flip. The operations of (13)–(15) are thus realizable. The current state of play with experiments is that they are just about there. The microwave pulses are old hat; the phase shift for very weakly excited cavities is rather harder but is now possible [43]. An experimentally feasible implementation of the XOR process using atomic beams and cavities is discussed in [44] (in the context of teleportation). It seems clear that the environment can be kept at bay sufficiently for individual atomic quantum gates to operate. However, what is not clear at present is the number of such gates which might be able to sustain a useful reversible quantum interaction within the coherence time t_d of the whole coupled system. No doubt this will be a topic of future research.

Progress has also been made up at optical frequencies [45]. Conditional phase shifts for a coupled cesium atom and high-Q optical cavity (with a photon number less than unity) have been measured [45]. These could form the basis for a quantum-phase logic gate.

- *Interacting Dipoles* [55], [105], [106], [138]–[141]. The dipoles could be electric or magnetic. In the electric case, an electron trapped in a quantum dot (Section III-C) forms a dipole moment (along with its image hole charge). This interacts with the moment of a similar adjacent dot. Each dot forms a qubit if only the lowest two energy levels come into play. This should not be a problem. An electron in a dot is similar to the model quantum problem of a particle in a box. Here the energy level *spacing* increases with increasing energy, so the lowest two levels are closer to each other than they are to any of the higher levels. The key is that the qubit levels are shifted by the dipolar coupling, so that the separation between the two levels of the target dot two depends on the state of the control dot one. Thus an external classical electromagnetic pulse (a π-pulse M_π defined above) from a laser will flip the state of dot two, or not, dependent upon the state of dot one, which is unaffected by the pulse. For a quantum system, a *resonant* transition between two energy levels can occur if the external pulse frequency equals that set by the difference between the levels. Transitions are strongly suppressed if these are unequal. Dot one thus dictates whether or not dot two is resonant with the external pulse. This realizes the XOR process. Current dot and laser technology is such that up to 10^4 individual dot operations might be possible before decoherence takes over [106]. However, as for atomic gates, it is not clear just how many dots could be coupled together in a controlled and coherent manner. Once again, this is work for the future.

  In the magnetic case [55] the two interacting dipoles could be those of fundamental particles such as atomic nuclei (Section III-D) or those of small superconducting circuits (Section III-E). The implementation of the XOR process is analogous to the electric case but with magnetic dipole interactions generating the level shifts. For nuclei, fabrication of controllable systems may not be so easy and decoherence in such fabricated arrangements might be a problem. These two problems can probably be overcome in the superconducting circuit case. Here, however, the interaction between two circuits might be tricky.[7] Experimental work on the application of controlled microwave pulses to superconducting quantum circuits is also much less advanced than say that on atoms in beams.

  At present, quantum dot nanotechnology looks to be the best bet for interacting dipole systems.

- *Ionic Crystal* [49], [50], [127]. Rather than just couple two qubits to form an XOR gate, n qubits could be interconnected if these are ions in a tiny crystal (Section III-B). One such system could even form a computer if n is big enough! The lowest two energy eigenstates of each ion represent the bit values. The ions interact via the crystal vibrations. Within the crystal, the average ionic separation is a few optical wavelengths (the appropriate wavelengths for coupling between the two energy levels of an ion) and so it is realistic to consider targeting individual ions with laser pulses fed in from outside. In a similar manner to the atom and dipole cases, the conditional dynamics arises from laser pulses in combination with ion-ion interactions. In principle, the XOR operation can be implemented, where the target ion state flips only if the control ion is excited [50]. In addition, more complicated n-bit operations can be performed [50]. In current experiments decoherence times for ions in traps can be very long and single ions can be probed accurately with external lasers. The extension to the n-ion case thus looks to be feasible; [50] discusses some model calculations for eight Ba^+ ions in a trap. The adaptation of an ion trap experiment to demonstrate the conditional dynamics of the XOR process has recently been reported [127]. In fact, this used the internal and external degrees of freedom of *one* ion for the two qubits. The next steps forward from this would appear to be the extensions to more qubits and more operations. This is also a very promising research avenue.

D. Patents

A current search reveals just one patent specifically for quantum computers [142]. It is extremely brief and indicates that such machines could be electronic, optical, chemical or biological in nature. No detailed description of a realization is given and (rather surprisingly) no reference is made to any published papers. At the *individual* quantum gate or device level there exists a vast array of patents.

VI. Quantum Teleportation

Teleportation is just one aspect of an area of quantum communication whose realization is somewhat further into the future, compared to basic cryptography. It relies crucially on Alice and Bob being able to share and store EPR pairs of quantum systems, such as the photon pair example of (9). Access to this facility would enable Alice and Bob to expand their cryptography business and offer other possibilities, such as teleportation and superdense coding. A short introduction to these phenomena is given in [143] and further discussion may be found in [13].

[7] The dominant interaction term between the two dipoles needs to be *diagonal* in the unperturbed energy eigenstate basis [105], [106]. This means that the unperturbed eigenstates must remain as eigenstates when the interaction is present. To a good approximation, this condition can be satisfied for the quantum dot and nuclear moment interactions, but it may not be for the conventional current-current magnetic interaction between two superconducting circuits.

The original reference for teleportation is [144] and for superdense coding is [145].

A. Teleportation

At a teleport, a customer would deliver to Alice a system—for simplicity assume that this is a single qubit—in an arbitrary quantum state. This state can be reproduced faithfully some distance away by Bob, assuming that he and Alice have previously shared an EPR pair of qubits. Only classical data is sent from Alice to Bob at this time; the customer's quantum state is teleported. This is a nontrivial feat, for note that Alice cannot simply make some measurement on the system and send the result to Bob. This would only work if the state is *known* to be *one* of a given basis set, if it is known to be an eigenstate of some operator. In this special case a measurement of the observable defining the basis will yield the appropriate eigenvalue, thus identifying the state. However, an arbitrary state would be a superposition in this basis. It would experience an irreversible projection upon measurement and the result of the single measurement will not identify the initial state.

This means that generally Alice is unable to infer by direct measurement the state of the system she is given. More than likely, she will have already destroyed this information. The damage to the customer's property would happen before transit, let alone during it! (Trying to do things this way, Alice is in effect playing the role acted by Eve in the cryptography situation.) The use of EPR pairs enables this problem to be avoided.

Suppose that Alice has qubit one of a pair and Bob has qubit two, for the state given by (9) with the notation $|\updownarrow\rangle = |1\rangle$ and $|\leftrightarrow\rangle = |0\rangle$. The unknown state of the customer's qubit three can be decomposed as in (2), $a|0\rangle_3 + b|1\rangle_3$ for some amplitudes a and b. The full state of the three particles is therefore the single product of qubit three with the EPR pair

$$|\psi\rangle_{123} = 2^{-1/2}(|1\rangle_1|1\rangle_2 + |0\rangle_1|0\rangle_2)(a|0\rangle_3 + b|1\rangle_3). \quad (24)$$

Alice performs a joint measurement (sometimes called a Bell measurement) on qubits one *and* three which involves use of the quantum XOR process of (13)–(15). This measurement can have one of four outcomes. These occur at random; however, this does not matter. Alice communicates the outcome to Bob using two classical bits. (Conventional classical error checking can be used to make sure that no mistakes occur.) Dependent upon Alice's message, Bob chooses one of four reversible quantum operations and applies it to his qubit two. This leaves qubit two in the unknown original state, ready to be handed over to the receiving customer at his end.

With the notation $|\Psi^{\pm}\rangle_{13} = 2^{-1/2}(|1\rangle_1|0\rangle_3 \pm |0\rangle_1|1\rangle_3)$ and $|\Phi^{\pm}\rangle_{13} = 2^{-1/2}(|1\rangle_1|1\rangle_3 \pm |0\rangle_1|0\rangle_3)$ the state (24) can be *rewritten* as

$$\begin{aligned}|\psi\rangle_{123} = &\tfrac{1}{2}\,|\Phi^{+}\rangle_{13}(a|0\rangle_2 + b|1\rangle_2) + \tfrac{1}{2}\,|\Phi^{-}\rangle_{13}\\ &\cdot(-a|0\rangle_2 + b|1\rangle_2) + \tfrac{1}{2}\,|\Psi^{+}\rangle_{13}(b|0\rangle_2 + a|1\rangle_2)\\ &+ \tfrac{1}{2}\,|\Psi^{-}\rangle_{13}(-b|0\rangle_2 + a|1\rangle_2). \qquad (25)\end{aligned}$$

Alice's Bell measurement is arranged to project onto one of these four terms; each happens with probability 1/4. In each case, Bob's qubit two is left in the appropriate state in that term. A simple reversible quantum operation on this state, the operation being chosen in the light of the results transmitted by Alice, can then leave qubit two in the original state of qubit three. For example, if Alice happens to project to the first term, Bob does nothing! If the projection is to one of the other terms then clearly a sign change and/or an interchange of the amplitudes a and b is required. In the case of photon polarizations, these operations can be achieved easily with combinations of half-wave plates [144].

Alice performs her Bell measurement by using the quantum XOR process of (14) and (15). She first applies the XOR C_{13} to qubits one and three to disentangle them. In the polarization language, Alice then measures qubit one in the diagonal basis and qubit three in the rectilinear basis. This yields one of four unique results, enabling her to identify to which of the terms in (25) her action has projected the state $|\psi\rangle_{123}$.

The initial nonlocal entanglement between qubits one and two is crucial to the success of the teleportation. This ensures that whatever outcome Alice's irreversible measurement causes at the transmitting station, there occurs a sympathetic change to qubit two which enables Bob to reform the original state upon receiving Alice's data. Note that although Bob already has his EPR qubit, he cannot recreate the state in advance of receiving Alice's data and so there is no instantaneous transfer of information. In addition, *no record* of the transmitting customer's state is left with Alice; the state is not copied or cloned. Alice must be left empty-handed because it is in fact impossible to clone a quantum state [146].

B. Superdense Coding

If there exists a good quantum channel between Alice and Bob—either the environment is quiet at the time, or they have a heavily shielded link—then they can also offer their customers superdense coding [145], [147]. Here, for every subsequent quantum system sent down the link *two* classical bits can be delivered.

Alice and Bob do things the other way around for coding. Alice uses the four possible reversible quantum operations Bob used in the teleportation. She applies one of these to her EPR qubit one, in order to encode two classical bits. She then sends this qubit to Bob. He performs a Bell measurement on this and his own EPR qubit two and from this extracts the two bits of classical data. The underlying physics for superdense coding is clearly the same as that for cryptography with EPR pairs; it is really just the application which differs. If secrecy is required, it is probably best to employ the cryptographic scheme and to use the EPR pairs to establish a key, rather than for actual data transmission. However, when there is no need for security, the coding is potentially useful if the pairs are shared in advance. Then, in effect, a doubling of the data rate can be achieved. There is no magic here, this doubling is only possible because of the *prior* sharing of the EPR pairs. In a sense, the spatial nonlocality between the entangled qubits translates into temporal nonlocality. It is as if the one data bit gets sent before it is encoded, or perhaps even before it exists! Stated more formally, the channel capacity for communication using entanglement does not violate the Kholevo bound for a quantum communication channel. For a proper discussion relating superdense coding to the standard results on channel capacity, see [147].

If a permanent quantum channel exists between Alice and Bob, then it might be argued that teleportation is unnecessary. If it is transportable, the customer's quantum system can be sent straight down the channel. Teleportation is safer, of course, since the loss of the classical bits can be rectified whereas the loss of the actual quantum state can not. However, it is also amusing to note that if teleportation is used, Alice does not even have to know Bob's location! If she broadcasts the two classical bits publicly, then, provided that Bob picks up the message and as long as his qubit two is still quantum coherent, he is able to reconstruct the original quantum state. If Alice sends the individual quantum state directly, she has to know where to mail it as she cannot clone it and broadcast it publicly.

As something of an aside, it is worth mentioning the situation where the the customers provide quantum states which are transportable *and* where there exists a permanent good quality quantum channel. Even in this case Alice and Bob may still be able to do business, by providing a quantum data compression service. Benjamin Schumacher has shown how a large number of quantum states which contain some redundancy can be compressed [148], [149], [13]. An example is a long sequence of states, each one being $|\updownarrow\rangle$ or $|\swarrow\!\!\nearrow\rangle$. Each of these contains a component of the other; they are not *orthogonal*. Hence the redundancy in the encoded information. The compression is accomplished by Alice performing a reversible (unitary) quantum operation on the *complete* data set and then discarding a chunk which contains almost no information. Upon receiving this compressed string of quantum states, Bob adds a chunk which in effect contains no information and then reverses the unitary quantum operation. This reproduces the customer's full data set with an extremely high fidelity.

There is one final point concerning the transmission of quantum states, whether it be via teleportation or direct. The state might be that of a system which is in no way transportable and the requirement might be to place an equally immobile system in this state at the receiving end. These could be the output and input quantum registers of different computers, for example, or even spatially separated registers within the same machine. Provided that these systems are able to interact with mobile systems like particles and in a reversible quantum manner, all is not lost. Quantum state swapping, as given by (16), can be employed to move the states of interest between different systems.

C. Practicalities

There are two main practical problems which must be overcome in order to make teleportation and superdense coding viable in the laboratory. These are the performance of Bell measurements on appropriate quantum systems and the distribution and storage of EPR pairs.

The crux of a Bell measurement is the operation of a quantum XOR gate. The remainder simply needs (good quality) conventional projective quantum measurements applied to the two systems. As discussed in Section V-C, individual XOR gates are feasible with certain quantum systems. The Bell measurement problem is therefore unlikely to be the major one. However, whether or not the XOR gates which are suitable as components of a quantum computer are also suitable for teleportation is not completely clear cut. This will depend on the sort of particles chosen for the EPR pairs, which relates to the second problem.

There is no doubt that photons (Section III-A) are extremely good for stretching out quantum entanglement. For example, the experiments reported in [75] show evidence for this down 4.3 km of optical fiber. However, the capture and storage of such traveling photons is at present an unsolved problem. It is hard to see how this might be done. Recall that any *irreversible* interaction with either photon of an EPR pair will destroy the entanglement and render the pair useless. It will require great ingenuity to devise a method for stopping a traveling photon in its tracks and then storing it, all done in a reversible quantum mechanical manner. It is not clear to me that this is possible in principle, let alone in practice. Even if the photons were to be used as they arrive, in an attempt to bypass the storage problem, it is still not clear how to involve them in Bell measurements made jointly with some other system. It is notable that none of the proposed XOR gates discussed in Section V-C use states of *traveling* photons as qubits.

The balance of problems changes if trapped cavity photons (Section III-A) and atoms (Section III-B) are contemplated. Bell measurements should be possible; one of the proposed XOR gates uses Rydberg atoms and trapped microwave photons. Storage of entangled systems of this type, at least for short times, looks to be feasible. The big problem here is the sharing of the entanglement over significant distances. Compared to photons propagating down fibers, atoms in a beam are extremely delicate. They also travel rather more slowly than photons. (A thermal velocity of a Rydberg atom might be around 70 ms^{-1}.) It is certainly the case that teleportation might soon be a reality over short distances and under laboratory conditions. Reference [44] discusses a feasible experimental arrangement to teleport an atomic state using entangled trapped cavity photons for the EPR pair. Remarkable though this would be, it is hard to see how such experiments might be stretched out over potentially useful distances.

Until the problems raised above are solved, teleportation and superdense coding should be regarded as still very much on the drawing board. Even if these problems are overcome, there is another potential worry because any real set of shared EPR pairs will never be perfect. Some of them are bound to have been corrupted by their environment. However, the theoretical problem of distilling a smaller set of good pairs, in effect weeding out the corrupted ones, has been solved [150], [13]. This is similar in spirit to the error detection and privacy amplification of cryptography (Section IV-B), although here, of course, all the operations on the retained pairs must be *reversible* to maintain the entanglement. If teleportation ever gets off the drawing board and to the practical level, this distillation technique will be invaluable.

D. Patents

To date one patent has been granted in this area [151]. This patent covers a scheme closely related to the superdense coding arrangement, where both partners of entangled pairs are used to carry information from a sender to a receiver. To function, an eavesdropper must intercept and recombine *both* channels and such an action is detectable. The receiver must clearly also recombine both channels to produce the original input. The implementation described uses photons.

VII. Comments

I have tried to give a reasonably comprehensive view of the current state of quantum information processing. However, what is to be made of all this? Is quantum information technology feasible and, if so, can it offer significant gains over its existing classical counterpart?

Quantum cryptography currently works in laboratory prototype form, with the potential for reasonable distances ($\sim$10 km) and bit rates ($\sim$10 kbit/s^{-1}). Very weak pulses of light are used for these devices. The possibility of using genuine single photons, or even entangled pairs of photons, exists. At present, no other types of quantum system seem to be realistic contenders for use in cryptosystems. The main obstacle impairing the improvement of current cryptosystems is the lack of good single photon detectors for the wavelengths at which optical fibers work best. Continuing fundamental research on this problem is certainly worthwhile; no doubt such detectors would find useful employment in others areas as well. I assume that research to improve optical fibers, given their vast use in classical communications systems, will continue in any case.

However, probably the main point to mull over regarding quantum cryptography is the advantage it offers over conventional classical methods. It certainly has one, in that it provides *verifiably* secure cryptographic key exchange because quantum information cannot be read without disturbing it whereas classical information can. Nevertheless, it is not clear to me that this advantage is sufficient to generate a market. The ruination of conventional public key cryptosystems could well strengthen the case. (Recall that the construction of a quantum computer capable of factorizing large composite integers would ruin RSA! This is a long way off, though.) However, even then, any investment in quantum cryptography could equally well be put into making a similar classical data transmission physically more secure. Surrounding a communication fiber with a jacket whose penetration would be extremely difficult to disguise is one such example. Improvements in bit rate and propagation distance for the quantum approach, up to those achievable classically, would make this a more even contest. Until such progress is made, it is not clear to me that a quantum cryptosystem will constitute a saleable product.

It is likely that even the fundamental researchers in the field, both theoretical and experimental, share, or at least acknowledge, this view. They have made a point of stressing that cryptosystems have other uses [24], such as in message authentication or in the provision of genuine secret ballots. In the former example, if the messages are short financial transactions this might ease the demand on bit rate, but not on the operating distance. (The actual transmission speed is the speed of light, of course.) In the latter example, a public decision can be reached in effect by quantum voting. No intermediary is needed to collect votes; these are input into a (more complicated derivative of a) cryptosystem which arrives at the result and keeps no record of the individual opinions. This example could ease the demand on bit rate and on operating distance. It should also be noted, however, that the absolute security of some of these additional applications is questionable. Unscrupulous users can potentially cheat them using quantum entanglement [152]. I am thus not convinced that quantum cryptosystems are marketable at this point in time.

The whole situation is somewhat different for quantum computers. They are much further away from realization, even as prototypes. However, if they can ever be built, and it is a big "if," there will undoubtedly be a demand for them. Over the next couple of years it seems likely that a variety of quantum gates, suitable as building blocks for quantum computers, will come into existence. Atoms interacting with cavities, ions in traps, and coupled nanostructures seem to be the best candidates. It looks like the disruptive effects of the environment can be held back sufficiently for these systems to perform the required quantum operations and it may well be possible to connect a few of them together. If so, an encoding of a single qubit to protect it against decoherence will be achievable. However, the *big* problems are in connecting sufficient (something like 1000, perhaps [13]) gates together. This construction has to be accurate enough for them to perform the evolution that they are supposed to. The environment also has to be held back to maintain quantum coherence for long enough to perform the desired tasks. It is harder to construct more complex systems and to keep them decoupled from their environment. Certainly it will not be possible to make perfect complex systems, so the questions to address will be whether or not useful tasks can be performed within the shorter of their decoherence time [121] and the time it takes construction imperfections to bite [119]. Quantum error correction [130]–[135] might be employed to buy more time, but will it be enough? This is still an open question. Nevertheless, I believe that fundamental research in this whole area (both experimental and theoretical) should be strongly encouraged. Successful construction of quantum computers would generate a significant payback.

It is very nice that problems intractable to any classical computer but soluble by quantum means have already been identified. However, Shor's factorizing algorithm really just starts the ball rolling. Quantum computers go about their business in a fundamentally different way from classical machines. It should be stressed that machines which operate classically, but by some sort of probabilistic or "fuzzy" algorithm, are not equivalent. They cannot incorporate quantum parallelization due to superposition of states. The advantage of quantum machines looks to be in generating short sharp answers to big involved problems, or in finding any one of a large set of solutions to a problem, rather than generating masses of data. I believe that making such machines available to people would encourage them to think differently and to change their complete style of problem formulation. The impact could be enormous. If quantum computers can ever be built, I believe that they will form a whole new industry.

Quantum teleportation is unlikely to be practicable in the near future. It may well function in a laboratory, transmitting elementary quantum states over short distances [44]. However, I have yet to see proposals, even just in principle, for stretching out quantum entanglement over appreciable distances *and* storing it for reasonable times. This is what would be required to progress out of the laboratory. There is no doubt that teleportation could be useful in the very distant future. Connecting quantum computers together, to form quantum local area networks, would need the faithful transfer of quantum states from one machine to another. However, the machines have to be built first!

VIII. Summary

Here are three bullets, for those of you who read only the first and last paragraphs of articles.

- Quantum cryptography works in prototype form, over distances ~10 km and with bit rates ~10 kbit/s^{-1}. It does provide verifiably secure exchange of information, because quantum information cannot be read without disturbing it whereas classical data can. However, even if we could quantize our credit cards, for example, it is not clear that the additonal security benefit could justify the investment required.
- Prototype quantum computers are a long way off. However, individual gates which would form their buildings blocks are just about with us. The accurate construction of complex machines containing many such gates, keeping the disruptive effect of the environment at bay, will be at best a truly formidable task. Nevertheless, the incentive is there; it would be a quantum leap forward for the computer industry.
- None of us will ever utter that immortal phrase: "Beam me up, Scotty." "Beam me that elementary state down the quantum teleport, Scotty," perhaps, but even this is some way off. Laboratory teleportation of an atomic state over a short distance may soon be possible; however, it is hard to see how this might be scaled up to be of use.

Appendix
Density Operators and Irreversibility

To illustrate the crucial difference between a superposition state and a lack of classical knowledge about the members of an ensemble of quantum systems, suppose that you are given two different ensembles of qubits. In the first, *every* member of the ensemble is describable by the superposition state (2). In the second, a fraction $|a|^2$ are *definitely* in the state $|0\rangle$ and a fraction $|b|^2$ $(= 1 - |a|^2)$ are *definitely* in the state $|1\rangle$, but you are not told which qubits are in which states. This latter case is what I mean by a lack of classical knowledge about the ensemble.

The two ensembles are clearly physically different. The first is called *pure* and the second *mixed*. The density operator (or matrix) ρ is the standard tool in quantum mechanics for dealing with both of these cases. It provides a direct description of ensembles of systems and is used to define familiar statistical quantities such as the entropy.

The pure density operator for the first ensemble, with *every* member in state $|\psi\rangle$, is defined as the *outer product* of the state and its Hermitian conjugate, $\rho = |\psi\rangle\langle\psi|$. In the vector and matrix representation of states and operators ρ is a simple matrix, constructed from products of pairs of the state amplitudes with $|\psi\rangle$ dictating the row and $\langle\psi|$ dictating the column. Thus with $|\psi\rangle$ represented by $\left(\begin{smallmatrix} b \\ a \end{smallmatrix}\right)$, the first ensemble has a density matrix $\rho_1 = \left(\begin{smallmatrix} b \\ a \end{smallmatrix}\right)(b^* \; a^*) = \left(\begin{smallmatrix} |b|^2 & ba^* \\ ab^* & |a|^2 \end{smallmatrix}\right)$. In this approach, *expectation values* are calculated by matrix multiplication between ρ and the matrix for the observable, followed by tracing (summing the *diagonal* elements). For ensemble one, the expectation value of the bit value B is simply $\mathrm{Trace}\,(\rho_1 B) = \mathrm{Trace}\left(\begin{smallmatrix} |b|^2 & 0 \\ ab^* & 0 \end{smallmatrix}\right) = |b|^2$, in agreement with $\langle\psi|B|\psi\rangle$ evaluated in Section II-A. The members of a pure ensemble are always each describable by the same state $|\psi\rangle$, whatever that happens to be, so *any* pure density operator can always be written in the form $|\psi\rangle\langle\psi|$. It follows that $\rho^2 = \rho$ identically in the pure case. The normalization of $|\psi\rangle$ is equivalent to the condition $\mathrm{Trace}\,(\rho) = 1$, which must hold given the probability interpretation of the (modulus squared) amplitudes in quantum physics.

A mixed density operator incorporating a lack of classical knowledge about an ensemble *cannot* be written as one such outer product. As the ensemble is a *mixture* of a number of pure ensembles, ρ is written as a sum of the appropriate pure operators weighted with the appropriate classical probabilities. (The weighting ensures that $\mathrm{Trace}\,(\rho) = 1$ even in this mixed situation.) A mixed density operator is not equal to its own square. For ensemble two the density operator is the weighted sum $\rho_2 = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|$; as a matrix this reads $\rho_2 = \left(\begin{smallmatrix} |b|^2 & 0 \\ 0 & |a|^2 \end{smallmatrix}\right)$. This clearly differs from ρ_1 as it lacks the off-diagonal terms. However, it possesses the same diagonal ones and so, for example, does give the same expectation value for B as ensemble one. This is why confusion can sometimes arise about the distinction between such ensembles.

A clear-cut way to show the distinction between pure and mixed ensembles is through the *entropy* S, defined as [19]

$$S = -k\,\mathrm{Trace}\,(\rho \ln \rho). \tag{26}$$

S is the entropy per system in the ensemble and k is Boltzmann's constant. In statistical physics the entropy is used as a measure of the disorder, or lack of knowledge about, an ensemble. The fact that $\rho^2 = \rho$ for any pure ensemble yields $S = 0$. (The natural logarithm, or any such mathematical function, of an operator or matrix can be thought of as an expansion in powers of the operator; the ln in (26) can be expanded to show that $S = 0$ when $\rho^2 = \rho$.) A pure ensemble has zero entropy; there is no lack of knowledge or "missing information" as every member of the ensemble is in the same quantum state. A mixed ensemble always has finite entropy $S > 0$. A simple calculation for ensemble two yields $S = -k(|a|^2 \ln |a|^2 + |b|^2 \ln |b|^2)$. For the case $|a|^2 = |b|^2 = 1/2$ the entropy (per qubit) is $S = k \ln 2$, its largest possible value for an ensemble of qubits. This case is the most disordered one, your lack of knowledge about a qubit is greatest when you choose it from this example of ensemble two.

Applying the Schrödinger equation (3) to a pure density operator $|\psi\rangle\langle\psi|$, or term by term to a mixed one, gives the equivalent equation for the quantum evolution of a density operator

$$\frac{\partial \rho}{\partial t} = \frac{-i}{\hbar}[H, \rho] \tag{27}$$

where $[H, \rho] = H\rho - \rho H$ is the *commutator* between the two operators. In general the commutator between two operators does not vanish, as it would if they were mere numbers. This is clear from the matrix representation of operators because in general matrix multiplication is not commutative. It is a simple exercise to show that the Schrödinger evolution (27) *preserves* the entropy S in time, that is $\partial S/\partial t = 0$. (Trace$(\rho) = 1$ and the cyclic property of the Trace operation applied to any product of operators/matrices, Trace(ABC) = Trace(CAB) = Trace(BCA), for example, are used in the derivation.) It is for this reason that unitary Schrödinger evolution is called *reversible*. The meaning is the same as in thermodynamics; there is no change in entropy during reversible evolution.

Things are different if each quantum system in the ensemble is coupled to some form of environment. A very simple example of this for the qubits can be described by the density operator evolution

$$\frac{\partial \rho}{\partial t} = \kappa(2B\rho B - \rho B^2 - B^2\rho). \tag{28}$$

These terms, which should be thought of as additional to the evolution described by (27), generate *nonunitary* evolution of ρ. Coupling to an environment induces behavior fundamentally different from the *unitary* evolution of isolated quantum systems. Although I consider only a few simple cases, this holds quite generally. It is instructive to examine the behavior of an ensemble of qubits described initially (at $t = 0$) by the pure density matrix ρ_1, ignoring the Schrödinger evolution (27), (so assume that $H = 0$). The solution to (28) is simply $\rho = \begin{pmatrix} |b|^2 & ba^* \exp(-\kappa t) \\ ab^* \exp(-\kappa t) & |a|^2 \end{pmatrix}$. The diagonal terms remain constant but the off-diagonal terms decay away at a rate set by the constant κ, so at large times our ensemble is described by the mixture ρ_2! This evolution is called *irreversible* because a change in entropy occurs, in this case from zero to $S = -k(|a|^2 \ln |a|^2 + |b|^2 \ln |b|^2)$. A physical interpretation of this particular irreversible evolution is that of a *measurement of the bit value* B, the operator which appears in (28). In this case, the environment coupled to each qubit in the ensemble is an apparatus which measures its value. The strength of the coupling is set by the parameter κ; the characteristic time for the measurement process to occur is $\sim\kappa^{-1}$.

The intuitive "picture" of what happens to an individual qubit during a measurement interaction is that the initial state $|\psi\rangle$ evolves randomly to $|0\rangle$ (with probability $|a|^2$) or to $|1\rangle$ (with probability $|b|^2$.) The state localizes into one of the two possible classical bit states. The recent interest in individual quantum systems has helped stimulate the development of theoretical models which actually describe measurement and other forms of irreversible environment interaction applied to single systems [15], [20]–[22]. These basically involve modifications of the Schrödinger equation (3), introducing nonlinear and stochastic terms due to the effect of the environment on the state of the system. While producing the correct statistical behavior, such as that generated in (28), the models actually produce results which correspond to intuitive "pictures" of individual quantum events. In the qubit measurement case, $|\psi\rangle$ really does project randomly to $|0\rangle$ or $|1\rangle$ run by run.

Another simple example of irreversible behavior is the photon polarization one from Section II-C. The state of an *individual* photon which has interacted with the model fiber is given by (5). If the interaction is irreversible it introduces a *random* phase ϕ. Assuming that all possible ϕ are equally likely, the density operator corresponding to an ensemble of such photons is found by summing $|\psi\rangle\langle\psi|$ over all possible angles and with equal weight, leading to

$$\begin{aligned}\rho &= \frac{1}{2\pi}\int_0^{2\pi} d\phi|\psi\rangle\langle\psi| = \frac{1}{2}(|\updownarrow\rangle\langle\updownarrow| + |\leftrightarrow\rangle\langle\leftrightarrow|)\\ &= \frac{1}{2}(|\text{⤢}\rangle\langle\text{⤢}| + |\text{⤡}\rangle\langle\text{⤡}|).\end{aligned} \tag{29}$$

Whichever way it is decomposed, this is clearly a mixture with a finite entropy of $k \ln 2$, the maximum value possible for a system with just two basis states. As the initial density operator $|\text{⤢}\rangle\langle\text{⤢}|$ is pure and has zero entropy, the irreversible action of the environment in randomizing the plane of polarization has increased the photon entropy by $k \ln 2$. This process could also be viewed as a model example of the *erasure* of a bit and shows that there is a characteristic entropy change of $\Delta S = k \ln 2$ associated with such an erasure.

A final example of irreversibility is thermal equilibrium. The *energy* eigenstates of a system, denoted by $|E_j\rangle$, are eigenstates of the Hamiltonian, so $H|E_j\rangle = E_j|E_j\rangle$ and the eigenvalues are E_j. The index j runs over the number of states in this basis. There are only two for a qubit; these may well correspond directly to the bit value eigenstates $|0\rangle$ and $|1\rangle$, although they could be superpositions of them instead. For a large complex system j runs over a much bigger range. Independent of how it starts, an ensemble of distinguishable systems which attain thermal equilibrium with a heat bath at temperature T can be described by the thermal density operator

$$\rho_{th} = \frac{1}{Z}\sum_j \exp\left(-E_j/kT\right)|E_j\rangle\langle E_j|. \qquad (30)$$

The exponential probabilities are the famous Boltzmann factors and Z is the normalizing partition function $\Sigma_j \exp\left(-E_j/kT\right)$. ρ_{th} is clearly mixed and has a nonzero entropy of $S = \overline{E}/T$ where $\overline{E}$ is the average system energy, the expectation value $\mathrm{Trace}\,(\rho_{th}H)$. The thermal "equilibrium" state of any *individual* member of the ensemble fluctuates randomly, but with a Boltzmann time average [153]. Thus *any* well-defined initial state, an energy eigenstate or a superposition, is destroyed and forgotten by the time thermal equilibrium is reached. This form of decoherence clearly needs to be avoided, or at least kept at bay for as long as possible, in all aspects of quantum information processing.

Acknowledgment

The author is indebted to the numerous researchers in the field with whom he has interacted, and particular thanks go to A. Ekert and A. Barenco.

References

[1] References [2]–[8] cover a broad range of quantum mechanics topics. These are heavy on the formalism and its applications, but lighter on the concepts and interpretation; two of my favorites are [2], [3]. Examples of books with more even or the reverse emphasis are [4]–[7]. Reference [8] is a one volume collection of many of the founding and classic papers.

[2] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 4th ed. Oxford, U.K.: Oxford Univ. Press, 1958; reprinted 1978.

[3] L. D. Landau and E. M. Lifshitz, *Quantum Mechanics (Nonrelativistic Theory)*, 3rd ed. New York: Pergamon, 1977; reprinted 1987.

[4] R. P. Feynman, R. B. Leighton, and M. Sands, *The Feynman Lectures on Physics*, vol. 3. Reading, MA: Addison-Wesley, 1965.

[5] J. R. Brown and P. C. W. Davies, Eds., *The Ghost in the Atom*. Cambridge, U.K.: Cambridge Univ. Press, 1986.

[6] A. I. M. Rae, *Quantum Physics: Illusion or Reality?* Cambridge, U.K.: Cambridge Univ. Press, 1986; reprinted 1991.

[7] R. Omnes, *The Interpretation of Quantum Mechanics*. Princeton, NJ: Princeton Univ. Press, 1994.

[8] J. A. Wheeler and W. H. Zurek, Eds., *Quantum Theory and Measurement*. Princeton, NJ: Princeton Univ. Press, 1983.

[9] H. Grabert and H. Horner, Eds., "Special issue on single charge tunnelling," *Z. Phys.*, vol. B85, no. 3, pp. 317–467, 1991.

[10] H. Koch and H. Lübbig, Eds., *Single-Electron Tunneling and Mesoscopic Devices* (Springer Series in Electronics and Photonics 31). Berlin: Springer-Verlag, 1992.

[11] W. P. Kirk and M. A. Reed, *Nanostructures and Mesoscopic Systems*. New York: Academic, 1992.

[12] P. R. Berman, Ed., *Cavity Quantum Electrodynamics* (Advances in Atomic, Molecular, and Optical Physics, Suppl. 2). New York: Academic, 1994.

[13] C. H. Bennett, "Quantum information and computation," *Phys. Today*, vol. 48, pp. 24–30, Oct. 1995.

[14] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*. Cambridge, U.K.: Cambridge Univ. Press, 1987.

[15] ——, "Against 'measurement,'" *Phys. World*, vol. 3, pp. 33–40, Aug. 1990.

[16] A. O. Caldeira and A. J. Leggett, "Influence of dissipation on quantum tunnelling in macroscopic systems," *Phys. Rev. Lett.*, vol. 46, pp. 211–214, 1981.

[17] U. Weiss, *Quantum Dissipative Systems* (Series in Modern Condensed Matter Physics, vol. 2). London: World Scientific, 1993.

[18] K. Gottfried, *Quantum Mechanics*. London: Benjamin-Cummings, 1966, ch. 4, pp. 165–190; reprinted by Addison-Wesley, 1989.

[19] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*. Princeton, NJ: Princeton Univ. Press, 1955, ch. 5.

[20] G. C. Ghirardi, A. Rimini, and T. Weber, "Unified dynamics for microscopic and macroscopic systems," *Phys. Rev.*, vol. D34, pp. 470–491, 1986.

[21] N. Gisin and I. C. Percival, "The quantum-state diffusion model applied to open systems," *J. Phys.*, vol. A25, pp. 5677–5691, 1992.

[22] L. Diósi and B. Lukács, Eds., *Stochastic Evolution of Quantum States in Open Quantum Systems and in Measurement Processes*. London: World Scientific, 1994.

[23] R. A. Houstoun, *A Treatise on Light*, 7th ed. London: Longmans, 1938, p. 205; L. D. Landau, E. M. Lifshitz, and L. P. Pitaevskii, *Electrodynamics of Continuous Media*, 2nd ed. New York: Pergamon, 1984, p. 339.

[24] C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum cryptography," *Scientif. Amer.*, pp. 26–33, Oct. 1992.

[25] Y. Mizobuchi and Y. Ohtaké, "An experiment to show both the classical wave and particle behaviors of light," *Japan. J. Appl. Phys.*, Ser. 9, pp. 201–204, 1993.

[26] J. G. Rarity, "Dreams of a quiet light," *Phys. World*, vol. 7, pp. 46–51, June 1994.

[27] G. Badurek, H. Rauch, and D. Tuppinger, "Neutron interferometric double-resonance experiment," *Phys. Rev.*, vol. A34, pp. 2600–2608, 1986.

[28] J. P. Vigier, "New theoretical implications of neutron interferometric double resonance experiments," *Physica*, vol. B151, pp. 386–392, 1988.

[29] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev.*, vol. 47, pp. 777–780, 1935.

[30] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Phys.*, vol. 1, pp. 195–200, 1964.

[31] ——, "On the problem of hidden variables in quantum mechanics," *Rev. Mod. Phys.*, vol. 38, pp. 447–452, 1966.

[32] A. Aspect, "Testing Bell's inequalities," *Europhys. News*, vol. 22, pp. 73–75, Apr. 1991.

[33] C. Jack, "Sherlock Holmes investigates the EPR paradox," *Phys. World*, vol. 8, pp. 39–42, Apr. 1995.

[34] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via Bell's theorem," *Phys. Rev. Lett.*, vol. 47, pp. 460–463, 1981.

[35] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of Bell's inequalities using time-varying analyzers," *Phys. Rev. Lett.*, vol. 49, pp. 1804–1807, 1982.

[36] A. Aspect, P. Grangier, G. Roger, and J. Dalibard, *Atomic Phys.*, vol. 8, p. 103, 1983.

[37] Y. H. Shih and C. O. Alley, "New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta," *Phys. Rev. Lett.*, vol. 61, pp. 2921–2924, 1988.

[38] Z.-Y. Ou and L. Mandel, "Violation of Bell's inequality and classical probability in a two-photon correlation experiment," *Phys. Rev. Lett.*, vol. 61, pp. 50–53, 1988.

[39] J. G. Rarity and P. R. Tapster, "Experimental violation of Bell's inequality based on phase and momentum," *Phys. Rev. Lett.*, vol. 64, pp. 2495–2498, 1990.

[40] V. B. Braginsky, V. P. Mitrofanov, and V. I. Panov, *Systems with Small Dissipation*. Chicago: Univ. Chicago Press, 1985.

[41] N. F. Ramsey, *Molecular Beams*. Oxford, U.K.: Oxford Univ. Press, 1985.

[42] L. Davidovich *et al.*, "Quantum switches and nonlocal microwave fields," *Phys. Rev. Lett.*, vol. 71, pp. 2360–2363, 1993.

[43] M. Brune *et al.*, "From Lamb shift to light shifts: Vacuum and subphoton cavity fields measured by atomic phase sensitive detection," *Phys. Rev. Lett.*, vol. 72, pp. 3339–3342, 1994.

[44] L. Davidovich *et al.*, "Teleportation of an atomic state between two cavities using nonlocal microwave fields," *Phys. Rev.*, vol. A50, pp. R895–R898, 1994.

[45] Q. A. Turchette *et al.*, "Measurement of conditional phase shifts for quantum logic," *Phys. Rev. Lett.*, vol. 75, pp. 4710–4713, 1995.

[46] M. G. Raizen *et al.*, "Ionic crystals in a linear Paul trap," *Phys. Rev.*, vol. A45, pp. 6493–6501, 1992.

[47] H. Walther, "Atoms in cavities and traps," *Adv. in At., Mol. and Opt. Phys.*, vol. 32, pp. 379–405, 1994.

[48] D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen, "Squeezed atomic states and projection noise in spectroscopy," *Phys. Rev.*, vol. A50, pp. 67–88, 1994.

[49] J. I. Cirac, R. Blatt, A. S. Parkins, and P. Zoller, "Preparation of Fock states by observation of quantum jumps in an ion trap," *Phys. Rev. Lett.*, vol. 70, pp. 762–765, 1993.

[50] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Phys. Rev. Lett.*, vol. 74, pp. 4091–4094, 1995.

[51] D. R. Tilley and J. Tilley, *Superfluidity and Superconductivity*, 2nd ed. London: Adam Hilger, 1986.

[52] B. D. Josephson, "Possible new effects in superconductive tunnelling," *Phys. Lett.*, vol. 1, pp. 251–253, 1962.

[53] T. P. Spiller, T. D. Clark, R. J. Prance, and A. Widom, "Quantum phenomena in circuits at low temperature," *Prog. Low Temp. Phys.*, vol. 8, pp. 219–265, 1992.

[54] K. K. Likharev and A. N. Korotov, "Single-electron parametron: Reversible computation in a discrete-state system," *Sci.*, vol. 273, pp. 763–765, 1996.

[55] D. P. DiVincenzo, "Quantum computation," *Sci.*, vol. 270, pp. 255–261, 1995.

[56] C. D. Tesche, "Macroscopic quantum coherence: An experimental strategy," in *SQUID'85, Superconducting Quantum Interference Devices and their Applications*, H. D. Hahlbohm and H. Lübbig, Eds. Berlin: de Gruyter, 1985, pp. 355–359.

[57] ——, *New Techniques and Ideas in Quantum Measurement Theory*, D. M. Greenberger, Ed. New York: Acad. Sci., vol. 480, p. 36, 1986.

[58] ——, "EPR as a guide to understanding the MQC measurement scheme," in *Macroscopic Quantum Phenomena*, T. D. Clark *et al.* Eds. London: World Scientific, 1991, pp. 67–72.

[59] G. Diambrini-Palazzi, "A proposal for an experiment to detect macroscopic quantum coherence with a system of SQUID's," in *Waves and Particles in Light and Matter*, A. van der Merwe and A. Garuccio, Eds. New York: Plenum, 1994, pp. 251–257.

[60] H. Prance *et al.*, "The energy band structure of ultra-small capacitance weak links–QED in condensed matter," *Nucl. Phys. (Proc. Suppl.)*, vol. 33C, pp. 35–59, 1993.

[61] R. J. Prance *et al.*, "Reactive probing of macroscopically quantum mechanical SQUID rings," *Physica*, vol. B203, pp. 381–387, 1994.

[62] S. Han, R. Rouse, and J. E. Lukens, "Generation of a population inversion between quantum states of a macroscopic variable," *Phys. Rev. Lett.*, vol. 76, pp. 3404–3407, 1996.

[63] R. Rivest, A. Shamir, and L. Adleman, "On digital signatures and public key cryptosystems," Tech. Rep. MIT/LCS/TR-212, MIT Lab. Computer Sci., Jan. 1979.

[64] M. E. Hellman, "The mathematics of public-key cryptography," *Scientif. Amer.*, vol. 241, pp. 130–139, Aug. 1979.

[65] C. H. Bennett, G. Brassard, S. Briedbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology: Proceeedings of Crypto '82*. New York: Plenum, 1982, pp. 267–275.

[66] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Conf. on Computers, Syst. and Signal Process.*, pp. 175–179, 1984.

[67] ——, "Quantum public key distribution system," IBM Techn. Disclosure Bull., vol. 28, pp. 3153–3163, 1985.

[68] S. Wiesner, "Conjugate coding," *Sigact News*, vol. 15, pp. 78–88, 1983.

[69] C. H. Bennett *et al.* "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, pp. 3–28, 1992.

[70] ——, "Special issue: Quantum communication," *J. Mod. Opt.*, vol. 41, no. 12, Dec. 1994.

[71] D. Deutsch, "Quantum communication thwarts eavesdroppers," *New Sci.*, vol. 124, no. 1694, pp. 25–26, 9 Dec. 1989.

[72] A. K. Ekert, "Quantum keys for keeping secrets," *New Sci.*, vol. 137, no. 1856, pp. 24–28, 16 Jan. 1993.

[73] S. Bengio *et al.*, "Secure implementation of identification systems," *J. Cryptol.*, vol. 4, pp. 175–183, 1991.

[74] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, pp. 210–229, 1988.

[75] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, "Quantum random number generation and key sharing," *J. Mod. Opt.*, vol. 41, no. 12, Dec. 1994, pp. 2435–2444.

[76] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.

[77] A. K. Ekert, J. G. Rarity, P. R. Tapster, and M. Palma, "Practical quantum cryptography based on two-photon interferometry," *Phys. Rev. Lett.*, vol. 69, pp. 1293–1295, 1992.

[78] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, 1992.

[79] C. H. Bennett and G. Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working!," *Sigact News*, vol. 20, no. 4, pp. 78–82, 1989.

[80] J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibers: Experimental and practical limits" [70, pp. 2405–2412].

[81] M. V. Berry, "Quantal phase factors accompanying adiabatic changes," *Proc. R. Soc. London*, vol. A392, pp. 45–57, 1984.

[82] R. Y. Chiao and Y. S. Wu, "Manifestations of Berry's topological phase for the photon," *Phys. Rev. Lett.*, vol. 57, pp. 933–936, 1986.

[83] A. Tomita and R. Y. Chiao, "Observation of Berry's topological phase by use of an optical filter," *Phys. Rev. Lett.*, vol. 57, pp. 937–940, 1986.

[84] A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fiber," *Europhys. Lett.*, vol. 33, pp. 335–339, 1996.

[85] J. D. Franson and H. Ilves, "Quantum cryptography using polarization feedback," [70, pp. 2391–2396].

[86] P. D. Townsend and I. Thompson, "A quantum key distribution channel based on optical fiber," [70, pp. 2425–2433].

[87] C. H. Bennett, IBM Corp., "Interferometric quantum cryptographic key distribution system," U.S. Pat. No. 5,307,410, Apr. 1994.

[88] S. J. D. Phoenix and S. M. Barnett, "Quantum cryptography using discarded data," British Telecommun. PLC, Int. Pat. Pub. No. WO 94/08409, Apr. 1994.

[89] S. M. Barnett and S. J. D. Phoenix, "Information-theoretic limits to quantum cryptography," *Phys. Rev.*, vol. A48, pp. R5–R8, 1993.

[90] J. D. Franson, "Apparatus and method for quantum mechanical encryption for the transmission of secure communications," Johns Hopkins Univ., Baltimore, MD, U.S. Pat. No. 5,243,649, Sept. 1993.

[91] J. Church, *Amer. J. Math.*, vol. 58, p. 435, 1936.

[92] A. M. Turing, "On computable numbers, with an application to the entscheidungsproblem," *Proc. London Math. Soc. Ser. 2*, vol. 442, pp. 230–265, 1936.

[93] Y. Lecerf, *Compt. Rend.*, vol. 257, pp. 2597–2601, 1963.

[94] C. H. Bennett, "Logical reversibility of computation," *IBM J. Res. Dev.*, vol. 17, pp. 525–532, 1973.

[95] R. Landauer, "Information is physical," *Phys. Today*, vol. 44, pp. 23–29, May 1991.

[96] E. Fredkin and T. Toffoli, "Conservative logic," *Int. J. Theor. Phys.*, vol. 21, pp. 219–253, 1982.

[97] C. H. Bennett, "The thermodynamics of computation—a review," *Int. J. Theor. Phys.*, vol. 21, pp. 905–940, 1982.

[98] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *J. Stat. Phys.*, vol. 22, pp. 563–591, 1980; "Quantum mechanical Hamiltonian models of Turing machines," *J. Stat. Phys.*, vol. 29, pp. 515–546, 1982; "Quantum mechanical models of Turing machines that dissipate no energy," *Phys. Rev. Lett.*, vol. 48, pp. 1581–1585, 1982.

[99] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, pp. 467–488, 1982.

[100] ——, "Quantum mechanical computers," *Opt. News*, vol. 11, p. 11, 1985; reprinted in *Found. Phys.*, vol. 16, pp. 507–531, 1986.

[101] D. Z. Albert, "On quantum mechanical automata," *Phys. Lett.*, vol. A98, pp. 249–252, 1983.

[102] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. R. Soc. London*, vol. A400, pp. 97–117, 1985.

[103] ——, "Quantum computation," *Phys. World*, vol. 5, pp. 57–61, June 1992.

[104] J. Glanz, "A quantum leap for computers?," *Sci.*, vol. 269, pp. 28–29, 1995.

[105] A. K. Ekert, "Quantum computation," in *AIP Conf. Proc. 323, XIV Int. Conf. on Atomic Physics*, Boulder, CO. New York: AIP, 1995, pp. 450–466.

[106] A. K. Ekert and R. Jozsa, "Shor's Quantum algorithm for factorising numbers," *Rev. Mod. Phys.*, 1996.

[107] A. Barenco, "Quantum physics and computers," *Contemporary Phys.*, 1996.

[108] D. Deutsch, "Quantum computational networks," *Proc. R. Soc. London*, vol. A425, pp. 73–90, 1989.

[109] A. C. C. Yao, *Proc. 34th IEEE Symp. on Foundations of Computer Science*. Los Alamitos, CA: IEEE Computer Soc. Press, 1993, p. 352.

[110] A. Barenco, "A universal two-bit gate for quantum computation," *Proc. R. Soc. London*, vol. A449, pp. 679–683, 1995.

[111] A. Barenco *et al.*, "Elementary gates for quantum computation," *Phys. Rev.*, vol. A52, pp. 3457–3467, 1995.

[112] S. Lloyd, "Almost any quantum logic gate is universal," *Phys. Rev. Lett.*, vol. 75, pp. 346–349, 1995.

[113] A. Barenco, A. K. Ekert, K.-A. Suominen, and P. Törmä, "Approximate quantum Fourier-transform and decoherence," *Phys. Rev.*, vol. A54, pp. 139–146, 1996.

[114] P. W. Shor, "Algorithms for quantum computation: Discrete log and factoring," in *Proc. 35th IEEE Symposium on Foundations of Computer Science*, S. Goldwasser, Ed. Los Alamitos, CA: IEEE Computer Soc. Press, 1994, p. 124.

[115] D. Coppersmith, IBM Res. Rep. RC19642, 1994.

[116] A. Barenco and A. K. Ekert, "Quantum computation," *Acta Physica Slovaca*, vol. 45, pp. 205–216, 1995.

[117] V. Vedral, A. Barenco, and A. K. Ekert, "Quantum networks for elementary arithmetic operations," *Phys. Rev.*, vol. A54, pp. 147–153, 1996.

[118] A. Berthiaume and G. Brassard, "Oracle quantum computing," [70], pp. 2521–2536.

[119] R. Landauer, "The physical nature of information," *Phys. Lett.*, vol. A217, pp. 188–193, 1996.

[120] A. Peres, "Reversible logic and quantum computers," *Phys. Rev.*, vol. A32, pp. 3266–3276, 1985.

[121] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, "Quantum computers, factoring and decoherence," *Sci.*, vol. 270, pp. 1633–1635, 1995.

[122] W. Unruh, "Maintaining coherence in quantum computers," *Phys. Rev.*, vol. A51, pp. 992–997, 1994.

[123] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," *Phys. Rev.*, vol. A51, pp. 1015–1022, 1995.

[124] M. B. Plenio and P. L. Knight, "Realistic lower bounds for the factorization time of large numbers on a quantum computer," *Phys. Rev. A*, 1996.

[125] G. M. Palma, K.-A. Suominen, and A. K. Ekert, "Quantum computers and dissipation," *Proc. R. Soc. London*, vol. A452, pp. 567–584, 1996.

[126] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, "Decoherence, continuous observation, and quantum computing: A cavity QED model," *Phys. Rev. Lett.*, vol. 75, pp. 3788–3791, 1995.

[127] C. Monroe *et al.*, "Demonstration of a fundamental quantum logic gate," *Phys. Rev. Lett.*, vol. 75, pp. 4714–4717, 1995.

[128] C. Dove, "Quantum computers and possible wavefunction collapse," *Phys. Lett.*, vol. A207, pp. 315–319, 1995.

[129] T. P. Spiller, "The Zeno effect: measurement versus decoherence," *Phys. Lett.*, vol. A192, pp. 163–168, 1994.

[130] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev.*, vol. A52, p. 2493, 1995.

[131] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," quant-ph/9512032, *Phys. Rev. A*, 1996.

[132] A. M. Steane, "Multiple particle interference and quantum error correction," quant-ph/9601029, Univ. Oxford preprint 1996, *Proc. R. Soc. London.*

[133] I. L. Chuang and Y. Yamamoto, "Quantum bit regeneration," *Phys. Rev. Lett.*, vol. 76, pp. 4281–4284, 1996.

[134] S. L. Braunstein, "Quantum error correction of dephasing in 3 qubits," quant-ph/9603024, preprint 1996.

[135] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correction code," quant-ph/9602019, preprint 1996.

[136] W. H. Zurek and R. Laflamme, "Quantum logical operations on encoded qubits," quant-ph/9605013, preprint 1996.

[137] V. Vedral, M. A. Rippin, and M. B. Plenio, "Quantum correlations, local interactions and error correction," quant-ph/9608030, preprint 1996.

[138] K. Obermayer, W. G. Teich, and G. Mahler, "Structural basis of multistationary quantum systems. I. Effective single-particle dynamics," *Phys. Rev.*, vol. B37, pp. 8096–8110, 1988.

[139] W. G. Teich, K. Obermayer, and G. Mahler, "Structural basis of multistationary quantum systems. II. Effective few-particle dynamics," *Phys. Rev.*, vol. B37, pp. 8111–8121, 1988.

[140] S. Lloyd, "A potentially realizable quantum computer," *Sci.*, vol. 261, pp. 1569–1571, 1993.

[141] A. Barenco, D. Deutsch, A. K. Ekert, and R. Jozsa, "Conditional quantum dynamics and logic gates," *Phys. Rev. Lett.*, vol. 74, pp. 4083–4086, 1995.

[142] E.-G. Wille, "Computer (Quanten-Computer)," Hassdenteufel, German patent no. DE4139286A1, June 1993.

[143] D. Deutsch and A. K. Ekert, "Quantum communication moves into the unknown," *Phys. World*, vol. 6, pp. 22–23, June 1993.

[144] C. H. Bennett *et al.*, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1898, 1993.

[145] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, 1992.

[146] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[147] A. Barenco and A. K. Ekert, "Dense coding based on quantum entanglement," *J. Mod. Opt.*, vol. 42, pp. 1253–1259, 1995.

[148] B. Schumacher, "Quantum coding," *Phys. Rev.*, vol. A51, pp. 2738–2747, 1995.

[149] R. Jozsa and B. Schumacher, "A new proof of the quantum noiseless coding theorem," in [70], pp. 2343–2350.

[150] C. H. Bennett *et al.*, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, pp. 722–725, 1996.

[151] H. J. Kimble, Z.-Y. Ou, and S. E. Pereira, "Method and apparatus for quantum communication employing nonclassical correlations of quadrature phase amplitudes," Calif. Inst. Technol., U.S. Pat. No. 5,339,182, Aug. 1994.

[152] H.-K. Lo and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible," quant-ph/9605026, preprint 1996.

[153] T. P. Spiller, B. M. Garraway, and I. C. Percival, "Thermal equilibrium in the quantum state diffusion picture," *Phys. Lett.*, vol. A179, pp. 63–66, 1993.

Timothy P. Spiller received the B.A. degree in physics from the University of Oxford, U.K., followed by the Ph.D. degree in theoretical particle physics from the University of Durham, U.K.

From 1984 to 1995 he was with the Physics Department at the University of Sussex, where he spent two years as a U.K. Science Research Council Fellow and the remainder as a Royal Society Research Fellow. His research has covered many different aspects of quantum physics, ranging from the phenomenology of superconducting quantum circuits and other quantum devices, through macroscopic quantum effects, quantum state diffusion and quantum information, to the interpretational aspects of quantum theory. He has published numerous papers across this spectrum. In 1995 he joined the Mathematics Group at Hewlett–Packard Laboratories, Bristol, U.K., the European section of HP's Research Laboratories. There he maintains his research interests in quantum physics in addition to working in a number of other areas.

Dr. Spiller is a member of the UK Institute of Physics.