Downloaded from rsta.royalsocietypublishing.org

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Implementations of quantum logic: fundamental and experimental limits

S. Bose, P. L. Knight, M. Murao, M. B. Plenio and V. Vedral

Phil. Trans. R. Soc. Lond. A 1998 **356**, 1823-1839
doi: 10.1098/rsta.1998.0251

Email alerting service Receive free email alerts when new articles cite this article - sign up in the box at the top right-hand corner of the article or click **here**

To subscribe to *Phil. Trans. R. Soc. Lond. A* go to: **http://rsta.royalsocietypublishing.org/subscriptions**

This journal is © 1998 The Royal Society

Downloaded from rsta.royalsocietypublishing.org

The Royal Society

Implementations of quantum logic: fundamental and experimental limits

By S. Bose, P. L. Knight, M. Murao, M. B. Plenio and V. Vedral

Optics Department, The Blackett Laboratory, Imperial College of Science, Technology and Medicine, London SW7 2BZ, UK

Quantum information processing rests on our ability to manipulate quantum superpositions through coherent unitary transformations. In reality the quantum information processor (a linear ion trap, or cavity QED implementation for example) exists in a dissipative environment. Dephasing, and other technical sources of noise, as well as more fundamental sources of dissipation severely restrict quantum processing capabilities. The strength of the coherent coupling needed to implement quantum logic is not always independent of dissipation. The limitations these dissipative influences present will be described and the need for efficient error correction noted. Even if long and involved quantum computations turn out to be hard to realize, one can perform interesting manipulations of entanglement involving only a few gates and qubits, of which we give examples. Quantum communication also involves manipulations of entanglement which are simpler to implement than elaborate computations. We briefly analyse the notion of the capacity of a quantum communication channel.

Keywords: quantum computation; decoherence; entanglement; quantum communication

1. Introduction

Since Shor's discovery (Shor 1994; Ekert & Jozsa 1996) of an algorithm that allows the factorization of a large number by a quantum computer in polynomial time instead of in exponential time as in classical computing, interest in the practical realization of a quantum computer has been much enhanced. Recent advances in the preparation and manipulation of single ions as well as the engineering of preselected cavity light fields suggest that quantum optics may well be the field of physics that promises the first experimental realization of a quantum computer.

The realization of a quantum computer in a linear trap (Cirac & Zoller 1995) has been regarded as very promising as it was thought that decoherence could be suppressed sufficiently to preserve the superpositions necessary for quantum computation. Indeed, a single quantum gate in such an ion trap has been realized by Monroe *et al*. (1995). Nevertheless, the error rate in this experiment was too high to allow the realization of extended quantum networks. This experiment was limited by technical difficulties and one aim of future experiments is to reduce these to come closer to the fundamental limits, such that at least small networks can be realized. However, there remains the question of whether overcoming technical problems will be sufficient to realize practically useful computations such as factorization of big numbers on a quantum computer in a linear ion trap. Here we address the problem of the so-called threshold accuracy in quantum computation (Knill *et al*. 1996;

© 1998 The Royal Society
TEX Paper

Downloaded from rsta.royalsocietypublishing.org

Aharonov & Ben-Or 1996). This threshold implies that arbitrarily complicated (long) quantum computations can be performed once the error rate of a quantum gate can be pushed below a certain threshold. We will discuss whether the required thresholds (Knill *et al*. 1996; Aharonov & Ben-Or 1996) can be achieved or if spontaneous emission rules out this possibility (not to mention other error sources). We present a simple calculation to understand the order of magnitude of these thresholds and then calculate the spontaneous emission rate in one quantum gate. Even if long and involved quantum computations turn out to be hard to realize, one can perform some interesting manipulations of entanglement involving only a few gates and qubits, of which we give some examples. Quantum communication also involves manipulations of entanglement which are simpler to implement than elaborate computations. We briefly analyse the notion of the capacity of a quantum communication channel.

2. Elementary quantum gates, algorithms and implementation

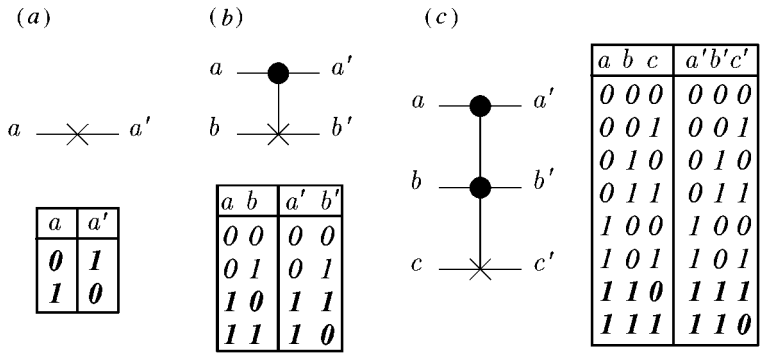
A quantum computer is a physical machine that can accept input states which represent a coherent superposition of many different possible inputs and subsequently evolve them into a corresponding superposition of outputs. Computation, i.e. a sequence of unitary transformations, affects simultaneously each element of the superposition, generating a massive parallel data processing capability albeit within one piece of quantum hardware (Deutsch 1985). This way quantum computers can efficiently solve some problems which are believed to be intractable on any classical computer (Deutsch 1992; Shor 1994). Apart from changing the complexity classes, the quantum theory of computation reveals the fundamental connections between the laws of physics and the nature of computation and mathematics (Deutsch 1997).

For the purpose of this paper a quantum computer will be viewed as a quantum network (or a family of quantum networks) composed of quantum logic gates; each gate performing an elementary unitary operation on one, two or more two-state quantum systems called *qubits* (Deutsch 1989). Each qubit represents an elementary unit of information; it has a chosen 'computational' basis $\{|0\rangle, |1\rangle\}$ corresponding to the classical bit values 0 and 1. Boolean operations which map sequences of 0s and 1s into another sequences of 0s and 1s are defined with respect to this computational basis.

Any unitary operation is reversible and that is why quantum networks effecting elementary arithmetic operations such as addition, multiplication and exponentiation cannot be directly deduced from their classical Boolean counterparts (classical logic gates such as AND or OR are clearly irreversible: reading 1 at the output of the OR gate does not provide enough information to determine the input, which could be either $(0,1)$, $(1,0)$ or $(1,1)$). Quantum arithmetic must be built from reversible logical components. It has been shown that reversible networks (a prerequisite for quantum computation) require some additional memory for storing intermediate results (Bennett 1989). Hence the art of building quantum networks is often reduced to minimizing this auxiliary memory or to optimizing the trade-off between the auxiliary memory and a number of computational steps required to complete a given operation in a reversible way.

Three elementary gates used in the construction of more complicated quantum networks (the NOT gate (which is obviously reversible), controlled-Not (C-NOT) gate and the Toffoli gate) are shown in figure 1.

Downloaded from rsta.royalsocietypublishing.org



a	a'
0	1
1	0

a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

a	b	c	$a'b'c'$
0	0	0	0 0 0
0	0	1	0 0 1
0	1	0	0 1 0
0	1	1	0 1 1
1	0	0	1 0 0
1	0	1	1 0 1
1	1	0	1 1 1
1	1	1	1 1 0

Figure 1. Elementary gates: (*a*) NOT gate; (*b*) C-NOT; (*c*) Toffoli gate.

By *basic* quantum gates we mean any set of quantum gates which can perform any desired quantum computation. A universal quantum gate is the one whose combination can be used to simulate any other quantum gate. A number of quantum algorithms have been developed (see elsewhere in this issue) from Deutsch's oracle algorithm to Shor's factorization algorithm and Grover's search algorithm. All may be realized, in principle, by using networks made up from one-bit rotations and C-NOT gates. The Shor algorithm for factorization uses Euclid's method and periodicity to find the factors of the given number N. This requires addition, multiplication and exponentiation networks and Fourier transformation (Vedral *et al*. 1996). The Grover search algorithm solves the problem of finding a special entry within a database of length N. Classically we need $\frac{1}{2}N$ tries, but a quantum computer can find the entry in $\sqrt{N}$ tries (Grover 1997).

We will not provide an exhaustive review of all possible implementations of quantum logic gates here. Many have been proposed, from coupled quantum dots, NMR spins, laser-cooled ions coupled through their centre of mass motion, to cavity QED in which atomic superpositions become entangled with quantized single-mode cavity fields. Quantum gate operation has been demonstrated experimentally for some of these, and we will concentrate in what follows on the special case of the linear ion-trap gate. This involves cooling ions to the lowest quantized state of motion within a trapping potential and then entangling internal and motional degrees of freedom of the trapped ions. Meekhof *et al*. (1996) have shown how a number of non-classical motional states of a Be^+ ion may be realized; their experiments reveal that they are limited to some extent by dephasing decoherence. Nevertheless, the same trap has been used to realize a C-NOT gate (Monroe *et al*. 1995). In what follows, we discuss the problem of decoherence in such a realization.

3. Decoherence problems

The ion-trap C-NOT gate involves cooling ions to their lowest vibrational state within the trap potential. Then single-photon (or two-photon Raman transitions) can excite internal electronic transitions within the ion; a suitable choice of detuning can simultaneously create (or annihilate) vibrational quanta. Meekhof *et al*. (1996) showed in particular how Fock states of motion can be realized by a clever choice of laser pulses and detunings. Were there to be *no* sources of decoherence, the trapped-ion dynamics should reflect the Jaynes–Cummings interaction of internal and vibrational

Downloaded from rsta.royalsocietypublishing.org

degrees of freedom (Shore & Knight 1993). For a Fock state, this would be a pure sinusoidal Rabi oscillation. What was observed (Meekhof *et al*. 1996) was a damped Rabi oscillation of the form

$$P_{\downarrow}(t) = \frac{1}{2}\left\{1 + \sum_n p_n \cos(B_n t)\mathrm{e}^{-A_n t}\right\}, \tag{3.1}$$

where $P_{\downarrow}(t)$ is the probability of being in the $|\downarrow\rangle$ internal ion state, p_n is the initial vibrational quantum number probability distribution, B_n is the coherent effective Rabi frequency and A_n is a phenomenologically introduced decoherence rate. These are substantially larger than expected, and are observed to be n-dependent as $A_n = \gamma_0(1+n)^{0.7}$. Possible sources of this decoherence include imperfect phase correlation for the field driving the Raman excitations and heating of the motional states. In what follows, we show how such decoherence affects the qubit-vibrational Jaynes–Cummings dynamics.

In the Lamb–Dicke limit of closely confined ion motion, the effective Hamiltonian for the trapped-ion experiment (Meekhof *et al*. 1996) in the interaction picture is given by the (anti)-Jaynes–Cummings Hamiltonian,

$$H^I_{\mathrm{eff}} = \hbar g(a^\dagger S_+ + aS_-), \tag{3.2}$$

where a, $a^\dagger$ are boson operators for the motional states ($|n\rangle_m$), and S_+, S_- are spin operations for the two relevant internal atomic levels ($|\downarrow\rangle_a$ and $|\uparrow\rangle_a$). The Jaynes–Cummings Hamiltonian (3.2) is the origin of the characteristic quantum dynamics of the system. In this section, we introduce phenomenologically new sources of decoherence in the interaction picture, which destroy this characteristic Jaynes–Cummings dynamics without energy relaxation (Murao & Knight 1998). We formulate the effects of decoherence by using a master equation describing the coupling of the internal and vibrational states to a quantum reservoir. In the high-temperature limit of the reservoir, within Markovian approximation, the master equation coincides with that for stochastic white noise. The advantage of using this quantum reservoir is that it not only describes quantum noise, but also provides a microscopic understanding of decoherence.

The effects of an environment coupled to the Jaynes–Cummings system are treated by coupling a quantum reservoir, which consists of an infinite number of bosons in a canonical distribution at temperature T for each mode. The choice of the coupling between the system operators and the reservoir operators determine the effect of the reservoir. If we choose the system operators that do not change the bosonic quantum number when they operate on the dressed states, the resulting master equation describes relaxation *within the dressed states* indicated by the bosonic quantum number n, but not energy relaxation between states with different n. The operators, S_z, $a^\dagger$, a, are obviously of this type, as these operators do not even change the motional states $|n\rangle_m$ as well as the dressed-state label n. The operator $a^\dagger S_+ + aS_-$ changes the motional state, but this operator does not change the dressed-state indication n, so $a^\dagger S_+ + aS_-$ is also of this type.

We consider in the following two possible alternatives for system–reservoir coupling

Downloaded from rsta.royalsocietypublishing.org

as potential candidates for the source of 'decoherence without energy relaxation':

$$H_{\rm sr} = \hbar(a^\dagger S_+ + aS_-)\sum_l g_l'(B_l^\dagger + B_l), \tag{3.3}$$

$$H_{\rm sr}' = \hbar a^\dagger a \sum_l g_l'(B_l^\dagger + B_l), \tag{3.4}$$

where ω_l is the lth reservoir frequency, and $B_l^\dagger$ and B_l are the creation and annihilation operators of the reservoir bosons. The coupling (3.3) describes imperfect dipole transitions between the level $|0\rangle_a$ (the intermediate state for the Raman transitions) and the level $|j\rangle_a$ $(j = \uparrow, \downarrow)$ due to fluctuations of the driving laser intensity. The coupling (3.4) describes fluctuations of the trap potential.

Then the master equation for the reduced-system operator in the interaction picture $\rho^I(t)$ due to the system–reservoir coupling is obtained by using a time convolution-less (TCL) formalism (Shibata & Arimitsu 1980) and the rotating wave approximation on the master equation (Murao 1997),

$$\frac{\partial}{\partial t}\rho^I(t) = \frac{1}{\mathrm{i}\hbar}[H_{\rm eff}^I, \rho^I(t)] + \Gamma\rho^I(t), \tag{3.5}$$

with the damping term $\Gamma\rho^I(t)$ given by (Murao & Shibata 1995)

$$\begin{aligned}\Gamma\rho^I(t) = \sum_l g_l'^2 \int_0^t \mathrm{d}t' \{&(\langle B_l^\dagger(t')B_l\rangle_B + \langle B_l(t')B_l^\dagger\rangle_B) \\ &\times ([C_{\rm s}(-t')\rho^I(t), C_{\rm s}^\dagger] + [C_{\rm s}^\dagger(-t')\rho^I(t), C_{\rm s}]) \\ &+ (\langle B_l^\dagger(-t')B_l\rangle_B + \langle B_l(-t')B_l^\dagger\rangle_B) \\ &\times ([C_{\rm s}, \rho^I(t)C_{\rm s}^\dagger(-t')] + [C_{\rm s}^\dagger, \rho^I(t)C_{\rm s}(-t')])\},\end{aligned} \tag{3.6}$$

where $C_{\rm s}$ represents the system operators $a^\dagger S^+$ and $a^\dagger a$, which couple to the reservoir. Time evolution of the system operators are determined by (3.2).

The master equation (3.5) can be solved by expanding all system operators in terms of the dressed states, which are eigenstates of the effective Hamiltonian (3.2), under certain reservoir conditions (Murao 1997). We take the continuum limit of the reservoir modes. We also require the time-scale of the reservoir variables to be much shorter than the system variables so we can take the Markovian limit. If we assume an initial condition of a product state $|\downarrow\rangle_a\langle\downarrow| \otimes \sum_n p_n|n\rangle_m\langle n|$, the population of the lower atomic state, given by

$$P_\downarrow(t) = \frac{1}{2}\left\{1 + \sum_n p_n \cos(B_n t)\mathrm{e}^{-A_n t}\right\}, \tag{3.7}$$

is obtained from the analytical solution of an off-diagonal element of the density matrix in the dressed-state basis $\rho_{12}^{nn}(t) = \mathrm{e}^{(-A_n \pm \mathrm{i}B_n)t}\rho_{12}^{nn}(0)$. The damping rate A_n is

$$A_n = (n+1)\kappa(n)\{\hat{n}(n) + \tfrac{1}{2}\} \equiv A_n^{\rm di}, \tag{3.8}$$

$$A_n = \tfrac{1}{2}\kappa(n)\{\hat{n}(n) + \tfrac{1}{2}\} \equiv A_n^{\rm vi}, \tag{3.9}$$

for the imperfect dipole transition case (3.8), and for the fluctuation of the vibrational potential case (3.9), where $\bar{n}(n)$ is the mean reservoir boson number given by

$$\hat{n}(n) = (\mathrm{e}^{2\hbar g\sqrt{n+1}/k_{\rm B}T} - 1)^{-1},$$

Downloaded from rsta.royalsocietypublishing.org

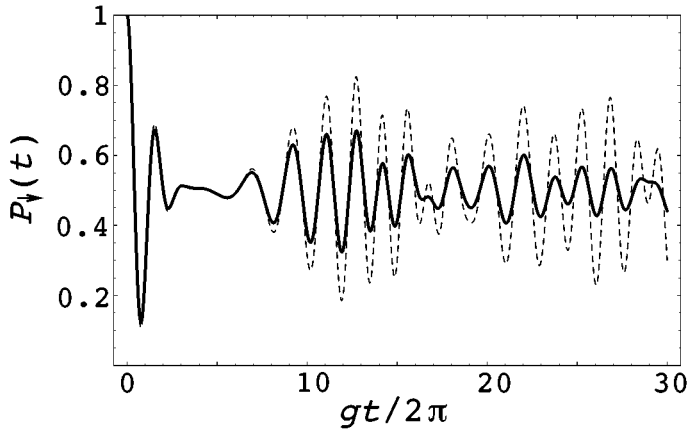


Figure 2. The population of the lower atomic state $P_\downarrow(t)$ with the initial state being the product of $|\downarrow\rangle_a$ for the atomic state and a *coherent* state $|3.0\rangle_m$ for the motional state. The dashed line is for no decoherence and the solid line is for the case of imperfect dipole transition with the coefficients $d = 0.4$ and $\tilde{\gamma}_0 = 0.127$, which corresponds to the experiment of Meekhof *et al.* (1996).

and $\kappa(n)$ is assumed to be given:

$$\kappa(n) \approx (2\hbar g\sqrt{n+1})^d.$$

The effects of the zero-frequency reservoir bosons are neglected. The coherent part B_n is given by

$$B_n = \sqrt{4g^2(n+1) - A_n^2}.$$

The results for the decoherence rates $A_n^{\rm di}$ (3.8) and $A_n^{\rm vi}$ (3.9) show that decoherence originates in the relaxation of density matrix elements that are diagonal in the boson quantum number but off-diagonal in the spin quantum numbers in the dressed-state basis. This relaxation is caused by the coupling to reservoir bosons at frequencies of $2g\sqrt{n+1}$. The effective contribution of reservoir bosons at frequencies of $2g\sqrt{n+1}$ is a key to understanding the decoherence rate. The Rabi frequency g in the experiment (Meekhof *et al.* 1996) is around 100 kHz, so reservoir bosons of order 100 kHz may be responsible for decoherence. These reservoir bosons have much lower frequencies than those responsible for spontaneous emission of atomic states, which are of the order of GHz, and also population decay of motional states, which are of the order 10 MHz. This low-frequency nature of the reservoir boson suggests that the reservoir has a *high-temperature* nature, whereas in the optical frequency regime, the corresponding reservoir is often approximated at zero temperature. Thus we can have the high-temperature limit. This limit represents the classical noise where the reservoir operators commute. Introducing normalized values, $\tilde{A}_n^{\rm di} = A_n^{\rm di}/g$, $\tilde{A}_n^{\rm vi} = A_n^{\rm vi}/g$, $\tilde{\gamma}_0 = \gamma_0/g$, $\tilde{\kappa}(n) = \kappa(n)/g$, the normalized decoherence rates are

$$\tilde{A}_n^{\rm di} = \tilde{\gamma}_0(n+1)^{(d+1)/2}, \tag{3.10}$$

$$\tilde{A}_n^{\rm vi} = \tilde{\gamma}_0(n+1)^{(d-1)/2}. \tag{3.11}$$

To get an exponent of 0.7 for the factor $(n+1)$ suggested by the experiment (Meekhof *et al.* 1996), we need $d \approx 0.4$ for the imperfect dipole transition case and $d \approx 2.4$ for

Downloaded from rsta.royalsocietypublishing.org

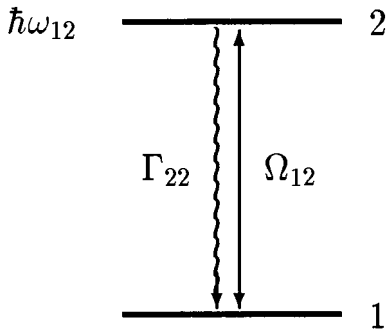


Figure 3. A two-level system storing a quantum bit.

the case of fluctuations of the vibrational potential. Figure 2 illustrates the effect of such decoherence on ion state populations.

The sources of decoherence so far considered derive from instrumental imperfections which are likely to improve in the future. If we imagine they can be entirely overcome, only fundamental sources of decoherence such as spontaneous emission would remain. We now examine the consequences for quantum computation of this kind of decoherence (Plenio & Knight 1996, 1997). Spontaneous decay would terminate the coherent superposition necessary for quantum computation.

An *elementary time-step* (a coherent gate operation) takes the time $\tau_{\rm el}$ and factorization of an L-bit number requires of the order of ϵL^3 elementary time-steps where ϵ is of order 400. This results in a total computation time T of

$$T \sim \epsilon \tau_{\rm el} L^3. \tag{3.12}$$

The *decoherence time* of a single qubit is $\tau_{\rm dec}$ and the decoherence time for $5L+2$ (this number is required for factorization) qubits is

$$\tau_{\rm dec} = \tau_{\rm qb}/5L. \tag{3.13}$$

To prevent spontaneous emission during the computation we need $\tau_{\rm qb} \gg 5\epsilon\tau_{\rm el}L^4$. However, the larger the decoherence time $\tau_{\rm qb}$, the longer is the elementary time-step $\tau_{\rm el}$ (Plenio & Knight 1996)!

If we use a two-level system as a qubit, as shown in figure 3, then the coherent gate operation is determined by the coherent Rabi frequency Ω_{12} But the Rabi frequency Ω_{12} and the spontaneous emission decay rate Γ_{22} are *not independent*. We have

$$\frac{\Omega_{12}^2}{\Gamma_{22}} = \frac{6\pi c^3 \epsilon_0}{\hbar\omega_{12}^3} E^2, \tag{3.14}$$

where E is the electric field strength of the laser (Plenio & Knight 1996, 1997). An upper limit for E is the tunnelling ionization field strength, which for hydrogen has the value $E \cong 5.8 \times 10^{11}\ \mathrm{V\,m^{-1}}$.

In the implementation of a C-NOT in an ion trap, the COM mode has to be excited and de-excited twice. This requires a full 4π rotation with the Hamiltonian

$$H = \frac{\eta}{\sqrt{5L}} \tfrac{1}{2}\Omega_{12}[|e\rangle\langle g|a + |g\rangle\langle e|a^\dagger], \tag{3.15}$$

Downloaded from rsta.royalsocietypublishing.org

Table 1. *Factorization limits*

L	$T \gg$	$\Gamma \ll$
4	6.4×10^{-3} s	77×10^{-2} s^{-1}
40	6.4×10^{5} s	77×10^{-11} s^{-1}

where η is the Lamb–Dicke parameter, and a, $a^{\dagger}$ are the vibrational annihilation and creation operators. One needs ϵL^3 elementary steps τ_{el} so that

$$T \approx 4\pi \frac{\sqrt{5L}}{\eta \Omega_{12}} \epsilon L^3. \tag{3.16}$$

To have no spontaneous emission during the calculation we require

$$\frac{1}{5L\Gamma_{22}} = \tau_{\mathrm{dec}} \gg T = \frac{4\pi\epsilon}{\Omega_{12}} \sqrt{\frac{5L^7}{\eta^2}}. \tag{3.17}$$

Using equation (3.14) this leads to

$$\frac{1}{\Gamma_{22}} \gg \frac{2000\pi^2\epsilon^2}{\eta^2} \frac{\Gamma_{22}}{\Omega_{12}^2} L^9. \tag{3.18}$$

For the total computation time we obtain

$$T \gg 400\pi^2 \left(\frac{\epsilon}{\eta}\right)^2 \frac{\Gamma_{22}}{\Omega_{12}^2} L^8. \tag{3.19}$$

Some values for T assuming $\eta = 1$, $\Omega^2/\Gamma = 10^{16}$ s$^{1/2}$ and $\epsilon = 500$ are shown in table 1.

For example, to factorize the 23-digit number

$$41\,141\,158\,551\,285\,430\,224\,619 = 34\,802\,904\,313 \times 1\,182\,118\,543\,363 \tag{3.20}$$

on a quantum computer one needs about

$$1.4 \times 10^8 \text{ s} \approx 3.6 \text{ years}. \tag{3.21}$$

MATHEMATICA does it in 25 s on a workstation! Some of us have shown elsewhere how breakdown of the two-state model for the qubit imposes even more stringent restrictions on quantum computation (Plenio & Knight 1997).

These considerations showed the need to use quantum error correction methods to stabilize the system against noise. However, quantum error correction methods are implemented as short quantum computations themselves and suffer from errors. To avoid this problem the new idea of fault-tolerant quantum computation (Shor 1994, 1995) was introduced. The idea is to encode the qubits in such a way that the encoding does not introduce more errors than previously were present. If the error stays at the same level we then keep performing error correction until the error has decreased in magnitude (Shor 1996; DiVincenzo & Shor 1996; Plenio *et al.* 1997). The present state of the art requires 5–10 qubits to encode a single qubit against a single error. It is the iterative application 'in depth' of the encoding that will enable us to reduce error to an arbitrarily small level providing it is below a certain level to start with. In other words we will be encoding the encoding bits.

Downloaded from rsta.royalsocietypublishing.org

We have seen above how to estimate the accuracy threshold for quantum computation with a simple argument and we have given elsewhere (Plenio & Knight 1997) the numbers that arise from more precise explicit constructions of error correction schemes. We have seen that the incoherent error rate per quantum gate should not be higher than around 10^{-6}. In a more detailed analysis (Knill *et al*. 1996) it was shown that the execution of one quantum gate on an encoded qubit requires in the order of $N = 10^6$ operations, which confirms the qualitative estimates given by arguments of the kind given above. We will now see whether accuracies of that order can be achieved in a linear ion-trap realization of the quantum computer by using Zeeman sublevels as qubits in the chosen ions. We emphasize that we take into account only the spontaneous emission of the ions and assume that all the other errors have been eliminated.

We calculate the probability of suffering at least one spontaneous emission during the implementation of N quantum gates. This probability has to be smaller than unity. We represent the qubit by two Zeeman sublevels and use Raman pulses to transfer population between the two states. For the time required to perform N quantum gates we find $T = N8\pi\Delta_2/\Omega_{02}^2$. From that we obtain the probability for a spontaneous emission from level two as $p_2 = 8\pi\Gamma_{22}N/\Delta_2$. Again we have to take into account the fact that the two-level approximation can break down. This leads to an additional independent source of spontaneous emission via extraneous levels. One finally obtains the probability of having a spontaneous emission from an extraneous level:

$$p_3 = \frac{80\Gamma_{33}^2\pi^2N^2L}{\Delta_{13}^2\beta\eta^2}\left(\frac{\omega_{12}}{\omega_{13}}\right)^3. \tag{3.22}$$

The total probability of a spontaneous emission is $p_{\mathrm{tot}} = p_2 + p_3$ and therefore the error rate per quantum gate is

$$r = \frac{p_{\mathrm{tot}}}{N} = \sqrt{\frac{320L}{\beta}}\frac{\pi\Gamma_{33}}{\Delta_{13}\eta}\left(\frac{\omega_{12}}{\omega_{13}}\right)^{3/2}. \tag{3.23}$$

We use the data for the ions given in (Plenio & Knight 1997). If we assume $\eta = 1$, $\beta = 1$ (Knill *et al*. 1996), $L = 7$ and an optimistic $N = 10^6$ we see that even for barium the probability for at least one emission is almost unity. The explicit values are: for barium, $r = 0.44 \times 10^{-6}$; for mercury, $r = 9.26 \times 10^{-6}$; and for calcium, $r = 2.03 \times 10^{-6}$. This means that unless the encoding procedures given in Knill *et al*. (1996) and Aharonov & Ben-Or (1996) can be improved substantially the accuracy threshold for quantum computation will not be achievable. Some progress in this direction has been made recently (Steane 1997). We conclude that the ion-trap computer is at present incapable of very large-scale computations, so we next look at some simpler, but equally fundamental and useful problems, which can be solved by using such realizations.

4. Generalization of entanglement swapping

There are many interesting manipulations of entanglement (though not computations) that one can do with a limited number of qubits, and as such these are potentially testable applications. An interesting scheme in this category is entanglement swapping. We first briefly recapitulate the original version of this scheme (Zukowski

Downloaded from rsta.royalsocietypublishing.org

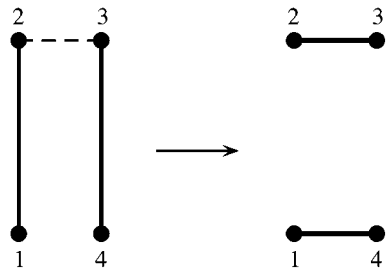


Figure 4. The swapping of entanglement between pairs of particles due to a Bell state measurement on two of them is shown. The bold lines connect particles in Bell states and the dashed line connects particles on which the Bell state measurement is made.

et al. 1993). Consider an initial state of four particles 1, 2, 3 and 4, in which particles 1 and 2 are mutually entangled (in a Bell state), and particles 3 and 4 are mutually entangled (also in a Bell state). If one conducts a measurement of the Bell operator on particles 2 and 3 (which projects particles 2 and 3 to a Bell state), then the particles 1 and 4 are also instantaneously projected to one of the Bell states. Whereas prior to the measurement, the Bell pairs were $(1,2)$ and $(3,4)$, after the measurement the Bell pairs are $(2,3)$ and $(1,4)$. A pictorial way of representing the above process is given in figure 4. It is clear that the most interesting aspect of this scheme is that particles 1 and 4, which do not share any common past, are entangled after the swapping.

We have generalized the method of entanglement manipulation described above to cases where a greater number of particles are involved (Bose *et al*. 1998). But before that we need to introduce some notation and terminology. In terms of a binary variable $u_i \in \{0,1\}$ and its complement u_i^c (defined as $1-u_i$), one can write down any Bell state (not normalized) of two particles i and j as

$$|\Psi(i,j)\rangle_{\pm} = |u_i, u_j\rangle \pm |u_i^c, u_j^c\rangle. \tag{4.1}$$

In the above it is understood that $|u_i\rangle$ and $|u_i^c\rangle$ are two orthogonal states of a two-state system. Then N-particle generalization of Bell states will be states of the type

$$|\psi\rangle = \prod_{i=1}^{N} |u_i\rangle \pm \prod_{i=1}^{N} |u_i^c\rangle. \tag{4.2}$$

For the $N=2$ they reduce to the Bell states and for $N=3,4$ they represent the GHZ states. For a general N we shall call them cat states. We shall show that the original entanglement swapping scheme can be generalized to the case of starting with cat states involving any number of particles, doing local measurements by selecting any number of particles from the different cat states and also ending up with cat states involving any number of particles. To see that consider an initial state in which there are N different sets of entangled particles in cat states. Let each of these sets be labelled by m (where $m=1,2,\ldots,N$), the ith particle of the mth set be labelled by $i(m)$ and the total number of particles in the mth set be n_m. Then the initial state can be represented by

$$|\Psi\rangle = \prod_{m=1}^{N} |\Psi\rangle_m, \tag{4.3}$$

Downloaded from rsta.royalsocietypublishing.org

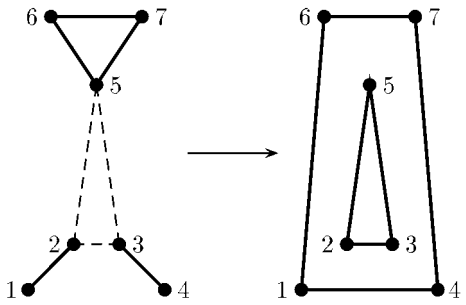


Figure 5. The conversion of two Bell states and a three-particle GHZ state to a three-particle GHZ state and a four particle GHZ state due to a GHZ state projection on three particles (one taken from each of the initially entangled sets) is shown. The bold lines connect mutually entangled particles and the dashed lines connect particles on which the GHZ state projection is made.

in which each of the cat states $|\Psi\rangle_m$ is given by

$$|\Psi\rangle_m = \prod_{i=1}^{n_m} |u_{i(m)}\rangle \pm \prod_{i=1}^{n_m} |u^{\mathrm{c}}_{i(m)}\rangle, \tag{4.4}$$

where the symbols $u_{i(m)}$ stand for binary variables $\in \{0,1\}$ with $u^{\mathrm{c}}_{i(m)} = 1 - u_{i(m)}$. Now imagine that the first p_m particles from all the entangled sets are brought together (i.e. there is a total of $p = \sum_{m=1}^{N} p_m$ particles) and a joint measurement is performed on all of them. Note that the set of all cat states of p particles forms a complete orthonormal basis. Let the nature of the measurement on the selected particles be such that it projects them to this basis. Such a basis will be composed of states of the type,

$$|\Psi(p)\rangle = \prod_{m=1}^{N} \prod_{i=1}^{p_m} |u_{i(m)}\rangle \pm \prod_{m=1}^{N} \prod_{i=1}^{p_m} |u^{\mathrm{c}}_{i(m)}\rangle. \tag{4.5}$$

By simply operating with $|\Psi(p)\rangle\langle\Psi(p)|$ on $|\Psi\rangle$ of equation (4.3), we find that the rest of the particles (i.e. those not being measured) are projected to states of the type,

$$\left|\Psi\left(\sum_{m=1}^{N} n_m - p\right)\right\rangle = \prod_{m=1}^{N} \prod_{i=p_m+1}^{n_m} |u_{i(m)}\rangle \pm \prod_{m=1}^{N} \prod_{i=p_m+1}^{n_m} |u^{\mathrm{c}}_{i(m)}\rangle, \tag{4.6}$$

which represents a cat state of the rest of the particles. In a schematic way the above process can be represented as

$$\prod_{m=1}^{N} |E(n_m)\rangle \rightarrow |E(p)\rangle \otimes \left|E\left(\sum_{m=1}^{N} n_m - p\right)\right\rangle, \tag{4.7}$$

where $|E(n)\rangle$ denotes an n-particle cat state. As a specific example, in figure 5, we have shown the conversion of a collection of two Bell states and a three-particle GHZ state to a three-particle GHZ state and a four-particle GHZ state due to a projection of three of these particles to a three-particle GHZ state.

As must be evident from figure 5, there is a general 'pencil and paper' rule for finding out the result when our method of entanglement manipulation is applied to

Downloaded from rsta.royalsocietypublishing.org

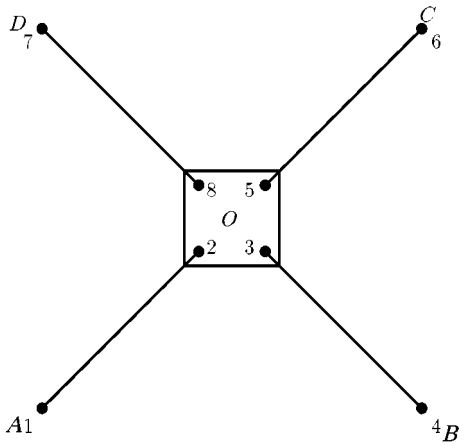


Figure 6. The configuration used for the distribution of entanglement. Initially users A, B, C and D share Bell pairs with the central exchange O. Subsequently, a local measurement at O is sufficient to entangle particles belonging to any subset of users chosen from A, B, C and D.

a certain collection of cat states of particles. One just has to connect the particles being measured to frame a polygon and those not being measured to frame a complementary polygon. These two polygons represent the two multiparticle cat states obtained after the manipulation.

This scheme can be used for practical purposes such as constructing a *quantum telephone exchange*, speeding up the distribution of entangled particles between two parties and a sort of series purification (Bose *et al*. 1998). We describe the first application in some detail below.

5. Quantum telephone exchange

Suppose there are N users in a communication network. To begin with, each user of the network needs to share entangled pairs of particles (in a Bell state) with a central exchange. Consider figure 6: A, B, C and D are users who share the Bell pairs $(1,2)$, $(3,4)$, $(5,6)$ and $(7,8)$, respectively, with a central exchange O. Now suppose that A, B and C wish to share a GHZ triplet. Then a measurement which projects particles 2, 3 and 5 to GHZ states will have to be performed at O. Immediately, particles 1, 4 and 6 belonging to A, B and C, respectively, will be reduced to a GHZ state. In a similar manner one can entangle particles belonging to any N users of the network and create an N-particle cat state.

The main advantages of using this technique for establishing entanglement over the simple generation of N-particle entangled states at a source and their subsequent distribution are as follows.

(1) Each user can at first purify a large number of partially decohered Bell pairs shared with the central exchange to obtain a smaller number of pure shared Bell pairs. These can then be used as the starting point for the generation of any types of multiparticle cat states of the particles possessed by the users. The problems of decoherence during propagation of the particles can thus be avoided in principle. Also the necessity of having to purify N-particle cat states can be totally avoided.

Downloaded from rsta.royalsocietypublishing.org

Purification of singlets followed by our scheme will generate N-particle cat states in their purest form.

(2) Our method allows a certain degree of freedom to entangle particles belonging to any set of users only if the necessity arises. It may not be known in advance exactly which set of users will need to share an N-particle cat state. To arrange for all possibilities in an *a priori* fashion would require selecting all possible combinations of users and distributing particles in multiparticle entangled states among them. That is very uneconomical. On the other hand, generating entangled N-tuplets at the time of need and supplying them to the users who wish to communicate is definitely time consuming.

It is pertinent to compare our scheme with the Biham–Huttner–Mor cryptographic network with exchanges (Biham *et al*. 1996). There are two main differences: first, they used a time-reversed Einstein–Podolsky–Rosen scheme for setting up the connections and had quantum memories to protect their states. We use a multiparticle generalization of entanglement swapping. Secondly, their prime focus was to connect any pair of users of an N-user network on request, while our main focus is to establish multiparticle entangled states of the particles possessed by the users. Of course, for completeness, we must highlight some uses of distributed multiparticle entanglement. An application that readily comes to mind is multiparty cryptographic conferencing. We have found another interesting application. When $N+1$ users in a network share one particle each from an $N+1$-particle cat state, then one of these users can read messages sent by all the others through a single measurement. This is a multiparticle generalization of the superdense coding scheme (Bennett & Wiesner 1992). We have been able to show that though our scheme uses a far less number of particles, the rate at which a receiver receives information in this scheme is the same as the rate at which he would receive information if he was separately doing superdense coded communication with each of the users (Bose *et al*. 1998).

6. Quantum communication

Having demonstrated how entanglement may be manipulated, we next turn to a discussion of how it may be used to improve communication channel capacities. But first we need to quantify how much entanglement we possess within a given state. We have recently shown how to construct a whole class of measures of entanglement (Vedral *et al*. 1997; Vedral & Plenio 1998), and also imposed conditions that any candidate for such a measure has to satisfy (Vedral *et al*. 1997). In short, we consider the disentangled states which form a convex subset of the set of all quantum states. Entanglement is then defined as a distance (not necessarily in the mathematical sense) from a given state to this subset of disentangled states. An attractive feature of our measure is that it is independent of the number of systems and their dimensionality, and is therefore completely general (Vedral *et al*. 1997; Vedral & Plenio 1998). It should be noted that in much the same way we can quantify the amount of classical correlation in a state. One would then define another subset, namely that of all product states which do not contain any classical correlations. Given a disentangled state one would then look for the closest uncorrelated state. The distance could be interpreted as a measure of classical correlation. Let $E(\sigma)$ be the amount of entanglement in a state σ. Then we impose the following physically motivated conditions.

Downloaded from rsta.royalsocietypublishing.org

(E1) $E(\sigma) = 0$ iff σ is separable (disentangled), i.e.

$$\sigma = \sum p_i \sigma_A^i \otimes \sigma_B^i.$$

(E2) Local unitary operations leave $E(\sigma)$ invariant, i.e.

$$E(\sigma) = E(U_A \otimes U_B \sigma U_A^\dagger \otimes U_B^\dagger).$$

(E3) The expected entanglement cannot increase under local operations aided with classical communication, given by $\sum V_i^\dagger V_i = \mathbf{1}$, i.e.

$$\sum \mathrm{tr}(\sigma_i) E(\sigma_i/\mathrm{tr}(\sigma_i)) \leqslant E(\sigma), \tag{6.1}$$

where $\sigma_i = V_i \sigma V_i^\dagger$.

(E4) $E(\sigma)$ is continuous.

(E5) $E(\sigma)$ reduces to the von Neumann entropy for pure states.

(E6) Additivity of $E(\sigma)$: $E(\sigma_1 \otimes \sigma_2) = E(\sigma_1) + E(\sigma_2)$, meaning that the entanglement of two separated entangled pairs is equal to the sum of the entanglement of the individual pairs.

The only choice that we have found so far satisfying the above is

$$E(\sigma) := \min_{\rho \in \mathcal{D}} S(\sigma || \rho), \tag{6.2}$$

where $S(\sigma||\rho) = \mathrm{tr}(\sigma \ln \sigma - \sigma \ln \rho)$ is the quantum relative entropy, and $\mathcal{D}$ is the set of disentangled (separable) states. We call this measure the *relative entropy of entanglement*.

What is interesting is that this quantity in addition represents an upper bound to any purification procedure (see, for example, Bennett *et al*. 1996). Namely, if Alice and Bob start with an ensemble of N entangled qubits in a state σ, then the maximum number of singlets, M, distillable by local operations is governed by the formula

$$NE(\sigma) \geqslant M \ln 2. \tag{6.3}$$

This being so, we can easily see that $E(\sigma)$ provides an upper bound related to the quantum capacity of certain quantum communication channels. In a quantum communication protocol Alice receives a quantum system in an unknown state which she then wishes to transmit to Bob as reliably as possible through a noisy quantum channel. They might use any quantum resource including entanglement to achieve this. For example, Alice might create a maximally entangled pair, and send one of the particles to Bob through the noisy channel. Once they share a number of partly entangled pairs they can purify them to singlets and then use a teleportation protocol for perfect transmission. In this case, the rate at which Alice can transmit quantum information (i.e. the channel capacity) will depend on how efficiently they can purify and that in turn depends on the entanglement of the shared imperfect pairs. In this case the capacity would be equal to $E(\sigma)$. It remains to be seen whether this is the most efficient way of quantum transmission, and at present the question of quantifying the quantum channel capacity remains unclear (Lloyd 1997; Schumacher & Nielsen 1996).

Downloaded from rsta.royalsocietypublishing.org

7. Conclusions

We have studied the impact of spontaneous emission on the practical applicability of quantum computation in linear ion traps and especially the possibility of using a quantum computer to factorize large numbers. We conclude that with present technology such a factorization will not be possible even if we employ sophisticated methods of quantum error correction. We have shown that the numbers that can be factorized will be restricted to almost trivial sizes. We then investigated the minimal error rate per quantum gate and compared it to recently established accuracy thresholds that would, in principle, allow arbitrarily complicated quantum computations. We find that the presently known thresholds cannot be achieved because of spontaneous emission alone. Other sources of error would lead to even stronger limitations. We conclude that new physical ideas are therefore necessary if the goal of practically useful quantum computation is to be reached. For this reason we have turned to applications which require only small-scale quantum systems.

This work was supported by a European TMR Research Network ERB 4061PL95-1412 grant, the European TMR Research Network on Cavity QED, the UK Engineering and Physical Sciences Research Council, by a Feodor-Lynen grant of the Alexander von Humboldt Foundation, by the Japan Society for the Promotion of Science and by the Knight Trust.

References

Aharonov, D. & Ben-Or, M. 1996 Fault tolerant quantum computation with constant error. quant-ph/9611029.

Bennett, C. H. 1989 Time–space trade-offs for reversible computation. *SIAM Jl Comput.* **18**, 766–776.

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

Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A. & Wootters, W. K. 1996 Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722.

Biham, E., Huttner, B. & Mor, T. 1996 Quantum cryptographic network-based on quantum memories. *Phys. Rev.* A **54**, 2651–2658.

Bose, S., Vedral, V. & Knight, P. L. 1998 Multiparticle generalization of entanglement swapping. *Phys. Rev.* A **57**, 822–829.

Cirac, J. I. & Zoller, P. 1995 Quantum compuation with cold trapped ions. *Phys. Rev. Lett.* **74**, 4091–4094.

Deutsch, D. 1985 Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. Lond.* A **400**, 97–117.

Deutsch, D. 1989 Quantum computational networks. *Proc. R. Soc. Lond.* A **425**, 73–90.

Deutsch, D. 1997 *The fabric of reality*. London: Viking–Penguin.

Deutsch, D. & Jozsa, R. 1992 Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond.* A **439**, 553–558.

DiVincenzo, D. P. & Shor, P. W. 1996 Fault-tolerant error correction with efficient quantum codes. *Phys. Rev. Lett.* **77**, 3260–3263.

Ekert, A. & Jozsa, R. 1996 Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.* **68**, 733–753.

Grover, L. K. 1997 Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325–328.

Downloaded from rsta.royalsocietypublishing.org

Knill, E., Laflamme, R. & Zurek, W. 1996 Accuracy threshold for quantum computation. quant-ph/9610011.

Lloyd, S. 1997 Capacity of the noisy quantum channel. *Phys. Rev.* A **55**, 1613–1622.

Meekhof, D. M., Monroe, C., King, B. E., Itano, W. M. & Wineland, D. J. 1996 Generation of nonclassical motional states of a trapped atom. *Phys. Rev. Lett.* **76**, 1796–1799.

Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M. & Wineland, D. J. 1995 Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.* **75**, 4714–4717.

Murao, M. 1997 Relaxation and decoherence of two strongly coupled spin-$\frac{1}{2}$ particles. *J. Phys. Soc. Jap.* **66**, 2314–2323.

Murao, M. & Knight, P. L. 1998 Decoherence in nonclassical motional states of a trapped ion. *Phys. Rev.* A. (In the press.)

Murao, M. & Shibata, F. 1995 Dynamics of a dissipative Jaynes–Cummings model. *J. Phys. Soc. Jap.* **64**, 2394–2404.

Plenio, M. B. & Knight, P. L. 1996 Realistic lower bounds for the factorization time of large numbers on a quantum computer. *Phys. Rev.* A **53**, 2986–2990.

Plenio, M. B. & Knight, P. L. 1997 Decoherence limits to quantum computation using trapped ions. *Proc. R. Soc. Lond.* A **453**, 2017–2041.

Plenio, M. B., Vedral, V. & Knight, P. L. 1997 Conditional generation of error syndromes in fault-tolerant error correction. *Phys. Rev.* A **55**, 4593–4596.

Schumacher, B. & Nielsen, M. A. 1996 Quantum data processing and error correction. *Phys. Rev.* A **54**, 2629–2635.

Shibata, F. & Arimitsu, T. 1980 Expansion formulae in nonequilibirum statistical mechanics. *J. Phys. Soc. Jap.* **49**, 891–897.

Shor, P. W. 1994 In *Proc. 35th A. Symp. on the Theory of Computer Science* (ed. S. Goldwasser), p. 124. Los Alamitos, CA: IEEE.

Shor, P. W. 1995 Scheme for reducing decoherence in quantum computer memory. *Phys. Rev.* A **52**, 2493–2496.

Shor, P. W. 1996 Fault-tolerant quantum computation. quant-ph/9605011.

Shore, B. W. & Knight, P.L. 1993 The Jaynes–Cummings model. *J. Mod. Opt.* **40**, 1195–1238.

Steane, A. M. 1997 Active stabilization, quantum computation and quantum state synthesis. *Phys. Rev. Lett.* **78**, 2252–2255.

Vedral, V. & Plenio, M. B. 1998 Entanglement measures and purification procedures. *Phys. Rev.* A **57**, 1619–1633.

Vedral, V., Barenco, A. & Ekert, A. 1996 Quantum networks for simple arithmetic operations. *Phys. Rev.* A **54**, 147–153.

Vedral, V., Plenio, M. B., Rippin, M. A. & Knight, P. L. 1997 Quantifying entanglement. *Phys. Rev. Lett.* **78**, 2275–2279.

Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. 1993 Event-ready-detections Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287–4290.

Discussion

B. Christianson (*Computer Science Department, University of Hertfordshire, Hatfield, UK*). Presumably, photon teleportation would allow quantum cryptographic link-pairs to be connected into a network providing an end-to-end key service with strong privacy. The switching crossbar consists of a bank of Bell measurement devices that entangle the correct pairs of photons using routing information provided over a classical side-channel. The end-points act as if directly connected (except one end must transform measurements by the rotations notified over the side-channel). The end-points need not trust the honesty or competence of the teleporting switches,

Downloaded from rsta.royalsocietypublishing.org

which they treat simply as suspected eavesdroppers. The number of link-pairs required drops from order N^2 to order N, but trust is still end-to-end. Of course, just as with a single quantum link (and just as with classical cryptography), some conceptually separate mechanism is needed to verify the authenticity/identity of the actual partner end-point with which they key has been privately shared.

P. L. Knight. I agree with Dr Christian on this privacy aspect to teleported signals, and with the need for authentification procedures.

B. Josephson (*Cavendish Laboratory, University of Cambridge*). I am finding these manipulations one can perform with quantum information fascinating, and was struck particularly by Professor Knight's comments concerning 'coherent manipulation at a distance'. Can there be a connection between these phenomena, and the much-derided 'paranormal phenomena' (examples of the latter being psychokinesis and extra-sensory perception)? If biosystems have learned to execute the kinds of subtle manipulation that we scientists are only just beginning to acquire the ability to perform ourselves (and which organisms may well be able to use with some benefit), then phenomena of the kind we term paranormal may be the natural consequence.

P. L. Knight. Coherent manipulation of quantum states and teleportation are highly sensitive to dissipation. Living systems are of course *open* systems, dependent on dissipation, and may not be viewed as the closed quantum systems shielded from decoherence that we are concerned with in quantum information processing. Nevertheless, biological systems can and do use quantum effects (such as energy exchange in photosynthesis). I do not know of any evidence for quantum coherence in biological systems of the type discussed here.

Th. Beth (*University of Karlsruhe, Germany*). Quantum cryptography is not there to encypher information but rather to provide a secure random key exchange (similar to public key exchange). What evidence is there that the decoherence time is reciprocal to the number of qubits in the system?

P. L. Knight. Of course I agree that quantum cryptography is designed to provide secure key exchange so that encrypted messages can be sent on public channels. On the separate question of the dependence of decoherence rates on the reciprocal of the number of qubits, I note that this has been tested experimentally by the Paris group of Serge Haroche, who studied the effects of dissipation on cavity field superpositions. No experiments have been done yet, to my knowledge, on the decoherence rate of entangled two-state systems.

Downloaded from rsta.royalsocietypublishing.org

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES