Long-distance quantum communication with atomic ensembles and linear optics

L.-M. Duan*†, M. D. Lukin‡, J. I. Cirac* & P. Zoller*

** Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*
† Laboratory of Quantum Communication and Computation, USTC, Hefei 230026, China
‡ Physics Department and ITAMP, Harvard University, Cambridge, Massachusetts 02138, USA

Quantum communication holds promise for absolutely secure transmission of secret messages and the faithful transfer of unknown quantum states. Photonic channels appear to be very attractive for the physical implementation of quantum communication. However, owing to losses and decoherence in the channel, the communication fidelity decreases exponentially with the channel length. Here we describe a scheme that allows the implementation of robust quantum communication over long lossy channels. The scheme involves laser manipulation of atomic ensembles, beam splitters, and single-photon detectors with moderate efficiencies, and is therefore compatible with current experimental technology. We show that the communication efficiency scales polynomially with the channel length, and hence the scheme should be operable over very long distances.

The goal of quantum communication is to transmit quantum states between distant sites. Such transmission has potential application in the secret transfer of classical messages by means of quantum cryptography[1], and is also an essential element in the construction of quantum networks. The basic problem of quantum communication is to generate nearly perfect entangled states between distant sites. Such states can be used, for example, to implement secure quantum cryptography using the Ekert protocol[1], and to faithfully transfer quantum states via quantum teleportation[2]. All realistic schemes for quantum communication are at present based on the use of photonic channels. However, the degree of entanglement generated between two distant sites normally decreases exponentially with the length of the connecting channel, because of optical absorption and other channel noise. To regain a high degree of entanglement, purification schemes can be used[3], but this does not fully solve the long-distance communication problem. Because of the exponential decay of the entanglement in the channel, an exponentially large number of partially entangled states are needed to obtain one highly entangled state, which means that for a sufficiently long distance the task becomes nearly impossible.

To overcome the difficulty associated with the exponential fidelity decay, the concept of quantum repeaters can be used[4]. In principle, this allows the overall communication fidelity to be made very close to unity, with the communication time growing only polynomially with transmission distance. In analogy to fault-tolerant quantum computing[5,6], the proposed quantum repeater is a cascaded entanglement-purification protocol for communication systems. The basic idea is to divide the transmission channel into many segments, with the length of each segment comparable to the channel attenuation length. First, entanglement is generated and purified for each segment; the purified entanglement is then extended to a greater length by connecting two adjacent segments through entanglement swapping[2,7]. After this swapping, the overall entanglement is decreased, and has to be purified again. The rounds of entanglement swapping and purification can be continued until nearly perfect entangled states are created between two distant sites.

To implement the quantum repeater protocol, we need to generate entanglement between distant quantum bits (qubits), store them for a sufficiently long time and perform local collective operations on several of these qubits. Quantum memory is essential, because all purification protocols are probabilistic. When entanglement purification is performed for each segment of the channel, quantum memory can be used to keep the segment state if the purification succeeds, and to repeat the purification for the segments only where the previous attempt fails. This is essential for ensuring polynomial scaling in the communication efficiency, because if there were no available memory, the purifications for all the segments would need to succeed at the same time; the probability of such an event decreases exponentially with channel length. The requirement of quantum memory implies that we need to store the local qubits in atomic internal states instead of photonic states, as it is difficult to store photons for a reasonably long time. With atoms as the local information carriers, it seems to be very hard to implement quantum repeaters: normally, one needs to achieve the strong coupling between atoms and photons by using high-finesse cavities for atomic entanglement generation, purification, and swapping[8,9], which, in spite of recent experimental advances[10–12], remains a very challenging technology.

Here we propose a different scheme, which realizes quantum repeaters and long-distance quantum communication with simple physical set-ups. The scheme is a combination of three significant advances in entanglement generation, connection, and applications, with each of the steps having built-in entanglement purification and resilience to realistic noise. The scheme for fault-tolerant entanglement generation originates from earlier proposals to entangle single atoms through single-photon interference at photodetectors[13,14]. But the present approach involves collective excitations in atomic ensembles rather than in single particles, which allows simpler realization and greatly improved generation efficiency. This is due to collectively enhanced coupling to light, which has been recently investigated both theoretically[15–19] and experimentally[20–22]. The entanglement connection is achieved through simple linear optical operations, and is inherently robust against realistic imperfections. Different schemes with linear optics have been proposed recently for quantum computation[23] and purification[24]. Finally, the resulting state of ensembles after the entanglement connection finds direct applications in realizing entanglement-based quantum communication protocols, such as quantum teleportation, cryptography, and Bell inequality detection. In all of these applications, the mixed entanglement is purified automatically to nearly perfect entanglement. As a combination of these three advances, our scheme circumvents the realistic noise and imperfections, and provides a feasible method of long-distance high-fidelity quantum communication. The required overhead in communication time increases with distance only polynomially.

Entanglement generation

The basic element of our system is a cloud of N_a identical atoms with

the relevant level structure shown in Fig. 1. A pair of metastable lower states $|g\rangle$ and $|s\rangle$ can correspond to—for example—hyperfine or Zeeman sublevels of the electronic ground state of alkali-metal atoms. Long lifetimes for the relevant coherence have been observed both in a room-temperature dilute atomic gas (see, for example, ref. 21) and in a sample of cold trapped atoms (see, for example, refs 20, 22). To facilitate enhanced coupling to light, the atomic medium is preferably optically thick along one direction. This can be achieved either by working with a pencil-shaped atomic sample[20–22] or by placing the sample in a low-finesse ring cavity[17,25] (see Supplementary Information).

All the atoms are initially prepared in the ground state $|g\rangle$. A sample is illuminated by a short, off-resonant laser pulse that induces Raman transitions into the states $|s\rangle$. We are particularly interested in the forward-scattered Stokes light that is co-propagating with the laser. Such scattering events are uniquely correlated with the excitation of the symmetric collective atomic mode S (refs 15–22) given by $S \equiv (1/\sqrt{N_a})\Sigma_i |g\rangle_i \langle s|$, where the summation is taken over all the atoms. In particular, an emission of the single Stokes photon in a forward direction results in the state of atomic ensemble given by $S^\dagger|0_a\rangle$, where the ensemble ground state $|0_a\rangle \equiv \otimes_i |g\rangle_i$).

We assume that the light–atom interaction time t_Δ is short, so that the mean photon number in the forward-scattered Stokes pulse is much smaller than 1. We can define an effective single-mode bosonic operator a for this Stokes pulse with the corresponding vacuum state denoted by $|0_p\rangle$. The whole state of the atomic collective mode and the forward-scattering Stokes mode can now be written in the following form (see Supplementary Information for details)

$$|\phi\rangle = |0_a\rangle|0_p\rangle + \sqrt{p_c}S^\dagger a^\dagger|0_a\rangle|0_p\rangle + o(p_c) \quad (1)$$

where p_c is the small excitation probability, and $o(p_c)$ represents the terms with more excitations whose probabilities are equal to or smaller than p_c^2. Before proceeding, we note that a fraction of light is emitted in other directions owing to spontaneous emissions. But whenever N_a is large, the contribution from the spontaneous emissions to the population in the symmetric collective mode is small[15–22]. As a result, we have a large signal-to-noise ratio for the processes involving the collective mode, which greatly enhances the efficiency of the present scheme (see Box 1 and Supplementary Information).

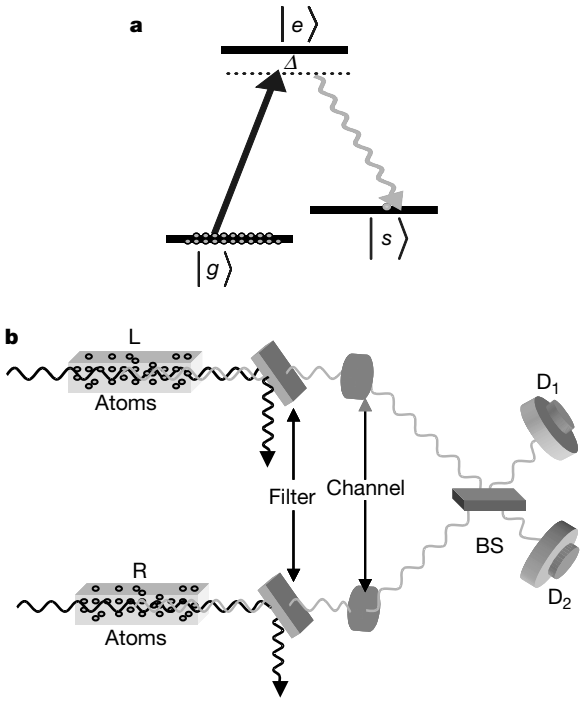

Figure 1 Set-up for entanglement generation. **a**, The relevant level structure of the atoms in the ensemble, with $|g\rangle$, the ground state, $|s\rangle$, the metastable state for storing a qubit, and $|e\rangle$, the excited state. The transition $|g\rangle \rightarrow |e\rangle$ is coupled by the classical laser (the pumping light) with the Rabi frequency Ω, and the forward-scattered Stokes light comes from the transition $|e\rangle \rightarrow |s\rangle$, which has a different polarization and frequency to the pumping light. For convenience, we assume off-resonant coupling with a large detuning Δ. **b**, Schematic set-up for generating entanglement between the two atomic ensembles L and R. The two ensembles are pencil-shaped, and illuminated by the synchronized classical pumping pulses. The forward-scattered Stokes pulses are collected and coupled to optical channels (such as fibres) after the filters, which are polarization- and frequency-selective to filter the pumping light. The pulses after the transmission channels interfere at a 50%-50% beam splitter BS, with the outputs detected respectively by two single-photon detectors D_1 and D_2. If there is a click in D_1 or D_2, the process is finished and we successfully generate entanglement between the ensembles L and R. Otherwise, we first apply a repumping pulse (to the transition $|s\rangle \rightarrow |e\rangle$) to the ensembles L and R, to set the state of the ensembles back to the ground state $|0_a\rangle_L \otimes |0_a\rangle_R$, then the same classical laser pulses as the first round are applied to the transition $|g\rangle \rightarrow |e\rangle$ and we detect again the forward-scattered Stokes pulses after the beam splitter. This process is repeated until finally we have a click in the D_1 or the D_2 detector.

Box 1

Collective enhancement

Long-lived excitations in atomic ensembles can be viewed as waves of excited spins. We are here particularly interested in the symmetric spin wave mode S. For a simple demonstration of collective enhancement, we assume that the atoms are placed in a low-finesse ring cavity[25], with a relevant cavity mode corresponding to forward-scattered Stokes radiation. The cavity-free case corresponds to the limit where the finesse tends to 1 (ref. 17). The interaction between the forward-scattered light mode and the atoms is described by the hamiltonian

$$H = \hbar\left(\sqrt{N_a}\Omega g_c/\Delta\right)S^\dagger b^\dagger + \text{h.c.}$$

where *h.c.* is the hermitian conjugation, $b^\dagger$ is the creation operator for cavity photons, Ω is the laser Rabi frequency, and g_c the atom–field coupling constant. In addition to coherent evolution, the photonic field mode can leak out of the cavity at a rate κ, whereas atomic coherence is dephased by spontaneous photon scattering into random directions that occurs at a rate $\gamma_s' = \Omega^2/\Delta^2\gamma_s$ for each atom, with γ_s being the natural linewidth of the electronic excited state. We emphasize that in the absence of superradiant effects, spontaneous emission events are independent for each atom.

In the bad-cavity limit, we can adiabatically eliminate the cavity mode, and the resulting dynamics for the collective atomic mode is described by the Heisenberg–Langevin equation (see Supplementary Information for details)

$$\dot{S}^\dagger = \frac{(\kappa' - \gamma_s')}{2}S^\dagger - \sqrt{\kappa'}b_{in}(t) + \text{noise}$$

where $\kappa' = 4|\Omega|^2 g_c^2 N_a/(\Delta^2\kappa)$, b_{in} is a vacuum field leading into the cavity, and the last term represents the fluctuating noise field corresponding to spontaneous emission. We note that the nature of the dynamics is determined by the ratio between the build-up of coherence due to forward-scattered photons κ' and coherence decay due to spontaneous emission γ_s'. The signal-to-noise ratio is therefore given by $R = \kappa'/\gamma_s' \equiv 4N_a g_c^2/(\kappa\gamma_s)$, which is large when a many-atom ensemble is used. In the cavity-free case, this expression corresponds to the optical depth (density-length product) of the sample. The result should be compared with the signal-to-noise ratio in the single-atom case $N_a = 1$, where to obtain $R > 1$ a high-Q microcavity is required[10–12]. The collective enhancement takes place because the coherent forward scattering involves only one collective atomic mode S, whereas the spontaneous emissions distribute excitation over all atomic modes. Therefore only a small fraction of spontaneous emission events influences the symmetric mode S, which results in a large signal-to-noise ratio.

We now show how to use this set-up to generate entanglement between two distant ensembles L (left) and R (right) using the configuration shown in Fig. 1. Here two laser pulses excite both ensembles simultaneously, and the whole system is described by the state $|\phi\rangle_L \otimes |\phi\rangle_R$, where $|\phi\rangle_L$ and $|\phi\rangle_R$ are given by equation (1) with all the operators and states distinguished by the subscript L or R. The forward-scattered Stokes light from both ensembles is combined at the beam splitter, and a photodetector click in either D_1 or D_2 measures the combined radiation from two samples, $a_+^\dagger a_+$ or $a_-^\dagger a_-$ with $a_\pm = (a_L \pm e^{i\varphi} a_R)/\sqrt{2}$. Here, φ denotes an unknown difference of the phase shifts in the left and the right side channels. We can also assume that φ has an imaginary part to account for the possible asymmetry of the set-up, which will also be corrected automatically in our scheme. But the set-up asymmetry can be easily made very small, and for simplicity of expressions we assume that φ is real in the following. Conditional on the detector click, we should apply a_+ or a_- to the whole state $|\phi\rangle_L \otimes |\phi\rangle_R$, and the projected state of the ensembles L and R is nearly maximally entangled, with the form (neglecting the high-order terms $o(p_c)$):

$$|\Psi_\varphi\rangle_{LR}^{\pm} = (S_L^\dagger \pm e^{i\varphi} S_R^\dagger)/\sqrt{2}|0_a\rangle_L |0_a\rangle_R \qquad (2)$$

The probability of getting a click is given by p_c for each round, so we need to repeat the process about $1/p_c$ times for a successful entanglement preparation, and the average preparation time is given by $T_0 \approx t_\Delta/p_c$. The states $|\Psi_\varphi\rangle_{LR}^{+}$ and $|\Psi_\varphi\rangle_{LR}^{-}$ can be transformed to each other by a simple local phase shift. Without loss of generality, we assume in the following that we generate the entangled state $|\Psi_\varphi\rangle_{LR}^{+}$.

As will be shown below, the presence of noise modifies the projected state of the ensembles to

$$\rho_{LR}(c_0, \varphi) = \frac{1}{c_0 + 1}(c_0 |0_a 0_a\rangle_{LR}\langle 0_a 0_a| + |\Psi_\varphi\rangle_{LR}^{+}\langle\Psi_\varphi|) \qquad (3)$$

where the 'vacuum' coefficient c_0 is determined by the dark count rates of the photon detectors. It will be seen below that any state in the form of equation (3) will be purified automatically to a maximally entangled state in the entanglement-based communication schemes. We therefore call this state an effective maximally entangled (EME) state, with the vacuum coefficient c_0 determining the purification efficiency.

Entanglement connection through swapping

After the successful generation of entanglement within the attenuation length, we want to extend the quantum communication distance. This is done through entanglement swapping with the configuration shown in Fig. 2. Suppose that we start with two pairs of entangled ensembles described by the state $\rho_{LI_1} \otimes \rho_{I_2R}$, where ρ_{LI_1} and ρ_{I_2R} are given by equation (3). In the ideal case, the set-up shown in Fig. 2 measures the quantities corresponding to operators $S_\pm^\dagger S_\pm$ with $S_\pm = (S_{I_1} \pm S_{I_2})/\sqrt{2}$. If the measurement is successful (that is, one of the detectors registers one photon), we will prepare the ensembles L and R into another EME state. The new φ-parameter is given by $\varphi_1 + \varphi_2$, where φ_1 and φ_2 denote the old φ-parameters for the two segment EME states. As will be seen below, even in the presence of realistic noise and imperfections, an EME state is still created after a detector click. The noise only influences the success probability of getting a click and the new vacuum coefficient in the EME state. In general, we can express the success probability p_1 and the new vacuum coefficient c_1 as $p_1 = f_1(c_0)$ and $c_1 = f_2(c_0)$, where the functions f_1 and f_2 depend on the particular noise properties.

The above method for connecting entanglement can be cascaded to arbitrarily extend the communication distance. For the ith $(i = 1, 2, \ldots, n)$ entanglement connection, we first prepare in parallel two pairs of ensembles in the EME states with the same vacuum coefficient c_{i-1} and the same communication length L_{i-1}, and then perform entanglement swapping as shown in Fig. 2, which now succeeds with a probability $p_i = f_1(c_{i-1})$. After a successful detector click, the communication length is extended to $L_i = 2L_{i-1}$, and the vacuum coefficient in the connected EME state becomes $c_i = f_2(c_{i-1})$. As the ith entanglement connection needs to be repeated on average $1/p_i$ times, the total time needed to establish an EME state over the distance $L_n = 2^n L_0$ is given by $T_n = T_0 \Pi_{i=1}^{n}(1/p_i)$, where L_0 denotes the distance of each segment in the entanglement generation.

Entanglement-based communication schemes

After an EME state has been established between two distant sites, we would like to use it in communication protocols, such as quantum teleportation, cryptography, and Bell inequality detection. It is not obvious that the EME state of equation (3), which is entangled in the Fock basis, is useful for these tasks, as in the Fock basis it is experimentally hard to do certain single-bit operations. We will now show how the EME states can be used to realize all these protocols with simple experimental configurations.

Quantum cryptography and Bell inequality detection are achieved with the set-up shown by Fig. 3a. The state of the two

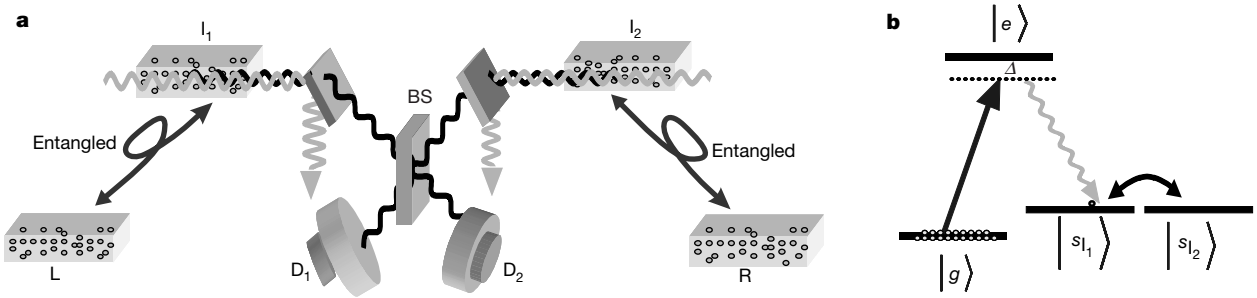

Figure 2 Set-up for entanglement connection. **a**, Illustrative set-up for the entanglement swapping. We have two pairs of ensembles—L and I_1, and I_2 and R—distributed at three sites L, I and R. Each of the ensemble-pairs L and I_1, and I_2 and R is prepared in an EME state in the form of equation (3). The stored atomic excitations of two nearby ensembles I_1 and I_2 are converted simultaneously into light. This is achieved by applying a retrieval pulses of suitable polarization that is near-resonant with the atomic transition $|s\rangle \rightarrow |e\rangle$, which causes coherent conversion of atomic excitations into photons that have a different polarization and frequency to the retrieval pulse[18,21,22]. The efficiency of this transfer can be very close to unity even at a single quantum level owing to collective enhancement[18,21,22]. After the transfer, the stimulated optical excitations interfere at a 50%-50% beam splitter, and then detected by the single-photon detectors D_1 and D_2. If either D_1 or D_2 clicks, the protocol is successful and an EME state in the form of equation (3) is established between the ensembles L and R with a doubled communication distance. Otherwise, the process fails, and we need to repeat the previous entanglement generation and swapping until finally we have a click in D_1 or D_2, that is, until the protocol finally succeeds. **b**, The two intermediate ensembles I_1 and I_2 can also be replaced by one ensemble but with two metastable states I_1 and I_2 to store the two different collective modes. The 50%-50% beam splitter operation can be simply realized by a $\pi/2$ pulse applied to the two metastable states before the collective atomic excitations are transferred to the optical excitations.

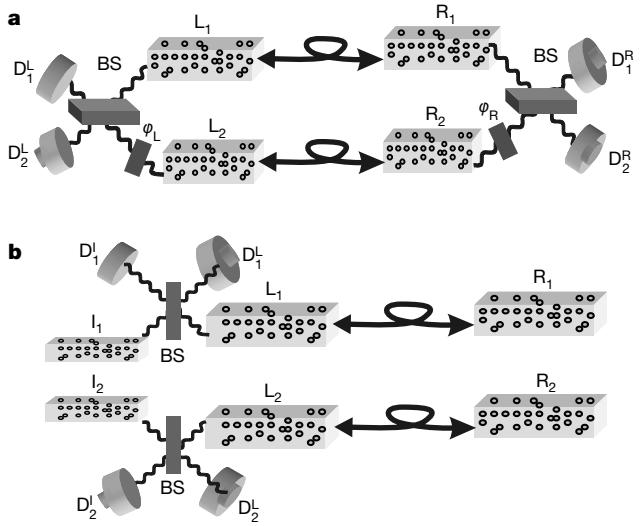

Figure 3 Set-up for entanglement-based communication schemes. **a**, Schematic set-up for the realization of quantum cryptography and Bell inequality detection. Two pairs of ensembles L_1, R_1 and L_2, R_2 (or two pairs of metastable states as shown in **b**) have been prepared in the EME states. The collective atomic excitations on each side are transferred to the optical excitations, which, respectively after a relative phase shift φ_L or φ_R and a 50%-50% beam splitter, are detected by the single-photon detectors D_1^L, D_2^L and D_1^R, D_2^R. We look at the four possible coincidences of D_1^R, D_2^R with D_1^L, D_2^L, which are functions of the phase difference $\varphi_L - \varphi_R$. Depending on the choice of φ_L and φ_R, this set-up can realize both the quantum cryptography and the Bell inequality detection. **b**, Schematic set-up for probabilistic quantum teleportation of the atomic 'polarization' state. Similarly, two pairs of ensembles L_1, R_1 and L_2, R_2 are prepared in the EME states. We want to teleport an atomic 'polarization' state $(d_0 S_{I_1}^\dagger + d_1 S_{I_2}^\dagger)|0_g 0_a\rangle_{I_1 I_2}$ with unknown coefficients d_0, d_1 from the left to the right side, where $S_{I_1}^\dagger$, $S_{I_2}^\dagger$ denote the collective atomic operators for the two ensembles I_1 and I_2 (or two metastable states in the same ensemble). The collective atomic excitations in the ensembles I_1, L_1 and I_2, L_2 are transferred to the optical excitations, which, after a 50%-50% beam splitter, are detected by the single-photon detectors D_1^I, D_1^L and D_2^I, D_2^L. If, and only if, there is one click in D_1^I D_1^L, and one click in D_2^Ior D_2^I, the protocol is successful. When the protocol succeeds, the collective excitation in the ensembles R_1 and R_2, if appearing, would be found in the same 'polarization' state $(d_0 S_{R_1}^\dagger + d_1 S_{R_2}^\dagger)|0_g 0_a\rangle_{R_1 R_2}$ up to a local π-phase rotation.

pairs of ensembles is expressed as $\rho_{L_1R_1} \otimes \rho_{L_2R_2}$, where $\rho_{L_iR_i}$ $(i = 1, 2)$ denote the same EME state with the vacuum coefficient c_n if we have done entanglement connection n times. The φ-parameters in $\rho_{L_1R_1}$ and $\rho_{L_2R_2}$ are the same, provided that the two states are established over the same stationary channels. We register only the coincidences of the two-side detectors, so the protocol is successful only if there is a click on each side. Under this condition, the vacuum components in the EME states, together with the state components $S_{L_1}^\dagger S_{L_2}^\dagger|\text{vac}\rangle$ and $S_{R_1}^\dagger S_{R_2}^\dagger|\text{vac}\rangle$, where $|\text{vac}\rangle$ denotes the ensemble state $|0_a 0_a 0_a 0_a\rangle_{L_1R_1L_2R_2}$, have no contributions to the experimental results. So, for the measurement scheme shown by Fig. 3, the ensemble state $\rho_{L_1R_1} \otimes \rho_{L_2R_2}$ is effectively equivalent to the following 'polarization' maximally entangled (PME) state (the terminology of 'polarization' comes from an analogy to the optical case):

$$|\Psi\rangle_{\text{PME}} = (S_{L_1}^\dagger S_{R_2}^\dagger + S_{L_2}^\dagger S_{R_1}^\dagger)/\sqrt{2}|\text{vac}\rangle \qquad (4)$$

The success probability for the projection from $\rho_{L_1R_1} \otimes \rho_{L_2R_2}$ to $|\Psi\rangle_{\text{PME}}$ (that is, the probability of getting a click on each side) is given by $p_a = 1/[2(c_n + 1)^2]$. We can also check that in Fig. 3, the phase shift φ_Λ ($\Lambda = \text{L}$ or R) together with the corresponding beam-splitter operation are equivalent to a single-bit rotation in the basis $\{|0\rangle_\Lambda \equiv S_{\Lambda_1}^\dagger|0_a 0_a\rangle_{\Lambda_1\Lambda_2}, |1\rangle_\Lambda \equiv S_{\Lambda_2}^\dagger|0_a 0_a\rangle_{\Lambda_1\Lambda_2}\}$ with the rotation angle $\theta = \varphi_\Lambda/2$. Now it is clear how to do quantum cryptography and Bell inequality detection, as we have the PME state and we can perform the desired single-bit rotations in the corresponding basis. For instance, to distribute a quantum key between the two remote sides, we simply choose φ_Λ randomly from the set $\{0, \pi/2\}$ with an equal probability, and keep the measurement results (to be 0 if D_1^Λ clicks, and 1 if D_2^Λ clicks) on both sides as the shared secret key if the two sides become aware that they have chosen the same phase shift after the public declaration of φ_Λ. This is exactly the Ekert scheme[1], and its absolute security follows directly from the proofs in refs 26 and 27. For the Bell inequality detection, we infer the correlations $E(\varphi_L, \varphi_R) \equiv P_{D_1^L D_1^R} + P_{D_2^L D_2^R} - P_{D_1^L D_2^R} - P_{D_2^L D_1^R} = \cos(\varphi_L - \varphi_R)$ from the measurement of the coincidences $P_{D_1^L D_1^R}$ and so on. For the set-up shown in Fig. 3a, we would have $|E(0, \pi/4) + E(\pi/2, \pi/4) + E(\pi/2, 3\pi/4) - E(0, 3\pi/4)| = 2\sqrt{2}$, whereas for any local hidden variable theories, the CHSH inequality[28] implies that this value should be below 2.

We can also use the established long-distance EME states for faithful transfer of unknown quantum states through quantum teleportation, with the set-up shown in Fig. 3b. As described in the figure legend, this set-up is used to teleport the polarization state of the collective atomic excitation in a probabilistic fashion. That is, even if the protocol succeeds—that is, two of the detectors register the counts on the left-hand side—an excitation is not necessarily present in the right (target) ensembles because the product of the EME states $\rho_{L_1R_1} \otimes \rho_{L_2R_2}$ contains vacuum components. However, if a collective excitation appears from the right-hand side, its 'polarization' state is exactly the same as the one input from the left side. So, as in the experiment of ref. 29, such a probabilistic teleportation needs posterior confirmation of the presence of the excitation; but if the presence is confirmed, the teleportation fidelity of its polarization state is nearly perfect. The success probability for the teleportation is also given by $p_a = 1/[2(c_n + 1)^2]$, which determines the average number of repetitions needed for a final successful teleportation.

Noise and built-in entanglement purification

We now discuss noise and imperfections in our schemes for entanglement generation, connection, and applications. In particular, we show that each step contains built-in entanglement purification, which makes the whole scheme resilient to realistic noise and imperfections.

In the entanglement generation, the dominant noise is due to photon loss, which includes contributions from channel attenuation, spontaneous emissions in the atomic ensembles (which result in the population of the collective atomic mode with the accompanying photon going in other directions), coupling inefficiency of the Stokes light into and out of the channel, and inefficiency of the single-photon detectors. The loss probability is denoted by $1 - \eta_p$ with the overall efficiency $\eta_p = \eta_p' e^{-L_0/L_{\text{att}}}$, where we have separated the channel attenuation $e^{-L_0/L_{\text{att}}}$ (L_{att} is the channel attenuation length) from other noise contributions η_p', with η_p' independent of the communication distance L_0. The photon loss decreases the success probability for getting a detector click from p_c to $\eta_p p_c$, but it has no influence on the resulting EME state. Owing to this noise, the entanglement preparation time should be replaced by $T_0 \approx t_\Delta/(\eta_p p_c)$. The second source of noise comes from the dark counts of the single-photon detectors. The dark count gives a detector click, but without population of the collective atomic mode, so it contributes to the vacuum coefficient in the EME state. If the dark count comes up with a probability p_{dc} for the time interval t_Δ, the vacuum coefficient is given by $c_0 = p_{\text{dc}}/(\eta_p p_c)$, which is typically much smaller than 1 as the Raman transition rate is much larger than the dark count rate. The final source of noise, which influences the fidelity of getting the EME state, is caused by the event in which more than one atom is excited to the collective mode S whereas there is only one click in D_1 or D_2. The conditional probability for that event is given by p_c, so we can estimate the fidelity imperfection $\Delta F_0 \equiv 1 - F_0$ for the entanglement

generation by:

$$\Delta F_0 \approx p_c \tag{5}$$

Note that by decreasing the excitation probability p_c, we can make the fidelity imperfection closer and closer to zero—with the price of a longer entanglement preparation time T_0. This is the basic idea of the entanglement purification. So, in this scheme, the confirmation of the click from the single-photon detector generates and purifies entanglement at the same time.

In the entanglement swapping, the dominant noise is still due to the losses, which include contributions from detector inefficiency, the inefficiency of the excitation transfer from the collective atomic mode to the optical mode[21,22], and the small decay of atomic excitation during storage[20–22]. Note that by introducing the detector inefficiency, we have automatically taken into account the imperfection that the detectors cannot distinguish between one and two photons. With all these losses, the overall efficiency in entanglement swapping is denoted by η_s. The loss in entanglement swapping gives contributions to the vacuum coefficient in the connected EME state, as in the presence of loss a single detector click might result from two collective excitations in the ensembles I_1 and I_2, and in this case, the collective modes in the ensembles L and R have to be in a vacuum state. After taking into account the realistic noise, we can specify the success probability and the new vacuum coefficient for the ith entanglement connection by the recursion relations $p_i \equiv f_1(c_{i-1}) = \eta_s(1 - \{\eta_s/[2(c_{i-1}+1)]\})/(c_{i-1}+1)$ and $c_i \equiv f_2(c_{i-1}) = 2c_{i-1} + 1 - \eta_s$. The coefficient c_0 for the entanglement preparation is typically much smaller than $1 - \eta_s$, so we have $c_i \approx (2^i - 1)(1 - \eta_s) = (L_i/L_0 - 1)(1 - \eta_s)$, where L_i denotes the communication distance after i times entanglement connection. With the expression for the c_i, we can evaluate the probability p_i and the communication time T_n for establishing an EME state over the distance $L_n = 2^n L_0$. After the entanglement connection, the fidelity of the EME state also decreases, and after n times connection, the overall fidelity imperfection $\Delta F_n \approx 2^n \Delta F_0 \approx (L_n/L_0)\Delta F_0$. We need to make ΔF_n small by decreasing the excitation probability p_c in equation (5).

We note that our entanglement connection scheme also has a built-in entanglement-purification function. This can be understood as follows: each time we connect entanglement, the imperfections of the set-up decrease the entanglement fraction $1/(c_i + 1)$ in the EME state. However, this fraction decays only linearly with distance (the number of segments), which is in contrast to the exponential decay of entanglement for connection schemes without entanglement purification. The reason for the slow decay is that for each time of entanglement connection, we need to repeat the protocol until there is a detector click, and the confirmation of a click removes part of the added vacuum noise, as a larger vacuum component in the EME state results in more repetitions. The built-in entanglement purification in the connection scheme is essential for the polynomial scaling law of the communication efficiency.

As in the entanglement generation and connection schemes, our entanglement application schemes also have built-in entanglement purification, which makes them resilient to realistic noise. First, we have seen that the vacuum components in the EME states are removed from the confirmation of the detector clicks, and thus have no influence on the fidelity of all the application schemes. Second, if the single-photon detectors and the atom-to-light excitation transitions in the application schemes are imperfect, with the overall efficiency denoted by η_a, we can show that these imperfections only influence the efficiency of getting detector clicks—with the success probability replaced by $p_a = \eta_a/[2(c_n + 1)^2]$—and have no effect on communication fidelity. Last, we have seen that the phase shifts in the stationary channels and the small asymmetry of the stationary set-up are removed automatically when we project the EME state to the PME state, and thus have no influence on the communication fidelity.

Noise not correctable by our scheme includes the detector dark count in the entanglement connection, the non-stationary channel noise and set-up asymmetries. The fidelity imperfection resulting from the dark count increases linearly with the number of segments L_n/L_0, and the imperfections from the non-stationary channel noise and set-up asymmetries increase by the random-walk law $\sqrt{L_n/L_0}$. For each time of entanglement connection, the dark count probability is about 10^{-5} if we make a typical choice that the collective emission rate is about 10 MHz and the dark count rate is 10^2 Hz. So this noise is negligible, even if we have communicated over a long distance (10^3 times the channel attenuation length $L_{\rm att}$, for instance). The non-stationary channel noise and set-up asymmetries can also be safely neglected for such a distance. For instance, it is relatively easy to control the non-stationary asymmetries in local laser operations to values below 10^{-4} with the use of accurate polarization techniques[30] for Zeeman sublevels (as in Fig. 2b).

Scaling of the communication efficiency

We have shown that each of our entanglement generation, connection, and application schemes has built-in entanglement purification, and as a result of this property, we can fix the communication fidelity to be nearly perfect, and at the same time require the communication time to increase only polynomially with distance. Assume that we want to communicate over a distance $L = L_n = 2^n L_0$. By fixing the overall fidelity imperfection to be a desired small value ΔF_n, the entanglement preparation time becomes $T_0 \approx t_\Delta/(\eta_p \Delta F_0) \approx (L_n/L_0)t_\Delta/(\eta_p \Delta F_n)$. For effective generation of the PME state of equation (4), the total communication time $T_{\rm tot} \approx T_n/p_a$ with $T_n \approx T_0 \Pi_{i=1}^n (1/p_i)$. So the total communication time scales with distance by the law

$$T_{\rm tot} \approx 2(L/L_0)^2/(\eta_p p_a \Delta F_n \Pi_{i=1}^n p_i) \tag{6}$$

where the success probabilities p_i, p_a for the ith entanglement connection and for the entanglement application have been specified above.

Equation (6) confirms that the communication time $T_{\rm tot}$ increases with distance L only polynomially. We show this explicitly by taking two limiting cases. In the first case, the inefficiency $1 - \eta_s$ for entanglement swapping is assumed to be negligibly small. We can deduce from equation (6) that in this case the communication time $T_{\rm tot} \approx T_{\rm con}(L/L_0)^2 e^{L_0/L_{\rm att}}$, with the constant $T_{\rm con} \equiv 2t_\Delta/(\eta_p' \eta_a \Delta F_n)$ being independent of the segment length and the total distance L_0 and L. The communication time $T_{\rm tot}$ increases with L quadratically. In the second case, we assume that the inefficiency $1 - \eta_s$ is fairly large. The communication time in this case is approximated by $T_{\rm tot} \approx T_{\rm con}(L/L_0)^{[\log_2(L/L_0)+1]/2+\log_2(1/\eta_s-1)+2} e^{L_0/L_{\rm att}}$, which increases with L still polynomially (or, more accurately, sub-exponentially, but this makes no difference in practice as the factor $\log_2(L/L_0)$ is well bounded from above for any reasonably long distance). If $T_{\rm tot}$ increases with L/L_0 by the mth power law $(L/L_0)^m$, there is an optimal choice of segment length ($L_0 = mL_{\rm att}$) to minimize the time $T_{\rm tot}$. As a simple estimation of the improvement in communication efficiency, we assume that the total distance L is about $100L_{\rm att}$; for a choice of the parameter $\eta_s \approx 2/3$, the communication time $T_{\rm tot}/T_{\rm con} \approx 10^6$ with the optimal segment length $L_0 \approx 5.7L_{\rm att}$. This is a notable improvement over the direct communication case, where the communication time $T_{\rm tot}$ for getting a PME state increases with distance L by the exponential law $T_{\rm tot} \approx T_{\rm con} e^{L/L_{\rm att}}$. For the same distance $L \approx 100L_{\rm att}$, we need $T_{\rm tot}/T_{\rm con} \approx 10^{43}$ for direct communication, which means that for this example the present scheme is 10^{37} times more efficient.

Outlook

We have presented a scheme for implementation of quantum repeaters and long-distance quantum communication. The proposed technique allows the generation and connection of entangle-

ment, and its use in quantum teleportation, cryptography, and tests of Bell inequalities. All of the elements of the present scheme are within reach of current experimental technology, and all have the important property of built-in entanglement purification—which makes them resilient to realistic noise. As a result, the overhead required to implement the present scheme, such as the communication time, scales polynomially with the channel length. This is in marked contrast to direct communication, where an exponential overhead is required. Such efficient scaling, combined with the relative simplicity of the experimental set-up, opens up realistic prospects for quantum communication over long distances. □

Received 16 May; accepted 12 September 2001.

1. Ekert, A. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
2. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **73,** 3081–3084 (1993).
3. Bennett, C. H. *et al.* Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76,** 722–725 (1991).
4. Briegel, H.-J., Duer, W., Cirac, J. I. & Zoller, P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81,** 5932–5935 (1998).
5. Knill, E., Laflamme, R. & Zurek, W. H. Resilient quantum computation. *Science* **279,** 342–345 (1998).
6. Preskill, J. Reliable quantum computers. *Proc. R. Soc. Lond. A* **454,** 385–410 (1998).
7. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71,** 4287–4290 (1993).
8. Cirac, J. I., Zoller, P., Kimble, H. J. & Mabuchi, H. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.* **78,** 3221–3224 (1997).
9. Enk, S. J., Cirac, J. I. & Zoller, P. Photonic channels for quantum communication. *Science* **279,** 205–207 (1998).
10. Ye, J., Vernooy, D. W. & Kimble, H. J. Trapping of single atoms in cavity QED. *Phys. Rev. Lett.* **83,** 4987–4990 (1999).
11. Hood, C. J. *et al.* The atom-cavity microscope: Single atoms bound in orbit by single photons. *Science* **287,** 1447–1453 (2000).
12. Pinkse, P. W. H., Fischer, T., Maunz, T. P. & Rempe, G. Trapping an atom with single photons. *Nature* **404,** 365–368 (2000).
13. Cabrillo, C., Cirac, J. I., G-Fernandez, P. & Zoller, P. Creation of entangled states of distant atoms by interference. *Phys. Rev. A* **59,** 1025–1033 (1999).
14. Bose, S., Knight, P. L., Plenio, M. B. & Vedral, V. Proposal for teleportation of an atomic state via cavity decay. *Phys. Rev. Lett.* **83,** 5158–5161 (1999).
15. Raymer, M. G., Walmsley, I. A., Mostowski, J. & Sobolewska, B. Quantum theory of spatial and temporal coherence properties of stimulated Raman scattering. *Phys. Rev. A* **32,** 332–344 (1985).
16. Kuzmich, A., Mölmer, K. & Polzik, E. S. Spin squeezing in an ensemble of atoms illuminated with squeezed light. *Phys. Rev. Lett.* **79,** 481 (1998).
17. Kuzmich, A., Bigelow, N. P. & Mandel, L. Atomic quantum non-demolition measurements and squeezing. *Europhys. Lett. A* **42,** 481–486 (1998).
18. Lukin, M. D., Yelin, S. F. & Fleischhauer, M. Entanglement of atomic ensembles by trapping correlated photon states. *Phys. Rev. lett.* **84,** 4232–4235 (2000).
19. Duan, L. M., Cirac, J. I., Zoller, P. & Polzik, E. S. Quantum communication between atomic ensembles using coherent light. *Phys. Rev. Lett.* **85,** 5643–5646 (2000).
20. Hald, J., Sorensen, J. L., Schori, C. & Polzik, E. S. Spin squeezed state: A macroscopic entangled ensemble created by light. *Phys. Rev. Lett.* **83,** 1319–1322 (1999).
21. Phillips, D. F. *et al.* Storage of light in atomic vapor. *Phys. Rev. Lett.* **86,** 783–786 (2001).
22. Liu, C., Dutton, Z., Behroozi, C. H. & Hau, L. V. Observation of coherent optical information storage in an atomic medium using halted light pulses. *Nature* **409,** 490–493 (2001).
23. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409,** 46–52 (2001).
24. Pan, J. W., Simon, C., Brukner, C. & Zeilinger, A. Feasible entanglement purification for quantum communication. *Nature* **410,** 1067–1070 (2001).
25. Roch, J.-F. *et al.* Quantum nondemolition measurements using cold trapped atoms. *Phys. Rev. Lett.* **78,** 634–637 (1997).
26. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 2050–2056 (1999).
27. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
28. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880–884 (1969).
29. Bouwmeester, D. *et al.* Experimental quantum teleportation. *Nature* **390,** 575–579 (1997).
30. Budker, D., Yashuk, V. & Zolotorev, M. Nonlinear magneto-optic effects with ultranarrow width. *Phys. Rev. Lett.* **81,** 5788–5791 (1998).

Supplementary Information accompanies the paper on *Nature*'s website (http://www.nature.com).

Acknowledgements

This work was supported by the Austrian Science Foundation, the Europe Union project EQUIP, the ESF, the European TMR network Quantum Information, and the NSF through a grant to the ITAMP and ITR program. L.-M.D. was also supported by the Chinese Science Foundation.

Correspondence and requests for materials should be addressed to J.I.C. (e-mail: ignacio.cirac@uibk.ac.at).