Quantum computing and quantum communication with atoms

L.-M. Duan[1,2], W. Dür[1,3], J.I. Cirac[1,3]
D. Jaksch[1], G. Vidal[1,2], P. Zoller[1]
[1] *Institute for Theoretical Physics, University of Innsbruck, A-6020 Innsbruck, Austria*
[2] *Institute for Quantum Information, Caltech, Pasadena, CA 91125 USA*
[3] *Max-Planck Institut für Quantenoptik, D-85748 Garching, Germany*

Abstract

We review recent theoretical proposals for implementation of quantum computing and quantum communication with atoms. The first example deals with the realization of a universal quantum simulator with atoms and ions. The second example outlines the implementation of a quantum repeater with atomic ensembles.

1 Introduction

Below we discuss two examples of recent progress of implementing quantum computing and quantum communication with atoms [1]. The first example illustrates a universal quantum simulator [2] with cold atoms and ions [3]. The problem of interest is simulation of spin systems. The second example outlines a quantum repeater protocol for long distance quantum communication with an atomic ensemble - a scheme significantly simpler to realize in practice than any of the previous proposals in this direction [10].

2 Universal Quantum Simulator with Cold Atoms in Optical Lattices

Quantum optics is one of the very few fields in physics where controlled generation of entanglement has been demonstrated in the laboratory, and where small, although conceptually scalable, quantum processors can be built during the coming years. Examples of such quantum optical systems are trapped ions, cavity QED and, more recently, neutral atoms in optical lattices [1, 5, 4, 7, 8]. The main motivation for building a quantum computer comes from the expected exponential gain in efficiency for certain quantum algorithms with respect to a classical computer. A milestone in this direction is the Shor algorithm for factorizing large numbers. However, for quantum computers to overcome classical ones in tasks such as factorization, they would have to operate tens of thousands of two-level systems or quantum bits (qubits). This extraordinary enterprise requires a technology that may only be in reach decades from now. Thus an important question is to identify *nontrivial* applications of quantum computers in view of quantum processors with limited resources available in the lab at present or in the near future. Such an example is provided by *Feynman's universal quantum simulator* (UQS). A UQS is a controlled device that, operating itself on the quantum level, efficiently reproduces the dynamics of any other many-particle system that evolves according to short range interactions. Consequently, a UQS could be used to efficiently simulate the dynamics of a generic many-body system, and in this way function as a fundamental tool for research in many body physics. A particular example is provided by spin systems, where simulations, which are nontrivial from a classical computing point of view, are feasible even on the level of a few tens of spins, i.e. with very limited resources available in the lab in the near future.

According to Jane *et al.* [3] the very nature of the Hamiltonian available in quantum optical systems makes them best suited for simulating the evolution of systems whose building blocks are also two-level atoms, and having a Hamiltonian

$$H_N = \sum_a H^{(a)} + \sum_{a \neq b} H^{(ab)}$$

that decomposes into one-qubit terms $H^{(a)}$ and two-qubit terms $H^{(ab)}$. A starting observation concerning the simulation of quantum dynamics is that if a Hamiltonian $K = \sum_{j=1}^{s} K_j$ decomposes into terms K_j acting in a small constant subspace, then by the Trotter formula

$$e^{-iK\tau} = \lim_{m \to \infty} \left(e^{-iK_1\tau/m} e^{-iK_2\tau/m} \ldots e^{-iK_s\tau/m} \right)^m$$

we can approximate an evolution according to K by a series of short evolutions according to the pieces K_j. Therefore, we can simulate the evolution of an N-qubit system according to the Hamiltonian H_N by composing short one-qubit and two-qubit evolutions generated, respectively, by $H^{(a)}$ and $H^{(ab)}$. In quantum optics an evolution according to one-qubit Hamiltonians $H^{(a)}$ can be obtained directly by properly shining a laser beam on the atoms or ions that host the qubits. Instead, two-qubit Hamiltonians are achieved by processing some given interaction $H_0^{(ab)}$ (see the example below) that is externally enforced in the following way. Let us consider two of the N qubits, that we denote by a and b. By alternating evolutions according to some available, switchable two qubit interaction $H_0^{(ab)}$ for some time with local unitary transformations, one can achieve an evolution

$$U(t = \sum_{j=1}^{n} t_j) = \prod_{j=1}^{n} V_j \exp(-iH_0^{(ab)} t_j) V_j^{\dagger} = \prod_{j=1}^{n} \exp(-iV_j H_0^{(ab)} V_j^{\dagger} t_j)$$

where $t = \sum_{j=1}^{n} t_j$, $V_j = u_j^{(a)} \otimes v_j^{(b)}$ with u_j and v_j being one-qubit unitaries. For a small time interval

$$U(t) \simeq 1 - it \sum_{j=1}^{n} p_j V_j H_0^{(ab)} V_j^{\dagger} + O(t^2)$$

with $p_j = t_j/t$, so that by concatenating several short gates $U(t)$,

$$U(t) = \exp(-iH_{\text{eff}}^{(ab)} t) + O(t^2),$$

we can simulate the Hamiltonian

$$H_{\text{eff}}^{(ab)} = \sum_{j=1}^{n} p_j V_j H_0^{(ab)} V_j^{\dagger} + O(t)$$

for larger times. Note that the systems can be classified according to the availability of homogeneous manipulation, $u_j = v_j$, or the availability of local individual addressing of the qubits, $u_j \neq v_j$.

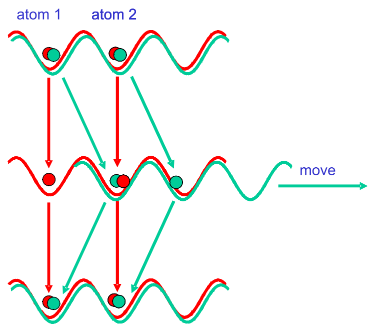

Figure 1: Entanglement via cold collision in an optical lattice: see text for details

As an example of a system available at present, let us consider cold atoms in an optical lattice. Following the theoretical proposal by Jaksch *et al.* [5] atoms can be loaded via a Mott insulator phase transition in a completely regular way in an optical lattice, so that ever lattice cell is occupied by exactly one particle. This has been demonstrated recently in a seminal experiment by I. Bloch and collaborators [7]. Furthermore, again following Jaksch *et al.* [4] atoms can be loaded in a double optical lattice, and cold controlled collisions provide a way of entangling these atoms. Again the basic mechanism of this entanglement via cold collisions has been seen in a very recent experiment by I. Bloch et al. This proposal assumes that atoms have two internal (ground) states $|0\rangle$ and $|1\rangle$ representing a qubit, and that we have two *internal state sensitive* lattices, one trapping the $|0\rangle$ state, and the second supporting the $|1\rangle$. An interaction between adjacent qubits is achieved by displacing one of the lattices with respect to the other as indicated in Fig. 1. In this way the $|1\rangle$ component of the atom a approaches in space the $|0\rangle$ component of atom $a+1$, and these collide in a controlled way. Then the two components of each atom are brought back together. This provides an example of implementing an Ising $\sum_{a\neq b} H_0^{(ab)} = \sum_a \sigma_z^{(a)} \otimes \sigma_z^{(a+1)}$ interaction between the qubits, where the $\sigma^{(a)\prime}$s denote Pauli matrices. By a sufficiently large, relative displacement of the two lattices, also interactions between more distant qubits could be achieved. A local unitary transformation can be enforced by shining a laser on the atoms, inducing an arbitrary rotation between $|0\rangle$ and $|1\rangle$. On the time scale of the collisions requiring a displacement of the lattice (the entanglement operation) these local operations can be assumed instantaneous. In the present example it is difficult to achieve an individual addressing of the qubits. Such an addressing would be available in an ion trap array as discussed in Ref. [6]. These operations provide us with the building blocks to obtain an effective Hamiltonian evolution by time averaging as outlined above.

As an example let us consider the ferromagnetic [antiferromagnetic] Heisenberg Hamiltonian

$$H = J \sum_{j=x,y,z} \sigma_j \otimes \sigma_j$$

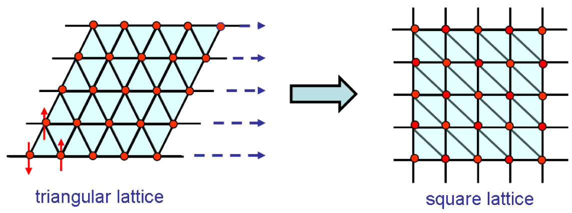

Figure 2: Illustration how triangular configurations of atoms with nearest neighbor interactions may be simulated in a rectangular lattice using only nearest neighbor interactions.

where $J > 0$ [$J < 0$]. An evolution can be simulated by short gates with $H_0^{(ab)} = \gamma\sigma_z \otimes \sigma_z$ alternated with local unitary operations

$$p_1 = \frac{1}{3}, \quad V_1 = \hat{1} \otimes \hat{1}$$
$$p_2 = \frac{1}{3}, \quad V_2 = \frac{\hat{1} - i\sigma_x}{\sqrt{2}} \otimes \frac{\hat{1} - i\sigma_x}{\sqrt{2}}$$
$$p_3 = \frac{1}{3}, \quad V_3 = \frac{\hat{1} - i\sigma_y}{\sqrt{2}} \otimes \frac{\hat{1} - i\sigma_y}{\sqrt{2}}$$

without local addressing, as provided by the standard optical lattice setup. The possibility to perform independent operations on each of the qubits would translate into the possibility to simulate all possible bipartite Hamiltonians.

An interesting aspect is the possibility to simulate effectively different lattice configurations: for example, in a 2D pattern a system with nearest neighbor interactions in a triangular configuration can be obtained from a rectangular array configuration. This is achieved making the subsystems in the rectangular array interact not only with their nearest neighbor but also with two of their next-to-nearest neighbors in the same diagonal (see Fig. 2).

One of the first and most interesting applications of quantum simulations is the study of quantum phase transitions. In this case one would obtain the ground state of a system, adiabatically connecting ground states of systems in different regimes of coupling parameters, allowing to determine its properties.

3 Quantum information processing with atomic ensembles: the quantum repeater

We now turn to recent advances of using atomic ensembles for quantum information processing [1]. In comparison with the usual requirements for implementing qubits by single atoms, and strong coupling conditions, atomic ensembles are from an experimental point of view significantly easier to deal with. It is remarkable that atomic ensembles can show collective enhancement of the signal-to-noise ratio for the coupling between light and atomic ensembles with suitable level configurations. Due to the collectively enhanced coupling, we can do various kinds of interesting quantum information processing simply by laser manipulation of atomic ensembles in weak coupling cavities or even in free space, which greatly simplifies their experimental demonstration. We will illustrate these ideas with the example of the quantum repeater. For details we refer to [11, 10].

3.1 Scalable long distance communication and the concept of the quantum repeater

Quantum communication is an essential element required for constructing quantum networks, and it also has the application of secret transfer of classical messages by means of quantum cryptography. The central 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, and to faithfully transfer quantum states via quantum teleportation. All the known realistic schemes for quantum communication are based on the use of the photonic channels. However, the degree of entanglement generated between two distant sites normally decreases exponentially with the length of the connecting channel due to the optical absorption and other channel noise. To regain a high degree of entanglement, purification schemes can be used. However, entanglement purification does not fully solve the long-distance quantum communication problem. Due to the exponential decay of the entanglement in the channel, one needs an exponentially large number of partially entangled states 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 [11]. In principle, it allows to make the overall communication fidelity very close to the unity, with the communication time growing only polynomially with the transmission distance. In analogy to fault-tolerant quantum computing, the quantum repeater proposal 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, one generates entanglement and purifies it for each segment; the purified entanglement is then extended to a longer length by connecting two adjacent segments through entanglement swapping. After entanglement swapping, the overall entanglement is decreased, and one has to purify it again. One can continue the rounds of the entanglement swapping and purification until nearly perfect entangled states are created between two distant sites.

To implement the quantum repeater protocol, one needs to generate entanglement between distant qubits, store them for sufficiently long time and perform local collective operations on several of these qubits. The requirement of quantum memory is essential since 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 essentially important for polynomial scaling properties of the communication efficiency since with no available memory we have to require that the purifications for all the segments succeeds at the same time; the probability of such event decreases exponentially with the channel length. The requirement of quantum memory implies that we need to store the local qubits in atomic internal states instead of the photonic states since 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 since normally one needs to achieve strong coupling between atoms and photons with high-finesse cavities for atomic entanglement generation, purification, and swapping, which, in spite of the recent significant experimental advances, remains a very challenging technology.

Below we summarize a very different scheme to realize quantum repeaters based on the use of *atomic ensembles*. The laser manipulation of the atomic ensembles, together with some simple linear optics devices and moderate efficiency single-photon detectors, provide the only resources required for long-distance quantum communication. Remarkably, the scheme is not only a significant simplification, in particular in comparison with the single-atom and high-Q cavity proposals, but also circumvents the realistic noise and imperfections, and at the same time keeps the overhead in the communication time increasing with the distance only polynomially.

3.2 Elements of the quantum repeater

The realization of the quantum repeater relies with atomic ensembles on three steps: (i) entanglement generation, (ii) entanglement connection via swapping, and (iii) application in communication protocols, such as quantum teleportation, cryptography, and Bell inequality detection. We give below a simplified description, refering to reference [10] for a detailed discussion.

Entanglement generation: The key element in the realization of entanglement generation is single-photon interference at photodetectors, where atomic ensembles allow for the *collective enhancement* of the signal-to-noise ratio. We consider a sample of atoms prepared in the ground state $|1\rangle$ in a Λ configuration according to Fig. 3a. For excitation with a weak and short laser pulse the signal mode a of the forward-scattered Stokes signal and the collective atomic mode $S \equiv \left(1/\sqrt{N_a}\right) \sum_i |1\rangle_i \langle 2|$ are in the state

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

where $p_c \ll 1$ denotes the (small) excitation probability, and $|0_a\rangle$ and $|0_p\rangle$ are respectively the atomic and optical vacuum states with $|0_a\rangle \equiv \bigotimes_i |1\rangle_i$.

To generate entanglement between two distant sites L and R (Fig. 3b) we excite the ensembles simultaneously, so that the system is described by the state $|\phi\rangle_L \otimes |\phi\rangle_R$, where $|\phi\rangle_L$ and $|\phi\rangle_R$ are given by Eq. (1). The forward scattered Stokes signal from both ensembles is combined at the beam splitter and a photodetector click in either D1 *or* D2 measures the combined radiation from two samples, $a_+^\dagger a_+$ or $a_-^\dagger a_-$ with $a_\pm = \left(a_L \pm a_R\right)/\sqrt{2}$. 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

$$|\Psi\rangle_{LR}^{\pm} = \left(S_L^\dagger \pm S_R^\dagger\right)/\sqrt{2}\,|0_a\rangle_L\,|0_a\rangle_R\,. \tag{2}$$

The probability for getting a click is given by p_c for each round, so we need repeat the process about $1/p_c$ times for a successful entanglement preparation.

Entanglement connection through swapping: We extend the quantum communication distance by entanglement swapping according to Fig. 4. Suppose that we start with two pairs of the entangled ensembles described by the state $|\Psi\rangle_{LI_1} \otimes |\Psi\rangle_{I_2R}$. In the ideal case, the setup shown in Fig. 4 measures the quantities corresponding to

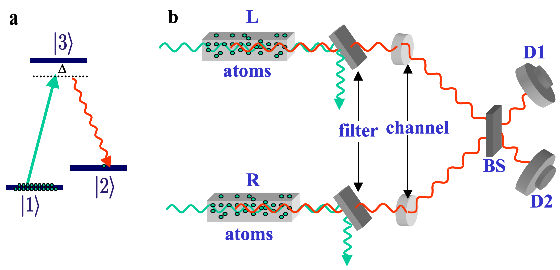

Figure 3: (a) The relevant level structure of the atoms in the ensemble with $|1\rangle$, the ground state, $|2\rangle$, the metastable state for storing a qubit, and $|3\rangle$, the excited state. The transition $|1\rangle \rightarrow |3\rangle$ is coupled by a laser, and the forward scattering Stokes light comes from the transition $|3\rangle \rightarrow |2\rangle$. (b) Setup for generating entanglement between the two atomic ensembles L and R. The ensembles are illuminated by the synchronized classical laser pulses, and the forward-scattering Stokes pulses are interfered at a 50%-50% beam splitter, with the outputs detected respectively by two single-photon detectors D1 and D2. If there is a click in D1 *or* D2, we successfully generated entanglement between the ensembles L and R. Otherwise, we apply a repumping pulse and repeat the process.

operators $S_{\pm}^{\dagger}S_{\pm}$ with $S_{\pm} = (S_{I_1} \pm S_{I_2})/\sqrt{2}$. If one of the detectors registers one photon, we will prepare the ensembles L and R into another maximally entangled state. This method for connecting entanglement can be cascaded to arbitrarily extend the communication distance.

Applications: entanglement-based communication schemes: After an effectively maximally entangled (EME) state has been established between two distant sites, we would like to use it in the communication protocols, such as quantum teleportation, cryptography, and Bell inequality detection. In the following we will show how the EME states can be used to realize all these protocols with simple experimental configurations.

Quantum cryptography and the Bell inequality detection are achieved with the setup shown by Fig. 5. The state of the two pairs of ensembles is expressed as $|\Psi\rangle_{L_1R_1} \otimes |\Psi\rangle_{L_2R_2}$. 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 $S_{L_1}^{\dagger}S_{L_2}^{\dagger}|\mathrm{vac}\rangle$ and $S_{R_1}^{\dagger}S_{R_2}^{\dagger}|\mathrm{vac}\rangle$, where $|\mathrm{vac}\rangle$ denotes the ensemble state $|0_a0_a0_a0_a\rangle_{L_1R_1L_2R_2}$, have no contributions to the experimental results. Thus, for the measurement scheme shown by Fig. 5, the ensemble state $|\Psi\rangle_{L_1R_1} \otimes |\Psi\rangle_{L_2R_2}$ is effectively equivalent to the following "polarization" maximally entangled (PME) state (the terminology of "polarization" comes from an analogy to the optical case)

$$|\Psi\rangle_{\mathrm{PME}} = \left(S_{L_1}^{\dagger}S_{R_2}^{\dagger} + S_{L_2}^{\dagger}S_{R_1}^{\dagger}\right)/\sqrt{2}\,|\mathrm{vac}\rangle\,. \tag{3}$$

One can check that in Fig. 5, the phase shift φ_{Λ} ($\Lambda = L$ or R) together with the

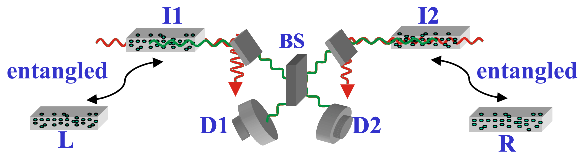

Figure 4: Setup for the entanglement swapping. We have two pairs of ensembles L, I_1 and I_2, R distributed at three sites L, I and R. Each of the ensemble-pairs L, I_1 and I_2, R is prepared in a maximally entangled state by photodetection. The excitations in the collective modes of the ensembles I_1 and I_2 are transferred simultaneously to the optical excitations by repumping pulses applied to the atomic transition $|2\rangle \to |3\rangle$, and the stimulated optical excitations, after a 50%-50% beam splitter, are detected by the single-photon detectors D1 and D2. If either D1 *or* D2 clicks, the protocol is successful and an entangled state is established between the ensembles L and R with a doubled communication distance. Otherwise, we need to repeat the previous entanglement generation and swapping until the protocol finally succeeds.

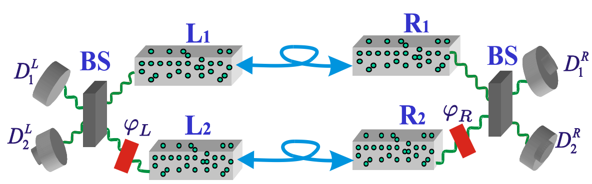

Figure 5: Schematic setup for the realization of quantum cryptography and Bell inequality detection. Two pairs of ensembles L_1, R_1 and L_2, R_2 have been prepared in entangled states. The collective atomic excitations on each side are transferred to the optical excitations, which, respectively after 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 setup can realize both the quantum cryptography and the Bell inequality detection.

corresponding beam splitter operation are equivalent to a single-bit rotation in the basis $\left\{ |0\rangle_{\Lambda} \equiv S^{\dagger}_{\Lambda_1} |0_a 0_a\rangle_{\Lambda_1 \Lambda_2},\ |1\rangle_{\Lambda} \equiv S^{\dagger}_{\Lambda_2} |0_a 0_a\rangle_{\Lambda_1 \Lambda_2} \right\}$ with the rotation angle $\theta = \varphi_{\Lambda}/2$. Now, it is clear how to do quantum cryptography and Bell inequality detection since 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_1^{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 declare. This is equivalent to the Ekert scheme. Similar arguments can be made for Bell inequality detection, and the established long-distance maximally entangled states can also be used for faithful transfer of unknown quantum states through probablilistic quantum teleportation, with the setup shown by Fig. 5.

Noise, built-in entanglement purification, and scaling of the communication efficiency: A central feature of the above protocol is the fact that entanglement generation, connection and application contains *built-in entanglement purification* which makes the whole scheme resilient to the realistic noise and imperfections. As an example, in entanglement generation and entanglement swapping the dominant noise is the photon loss. This includes channel attenuation, the spontaneous emissions in the atomic ensembles in the non-forward direction, the coupling inefficiency of the Stokes signal, and the inefficiency of the single-photon detectors. This photon loss decreases the success probably for getting a detector click, but it has no influence on the resulting entangled state.

The bottom line of the lengthy analysis of the influence of noise and imperfections is that for a fixed given fidelity the communication time scales polynomially with the distance L, which we illustrate here by a simple example. Consider a total communication distance L of $100L_{\rm att}$ with $L_{\rm att}$ the attentuation length of the fiber, and a photo detection efficiency of $\eta_s \approx 2/3$. The communication time in this case is $T_{\rm tot}/T_{\rm con} \sim 10^6$ with $T_{\rm con}$ the connection time for each segment and with an optimal segment length $L_0 \sim 5.7L_{\rm att}$. This result is a dramatic improvement compared with the direct communication case, where the communication time $T_{\rm tot}$ increases with the distance L by the exponential law $T_{\rm tot} \sim T_{\rm con} e^{L/L_{\rm att}}$. For the same distance $L \sim 100L_{\rm att}$, one needs $T_{\rm tot}/T_{\rm con} \sim 10^{43}$ for direct communication, which means that for this example the present scheme is 10^{37} times more efficient .

In summary, in this section we explained the recent atomic ensemble scheme for implementation of quantum repeaters and long-distance quantum communication. The proposed technique allows to generate and connect the entanglement and use it in quantum teleportation, cryptography, and tests of Bell inequalities. All of the elements of the scheme are within the reach of current experimental technology, and have the important property of built-in entanglement purification which makes them resilient to the realistic noise. As a result, the overhead required to implement the scheme, such as the communication time, scales polynomially with the channel length. This is in remarkable contrast to direct communication where an exponential overhead is required. Such an efficient scaling, combined with a relative simplicity of the proposed experimental setup, opens up realistic prospective for quantum communication over long distances.

References

[1] See the experimental talks at ICAP 2002 by D. Wineland and R. Blatt on ion traps, by E. Polzik on entanglement with atomic ensembles, and I. Bloch on entangling atoms via cold collisions.

[2] See S. Lloyd, Science, 273, 1073 (1996) and references cited.

[3] E. Jane, G. Vidal, W. Dür, P. Zoller, J.I. Cirac, quant-ph/0207011.

[4] D. Jaksch, H.-J. Briegel, J.I. Cirac, C. W. Gardiner, and P. Zoller, Phys. Rev. Lett. 82, 1975 (1999).

[5] D. Jaksch, C. Bruder, J.I. Cirac, C.W. Gardiner, and P. Zoller, Phys. Rev. Lett. 81, 3108 (1998).

[6] J.I. Cirac, and P. Zoller, Nature 404, 579 (2000).

[7] M. Greiner, O. Mandel, T. Esslinger, T. W. Hänsch, and I. Bloch, Nature 415, 39 (2002).

[8] M. Greiner, O. Mandel, T. W. Hänsch, and I. Bloch, Nature 419, 51 (2002).

[9] See the talk given by I. Bloch at the ICAP 2002.

[10] L.-M. Duan, M. Lukin, J.I. Cirac, P. Zoller, Nature 414, 413 (2001).

[11] H.-J. Briegel, W. Dür, J.I. Cirac and P. Zoller, Phys. Rev. Lett. 81, 5932 (1998).