with Alice encoding and transmitting random key-bits (0s and 1s) as either a right-circular, $|rcp>$ (taken here as 1), or horizontal, $|h>$ (taken here as 0), polarized dim pulse (an average of <1 photon per dim pulse). Bob must then collect the dim pulses and randomly test them for $|h>$ (with the polarization controller) or for $|rcp>$ (with the half-wave retarder). Bit exchange is completed when Bob openly communicates the location of his correlated observations with Alice's random bit string. The nonorthogonal basis states ensure that eavesdropping will be detected by the elevated error rate caused by the irreversible collapse of the wave function.[3]

The system efficiency, η [$\eta \equiv$ (the product of detector efficiency with total power output from all optical paths through the receiver)/(total power emitted by the transmitter)], was ~5%. This gave a key-rate (or bit-rate) of ~1,000 Hz at an average of ~0.7 photons per dim pulse when the laser was pulsed at a rate of 20 kHz and an average bit error rate of ~1.5% [BER ≡ (#bit-errors)/(#bits-received)].

Error corrections are accomplished with a two-dimensional parity check scheme, which generates error-free key material. A further stage of "privacy amplification" is necessary to reduce any partial knowledge gained by an eavesdropper to less than 1 bit of information.[4] Our QKD system incorporates "one time pad" encryption,[5] but supports any other symmetric key system.

1. S.F. Seward, P.R. Tapster, J.G. Walker, J.G. Rarity, Quant. Opt. **3,** 201–207 (1991).
2. C.H. Bennett, Phys. Rev. Lett. **68,** 3121–3124 (1992).
3. A.K. Ekert, B. Huttner, G.M. Palma, A. Peres, Phys. Rev. A **50,** 1047–1056 (1994).
4. C.H. Bennett, G. Brassard, C. Crepeau, U.M. Maurer, IEEE Trans. Inf. Th. **41,** 1915–1923 (1995).
5. G.S. Vernam, Trans. Am. Inst. Elect. Eng. **XLV,** 295–301 (1926).

QWB3 9:00 am

Physical implementations for quantum communication in quantum networks

S.J. van Enk, J.I. Cirac,* P. Zoller,*
H.J. Kimble, H. Mabuchi, *Norman Bridge Laboratory of Physics, California Institute of Technology 12-33, Pasadena, California 91125*

A quantum network where the data stored, processed, and communicated consists of quantum bits, would offer exciting possibilities including teleportation, dense coding, quantum money, secured quantum key distribution, and perhaps distributed quantum computing. But how to implement such a network?

In this contribution we describe a concrete physical implementation consisting of atoms placed inside high-Q optical cavities, connected by optical fibers, that allow the atoms to communicate with each other using a cavity photon as the information carrier. The scheme we have developed consists of several parts.

The first part is an explicit description of how to transfer a qubit from one atom in one cavity to another atom in a second cavity under ideal conditions (no errors). Several ideas have been discussed recently,[1] and alternative schemes are under development.

The second part is how to correct for the unavoidable errors during transmission: we devised protocols[2] that exploit quantum interferences and go beyond "standard" error correction schemes. Our scheme solves, for example, photon absorption errors irrespective of the (nonunity) error probability.

The third part is the standard assumption for solving transmission errors is that "local" measurements and operations (inside a single cavity) are simpler than nonlocal operations and are therefore assumed perfect. However, we also designed a physical model for correcting errors during local operations that involves two qubits, such as joint measurements and entanglement operations.[3]

We believe that these results substantially increase the prospects of experimentally implementing a quantum network.

Institut fuer Theoretische Physik, University of Innsbruck, A-6020 Innsbruck, Austria

1. J.I. Cirac *et al.*, Phys. Rev. Lett. **78,** 3221 (1997); see also T. Pellizzari, quant-ph/9707001.
2. S.J. van Enk, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **78,** 4293 (1997); and to be published.
3. S.J. van Enk, J.I. Cirac, P. Zoller, quant-ph/ 9708032.

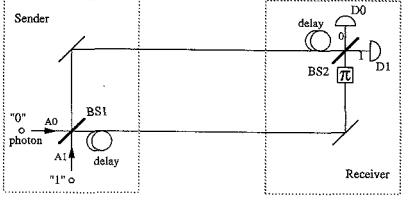
QWB4 9:15 am

Simple protocol of quantum cryptography based on two truly orthogonal states

M. Koashi, N. Imoto,, *NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-01, Japan; E-mail: koashi@will.brl.ntt.co.jp*

One of the simplest protocols of quantum cryptography proposed so far is the one based on two nonorthogonal states.[1] In this protocol, the receiver cannot determine every bit because there is no way to distinguish nonorthogonal states completely. Another simple protocol[2] uses two orthogonal states, and the receiver can always discriminate between the two states that represent the bit values 0 and 1. In this protocol, however, the sender must mix the third states (vacuum states) in the bit stream to prevent eavesdropping. Thus the following question arises: do more simple protocols exist in which the sender switches between only two states and the receiver can obtain every bit value? Here we show that such a protocol does exist.[3]

The key element that makes the protocol so simple is to transmit one-bit information in two steps so that only a fraction of the bit information is transferred at a time. A particular implementation is shown in Fig. 1, which consists of an asymmetric Mach-Zehnder interferometer. The two beam splitters (BS1 and BS2) are identical beam splitters with transmissivity T and reflectivity $R = 1 - T$. For the transmission of one bit of the key, the sender injects a single photon into the port A0 or A1 of BS1, depending on the chosen bit value. The receiver can determine the bit value by observing which of the detectors register the photon. The delay lines inserted in the two arms split the transfer of bit information into two steps, and the transmissivity T determines how much fraction of one-bit information is transmitted in each step. In the extreme case of $T = 0, 1$, the full one-bit information is transmitted in the first step. Eavesdroppers can freely read out the bit value without any trace in this case. In the case of $T = 0.5$ (this is the situation considered in the protocol of Goldenberg and Vaidam,[2] the first step transfers no bit information and the full one bit is delivered in the second step. This case is also vulnerable to eavesdroppers unless additional states are included in the protocol as in Goldenberg and Vaidam.[2] In the intermediate case of $T \neq 0, 0.5, 1$, the transfer of the bit information is parted into two steps. This case constitutes a simple protocol of quantum cryptography because we can prove that any attempts by an eavesdropper to read out the bit values inevitably result in changing the states that arrive at the receiver's site.



QWB4 Fig. 1. Schematic representation of the proposed scheme.

1. C.H. Bennett, Phys. Rev. Lett. **68,** 3121 (1992).
2. L. Goldenberg, L. Vaidman, Phys. Rev. Lett. **75,** 1239 (1995).
3. M. Koashi, N. Imoto, Phys. Rev. Lett. **79,** 2383 (1997).

QWB5 9:30 am

Nonlinear optics at the two-photon level

J.D. Franson, T.B. Pittman, *Applied Physics Laboratory, The Johns Hopkins University, Laurel, Maryland 20723*

Nonlinear optical effects are normally limited to high-intensity fields containing a large number of photons because the electric field associated with a single photon is usually very weak. Nonlinear phase shifts at the two-photon level previously have been observed using high-Q cavities and atomic beams.[1] The authors recently predicted[2] that nonlocal effects involving pairs of atoms in a medium could enhance the nonlinear interaction between two photons to the point that nonlinear phase shifts could be obtained in an ordinary medium without the use of resonant cavities.

The origin of the predicted nonlinear phase shift is illustrated by the Feynman diagram of Fig. 1. Two photons of frequencies ω_1 and ω_2 are assumed to be incident on a medium containing a large number N_A of atoms that are off resonance. Atom A can absorb photon 1 and re-emit photon 2, whereas atom B can absorb photon 2 and re-emit photon 1. This process changes the energy of the system, which produces a nonlinear phase shift. Under the ap-