All Linear Optical Quantum Memory Based on Quantum Error Correction

Robert M. Gingrich, Pieter Kok, Hwang Lee, Farrokh Vatan, and Jonathan P. Dowling

Quantum Computing Technologies Group, Section 367, Jet Propulsion Laboratory, California Institute of Technology, MS 126-347, 4800 Oak Grove Drive, California 91109-8099, USA

(Received 13 June 2003; published 18 November 2003)

When photons are sent through a fiber as part of a quantum communication protocol, the error that is most difficult to correct is photon loss. Here we propose and analyze a two-to-four qubit encoding scheme, which can recover the loss of one qubit in the transmission. This device acts as a repeater, when it is placed in series to cover a distance larger than the attenuation length of the fiber, and it acts as an optical quantum memory, when it is inserted in a fiber loop. We call this dual-purpose device a "quantum transponder."

DOI: 10.1103/PhysRevLett.91.217901 PACS numbers: 03.67.Pp, 03.67.Hk, 03.67.Lx, 42.81.–i

Storing qubits for indefinitely long periods of time is a critically important task in quantum information processing. Such a memory is needed whenever quantum teleportation protocols or feed-forward mechanisms are invoked. While photons are ideally suited for the transmission of quantum information, storing them is very difficult. Currently, techniques for mapping quantum information between photons and atomic systems are being developed [1–3]. Obviously the simplest quantum memory devices for photons are an optical fiber loop or a ring cavity. Recently, Pittman and Franson used a Sagnac interferometer to develop a quantum memory device for photons that is robust to dephasing [4]. They concluded that it is the photon loss that typically restricts the storage time.

In this Letter, we present a cyclic quantum memory for photons that can deal with photon loss. The idea is to use a delay line loop endowed with a small linear optical quantum computing (LOQC) circuit [5,6] that runs an error-correction code (ECC) over and over again on the loop, as depicted in Fig. 1. When multiple error-correcting circuits are placed in series, it allows the transmission of photons over a distance larger than the attenuation length of the fiber. A quantum repeater is typically a device that executes quantum purification and swapping protocols, with the goal of achieving remote, shared, entanglement [7–9]. Here, in contrast, we define a "quantum transponder" to be a simpler device; one which employs error correction to relay an unknown quantum state down a quantum channel with high fidelity. For quantum key distribution schemes such as the Bennett-Brassard 1984 (BB84) scheme [10], only a transponder is required for long-distance key transfer. However, we note that if the fidelity of the transponder is sufficiently high, we can also use it to distribute entanglement by relaying, say, one half of an entangled pair.

Let us first consider our error-correcting code. We use a two-to-four one-error–correcting scheme for protecting the data against photon loss. That is, we encode two qubits into four qubits such that the resulting code is capable of recovering from the loss of one photon. The encoding is as follows:

$$\begin{aligned} |00\rangle &\mapsto (|0000\rangle + |1111\rangle)/\sqrt{2}, \\ |01\rangle &\mapsto (|0110\rangle + |1001\rangle)/\sqrt{2}, \\ |10\rangle &\mapsto (|1010\rangle + |0101\rangle)/\sqrt{2}, \\ |11\rangle &\mapsto (|1100\rangle + |0011\rangle)/\sqrt{2}. \end{aligned} \tag{1}$$

This code was first introduced in 1997 by Grassl, Beth, and Pellizzari [11], and it can be implemented using the simple quantum circuit shown in Fig. 2.

The difference between this code and the usual error-correcting codes based on syndrome detection is that we do not destroy the ancillae. In other words, we recover from a single-photon loss without losing any of the four qubits. The error-correction process is shown in Fig. 3, where we assumed that the loss has occurred in the lowermost qubit (the conditional error-correcting operator consisting of a combination of σ_x and σ_z acts on the lowermost qubit mode; here, σ_x, σ_y, and σ_z are the Pauli matrices). Similar circuits work for photon loss in the other three modes.

We can demonstrate how this algorithm works by studying its action on one of the code words of the code of Eq. (1). For example, consider the code word $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)$, and suppose that the last qubit is lost (in accordance with Fig. 3). The state of the system is given by the following density operator, $\rho_1 = \frac{1}{2}(|011\rangle\langle 011| + |100\rangle\langle 100|)$, which is obtained from the

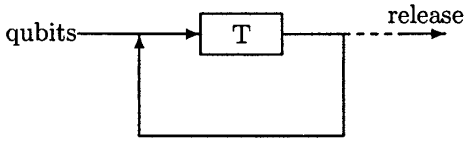

FIG. 1. A cyclic quantum memory using a quantum transponder (T) based on quantum error correction. Placed in series these devices act as simple quantum repeaters.

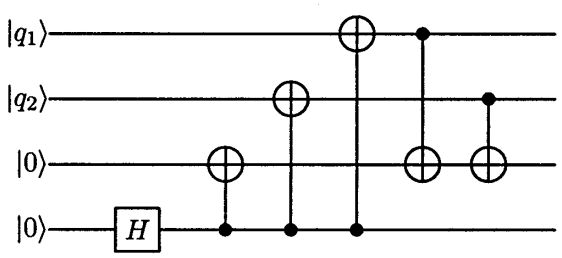

FIG. 2. Two-to-four qubit encoding, which converts the input $|q_1, q_2\rangle$ into a four-qubit state, as given in Eq. (1).

initial state $|\psi_0\rangle$ by tracing out the last qubit. In what follows, it is easier to consider the mixed state ρ_1 as a probability distribution over the pure states, instead of a density matrix. Thus the mixed state after photon loss can be written as $\rho_1 = \{(|011\rangle, \frac{1}{2}), (|100\rangle, \frac{1}{2})\}$.

The quantum nondemolition (QND) device that signals the loss of the last qubit is followed by a qubit state preparation device (photon gun) that substitutes the missing qubit with a new qubit in the ground state $|0\rangle$. The new density operator is then $\rho_2 = \{(|0110\rangle, \frac{1}{2}), (|1000\rangle, \frac{1}{2})\}$. Including the two ancilla bits, the total system is in the mixed state $\rho_3 = \rho_2 \otimes |00\rangle\langle 00| = \{(|0110\rangle|00\rangle, \frac{1}{2}), (|1000\rangle|00\rangle, \frac{1}{2})\}$. After applying the Hadamard transform on the ancilla bits, this becomes

$$\rho_4 = \{(\tfrac{1}{2}|0110\rangle(|00\rangle + |01\rangle + |10\rangle + |11\rangle), \tfrac{1}{2}), (\tfrac{1}{2}|1000\rangle(|00\rangle + |01\rangle + |10\rangle + |11\rangle), \tfrac{1}{2})\}. \quad (2)$$

The four controlled-σ_x (CNOT) and controlled-σ_z (CZ) operations, followed by the Hadamard transform on the ancilla bits, then yields the mixed state $\rho_5 = \{(\frac{1}{2}[(|0110\rangle + |1001\rangle)|00\rangle + (|0110\rangle - |1001\rangle)|10\rangle], \frac{1}{2}), (\frac{1}{2}[(|1000\rangle + |0111\rangle)|01\rangle + (|1000\rangle - |0111\rangle)|11\rangle], \frac{1}{2})\}$.

Finally, the measurement outcome of the two ancillae determines the error-correcting operator on the last qubit. These conditional operators are listed in Table I. Note that after the measurement of the ancillae, the result is always a *pure* state. Furthermore, all the results are equally likely, so this process does not reveal any information about the original encoded state. It follows immediately from Table I and Eq. (1) that this will correct the loss of the photon for this particular code word.

To see how the loss of a photon is connected to the loss of a qubit, let us consider the loss of a photon in the polarization basis. Suppose a quantum state of two qubits is described as $c_1|HH\rangle_{12} + c_2|VV\rangle_{12}$. Now suppose the loss of a photon happened in the first qubit. The loss can be described as $|0\rangle_1(c_1|H\rangle_2||h\rangle_{\text{en}} + c_2|V\rangle_2|v\rangle_{\text{en}})$, where $|0\rangle$ is the vacuum state, the subscript "en" denotes the Hilbert space of the environment, and h, v are the environment variables. Since the loss can happen in two distinct ways depending on which of the polarization modes lost the photon, the state of the second qubit is a mixed state

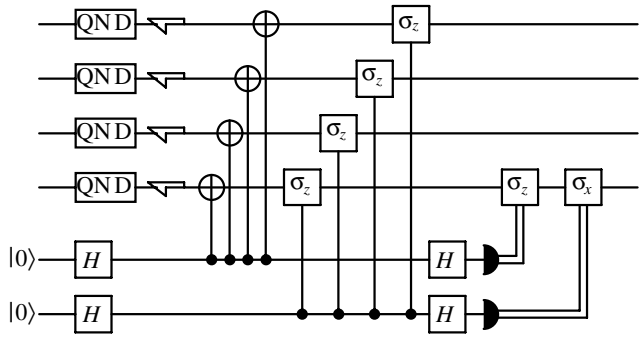

FIG. 3. Quantum transponder that recovers photon loss (here, for example, in the lower-most qubit) using two ancilla photons. The QND box represents a single-photon quantum nondemolition measurement device, followed by a single-photon source depicted by the gun-shaped polygon. H represents the Hadamard gate. Four CNOT (controlled by the first ancilla) and four CZ (controlled by the second ancilla) gates are followed by another Hadamard gate and measurement on the computational basis for each ancilla. The final one-qubit operations are for the channel where the loss has occurred, and depend on the measurement results; see Table I.

$|c_1|^2|H\rangle\langle H| + |c_2|^2|V\rangle\langle V|$ (after tracing out over the environment variables), not a pure state $c_1|H\rangle + c_2|V\rangle$. From this argument, we may conclude that photon loss has the same effect as simply tracing out over the corresponding qubit. A similar argument also holds for the photon loss in the "dual-rail" scheme where the qubit is denoted by the presence of a single photon in one rail or the other [5]. The two distinct ways of photon loss correspond to which dual-rail mode lost the photon.

In the remainder of this Letter we will consider optical implementations of this error-correcting code, where the qubits are encoded in two-mode single-photon states. These may either be two spatial modes or two polarization modes [5,12–14]. However, when we send our qubit through a fiber, we are encoding the information in the polarization of a photon, i.e., $|H\rangle \rightarrow |0\rangle$, $|V\rangle \rightarrow |1\rangle$.

When we send a photon through an optical fiber of length d, the probability of successfully transmitting the photon is given by $p(d) = \exp(-\alpha d)$. Here, the absorption coefficient of the fiber is given by α, which is a property of the fiber. The best fibers have an absorption length $1/\alpha$ of about 30 km. We wish to overcome this

TABLE I. The measurement outcomes of the ancillae and the conditional error-correcting operators that restore the state of the encoded qubits.

Observation	Projected state	Correcting operation
$\|00\rangle$	$\|0110\rangle + \|1001\rangle$	I
$\|01\rangle$	$\|1000\rangle + \|0111\rangle$	σ_x
$\|10\rangle$	$\|0110\rangle - \|1001\rangle$	σ_z
$\|11\rangle$	$\|1000\rangle - \|0111\rangle$	$\sigma_x\sigma_z$

length restriction with the ECC and the linear optical scheme for implementing two-qubit gates.

The ECC described above can recover two qubits, given the loss of a single-photon. With a perfectly working ECC, the probability of losing zero or one photon in the fiber over a distance d is given by $p_f = p^4 + 4p^3(1-p)$. Using p_f we can calculate an effective absorption length for the ECC, or equivalently $\alpha'(\alpha, d) = -\ln(p_f)/d = 3\alpha - \ln[4 - 3\exp(-\alpha d)]/d$. Since our ECC encodes two qubits, we compare α' with 2α, to see if our code is improving the situation or not. Define the function $f(x)$ with $x \equiv \alpha d$, such that $\alpha'/2\alpha = 3/2 - \ln[4 - 3\exp(-x)]/2x \equiv f(x)$. When $x < \ln(3) \approx 1.1$, $f(x) < 1$, our ECC (transponder) is increasing the effective absorption length for the qubits we are trying to transmit. So, if we make $d < \ln(3)/\alpha$ the transponder allows us to transmit qubits with higher fidelity than is possible without it. Note that $\lim_{x\to 0} f(x) = 0$, so the absorption length can be made arbitrarily large by making d smaller. However, by decreasing d we need to introduce more gates, and the gates introduce errors.

We employ the linear-optical scheme introduced by Knill, Laflamme, and Milburn (KLM) [5], to implement our quantum circuit. As a consequence, all one-qubit gates can be implemented with minimal errors. Furthermore, we can execute a controlled-NOT (CNOT) or controlled-sign (CZ) operation efficiently by using ancilla qubits. For $2n$ ancillae, a CNOT or CZ gate can be successfully executed with probability $[n/(n+1)]^2$, assuming all single-photon guns (SPG) and photon detections work perfectly. We are therefore sending our qubits in the polarization basis, but we are doing error correction in the dual-rail basis. This is not a problem because we can use a polarizing beam splitter and appropriate polarization rotators to convert between the two bases. In particular, every KLM-based gate has an equivalent implementation for polarization-encoded qubits.

With imperfect gates, our equation for $r \equiv \alpha'/2\alpha$ becomes

$$r \equiv \frac{\alpha'(x,n)}{2\alpha} = -\frac{\ln(p_f p_t)}{2x} = f(x) + \frac{1}{2x}\ln\left(\frac{1}{p_t}\right), \qquad (3)$$

where p_t is the probability that all the gates in the quantum transponder work correctly. We can see that for $p_t < 1$, the minimum of r is no longer at $x = 0$ (where the transponder stations are placed back-to-back), since the second term is infinite at that point. Figure 4 is a contour plot of Eq. (3) as a function of x and p_t. Note that the losses from the gates that do the encoding and decoding of the qubits are one-time losses, and become relatively unimportant for long transmission lines. Noting that there are four CNOT and four CZ gates in each transponder, we can write $p_t = [n/(n+1)]^{16}$. The value of n for which the minimum drops below one is at $n = 56$. So we need at least 112 ancilla qubits at each gate for the transponder to transmit qubits more reliably than the fiber without error correction.

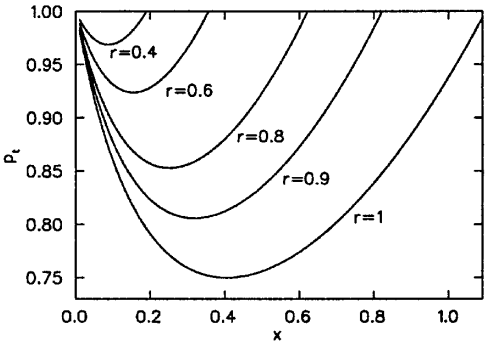

FIG. 4. A contour plot of $r = \alpha'(x,n)/2\alpha$, the relative absorption coefficient, as a function of x, the normalized distance, and the success probability of the transponder, p_t. Note that the minimum of the $r = 1$ curve is at $p_t = 3/4$.

Let us now consider the probability of success for a single quantum transponder with inefficient detectors. Suppose, as in Fig. 3, we use the QND device proposed by Kok *et al.* [15]. This device operates by teleporting the input photon to the output mode, using coincidence counting in a CNOT-operated Bell measurement. The photon loss is then signalled by finding a single detector click. In this case, there is always a photon in the output mode, and we do not need the four single-photon guns.

As shown in Fig. 3, the transponder consists of two SPGs, four QND devices, six one-qubit gates, four CNOT gates, four CZ gates, and two photodetectors (see the first row in Table II). The single-photon QND measurement can be accomplished with two SPGs, two CNOT gates, two Hadamard gates, and two photodetectors. The first Hadamard and CNOT gates are for Bell-state preparation, and the Bell-state measurement can be made by a CNOT and a Hadamard and measurements in the computational basis. For each CNOT gate, we have two one-qubit gates and a CZ gate. Given that we use $2n$ ancilla photons for each CZ gate, we need to have $2n$ SPGs and $2(n+1)$ photodetectors. Altogether, we need to have 38 one-qubit gates, 16 CZ gates, $10 + 32n$ SPGs, and $10 + 32(n+1)$

TABLE II. Number of single-photon guns, QND devices, CNOT, CZ, one-qubit gates, and photodetectors per transponder. (i) Each QND device consists of two SPG, two CNOT, and two photodetectors. (ii) Each CNOT can be considered as a CZ and two one-qubit gate. (iii) Each CZ requires $2n$ ancilla photons and $2(n+1)$ photodetectors (PD).

ECC	SPG	QND	CNOT	CZ	One	PD
	2	4	4	4	6	2
(i)	2 + 8	0	4 + 8	4	6 + 8	2 + 8
(ii)	10	0	0	16	14 + 24	10
(iii)	$10 + 32n$	0	0	16	38	$10 + 32(n+1)$

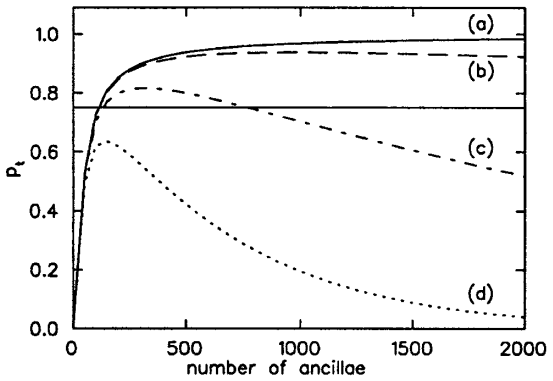

FIG. 5. The probability of transponder success p_t as a function of the number of ancillae n. The top graph (a) is for detector efficiency $\eta = 1$, and the descending graphs have detector efficiencies (b) $1–10^{-6}$, (c) $1–10^{-5}$, and (d) $1–10^{-4.5}$, respectively. A typical value that p_t needs to exceed is 0.75 (dashed line).

photodetectors. Hence the probability of success for the transponder is given by $p_t = p_{\text{one}}^{38} p_{\text{two}}^{16} p_{\text{SPG}}^{10+32n} \eta^{10+32n}$, where p_{one}, p_{two}, and p_{SPG} are the success probability of the QND measurement, the one-qubit gate, the two-qubit (CZ) gate, and a SPG, respectively. Note that η denotes the quantum efficiency of the photodetector, where $10 + 32n$ detectors among $10 + 32(n + 1)$ should click for perfect gate operations.

Now let us assume that the number of ancilla photons used for a two-qubit gate is $2n$, which gives $p_{\text{two}} = n^2/(n + 1)^2$. Hence, the number of ancilla photons may be optimized for a given quantum efficiency of the photodetectors and the success probability of the single-photon guns. Let us assume for now that $p_{\text{one}} = p_{\text{SPG}} = 1$. Then p_t is given by

$$p_t = p_{\text{two}}^{16} \eta^{10+32n} = \left(\frac{n}{n+1}\right)^{32} \eta^{10+32n}. \qquad (4)$$

For example, if $1 - \eta = 10^{-5}$, taking $n = 16$ yields $p_t \approx 0.14$. With $n = 160$ we have $p_t \approx 0.78$. A typical value that the success probability needs to beat is 0.75. In Fig. 5 we plot p_t as a function of the number of ancillae with different detector efficiencies η.

In conclusion, we have presented an error-correction scheme that encodes an unknown two-photon state into four photons, up to one of which can be lost in the transmission. This device acts as a simple repeater or quantum transponder when it is placed in series, and it acts as an optical quantum memory when it is inserted in an optical loop. Since the absorption length for two photons in a fiber is $1/(2\alpha)$, the storage time is given by $T_f = 1/(2\alpha\nu)$, where ν is the speed of light in the fiber. With error correction we can increase the storage time to T_f/r. We gave a quantitative analysis of the behavior of this quantum memory in several situations, deriving values for the optimal length of the loop, and characterizing the performance in the presence of detector losses.

Using this scheme, the conversion between flying qubits and stationary qubits in memory is not necessary, as the memory and quantum logic gates are composed of the same optical resources. The delay line, when rolled out, is a fiber quantum communication line with simple LOQC transponders, suitable for the BB84 quantum key distribution protocol [10].

This work was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. We thank J. D. Franson, G. J. Milburn, and T. B. Pittman for stimulating discussions, and we acknowledge support from the National Security Agency, the Advanced Research and Development Activity, the Defense Advanced Research Projects Agency, the National Reconnaissance Office, and the Office of Naval Research. R. M. G. and P. K. thank the National Research Council and NASA Code Y for support.

[1] C. Liu, Z. Dutton, C. H. Behroozi, and L. V. Hau, Nature (London) **409**, 490 (2001).
[2] D. F. Phillips, A. Fleischhauer, A. Mair, and M. D. Lukin, Phys. Rev. Lett. **86**, 783 (2001).
[3] C. Schori, B. Julsgaard, J. L. Sørensen, and E. S. Polzik, Phys. Rev. Lett. **89**, 057903 (2002).
[4] T. B. Pittman and J. D. Franson, Phys. Rev. A **66**, 062302 (2002).
[5] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[6] J. D. Franson, M. M. Donegan, M. J. Fitch, B. C. Jacobs, and T. B. Pittman, Phys. Rev. Lett. **89**, 137901 (2002).
[7] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[8] B. C. Jacobs, T. B. Pittman, and J. D. Franson, Phys. Rev. A **66**, 052307 (2002).
[9] P. Kok, C. P. Williams, and J. P. Dowling, Phys. Rev. A **68**, 022301 (2003).
[10] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[11] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
[12] M. Koashi, T. Yamamoto, and N. Imoto, Phys. Rev. A **63**, 030301 (2001).
[13] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **64**, 062311 (2001).
[14] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. Lett. **88**, 257902 (2002).
[15] P. Kok, H. Lee, and J. P. Dowling, Phys. Rev. A **66**, 063814 (2002).