Bit-flip-error rejection in optical quantum communication

Dik Bouwmeester

Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, OX1 3PU Oxford, United Kingdom

(Received 23 June 2000; revised manuscript received 23 October 2000; published 16 March 2001)

An optical scheme for the error-free transfer of quantum information through a noisy quantum channel is proposed. The scheme is inspired by quantum error-correction schemes, but it avoids the currently unfeasible requirement for a controlled-NOT operation between single photons. The quantum communication scheme presented here rejects bit-flip errors instead of correcting them and combines quantum-measurement properties of three-particle entangled states with properties of the quantum teleportation protocol.

DOI: 10.1103/PhysRevA.63.040301 PACS number(s): 03.67.−a

I. INTRODUCTION

The possibility of detecting and correcting errors in the evolution of a quantum system has been a most remarkable theoretical discovery [1–5]. This discovery, and the subsequent theoretical development of related ideas such as entanglement purification [6,7], the quantum repeater [8,9], and fault-tolerant quantum computation [10–12], turned the initial skepticism about implementing quantum computation and long distance quantum communication into (modest) optimism. At present, however, no practical realization of any of these ideas has been achieved in laboratories. Of particular interest would be an implementation in quantum optics, since this would enable secure quantum cryptography and quantum communication through optical channels such as optical fibers. The reason that no such implementation has been realized to date is that all theoretical schemes are based on controlled-NOT operations between single particles. For photons, this operation would require a strong nonlinear interaction between individual photons, which is extremely difficult to achieve. In this paper a scheme is proposed that rejects erroneous transmission of photon states without using controlled-NOT operations.

II. QUANTUM ERROR DETECTION

In order to explain the optical scheme, we first point out the main ideas underlying classical and quantum error detection. A particularly simple classical error detection scheme uses the transmission of several copies of the bits to be transferred and requires that the probability of a bit-flip error during transmission be much smaller than unity. By comparing the copies of each initial bit after transmission, one can determine the initial bits with high probability. Despite the fact that it is impossible to copy the state of an unknown quantum state, it is still possible to use a strategy similar to the classical one. Consider the state of a two-level system, a qubit, characterized by

$$|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle.$$

In order to make comparison measurements after the state transmission, and thereby detect errors, we have to encode the initial qubit onto several particles. If we restrict our attention to the case in which there is a small probability that a bit-flip error occurs, it is sufficient to encode the initial state onto the following three-particle entangled state:

$$|\Psi\rangle_{123}=\frac{1}{\sqrt{2}}(\alpha|000\rangle_{123}+\beta|111\rangle_{123}). \tag{1}$$

The left-hand side of Fig. 1 indicates how this encoding is obtained using two controlled-NOT operations with the initial qubit as control qubit and two auxiliary particles initially prepared in state $|0\rangle$ as target qubits.

After transmission of the three-particle entangled state through a ‘‘noisy’’ quantum channel, one can retrieve the initial qubit using the comparison measurements indicated on the right-hand side of Fig. 1. The measurements consist again of controlled-NOT operations, followed by detection of the two auxiliary particles in the $|0\rangle$, $|1\rangle$ basis. The detection acts as a parity check between the two particles on which the controlled-NOT operation acts: a $|0\rangle$ outcome indicates that in each term of the entangled state the two particles are the same, i.e., 00 or 11; a $|1\rangle$ outcome indicates that they are opposite, i.e., 01 or 10. If no error occurred during the transmission, both auxiliary particles should be detected in the state $|0\rangle$. However, if a bit-flip error occurred for the initial particle and not for the other two, both auxiliary particles will be detected in the state $|1\rangle$. In the case where an error occurred on one of the auxiliary particles, and not on the remaining two, the corresponding particle will be detected in

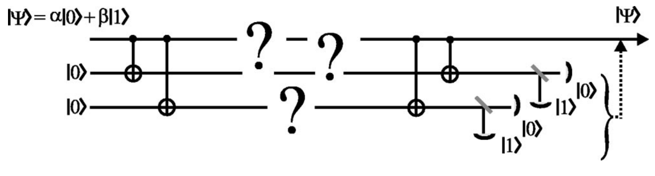

FIG. 1. Traditional scheme for the detection and correction of a bit-flip error. Using two controlled-NOT operations, an initial quantum state $|\Psi\rangle$ (the control qubit) is entangled with two auxiliary particles (the target qubits), each initially prepared in the state $|0\rangle$. After transmission of the three-particle entangled state through an area in which an error might occur, indicated by the question marks, each of the two auxiliary particles becomes the target particle of a controlled-NOT operation with the initial particle as the control particle. A final projection measurement on each of the two auxiliary particles onto the $|0\rangle$, $|1\rangle$ basis uniquely identifies a possible (single) error that can then be corrected.

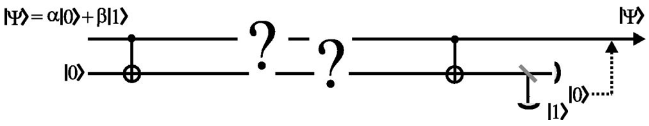

FIG. 2. Scheme for bit-flip error rejection. One auxiliary particle is sufficient in order to detect an error, without revealing on which particle the error occurred.

state $|1\rangle$ and the remaining auxiliary particle in state $|0\rangle$. After identification, a possible error can be corrected.

Crucial for the error detection/correction scheme is the fact that the parity-check measurements project the transmitted entangled state onto only four possible outcomes, namely, no error, or one error on one of the three particles. Therefore, although during the transmission through the noisy quantum channel any qubit-rotation error can occur, the final state is quantized to contain either a full bit-flip error or no error.

If more than one error occurred, the error-correction scheme is not useful. Therefore, it is crucial that the probability for an error on each particle is much smaller than unity ($P_{\text{error}} \ll 1$). Under this condition, it is reasonable to consider, for optical quantum communication purposes, a simplified scheme that rejects transmissions that contain an error instead of identifying a specific error and correcting for it. Such a simplified scheme requires only one auxiliary particle as shown in Fig. 2. If the parity check measurement yields the $|0\rangle$ result, no error took place, or, with the very small probability P^2_{error}, a fatal double error took place. If the measurement yields the $|1\rangle$ result, a single error occurred for one of the two particles and the transmission is invalidated.

III. AVOIDING CNOT OPERATIONS

To present our error-free optical quantum communication scheme, we note that the controlled-NOT operation in the preparation step of the schemes shown in Figs. 1 and 2 is used in order to encode an *arbitrary* initial quantum state onto a multiparticle entangled state. It is, however, not necessary to be able to encode an arbitrary input state. According to the teleportation scheme [13], illustrated in Fig. 3, the transmission of an arbitrary quantum state can be decomposed into the transmission of a *known* entangled state, a local Bell-state measurement, and the transmission of classical information. Therefore, in order to establish error-free quantum communication, it is sufficient to be able to exclude erroneous transmission of one of the particles of a fixed entangled state.

Consider a pair of entangled photons in the state

$$|\Psi\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2|0\rangle_3 + |1\rangle_2|1\rangle_3). \tag{2}$$

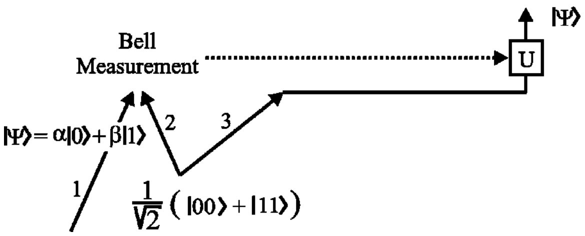

FIG. 3. Schematic drawing of the quantum teleportation protocol. The transmission of the unknown quantum state $|\Psi\rangle$ of particle 1 is broken down into the distribution of an auxiliary pair of entangled particles (2 and 3), a Bell-state measurement on particles 1 and 2 (i.e., a projection onto a complete basis of maximally entangled particles), and the transfer of classical information (the outcome of the Bell-state measurement). After receiving the classical information, the relation of the state of particle 3 to the initial state $|\Psi\rangle$ is fully determined. The initial state can therefore be recovered by a well-defined unitary transformation *U* on particle 3.

To be able to detect errors on the transmission of, say, photon 2, the preparation scheme shown on the left-hand side of Fig. 2 would produce the state

$$|\Psi\rangle_{234} = \frac{1}{\sqrt{2}}(|0\rangle_2|00\rangle_{34} + |1\rangle_2|11\rangle_{34}). \tag{3}$$

Since state (3) is a well-defined state, the use of the controlled-NOT operation is no longer necessary, as shown on the left-hand side of Fig. 4.

The right-hand side of Fig. 4 illustrates how the controlled-NOT operation for parity checking can also be avoided by using a polarizing beam splitter and a coincidence detection measurement in an appropriate basis. If a bit-flip error occurred for one of the two transmitted photons, both photons will exit the polarizing beam splitter in the

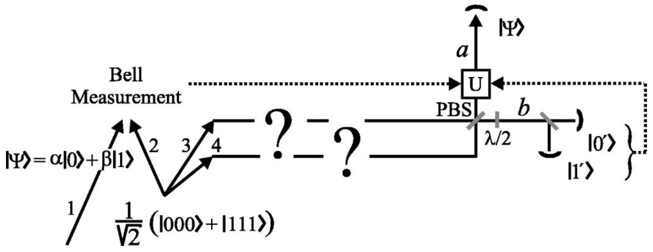

FIG. 4. Scheme for error-free quantum-state transmission without controlled-NOT operations. In order to transfer a quantum state it is sufficient to restrict the use of a quantum channel for the transmission of one of an entangled pair of particles (see Fig. 3). In order to reject erroneous transmissions, a three-particle entangled state is used. Two of the three entangled particles are sent through the ‘‘noisy’’ quantum channel. A parity check measurement on particles 2 and 3 identifies an error-free transmission and is obtained by using a polarizing beam splitter followed by a coincidence detection of one particle in arm *a* and the other in arm *b*. The measurement in arm *b* must be such that the remaining two particles are projected onto a well defined two-particle entangled state. This is achieved by performing the measurement in the linear basis rotated 45° with respect to the $|0\rangle$, $|1\rangle$ basis. After the result of the measurement on the particle in arm *b* is known, the remaining particles (one to be detected in arm *a* and particle 1) are guaranteed to be in a well defined entangled state and can be used for error-free quantum teleportation or quantum cryptography.

same output arm. Therefore, no coincidence will be observed between the detectors in arms *a* and *b*, and the transmission will be invalidated.

If no error occurred, the state after the polarizing beam splitter will have one photon in each output arm, indicating that the two outgoing photons have the same polarization relation as when initially prepared, i.e., the polarizations are parallel in each term of the entangled state (see note added in proof). The detection scheme proceeds by detecting the particle in arm *b* in the basis

$$|0'\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\qquad |1'\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle). \tag{4}$$

The specific measurement outcome corresponds to a projection of the remaining particles, provided a particle is present in arm *a*, onto one out of two well defined pure two-particle entangled states:

$$|0'\rangle_b\rightarrow\frac{1}{\sqrt{2}}(|0\rangle_2|0\rangle_a+|1\rangle_2|1\rangle_a), \tag{5}$$

$$|1'\rangle_b\rightarrow\frac{1}{\sqrt{2}}(|0\rangle_2|0\rangle_a-|1\rangle_2|1\rangle_a). \tag{6}$$

The teleportation procedure can now be completed by a Bell-state measurement and the transfer of classical information as illustrated in Fig. 4.

IV. POSTSELECTION

One might be alarmed by the fact that the photon in arm *a* has still to be detected in order to complete the error-free transmission scheme. This will in practical applications imply the destruction of the photon, although absorption-free detection of single photons has been demonstrated experimentally [14]. The fear of losing the photon before being able to use it is unjustified, at least for applications in quantum cryptography and other quantum communication protocols, since the detection of the photon is an integral part of all such applications. In fact, any realistic single-photon communication scheme needs a final verification step to guarantee that the fragile photon survived the transmission. The detection of the photon, therefore, plays the double role of enabling a projection onto a pure entangled state for photon 2 and the photon in arm *a*, as well as exploring this entanglement for quantum cryptography or for quantum communication purposes. The same arguments hold for tests of Bell's inequalities based on postselected entangled photons [15], for the Innsbruck quantum teleportation and entanglement swapping experiments [16,17], and for the recent Greenberger-Horne-Zeilinger (GHZ) entanglement experiments [18,19].

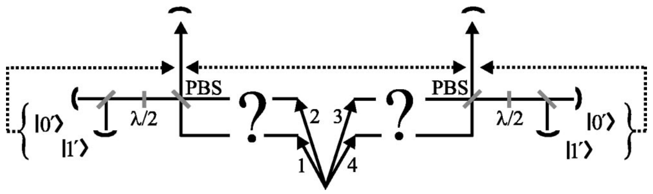

FIG. 5. Generalization of the error-free transmission of one of an entangled pair of particles to the error-free distribution of both entangled particles. Starting with a four-particle entangled state, an error-free entangled pair of particles can be obtained.

V. ERROR-FREE QUANTUM CRYPTOGRAPHY THROUGH HOSTILE QUANTUM CHANNELS

We will now briefly consider the importance of the present scheme for the security of quantum cryptography [5,20,21]. A major threat to the security of quantum cryptography based on entangled state distribution is that the entanglement distribution established between the two users is in general not perfect. The users have to agree on a minimum level of security corresponding to a certain purity of the distributed entanglement. There are many technical reasons for the accidental loss of entanglement (transmission through a noisy quantum channel), but one should also take into account the possibility that a third party is deliberately introducing small errors on what could otherwise be a perfect quantum channel (transmission through a *hostile* quantum channel). Since the users cannot distinguish between a noisy and a hostile quantum channel, they are forced to use imperfect entangled photon pairs for the distribution of a secret key at the risk of leaking some of the secret key to a third party. The scheme presented in this paper resolves both the ''noisy'' and the ''hostile'' quantum-channel problems. The users will obtain entangled photon pairs with the same purity as the initially created three-particle entanglement despite the fact that the quantum channel is imperfect. Any accidental or deliberately induced errors on the transmission will be systematically rejected. Note that a quantum key-distribution protocol based on the proposed scheme for error-free entanglement distribution will involve one more classical communication step in addition to the familiar classical communication steps, namely, the publication of the measurement result on the photon in arm *b*.

VI. DISCUSSIONS AND CONCLUSIONS

We have restricted our attention to the error-free transmission of half of an entangled pair. The scheme can easily be extended to error-free distribution of both particles of an entangled pair as illustrated in Fig. 5. Furthermore, we only discussed bit-flip errors. In addition, there could be phase errors. Error detection/correction schemes have been developed for correcting general errors consisting of both bit-flip and phase errors. Such schemes involve at least four auxiliary particles and more elaborate preparation and detection procedures. It remains to be seen whether an all-optical scheme is possible to reject both bit-flip and phase errors.

Currently we are working towards an experimental realization of the scheme presented in this paper. At first glance, it seems that previous experiments on quantum teleportation [16] and three-photon entanglement [18] provide all the necessary techniques to implement the scheme. Unfortunately, the source for three-particle entanglement reported in Refs. [18,19] is based on a postselection detection method that filters out the appropriate three-photon entanglement from a variety of other photon states. Since in the proposed scheme two of the three entangled photons are recombined on a beam splitter before detection, the postselection cannot be applied. What seems to be needed is a three-photon source that produces three spatially separated outgoing photons in a genuine three-photon GHZ state. Methods of encoding information on more than one degree of freedom of single photons (polarization and momentum) might also be employed to achieve an experimental realization [22–24].

Finally, we point out the generality of the two main ideas of this paper. First, errors on the evolution of entangled states can be detected by starting with higher-order entangled states. Second, it appears that an experimental implementation of the controlled-NOT operation, or any other universal two-qubit quantum gate, is not crucial for an experimental demonstration of the essence of a variety of quantum communication protocols.

Note added in proof: Recently research avoiding CNOT operations in an optical entanglement purification scheme has been reported [25].

ACKNOWLEDGMENT

I am very grateful to John Rarity, Sandu Popescu, Antia Lamas Linares, Christian Mikkelsen, and Micheal Seevinck for stimulating discussions and useful suggestions. This work was supported by the EPSRC GR/M88976 and the European QuComm (ISI-1999-10033) projects.

[1] A. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[2] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1995).

[3] P.W. Shor, Phys. Rev. A **52**, R2493 (1995).

[4] A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996).

[5] For an overview see *The Physics of Quantum Information*, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger (Springer-Verlag, Berlin, 2000).

[6] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[7] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. A **77**, 2818 (1996).

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

[9] W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999); **60**, 725(E) (1999).

[10] P.W. Shor, in *Proceedings of the 37th Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, 1996), p. 15.

[11] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 469 (1998).

[12] A.M. Steane, Nature (London) **399**, 124 (1999).

[13] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[14] G. Nogues, A. Rauschenbeutel, S. Osnaghi, M. Brune, J.M. Raimond, and S. Haroche, Nature (London) **400**, 239 (1999).

[15] Z.Y. Ou and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988); Y.H. Shih and C.O. Alley, *ibid.* **61**, 2921 (1988); P.G. Kwiat, A.M. Steinberg, and R.Y. Chiao, Phys. Rev. A **47**, R2472 (1993).

[16] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).

[17] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[18] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).

[19] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Nature (London) **403**, 515 (2000).

[20] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[21] A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[22] S. Popescu, LANL e-print quant-ph/9501020.

[23] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[24] M. Zukowski, Phys. Rev. Lett. **157**, 198 (1991).

[25] J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger, e-print quant-ph/0012026.