Entanglement purification for quantum communication

Jian-Wei Pan, Christoph Simon*, Caslav Brukner & Anton Zeilinger

Institut für Experimentalphysik, Universität Wien, Boltzmannsgasse 5, 1090 Wien, Austria

The distribution of entangled states between distant locations will be essential for the future large-scale realization of quantum communication schemes such as quantum cryptography1,2 and quantum teleportation3. Because of unavoidable noise in the quantum communication channel, the entanglement between two particles is more and more degraded the further they propagate. Entanglement purification4-7 is thus essential to distil highly entangled states from less entangled ones. Existing general purification protocols4-6 are based on the quantum controlled-NOT (CNOT) or similar quantum logic operations, which are very difficult to implement experimentally. Present realizations of CNOT gates are much too imperfect to be useful for long-distance quantum communication3. Here we present a scheme for the entanglement purification of general mixed entangled states, which achieves 50 per cent of the success probability of schemes based on the CNOT operation, but requires only simple linear optical elements. Because the perfection of such elements is very high, the local operations necessary for purification can be performed with the required precision. Our procedure is within the reach of current technology, and should significantly simplify the implementation of long-distance quantum communication.

Within the fledgling field of quantum information9, quantum communication has recently received much experimental attention. Entangled photons have been used to experimentally demonstrate dense coding10,11, teleportation12-14 and quantum cryptography15,16. Although these schemes are realizable for moderate distances (up to a few kilometres in the case of cryptography), serious problems occur beyond this distance scale. One of the problems is the absorption of photons in the transmission channel. Because quantum states cannot be copied17, the only way to solve this problem is by sending large numbers of photons. Nevertheless, photons still seem to be the best carriers of quantum information over long distances.

Another problem is that the quality of the entangled states generally decreases exponentially with the channel length. However, all the above protocols require that two distant parties, usually called Alice and Bob, share entangled pairs of high quality. Fortunately, various entanglement purification schemes have been suggested4-7, by which Alice and Bob can generate a certain number of almost perfectly entangled pairs out of a larger number of less-entangled pairs using local operations and classical communication, whose precision is independent of the imperfection of the quantum channel.

To show how entanglement purification works, the scheme introduced by Bennett et al.8 is illustrated in Fig. 1. The most important practical drawback of this scheme is that it requires the CNOT operation. In fact, the same is true for all known purification schemes working for general mixed entangled states. Although certain quantum logic gates have been experimentally demonstrated—for example, in ion traps19 and high-finesse microwave cavities20—there is at present no implementation of CNOT gates that could realistically be used for purification in the context of long-distance quantum communication, where the probability of

1. Present address: Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, UK.

Correspondence and requests for materials should be addressed to the author (e-mail: amelino@roma1.infn.it).

Received 24 May 2000; accepted 7 March 2001.
errors caused by the CNOT operation must not exceed a few per cent. This is far outside the range of the present implementations. Implementing purification following a recent proposal for realizing the CNOT operation with linear optics is also beyond the reach of current technology. We show here how this problem can be overcome by a general purification method that does not rely on the CNOT operation.

We consider qubits implemented as the polarization states of photons. We denote the state of a horizontally polarized photon by $|H\rangle$ and the state of a vertically polarized photon by $|V\rangle$. In the usual quantum information terminology, $|H\rangle$ and $|V\rangle$ correspond to $|0\rangle$ and $|1\rangle$.

Our purification scheme is based on a simple optical element, the polarizing beam splitter (PBS). Figure 2 shows how a PBS can be used to project two photons propagating in two different spatial modes into the subspace where they have equal polarization in the basis defined by the PBS. This is achieved by selecting only those events where there is one, and only one, photon in each output mode of the PBS.

We start the explanation of our purification scheme (shown in Fig. 3) by discussing a specific example. Suppose that Alice and Bob would like to share photon pairs in the specific maximally entangled state

$$|\Phi^{+}\rangle_{ab} = \frac{1}{\sqrt{2}}(|H\rangle_{a}|H\rangle_{b} + |V\rangle_{a}|V\rangle_{b})$$

where the photons at Alice's and Bob's locations are denoted by $a$ and $b$, respectively. Figure 2 shows that before purification the pairs they share are all in the mixed state

$$|\Psi^{+}\rangle_{ab} = (1/2)(|H\rangle_{a}|H\rangle_{b} + |V\rangle_{a}|V\rangle_{b})$$

where $|\Psi^{+}\rangle_{ab}$ is an admixture of the unwanted state $|\Phi^{+}\rangle_{ab}$. We note that in the state $|\Phi^{+}\rangle_{ab}$ the two photons have equal polarization, while in the state $|\Psi^{+}\rangle_{ab}$ they have opposite polarization in the $H/V$ basis. Here we assume the special form of equation (2) for simplicity only. The generality of our scheme will be proved later on.

Our proposed scheme is rather analogous to that of Bennett et al. We also proceed by operating on two pairs at the same time. The main difference between Fig. 3 and Fig. 1 is that now each CNOT gate is replaced by a PBS. An essential step in our purification scheme is to select those cases where there is exactly one photon in each of the four spatial output modes, which we will refer to as 'four-mode cases'. As explained above, this corresponds to a projection onto the subspace where the two photons at the same experimental station (Alice's or Bob's) have equal polarization. We note that the polarizations at the two stations do not have to be the same.

From equation (2) it follows that the original state of the two pairs can be seen as a probabilistic mixture of four pure states: with a probability of $F^2$, pairs 1 and 2 are in the state $|\Phi^{+}\rangle_{ab1}|\Phi^{+}\rangle_{ab2}$, with equal probabilities of $(1-F)$ in the states $|\Phi^{+}\rangle_{ab1}|\Psi^{+}\rangle_{ab2}$ and $|\Psi^{+}\rangle_{ab1}|\Phi^{+}\rangle_{ab2}$, and with a probability of $(1-F)^2$ in $|\Psi^{+}\rangle_{ab1}|\Psi^{+}\rangle_{ab2}$.

The cross-combinations $|\Phi^{+}\rangle_{ab1}|\Psi^{+}\rangle_{ab2}$ and $|\Psi^{+}\rangle_{ab1}|\Phi^{+}\rangle_{ab2}$ never lead to four-mode cases. This is because the two entangled photons have equal polarization in the state $|\Phi^{+}\rangle_{ab}$, while they have opposite polarization in the state $|\Psi^{+}\rangle_{ab}$. Therefore, if the polarizations on Alice's side are equal, the polarizations on Bob's side must be opposite, and vice versa. Thus, by selecting only four-mode cases we can eliminate the contribution of the cross terms. This is the basic principle of our purification method.

We now consider the two remaining combinations $|\Phi^{+}\rangle_{ab1}|\Phi^{+}\rangle_{ab2}$ and $|\Psi^{+}\rangle_{ab1}|\Psi^{+}\rangle_{ab2}$. Let us first discuss the $|\Phi^{+}\rangle_{ab1}|\Phi^{+}\rangle_{ab2}$ case. In Fig. 3 we show that following our protocol Alice and Bob will get the state $|\Phi^{+}\rangle_{ab3}$ whenever there is exactly one photon in each output mode, that is, with a probability of 50%. In the $|\Psi^{+}\rangle_{ab1}|\Psi^{+}\rangle_{ab2}$ case, following the same procedure Alice and Bob will project the remaining two photons $a3$ and $b3$ into the state $|\Psi^{+}\rangle_{ab3}$ with a probability of 50%.

Because the probabilities for $|\Phi^{+}\rangle_{ab1}|\Phi^{+}\rangle_{ab2}$ and $|\Psi^{+}\rangle_{ab1}|\Psi^{+}\rangle_{ab2}$ are $F^2$ and $(1-F)^2$, respectively, after performing the purification procedure Alice and Bob will obtain the state $|\Phi^{+}\rangle_{ab3}$ with a probability of 1. Therefore, the two parties are left with two long-distance Bell pairs.

Figure 2 Using a polarizing beam splitter as a polarization comparer. a, The polarizing beam splitter (PBS) transmits horizontally, and reflects vertically, polarization. This means, for example, that a vertically polarized photon incident along direction 1, denoted by $|V\rangle$, goes out along direction 3; that is, the state $|V\rangle$, is transformed into $|V\rangle$, by the action of the PBS. Similarly, $|H\rangle$, goes to $|H\rangle$, $|H\rangle$, goes to $|H\rangle$, and $|V\rangle$, goes to $|V\rangle$, b, Now consider two photons incident simultaneously, one in each input mode, with equal polarization—that is, in the state $|H\rangle,|H\rangle$, (top) or $|V\rangle,|V\rangle$, (bottom). Then they will always go out along different directions, so there will be one photon in each of the two output modes. c, On the other hand, if the two incident photons have opposite polarization—that is, one is $V$- and the other is $H$-polarized—then they will always go out along the same direction, so there will be two photons in one of the two outputs and none in the other. In b, the two photons have been both transmitted or both reflected. This implies that finding one photon in each output mode corresponds to a projection onto the subspace spanned by $|H\rangle,|H\rangle$, and $|V\rangle,|V\rangle$. Ultimately, the emerging photons will not be measured in the $H/V$ basis, but such that a coherent superposition of $|H\rangle,|H\rangle$, and $|V\rangle,|V\rangle$, results. This feature of the PBS, which was first described in ref. 27, has been used in the observation of multi-photon entanglement and also in recent proposals for spin-flip error correction and entanglement concentration in quantum communication. The PBS is also important in the simulation of quantum computation by linear optics.
probability of \( F^2 / 2 \), and the state \( |\Psi^+\rangle_{a_0b_3} \) with a probability of \((1 - F)^2 / 2\). By applying our purification procedure, they can thus create a new ensemble described by the density operator

\[
\rho_{a_0} = F^2 |\Phi^+\rangle_{a_0} \langle \Phi^+ | + (1 - F^2) |\Psi^+\rangle_{a_0} \langle \Psi^+ |
\]

with a larger fraction \( F^2 = F^2 |F^2 + (1 - F^2)| > F \) (for \( F > 1 / 2 \)) of pairs in the desired state \( |\Psi^+\rangle_{a_0} \) than before the purification. This concludes our discussion of purification for states of the form of equation (2). To show that our scheme also works for general input states, we now analyse in more detail the relation between our scheme and that of ref. 4.

There is a close formal correspondence between our purification scheme and the scheme of Bennett et al.4 Together with the subsequent measurements, the CNOT gates in ref. 4 in fact serve the same purpose as the PBSs in our procedure: they are used by Alice and Bob to determine whether the states of the two qubits at their respective locations are equal or opposite. From the logic table of the CNOT operation (00 \( \rightarrow \) 00, 01 \( \rightarrow \) 01, 10 \( \rightarrow \) 11 and 11 \( \rightarrow \) 10), it follows that after the operation the target particle (that is, the second) is in state 0 if originally the two particles were in equal states, and in state 1 if they were in opposite states. In the protocol of ref. 4, after the CNOT operations on both sides Alice and Bob measure their target particles and keep the source pair if the target particles are both in state 0 or both in 1. This means that the source pair is kept in two cases: first, when the two particles on Alice’s side were in equal states, and the two particles on Bob’s side were also in equal states (this corresponds to the case where both targets are in 0), and second, when the two particles on Alice’s side were in opposite states, and the two particles on Bob’s side were also in opposite states (this corresponds to the case where both targets are in 1). In these two cases, the state of the source pair will have higher entanglement than before.

The selection of four-mode cases behind the two PBS in our scheme exactly corresponds to the first case above: coincidences

\[
\begin{align*}
\text{Alice} & \quad a_3 \quad |+\rangle \quad \text{(Pair 1)} \\
\text{Bob} & \quad b_3 \quad |\pm\rangle \quad \text{(Pair 2)}
\end{align*}
\]

By applying our purifications procedure, they can thus create a new ensemble described by the density operator

\[
\rho_{a_0} = F^2 |\Phi^+\rangle_{a_0} \langle \Phi^+ | + (1 - F^2) |\Psi^+\rangle_{a_0} \langle \Psi^+ |
\]

with a larger fraction \( F^2 = F^2 |F^2 + (1 - F^2)| > F \) (for \( F > 1 / 2 \)) of pairs in the desired state \( |\Psi^+\rangle_{a_0} \) than before the purification. This concludes our discussion of purification for states of the form of equation (2). To show that our scheme also works for general input states, we now analyse in more detail the relation between our scheme and that of ref. 4.

There is a close formal correspondence between our purification scheme and the scheme of Bennett et al.4 Together with the subsequent measurements, the CNOT gates in ref. 4 in fact serve the same purpose as the PBSs in our procedure: they are used by Alice and Bob to determine whether the states of the two qubits at their respective locations are equal or opposite. From the logic table of the CNOT operation (00 \( \rightarrow \) 00, 01 \( \rightarrow \) 01, 10 \( \rightarrow \) 11 and 11 \( \rightarrow \) 10), it follows that after the operation the target particle (that is, the second) is in state 0 if originally the two particles were in equal states, and in state 1 if they were in opposite states. In the protocol of ref. 4, after the CNOT operations on both sides Alice and Bob measure their target particles and keep the source pair if the target particles are both in state 0 or both in 1. This means that the source pair is kept in two cases: first, when the two particles on Alice’s side were in equal states, and the two particles on Bob’s side were also in equal states (this corresponds to the case where both targets are in 0), and second, when the two particles on Alice’s side were in opposite states, and the two particles on Bob’s side were also in opposite states (this corresponds to the case where both targets are in 1). In these two cases, the state of the source pair will have higher entanglement than before.

The selection of four-mode cases behind the two PBS in our scheme exactly corresponds to the first case above: coincidences

\[
\begin{align*}
\text{Alice} & \quad a_3 \quad |+\rangle \quad \text{(Pair 1)} \\
\text{Bob} & \quad b_3 \quad |\pm\rangle \quad \text{(Pair 2)}
\end{align*}
\]

conditional on the coincidence being detected, the remaining two photons are left in the state \( |\Psi^+\rangle_{a_0b_3} \) with a probability of \((1 - F)^2 / 2\). By applying our purification procedure, they can thus create a new ensemble described by the density operator

\[
\rho_{a_0} = F^2 |\Phi^+\rangle_{a_0} \langle \Phi^+ | + (1 - F^2) |\Psi^+\rangle_{a_0} \langle \Psi^+ |
\]

with a larger fraction \( F^2 = F^2 |F^2 + (1 - F^2)| > F \) (for \( F > 1 / 2 \)) of pairs in the desired state \( |\Psi^+\rangle_{a_0} \) than before the purification. This concludes our discussion of purification for states of the form of equation (2). To show that our scheme also works for general input states, we now analyse in more detail the relation between our scheme and that of ref. 4.

There is a close formal correspondence between our purification scheme and the scheme of Bennett et al. Together with the subsequent measurements, the CNOT gates in ref. 4 in fact serve the same purpose as the PBSs in our procedure: they are used by Alice and Bob to determine whether the states of the two qubits at their respective locations are equal or opposite. From the logic table of the CNOT operation (00 \( \rightarrow \) 00, 01 \( \rightarrow \) 01, 10 \( \rightarrow \) 11 and 11 \( \rightarrow \) 10), it follows that after the operation the target particle (that is, the second) is in state 0 if originally the two particles were in equal states, and in state 1 if they were in opposite states. In the protocol of ref. 4, after the CNOT operations on both sides Alice and Bob measure their target particles and keep the source pair if the target particles are both in state 0 or both in 1. This means that the source pair is kept in two cases: first, when the two particles on Alice’s side were in equal states, and the two particles on Bob’s side were also in equal states (this corresponds to the case where both targets are in 0), and second, when the two particles on Alice’s side were in opposite states, and the two particles on Bob’s side were also in opposite states (this corresponds to the case where both targets are in 1). In these two cases, the state of the source pair will have higher entanglement than before.

The selection of four-mode cases behind the two PBS in our scheme exactly corresponds to the first case above: coincidences

\[
\begin{align*}
\text{Alice} & \quad a_3 \quad |+\rangle \quad \text{(Pair 1)} \\
\text{Bob} & \quad b_3 \quad |\pm\rangle \quad \text{(Pair 2)}
\end{align*}
\]
requirements on the local operations. Following our scheme, error probabilities at the one per cent level can be achieved with present technology. In particular, the precision of linear optical elements such as PBS can be extremely high, with errors as low as one-tenth of one per cent or even less. Finally, we emphasize that there is an enormous difference in the experimental effort required between implementing the CNOT operation and overlapping two photons on a PBS. We believe that the present proposal might be a vital ingredient in the future realization of long-distance quantum communication.

Acknowledgements

We thank L.-M. Duan, H. Ritsch, T. Tyc, L. Vaidman, P. Zoller and M. Zukowski for discussions. This work was supported by the Austrian Science Foundation FWF, the Austrian academy of sciences, and the TMR and QIPC programmes of the European Union.

Correspondence and requests for materials should be addressed to A.Z. (e-mail: Zeilinger-office@exp.univie.ac.at).

References


Solid silver halide glasses—where A indicates additive (AgI or Ag2Se) and B indicates chalcogenide base glass (GeSe4 or As2Se3)—using temperature-modulated differential scanning calorimetry (MDSC). Syntheses of the glasses are described in Methods. Some of these glasses are found to be intrinsically phase-separated10 (case I), and display bimodal Tg values—one ascribed to the base glass and the other to the additive solid-electrolyte glass phase. But some glass systems (case III) occur in which the additive and base materials

Mobile silver ions and glass formation in solid electrolytes

P. Boocland & W. J. Bresser

Department of Electrical & Computer Engineering and Computer Science, University of Cincinnati, Cincinnati, Ohio 45221-0030, USA

NATURE | VOL 410 | 26 APRIL 2001 | www.nature.com