Physics Letters A 376 (2012) 143–146

Contents lists available at SciVerse ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Efficient three-to-one entanglement purification protocol

Dong Pyo Chi [a], Taewan Kim [a], Soojoon Lee [b,*]

[a] Department of Mathematical Sciences, Seoul National University, Seoul 151-742, Republic of Korea
[b] Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Republic of Korea

ARTICLE INFO

Article history:
Received 25 August 2011
Received in revised form 5 October 2011
Accepted 9 November 2011
Available online 12 November 2011
Communicated by P.R. Holland

Keywords:
Entanglement purification protocol
Controlled-NOT operation

ABSTRACT

We present a new entanglement purification protocol on three copies of a state via two bilateral controlled-NOT operations. We show that one-round successful probability of our protocol is twice as large as that of the protocol by Feng et al. [Phys. Lett. A 271 (2000) 44], [8], and that our method can be applied to the existing best protocol so as to improve the efficiency.

1. Introduction

Quantum entanglement is a fundamental resource for many useful quantum communication protocols such as quantum teleportation [1], superdense coding [2] and quantum key distribution [3]. The quantum communication protocols rely on the availability of maximally entangled pairs. However, in the realization, it is difficult for the maximally entangled pairs to be perfectly transmitted due to the noise of the communication channels. Hence, the states shared between two or more parties become partially entangled rather than maximally entangled. Therefore, in order to perform a faithful quantum communication, we need an additional process to make a maximal entanglement out of many copies of the partially entangled pairs by using local operations and classical communication. The process is called the entanglement purification, and is of a great importance in quantum information science.

There are two kinds of entanglement purification protocols (EPPs). One is the recurrence protocol [4–9], and the other is the hashing/breeding protocol [5,10]. The hashing/breeding protocol works only when the fidelity with the maximally entangled state are sufficiently high. On the other hand, the recurrence protocol works for all distillable entangled states. Hence, in this Letter, we discuss the recurrence protocol which works for more general states. In particular, we deal with the N-to-one recurrence protocol which produces one output state from N copies of a state as an input state at each round.

Feng, Gong, and Xu (FGX) [8] proposed a three-to-one protocol more efficient than the first EPP which is one of well-known two-to-one protocols introduced by Bennett et al. (called the BBPSSW protocol) [4,5]. However, it has been shown that the FGX protocol is not superior to the BBPSSW protocol for all entangled states [11,12]. Even though Fujii and Yamamoto [9] showed that their three-to-one protocol has higher noise thresholds for imperfect local operations and communication channels than two-to-one protocols, it has not been known that a three-to-one protocol has the higher efficiency than the two-to-one protocols. On this account, one could naturally ask the following question: Does there exist a three-to-one protocol more efficient than the two-to-one protocols?

In this work, we present a new three-to-one protocol whose one-round successful probability is twice as large as that of the FGX protocol, and show that the efficiency of the existing best protocol can be improved by an application of our protocol. Hence, it could be a positive answer to the above question.

This Letter is organized as follows. In Section 2, we present a new three-to-one EPP and analyze its efficiency. In Section 3, we describe an application of our protocol to the existing best protocol. Finally, in Section 4, we summarize our results.

2. Our protocol

Our protocol is based on two bilateral controlled-NOT (CNOT) operations and Bell measurements on three copies of a state as seen in Fig. 1. Our three-to-one protocol consists of the following steps:

1. (Depolarization) Depolarize each of three identical copies of a given state to the isotropic state form by applying the methods in [4,5,13]:

* Corresponding author.
E-mail address: level@khu.ac.kr (S. Lee).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2011.11.006

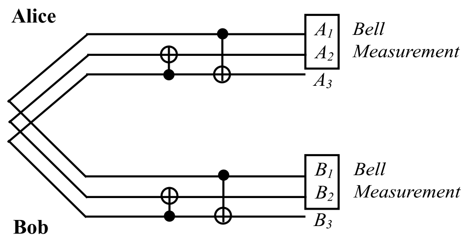

Fig. 1. Our protocol.

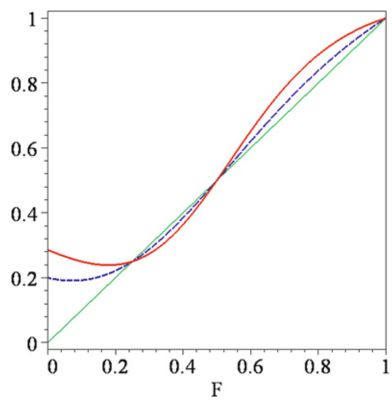

Fig. 2. Fidelity of the purified state as a function of the fidelity F of the initial state: The red solid curve represents the fidelity of the purified state by our protocol, and the blue dashed curve represents the fidelity by the BBPSSW protocol. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this Letter.)

$$\frac{1-F}{3}\big(|\Phi_{01}\rangle\langle\Phi_{01}| + |\Phi_{10}\rangle\langle\Phi_{10}| + |\Phi_{11}\rangle\langle\Phi_{11}|\big) + F|\Phi_{00}\rangle\langle\Phi_{00}| \tag{1}$$

with fidelity $F > 1/2$, where

$$|\Phi_{kl}\rangle = \frac{1}{\sqrt{2}}\sum_{j=0}^{1}(-1)^{jl}|j, j\oplus k\rangle, \tag{2}$$

which are the ordinary two-qubit Bell states.

2. (CNOT operations) First apply the bilateral CNOT operation for the source pair A_3B_3 and the target pair A_2B_2, and then apply the bilateral CNOT operation for the source pair A_1B_1 and the target pair A_3B_3, as seen in Fig. 1.
3. (Bell measurement) Measure the two-qubit states A_1A_2 and B_1B_2 locally in the Bell basis. If the measurement outcomes coincide, then keep the state of the pair A_3B_3. Otherwise, discard it.
4. (Iteration) Iterate the procedure from the step 1 to the step 3 by using the output states in the last step as the input states for the next round until the fidelity becomes greater than the target fidelity. Here, a round is the procedure from the step 1 to the step 3.

Given three copies of a state with fidelity $F = F_0$, it is straightforward to calculate the fidelity of the resulting state. The fidelity F_k after the successful k rounds is

$$F_k = \frac{2 - 7F_{k-1} + 14F_{k-1}^2}{7 - 14F_{k-1} + 16F_{k-1}^2}, \tag{3}$$

which fulfills $F_k > F_{k-1}$ for $F_0 > 1/2$. The fidelity of the purified state as a function of the fidelity of the initial state is shown in Fig. 2. It means that the final state after sufficiently many rounds in our protocol converges to the maximally entangled state $|\Phi_{00}\rangle$ faster than in the BBPSSW protocol as in the FGX protocol. In the k-th round, the successful probability of our protocol is

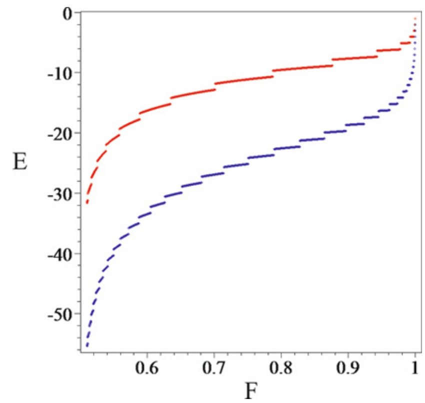

Fig. 3. Comparison of the efficiency of the BBPSSW protocol (blue) and our protocol (red) when the target fidelity is 0.9999: Our protocol is more efficient than the BBPSSW protocol, where F is the fidelity of the initial state, and E is the base-2 logarithm of the efficiency. Each discontinuity corresponds to a change of the number of rounds of the protocol. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this Letter.)

$$P_k = \frac{(1+2F_{k-1})(7-14F_{k-1}+16F_{k-1}^2)}{27}, \tag{4}$$

and the efficiency after N rounds is obtained by

$$\prod_{k=1}^{N}\frac{P_k}{3}. \tag{5}$$

Therefore, one-round successful probability of our protocol is twice as large as that of the FGX protocol, and hence our protocol is more efficient than the FGX protocol. Moreover, its efficiency implies that our three-to-one protocol is more efficient for all entangled states than the BBPSSW protocol which is one of the two-to-one protocols as seen in Fig. 3.

3. Application of our protocol

In this section, by applying our protocol to the Metwally protocol [7] which is the existing best protocol, we show that its efficiency can be improved.

3.1. Our modification of the Metwally protocol

The Metwally protocol includes applications of two unitary operations

$$U_A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \tag{6}$$

and

$$U_B = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \tag{7}$$

and it also includes rearrangement of the probabilities λ_{kl} of the general Bell diagonal state

$$\rho_{AB} = \sum_{k,l=0}^{1}\lambda_{kl}|\Phi_{kl}\rangle_{AB}\langle\Phi_{kl}| \tag{8}$$

with $\lambda_{00} > 1/2$. In order for our protocol to be combined with the Metwally protocol we need such applications and rearrangement. Our protocol with the local unitary operations U_A and U_B is shown in Fig. 4. We remark that if the initial state is the isotropic

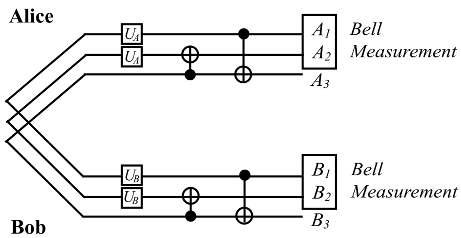

Fig. 4. Our protocol with local unitary operations U_A and U_B in Eqs. (6) and (7).

state, then the local unitary operations U_A and U_B can be regarded as the identity operation.

Our modification of the Metwally protocol consists of the following steps:

1. (Depolarization and rearrangement) Depolarize the input states into the Bell diagonal states ρ_{AB} in Eq. (8) by employing the methods in Refs. [5,13] and rearrange their probabilities so that the probabilities satisfy the following relations:

$$\lambda_{00} \geqslant \lambda_{01} \geqslant \lambda_{10} \geqslant \lambda_{11}. \tag{9}$$

2. (Unitary operations and CNOT operations) First apply the unitary operations $U_A \otimes U_A$ and $U_B \otimes U_B$ to the pairs A_1A_2 and B_1B_2 respectively, and then apply the bilateral CNOT operation for the source pair A_3B_3 and the target pair A_2B_2. Finally, apply the bilateral CNOT operation for the source pair A_1B_1 and the target pair A_3B_3, as seen in Fig. 4.
3. (Bell measurement) Measure the two-qubit states A_1A_2 and B_1B_2 locally in the Bell basis. If the measurement outcomes coincide, then keep the state of the pair A_3B_3. Otherwise, discard it.
4. (Iteration) Iterate the rounds of the Metwally protocol by using the output states in the last step as the input states for the next round, until the fidelity becomes greater than the target fidelity.

Our modification consists of one round of our protocol with the local unitary operations and the other rounds of the Metwally protocol, and hence its efficiency is

$$\frac{P_1}{3}\prod_{k=2}^{N}\frac{P_k}{2}. \tag{10}$$

For general Bell diagonal states, the efficiency of the Metwally protocol and its modification are shown in Fig. 5. It can be numerically shown that the binary states and the isotropic states have the maximum efficiency and the minimum efficiency over almost all of the initial states of both protocols, respectively. Here, the binary state is the Bell diagonal state whose two of the four probabilities vanish.

3.2. Improvement of the efficiency

In order to compare the efficiency of both protocols, we calculate the values of the efficiency for the cases that the initial states are the binary states and the isotropic states, respectively. The comparisons are seen in Fig. 6.

Let A_N and B_N be the smallest values of F_0 such that $F_N > 0.9999$ after the successful N rounds of the Metwally protocol and its modification, respectively, then the approximate values of A_N and B_N are numerically calculated in Table 1. By employing Table 1, it can be shown that if $A_N > F_0 > B_N$ then our modification of the Metwally protocol is more efficient whereas if $B_N > F_0 > A_{N+1}$ then the Metwally protocol is more efficient. Therefore, according to the fidelity of a given binary state, we can choose the more efficient protocol.

For the isotropic states, C_N and D_N can be defined by the same way as in the definitions of A_N and B_N, respectively, and their approximate values are numerically calculated in Table 2. As in the case of the binary states, it can be shown that if $C_N > F_0 > D_N$ then our modification of the Metwally protocol is more efficient whereas if $D_N > F_0 > C_{N+1}$ then the Metwally protocol is more efficient. Therefore, according to the fidelity of a given isotropic state, we can choose the more efficient protocol.

By comparing the efficiency of the two protocols for the binary states and the isotropic states with fidelity $F = F_0$, it can be shown that when $A_{N_1} > F_0 > B_{N_1}$ and $C_{N_2} > F_0 > D_{N_2}$, for example $F_0 = 0.6$, our modification of the Metwally protocol has the higher efficiency. In Section 3.1, it was shown that the binary states and the isotropic states have the maximum efficiency and the minimum efficiency over almost all of the initial states of both protocols, respectively. Therefore, we can say that our modification is more efficient than the original Metwally protocol for all states with fidelity $F = F_0$.

4. Conclusion

In conclusion, we have presented a new three-to-one EPP whose one-round successful probability is twice as large as that of

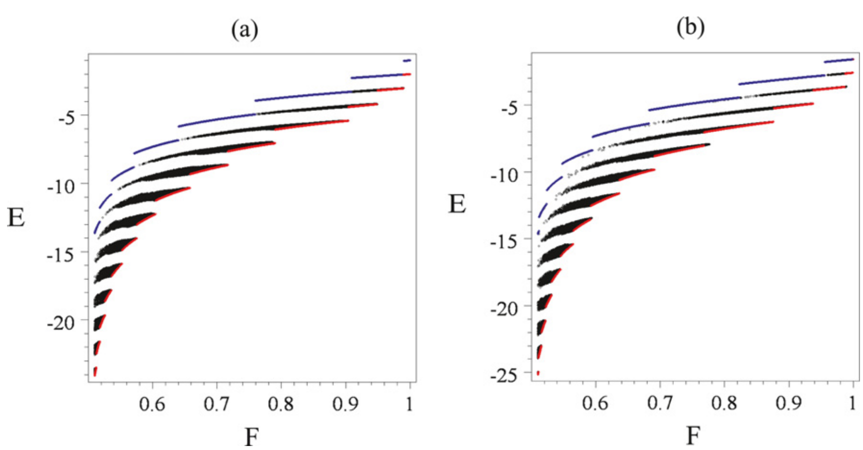

Fig. 5. Efficiency of the Metwally protocol and its modification when the target fidelity is 0.9999 for the isotropic states (red) and the binary states (blue) and 100,000 random Bell diagonal states (black): (a) efficiency of the Metwally protocol, (b) efficiency of our modification, where the binary state is the Bell diagonal state whose two of the four probabilities vanish, F is the fidelity of the initial state and, E is the base-2 logarithm of the efficiency. Each discontinuity corresponds to a change of the number of rounds of the protocol. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this Letter.)

Table 1
The smallest values of F_0 such that $F_N > 0.9999$ when the initial states are binary states.

N	A_N	B_N
0	0.9999	0.9999
1	0.9901	0.9557
2	0.9091	0.8228
3	0.7598	0.6830
4	0.6401	0.5948
5	0.5715	0.5479
6	0.5360	0.5240
7	0.5180	0.5120

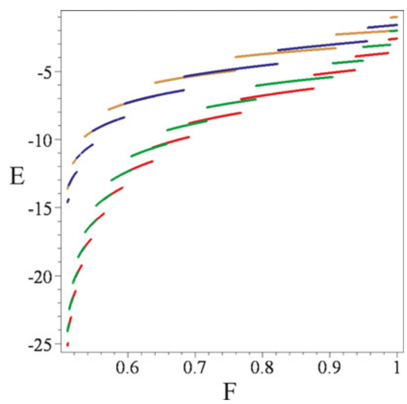

Fig. 6. Comparison of the efficiency with the Metwally protocol and its modification: Efficiency of the Metwally protocol for binary states (gold) and isotropic states (green), and efficiency of our modification for binary states (blue) and isotropic states (red), where F is the fidelity of the initial state, and E is the base-2 logarithm of the efficiency. Each discontinuity corresponds to a change of the number of rounds of the protocol. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this Letter.)

the FGX protocol. Even though we have not constructed a three-to-one protocol more efficient than the existing best two-to-one protocol, we have shown that our three-to-one protocol is more efficient than the BBPSSW protocol, and that the efficiency of the existing best two-to-one protocol can be improved by an application of our protocol.

In this Letter, our protocols have been designed for qubit states. It was known that the EPP can be generalized into higher dimensional quantum systems by the generalized CNOT gates and Bell measurements for two-qudit states [14], and it was furthermore shown that the generalized EPP is more efficient than the protocols for qubit states. Therefore, our method could be also generalized to qudit systems by exploiting the method in Ref. [14], and hence its efficiency could be improved.

Table 2
The smallest values of F_0 such that $F_N > 0.9999$ when the initial states are isotropic states.

N	C_N	D_N
0	0.9999	0.9999
1	0.9999	0.9998
2	0.9896	0.9869
3	0.9488	0.9376
4	0.9042	0.8763
5	0.7903	0.7680
6	0.7171	0.6911
7	0.6583	0.6365
8	0.6049	0.5922
9	0.5756	0.5648
10	0.5527	0.5454

Acknowledgements

This work was supported by the IT R&D program of the Ministry of Knowledge Economy [Development of Privacy Enhancing Cryptography on Ubiquitous Computing Environment]. S.L. was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant No. 2009-0076578).

References

[1] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Phys. Rev. Lett. 70 (1993) 1895.
[2] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881.
[3] A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
[4] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, Phys. Rev. Lett. 76 (1996) 722.
[5] C.H. Bennett, D. DiVincenzo, J.A. Smolin, W.K. Wootters, Phys. Rev. A 54 (1996) 3824.
[6] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. 77 (1996) 2818.
[7] N. Metwally, Phys. Rev. A 66 (2002) 054302.
[8] X.-L. Feng, S.-Q. Gong, Z.-Z. Xu, Phys. Lett. A 271 (2000) 44.
[9] K. Fujii, K. Yamamoto, Phys. Rev. A 80 (2009) 042308.
[10] E. Hostens, J. Dehaene, B.D. Moor, Phys. Rev. A 73 (2006) 062337.
[11] M. Okrasa, Z. Walczak, Phys. Lett. A 372 (2008) 3136.
[12] X.-L. Feng, S.-Q. Gong, Z.-Z. Xu, Phys. Lett. A 372 (2008) 3337.
[13] W. Dür, J.I. Cirac, M. Lewenstein, D. Bruß, Phys. Rev. A 61 (2000) 062313.
[14] G. Alber, A. Delgado, N. Gisin, I. Jex, J. Phys. A: Math. Gen. 34 (2001) 8821.