Entanglement purification with double selection

Keisuke Fujii and Katsuji Yamamoto
Department of Nuclear Engineering, Kyoto University, Kyoto 606-8501, Japan
(Received 17 November 2008; published 9 October 2009)

We investigate an entanglement purification protocol with double-selection process, which works under imperfect local operations. Compared with the usual protocol with single selection, this double-selection method has higher noise thresholds for the local operations and quantum communication channels and achieves higher fidelity of purified states. It also provides a yield comparable to that of the usual protocol with single selection. We discuss on general grounds how some of the errors which are introduced by local operations are left as intrinsically undetectable. The undetectable errors place a general upper bound on the purification fidelity. The double selection is a simple method to remove all the detectable errors in the first order, so that the upper bound on the fidelity is achieved in the low-noise regime. The double selection is further applied to purification of multipartite entanglement such as two-colorable graph states.

DOI: 10.1103/PhysRevA.80.042308 PACS number(s): 03.67.Hk, 03.67.Pp

I. INTRODUCTION

Recently a number of protocols based on entanglement have been developed in quantum communication and computation. For example, bipartite entanglement is employed in quantum teleportation, superdense coding, quantum cryptography, and quantum repeater [1–4]. Multipartite entanglement is further utilized in cluster state computation, quantum error correction, and multiparty cryptography [5–7]. The performance of these entanglement-based protocols highly depends on the fidelity of entangled states. That is, high-fidelity entangled states are essential for secure communication and reliable computation. In this viewpoint, it is a very important task to prepare and share high-fidelity entangled states.

Entanglement purification is a way to share high-fidelity entangled states via noisy communication channels. It was proposed originally to share Einstein-Podolsky-Rosen (EPR) states [8,9], and then extended for a large class of multipartite entangled states, including the Greenberger-Horne-Zeilinger (GHZ) states, two-colorable graph states, stabilizer states, and *W* states [10–16]. In a situation with noisy channels but perfect local operations, one may prepurify initial states with a recurrence protocol, which has a high threshold for the noise of the communication channel, but gives a low yield of purified states. Then, a hashing protocol may be implemented to get pure entangled states with a nonzero yield. The hashing protocol, however, breaks down as soon as local operations become slightly imperfect [12]. The entanglement purification under imperfect local operations was first analyzed in the context of quantum repeater [4], where the usual recurrence protocol [8,9] is adopted. The fidelity of purified states is indeed limited by the imperfection of local operations, and noise thresholds exist for successful purification. This is clearly distinct from the cases such as a hashing protocol where perfect local operations are assumed. One should confront the problem that errors are introduced inevitably by local operations themselves for purification even if the initial impurity is diminished. Thus, in order to realize entanglement-based protocols by using practical devices, which inevitably have imperfections, we need to develop purification methods which work well with noisy local operations.

In this paper we investigate an entanglement purification protocol with more accurate postselection through double verification process, which works under imperfect local operations. Compared with the usual protocol with single selection [4,8,9], this double-selection method has higher noise thresholds for the local operations and communication channels and achieves higher fidelity of purified states. It can be shown on general grounds how some of the errors which are introduced by local operations are left as intrinsically undetectable. This limitation on the achievable fidelity due to the undetectable errors is applicable to a wide variety of purification protocols [4,8–17]. The double selection is indeed a simple method to remove all the detectable errors in the first order, so that in the low-noise regime the purification fidelity reaches the general upper bound which is placed by the undetectable errors. It may be considered that the elaborate postselection decreases the yield of purification by consuming many resources. However, this is not necessarily the case. The double-selection protocol provides a yield comparable to or even better than that of the single-selection protocol. This is because the double selection increases the fidelity faster by removing more errors in each purification round. The double selection is also applicable to purification of multipartite entanglement such as two-colorable graph states [11,12].

The rest of the paper is organized as follows. In Sec. II we investigate the double selection in the bipartite entanglement purification. The performance of the double-selection protocol is analyzed and compared with that of the usual protocol with single selection. In Sec. III the upper bound on the fidelity is discussed in terms of the intrinsically undetectable errors, which are introduced by local operations. This bound is really achieved by the double-selection protocol in the low-noise regime. In Sec. IV the double selection is applied to the multipartite entanglement purification, where the Steane seven-qubit code is investigated as an example of two-colorable graph states. Section V is devoted to conclusion. Detailed calculations of the transition probability tensors to characterize the purification maps are presented in the Appendix.

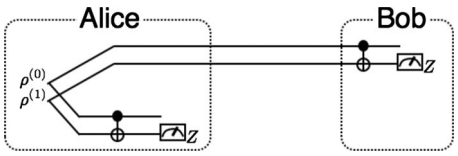

FIG. 1. Bipartite entanglement purification with single selection.

II. BIPARTITE ENTANGLEMENT PURIFICATION

A. Single selection

We first review the usual recurrence protocol for purification where the single selection is made [8,9]. This protocol is implemented by using two noisy copies of an EPR pair, a bilateral controlled-NOT (CNOT) gate, and a bilateral measurement in each round of purification. Here, a bilateral operation means a tensor product of two identical local operations which are simultaneously implemented by the two parties: Alice and Bob. The purification procedure is specifically described as follows (see Fig. 1):

(i) Alice and Bob share two identical EPR pairs $\rho^{(0)}$ and $\rho^{(1)}$ through a noisy quantum channel.

(ii) They operate a bilateral CNOT gate on $\rho^{(0)}$ and $\rho^{(1)}$ as the control and target qubits, respectively.

(iii) They bilaterally measure $\rho^{(1)}$ in the Z basis $\{|0\rangle,|1\rangle\}$ and obtain the measurement outcomes m_a (Alice) and m_b (Bob).

(iv) They keep $\rho^{(0)}$ if the measurement outcomes coincide as $m_a=m_b$. Otherwise, they discard $\rho^{(0)}$.

A single bilateral operation determines whether $\rho^{(0)}$ should be kept or discarded, namely, the single selection. Alice and Bob iterate procedures (ii)–(iv) by using the output states which survive the selection in procedure (iv) as the input states for the next round of purification where the direction (control and target) of the bilateral CNOT gate is inverted, and the measurement is made in the X basis (Oxford protocol) [9]. This inversion round by round may be done mathematically by applying a Hadamard transformation (perfect by itself) on each qubit to exchange the bases of the reference frame as $X \leftrightarrow Z$.

The noisy EPR pairs $\rho^{(0)}$ and $\rho^{(1)}$ are given as two copies of a Bell-diagonal state ρ,

$$\rho^{(0)} = \rho^{(1)} = \rho = \sum_{i=0}^{3} F_i \phi_i, \tag{1}$$

where the Bell states are

$$\phi_i \equiv |\phi_i\rangle\langle\phi_i|, \tag{2}$$

$$|\phi_i\rangle = \sigma_i \otimes \sigma_0(|00\rangle + |11\rangle)/\sqrt{2}, \tag{3}$$

with $\sigma_0=I$ and the Pauli operators σ_i $(i=1,2,3)$. In the rest of this paper, we simply use the term "EPR pair" to denote a noisy EPR pair as a Bell-diagonal mixed state, which passes through some noisy quantum communication channel and purification procedure. The above purification procedure generates a transformation of the input Bell-diagonal ρ with the state vector $\mathbf{F}=(F_0,F_1,F_2,F_3)$ to another Bell-diagonal ρ' with the state vector $\mathbf{F}'=(F_0',F_1',F_2',F_3')$, even when the Pauli noise is introduced for the local operations. The imperfect CNOT gate, which is operated locally by Alice, is described as a sequence of a perfect CNOT gate operation $\mathcal{U}$ and a two-qubit deporalizing noise with error probabilities p_{ij} as

$$\mathcal{N}(\rho_{\mathcal{U}}^{(0,1)}) = \sum_{ij} p_{ij}(\sigma_i \otimes \sigma_j)_A \otimes \mathbf{1}_B \rho_{\mathcal{U}}^{(0,1)}(\sigma_i \otimes \sigma_j)_A \otimes \mathbf{1}_B, \tag{4}$$

where $\rho_{\mathcal{U}}^{(0,1)}=\mathcal{U}(\rho^{(0)}\otimes\rho^{(1)})$, $p_{00}=1-p_g$ with $p_g=\Sigma_{ij\neq 00}p_{ij}$, the Pauli operators $(\sigma_i\otimes\sigma_j)_A$ act on the control and target qubits at Alice, respectively, and $\mathbf{1}_B$ indicates the identity operator acting on the qubits at Bob. The imperfect CNOT gate operated by Bob is described in the same manner. The imperfect measurement of a qubit in the Z basis is described by positive-operator-valued measure (POVM) elements with an error probability p_m as

$$E_0 = (1-p_m)|0\rangle\langle 0| + p_m|1\rangle\langle 1|, \tag{5}$$

$$E_1 = (1-p_m)|1\rangle\langle 1| + p_m|0\rangle\langle 0|. \tag{6}$$

The X measurement is also described by $E_+=HE_0H$ and $E_-=HE_1H$ with a Hadamard transformation H.

Given these imperfect operations, the purification map in the R^4 space

$$\mathbf{F}' = \mathcal{S}(\mathbf{F}) \tag{7}$$

is described specifically [4,9] as

$$F_i' = \frac{1}{p_S(\mathbf{F})} \sum_{jk} S_i^{jk}(p_{ab},p_m) F_j F_k, \tag{8}$$

where

$$p_S(\mathbf{F}) = \sum_{ijk} S_i^{jk}(p_{ab},p_m) F_j F_k \tag{9}$$

is the success probability responsible for the normalization $\Sigma_i F_i'=1$. The transition probability tensor $S_i^{jk}(p_{ab},p_m)$ is calculated in the Appendix including the error probabilities of a CNOT gate (p_{ab}) and a measurement (p_m). The maximum achievable fidelity of purified states is determined by iterating the purification map.

B. Double selection

The double-selection protocol is implemented by using three noisy copies of an EPR pair, two bilateral CNOT gates, and two bilateral measurements in each round of purification, as described in the following (see Fig. 2):

(i) Alice and Bob share three identical EPR pairs $\rho^{(0)}$, $\rho^{(1)}$, and $\rho^{(2)}$ through a noisy quantum channel.

(ii) They operate a bilateral CNOT gate on $\rho^{(0)}$ and $\rho^{(1)}$ as the control and target qubits, respectively.

(iii) Next they operate a bilateral CNOT gate on $\rho^{(2)}$ and $\rho^{(1)}$ as the control and target qubits, respectively.

(iv) They bilaterally measure $\rho^{(1)}$ and $\rho^{(2)}$ in the Z and X bases, respectively, and obtain the measurement outcomes $m_a^{(1)},m_a^{(2)}$ (Alice) and $m_b^{(1)},m_b^{(2)}$ (Bob).

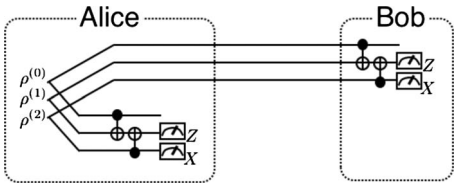

FIG. 2. Bipartite entanglement purification with double selection.

(v) They keep $\rho^{(0)}$ if the outcomes coincide for both of the measurements as $m_a^{(1)}=m_b^{(1)}$ and $m_a^{(2)}=m_b^{(2)}$. Otherwise, they discard $\rho^{(0)}$.

Similarly to the single-selection protocol, Alice and Bob iterate procedures (ii)–(v) by using the output states which survive the selection in procedure (v) as the input states for the next round where the X and Z bases of their reference frames are exchanged by a Hadamard transformation.

The above procedure provides a purification map

$$\mathbf{F}' = \mathcal{D}(\mathbf{F}), \tag{10}$$

which is given by cubic combinations of the initial-state components in the case of double selection as

$$F_i' = \frac{1}{p_{\mathcal{D}}(\mathbf{F})} \sum_{jkl} D_i^{jkl}(p_{ab},p_m) F_j F_k F_l, \tag{11}$$

where

$$p_{\mathcal{D}}(\mathbf{F}) = \sum_{ijkl} D_i^{jkl}(p_{ab},p_m) F_j F_k F_l. \tag{12}$$

The transition probability tensor $D_i^{jkl}(p_{ab},p_m)$ is calculated in the Appendix.

The double selection by the elaborate error detection with two ancilla EPR pairs can remove errors more efficiently than the single selection, as will be explained in Sec. III. This improves significantly the achievable fidelity and the noise threshold. Here, it should be mentioned that the purification protocol for large two-colorable graph states [12] also uses three copies of a state and two multilateral CNOT gates. In spite of this apparent similarity, the protocol of Ref. [12] is essentially different from the present double selection. In the double selection of Fig. 2 the source state $\rho^{(0)}$ is connected with the first ancilla $\rho^{(1)}$, and the first ancilla $\rho^{(1)}$ with the second ancilla $\rho^{(2)}$ for the optimal error detection and postselection. On the other hand, in the protocol of Ref. [12] both of the two ancilla states are connected with the source state by the CNOT gates in the same direction. This setup is adopted for the error correction to provide deterministically one purified state from three copies, which is efficient for the yield of purification. It, however, cannot remove fully the detectable errors, providing even lower fidelity than the single-selection protocol (see also a discussion in Sec. III). Generally, protocols based on postselection provide high fidelities and high noise thresholds, but exponentially diminishing yields as the size of purified state increases. Here, we aim to purify entangled states of relatively small size such as the EPR pair and the Steane seven-qubit code state, achieving a high fidelity and a high noise threshold with a tolerable yield.

C. Performance analysis

We now compare the single and the double selections in performance by considering the minimum fidelity required for the quantum communication channel, the maximum achievable fidelity of purified states, the working range for the noise of local operations, and the EPR resources consumed to achieve a target fidelity.

The EPR pairs of ϕ_0 are shared initially through a noisy communication channel $\mathcal{C}$ as

$$\mathcal{C}(\rho) = F_{\mathrm{ch}}\rho + \sum_{i=1}^{3} r_i \epsilon_{\mathrm{ch}} \sigma_i \otimes \sigma_0 \rho \sigma_i \otimes \sigma_0, \tag{13}$$

where F_{ch} and $r_i\epsilon_{\mathrm{ch}}$ with $\epsilon_{\mathrm{ch}} \equiv 1-F_{\mathrm{ch}}$ and $\Sigma_{i=1}^3 r_i = 1$ represent the channel fidelity and error probabilities, respectively. Then, the purification is started for a Bell-diagonal state $\mathcal{C}(\phi_0)$ as a noisy EPR pair with the state vector

$$\mathbf{F}^{(0)} = (F_{\mathrm{ch}}, r_1\epsilon_{\mathrm{ch}}, r_2\epsilon_{\mathrm{ch}}, r_3\epsilon_{\mathrm{ch}}). \tag{14}$$

By operating the purification map $\mathcal{A}$ ($\mathcal{S}$ or $\mathcal{D}$) recursively, the state vector $\mathbf{F}^{(n)}$ after the nth round is given by

$$\mathbf{F}^{(n)} = \mathcal{A}(\mathbf{F}^{(n-1)}). \tag{15}$$

The behavior of the Bell-diagonal states through the purification rounds is as follows. First, suppose that the errors of local operations are sufficiently small, that is, inside the working range. Then, if the initial fidelity $F_0^{(0)}=F_{\mathrm{ch}}$ is higher than some threshold value F_{min} (the minimum required fidelity), the state vector $\mathbf{F}^{(n)}$ approaches a fixed point in R^4 with a fidelity F_{max} (the maximum achievable fidelity), which is higher than F_{ch} ($>F_{\mathrm{min}}$). On the other hand, if $F_{\mathrm{ch}}<F_{\mathrm{min}}$, $\mathbf{F}^{(n)}$ goes to another fixed point $\mathbf{F}_{\mathrm{mix}}=(1/4,1/4,1/4,1/4)$ representing the completely mixed state. Next, if the errors are outside the working range, the purification map no longer admits the fixed point for F_{max}. Then, irrespective of the value of F_{ch}, $\mathbf{F}^{(n)}$ goes to $\mathbf{F}_{\mathrm{mix}}$, that is, the purification turns out to be impossible. We have checked these behaviors by numerical calculations. The values of the initial fidelity and error parameters have been taken by scanning over $1/4 \le F_{\mathrm{ch}} < 1$ and $0 \le p_g,\ p_m < 0.3$, where $p_{ij}=p_g/15$ $(ij \neq 00)$ and $p_{00}=1-p_g$ are adopted typically for the CNOT gate errors. Then, by tracing the transition of the Bell-diagonal states round by round according to the purification map, F_{min}, F_{max}, and the working range have been determined numerically, as done in the preceding study for the protocol with single selection [4]. Here, as in the Oxford protocol [9], the twirling operation to depolarize Bell-diagonal states to Werner states is not made in each round since the twirling with imperfect operations really lowers the achievable fidelity [4].

In the following, we show the results of numerical calculations on the performance of the present protocol, where a Werner state with $r_i=1/3$ is taken initially in Eq. (14) as a typical case. Similar results are obtained for general Bell-diagonal states with various r_i, as discussed later.

In Fig. 3, F_{max} (upper curves) and F_{min} (lower curves) are plotted as functions of the error probability p, where $p=p_g$

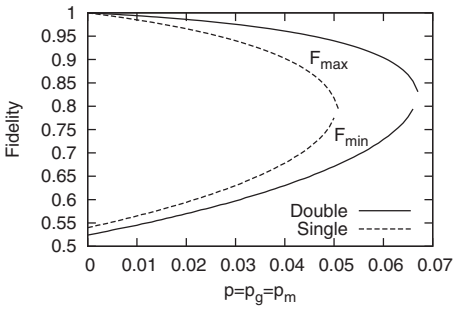

FIG. 3. Maximum achievable fidelity $F_{\max}$ (upper curves) and minimum required channel fidelity $F_{\min}$ (lower curves) are plotted as functions of the error probability $p=p_g=p_m$ for the double and single selections.

$=p_m$ are taken for definiteness. The double selection clearly achieves higher fidelity $F_{\max}$ with lower minimum required channel fidelity $F_{\min}$ compared with the single selection (Oxford protocol [4,9]). The working range of (p_g,p_m) is shown in Fig. 4. The purification is implemented successfully for $F_{\mathrm{ch}}>F_{\min}$ to achieve $F_{\max}$ if (p_g,p_m) is below each threshold curve. (The point on the threshold curve for $p=p_g=p_m$ really corresponds to the intersection point of the curves of $F_{\min}$ and $F_{\max}$ in Fig. 3.) It is found that the double-selection scheme has higher thresholds (the wider working range) for the errors of local operations than the single-selection scheme. We may also take $p_{i0}=p_{0i}=q_i$ and $p_{ij}=q_iq_j$ $(i,j\neq 0)$ for the error parameters, as adopted in Ref. [18]. Then, we estimate the threshold values 3.7% and 4.2% of p_g $(q_i=p_g/3)$ with $p_m=0$ for the single and double selections, respectively. The threshold value for the double selection is closer to an upper bound 5.3%, which is derived under some reasonable assumptions in Ref. [18]. The real bound would be located around 5% although it is outside our scope to determine it.

Here, we mention that the same achievable fidelity $F_{\max}$ is obtained even if general Bell-diagonal states with various r_i in Eq. (14) are taken initially. This is because $F_{\max}$ is given as the fixed point of the purification map, which is characterized by the local operations independently of the initial

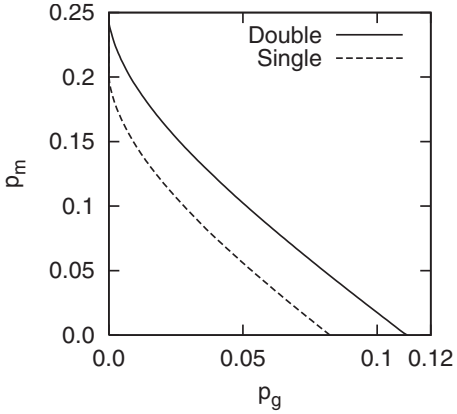

FIG. 4. Working range (p_g,p_m) of local operations. Each purification protocol $\mathcal{A}$ ($\mathcal{S}$ or $\mathcal{D}$) achieves $F_{\max}$ for $F_{\mathrm{ch}}>F_{\min}$ when the error probabilities p_g and p_m are below the threshold curve (solid line for $\mathcal{D}$ and dotted line for $\mathcal{S}$).

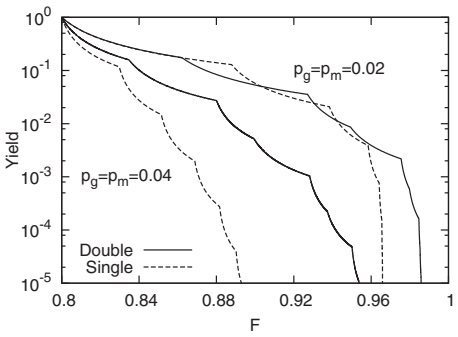

FIG. 5. The yield $Y_{\mathcal{A}}(F,F_{\mathrm{ch}}=0.8)$ is plotted as a function of the target fidelity F for each protocol with $p_g=p_m=0.02$ (upper curves) and $p_g=p_m=0.04$ (lower curves).

Bell-diagonal state. On the other hand, the minimum required channel fidelity $F_{\min}$ and the working range of (p_g,p_m) depend slightly on the choice of initial state. We have confirmed these features numerically by sampling the initial Bell-diagonal states with various r_i.

We next compare the yields of the two purification protocols. In the purification with imperfect local operations, the yield $Y_{\mathcal{A}}(F,F_{\mathrm{ch}})$ is defined as the inverse of the number of EPR pairs consumed to achieve a target fidelity F (<1) under the channel fidelity F_{ch} [16]. It is calculated for each protocol $\mathcal{A}=\mathcal{S},\mathcal{D}$ as

$$Y_{\mathcal{A}}(F,F_{\mathrm{ch}})=\left[\prod_{n=1}^{n_{\mathcal{A}}(F,F_{\mathrm{ch}})} N_{\mathcal{A}}/p_{\mathcal{A}}(\mathbf{F}^{(n-1)})\right]^{-1}, \qquad (16)$$

where $n_{\mathcal{A}}(F,F_{\mathrm{ch}})$ denotes the minimum number of rounds, which is required to achieve the fidelity F; $p_{\mathcal{A}}(\mathbf{F}^{(n-1)})$ denotes the probability to pass the purification procedure in the nth round, as given in Eqs. (9) and (12); and $N_{\mathcal{A}}$ denotes the number of EPR pairs consumed in each round ($N_{\mathcal{S}}=2$ and $N_{\mathcal{D}}=3$).

We plot in Fig. 5 the yield $Y_{\mathcal{A}}(F,F_{\mathrm{ch}}=0.8)$ as a function of the target fidelity F for each protocol with $p_g=p_m=0.02$ (upper curves) and $p_g=p_m=0.04$ (lower curves). By using less noisy local operations with $p_g=p_m=0.02$, both protocols provide comparable yields to achieve $F\approx 0.9$, where the numbers of purification rounds are $n_{\mathcal{S}}=4$ (single) and $n_{\mathcal{D}}=2$ (double), respectively. On the other hand, even when noisier local operations with $p_g=p_m=0.04$ are used, the double-selection protocol still provides a reasonable yield to achieve $F\approx 0.9$, where $n_{\mathcal{S}}=16$ and $n_{\mathcal{D}}=4$. Since the double selection uses three EPR pairs in each round, it may be thought to cost more resources than the single selection with two EPR pairs in each round. However, as seen in the above, the double selection provides a comparable or even better yield. This is because, by making the optimal error detection with two ancilla EPR pairs, the double selection can increase the fidelity of the source EPR pair considerably faster than the single selection, which will be discussed in the next section.

III. PURIFICATION FIDELITY LIMITED BY UNDETECTABLE ERRORS

Here, we discuss on general grounds how the errors of local operations limit the fidelity of purified states. Specifi-

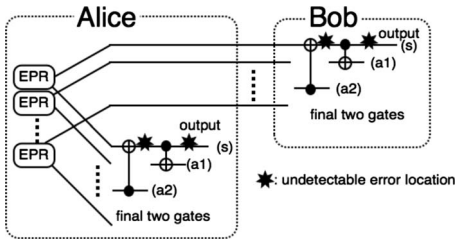

FIG. 6. Setup of a protocol of bipartite entanglement purification. An upper bound on the fidelity is determined in the first order by the undetectable errors (indicated by black stars) introduced by the final two CNOT gates. Similar bounds are obtained with other configurations of two-qubit gates.

cally, it is shown that some of the errors introduced by the gate operations in the final stage of purification are left as intrinsically undetectable. The double selection is indeed a simple method to remove all the detectable errors, other than the intrinsically undetectable ones, in the first order. Thus, in the low-noise regime it achieves the general upper bound on the purification fidelity, which is placed by the undetectable errors.

The final stage of any protocol of bipartite entanglement purification may be viewed as the combination of two bilateral CNOT gates, as shown in Fig. 6, or its variants as considered later. We inspect these final CNOT gate operations in Alice's site to observe the undetectable errors which are left on the output source qubit (s). (The same argument is made in Bob's site.) Passing through the final two gates, the preceding $\sigma_i^{(s)}$ errors $(i=1,2,3)$ on the source qubit (s) are propagated to either or both of the ancilla qubits (a1) and (a2). [It is possible that (a1)$\equiv$(a2).] Thus, these preceding errors are all detectable, and they can be removed by postselection after measuring the ancilla EPR pairs (a1) and (a2) in some appropriate way. The fidelity is limited ultimately by some of the errors introduced by the final two gates themselves (black stars in Fig. 6), which are *intrinsically undetectable without leaving any information on the ancillae*. As for the errors of the second-to-final CNOT gate, the $\sigma_3^{(s)} \otimes \sigma_0^{(a2)}$ error with the probability p_{30} is undetectable since $\sigma_3^{(s)}$ is not propagated to ancilla (a1), commuting with the final CNOT gate. The $\sigma_{1,2}^{(s)} \otimes \sigma_0^{(a2)}$ (through the final CNOT gate) and $\sigma_i^{(s)} \otimes \sigma_j^{(a2)}$ errors, on the other hand, affect ancillae (a1) and (a2), respectively, and thus they are detectable. The $\sigma_i^{(s)} \otimes \sigma_0^{(a1)}$ errors of the final CNOT gate with the probabilities p_{i0} are also undetectable since the output source (s) does not interact with any other ancillae afterward (by definition of the "final" CNOT gate). By subtracting the probabilities of these undetectable and thus irremovable errors at each party, an upper bound on the fidelity is placed in the first order as

$$F_{\text{upper}} = 1 - N\left(p_{30} + \sum_{i=1}^{3} p_{i0}\right), \tag{17}$$

where $N=2$ (Alice and Bob) for bipartite entanglement purification. Similar arguments are made for N-partite entanglement purification to derive this upper bound. Note that the measurement error is not involved in Eq. (17). A portion of the component of the right state ϕ_0 may be discarded due to the errors in measuring the ancillae for verification. This slight reduction in the right state is, however, cancelled in the first order by the renormalization after the postselection. The gate errors $\sigma_0^{(s)} \otimes \sigma_j^{(a1)}$ and $\sigma_0^{(s)} \otimes \sigma_j^{(a2)}$, which affect only the ancillae, do not contribute either to F_{upper} in the first order by the same reason as the measurement errors.

In another protocol the final two CNOT gates may be exchanged in Fig. 6. (This is actually the case in the recurrence protocols considered in Sec. II when the purification procedure is finished at an even round.) Similarly, by observing the undetectable errors, we obtain an upper bound on the fidelity as

$$F'_{\text{upper}} = 1 - N\left(p_{01} + \sum_{i=1}^{3} p_{0i}\right). \tag{18}$$

We note for completeness that if the final two CNOT gates are set in the same direction (e.g., both the CNOT gates are controlled by the source qubit) one of the preceding $\sigma_i^{(s)}$ errors on the source qubit cannot be detected, commuting with both the final two gates, to lower the fidelity. These upper bounds F_{upper} and F'_{upper} coincide with each other for the uniform distribution of the gate errors $p_{ij}=p_g/15$ $(ij \neq 00)$. In general, the upper bound is given by $\max[F_{\text{upper}}, F'_{\text{upper}}]$ depending on the error distribution; in a recurrence protocol one should determine whether the purification procedure is finished at an even or odd round. Other two-qubit Clifford gates instead of CNOT gates may also be used. Then, we obtain a similar upper bound with a suitable permutation among p_{ij}'s in Eq. (17) or Eq. (18) by counting the undetectable errors.

The recurrence protocols considered in Sec II, with either single or double selection, have the setup as shown in Fig. 6 by the exchange of the directions of the CNOT gates in each round. In the single selection (Fig. 1), however, the σ_3 (σ_1) error on the ancilla $\rho^{(1)}$ cannot be detected by the Z (X) measurement, while the σ_1 and σ_2 $(\sigma_2$ and $\sigma_3)$ errors are detected. The double selection (Fig. 2) is designed to detect even the σ_3 (σ_1) error on the primary ancilla $\rho^{(1)}$ [(a1) and (a2)] by using the secondary ancilla $\rho^{(2)}$ (not shown explicitly in Fig. 6). The errors on the source (s) are detectable if they leave any information on ancillae (a1) and (a2), that is, the ancilla errors play as the tracers of the source errors, as discussed so far. Thus, in the double-selection protocol all the detectable errors on the source (s) are removed by detecting fully the errors on ancillae (a1) and (a2) in the first order with the help of the extra ancillae. The upper bound on the fidelity is almost saturated as

$$F_{\text{max}}^{\mathcal{D}} = F_{\text{upper}} - O(p_e^2) \tag{19}$$

up to the higher-order error contributions $\sim p_e^2 = p_g^2$, $p_g p_m$, p_m^2. This estimate has been confirmed by the numerical calculation for $p_g < 2\%$ almost independent of $p_m < 5\%$ in Sec. II (see Fig. 3).

On the other hand, in the single selection the would-be detectable error $\sigma_3^{(s)} \otimes \sigma_1^{(a2)}$ of the second-to-final CNOT gate in Fig. 6, in addition to the undetectable error $\sigma_3^{(s)} \otimes \sigma_0^{(a2)}$, is not detected by the X measurement of ancilla (a2). As a result, these two σ_3 errors are left on the source (s) after the

second-to-final round of purification. This is just the same for ancilla (a1). The two σ_3 errors on ancilla (a1) are not detected by the Z measurement of ancilla (a1), and they are propagated to the source (s) as the two σ_3 errors through the final CNOT gate. The would-be detectable errors $\sigma_i^{(\mathrm{s})} \otimes \sigma_3^{(\mathrm{a1})}$ of the final CNOT gate are not detected either by the Z measurement of ancilla (a1). Due to these would-be detectable errors, but are not detected in practice, the achievable fidelity of the single-selection protocol is lowered from that of the double-selection protocol as

$$F_{\max}^{\mathcal{S}} = F_{\max}^{\mathcal{D}} - N(6/15)p_g - O(p_e^2), \tag{20}$$

with $p_{ij}=p_g/15$ $(ij \neq 00)$. This estimate on $F_{\max}^{\mathcal{S}}$ in the low-noise regime has also been confirmed by the numerical calculation in Sec. II.

The above limitation on the achievable fidelity, which is due to the errors introduced by some gate operations in the final stage, is applicable to a wide variety of purification protocols. The purification protocols proposed so far [4,8–17] do not achieve the fidelity higher than $F_{\max}^{\mathcal{S}}$ of the single selection. Specifically, in the protocol of Ref. [12] for large two-colorable graph states, which has an apparently similar setup to the double selection, the source state is connected with the two ancilla states by the two CNOT gates in order to extract sufficiently the error syndrome of the source state for the error correction. It is, however, realized that this setup just implements twice the error detections for the single selections. (The ancilla states are not inspected by using other ancilla states and CNOT gates. This is clearly different from the double selection.) Furthermore, one of the preceding errors on the source state cannot be detected, commuting with the two CNOT gates set in the same direction, as discussed so far. As a result, the achievable fidelity of this protocol [12] becomes lower than that of the single-selection protocol [11].

In the protocol of Ref. [17], $N-1$ EPR pairs are purified from noisy N EPR pairs by the single selection in order to improve the yield under perfect local operations for $N \geq 3$. An N to $N-2$ protocol with double selection may be considered as an extension to improve the achievable fidelity. However, the coincidence of all successful operations is required to pass the verification process with either single or double selection. Thus, as N increases the success probability for purification decreases substantially due to the multiple errors in the N to $N-1$ (or N to $N-2$) protocol. This indicates that the yield is not improved significantly in this sort of extension under imperfect local operations. We have made some numerical calculations for the 3–2 protocol with single selection and for the 4–2 protocol with double selection. The resultant yields Y ($F=0.9$, $F_{\mathrm{ch}}=0.8$) with $p_g=p_m=0.01$ are 0.025 and 0.085 for the 3–2 (single) and 4–2 (double) protocols, respectively, while $Y=0.15$ and 0.085 for the usual 2–1 (single) and 3–1 (double) protocols, respectively. On the other hand with $p_g=p_m=0.02$, the 3–2 (single) protocol cannot achieve $F=0.9$, and $Y=0.030$ for the 4–2 (double) protocol, while $Y=0.060$ and 0.055 for the usual 2–1 (single) and 3–1 (double) protocols, respectively. These results support the argument that this sort of extension does not improve the yield under imperfect local operations. Optimization for yield might be possible by combining the double selection with some appropriate methods, although it is beyond our scope.

The triple (or more) selection by using three ancilla EPR pairs also removes fully the detectable first-order errors, achieving the same F_{upper} in the low-noise regime as the double selection. It may further remove the higher-order errors to improve the fidelity and the noise threshold. We have considered a protocol with triple selection, which has a better noise threshold of 4.9% approaching the upper bound 5.3% [18], although it is not a purpose of the present study to pursue this possibility.

IV. MULTIPARTITE ENTANGLEMENT PURIFICATION

Recently purification is applied to a large class of multipartite entanglements including two-colorable graph states [11,12,14,15]. We can extend the present double-selection scheme for multipartite entanglement purification. Specifically, here we consider the purification of two-colorable graph states.

A graph is a set of vertices V connected in a specific way by edges E. Then, a stabilizer operator K_j is defined associated with each vertex V_j as

$$K_j = X_j \bigotimes_{\{k,j\} \in E} Z_k, \tag{21}$$

where V_k are the neighboring vertices connected with V_j by edges and the Pauli operators X_j and Z_k ($X \equiv \sigma_1$ and $Z \equiv \sigma_3$) act on the qubits on V_j and V_k, respectively [19]. A graph state $|\mu_1 \mu_2 \cdots \mu_N\rangle$ is an eigenstate of this set of stabilizer operators as

$$K_j |\mu_1 \mu_2 \cdots \mu_N\rangle = (-1)^{\mu_j} |\mu_1 \mu_2 \cdots \mu_N\rangle \quad (\mu_j = 0,1). \tag{22}$$

Especially, here we consider graph states associated with a two-colorable graph where the vertices are divided into two sets (colors) A and B in such a way that no vertices within one set are connected by edges. Namely, two-colorable graph states are described as

$$|\boldsymbol{\mu}_A, \boldsymbol{\mu}_B\rangle, \tag{23}$$

where $\boldsymbol{\mu}_A$ and $\boldsymbol{\mu}_B$ denote the sets of the eigenvalues of the stabilizers with colors A and B, respectively.

The entanglement purification with double selection for a noisy mixture of two-colorable graph states

$$\rho = \sum_{\boldsymbol{\mu}_A, \boldsymbol{\mu}_B} \lambda_{\boldsymbol{\mu}_A, \boldsymbol{\mu}_B} |\boldsymbol{\mu}_A, \boldsymbol{\mu}_B\rangle\langle \boldsymbol{\mu}_A, \boldsymbol{\mu}_B| \tag{24}$$

is implemented as follows (see Fig. 7):

(i) Alice, Bob, …, Nancy share three identical two-colorable graph states $\rho^{(0)}$, $\rho^{(1)}$, and $\rho^{(2)}$ through a noisy quantum channel. This means that the qubits at each party have the same color, i.e., the party has its own color A or B.

(ii) They operate a multilateral CNOT gate on $\rho^{(0)}$ and $\rho^{(1)}$, where for color A $\rho^{(0)}$ and $\rho^{(1)}$ are taken as the control and the target, respectively, while for color B $\rho^{(0)}$ and $\rho^{(1)}$ are taken as the target and the control, respectively

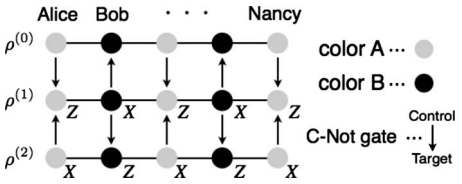

FIG. 7. Purification of two-colorable graph states with double selection.

(iii) Next they operate a multilateral CNOT gate on $\rho^{(2)}$ and $\rho^{(1)}$, similarly to the case of $\rho^{(0)}$ and $\rho^{(1)}$.

(iv) They make multilateral measurements, where for color A $\rho^{(1)}$ and $\rho^{(2)}$ are measured in the Z and X bases, respectively, while for color B $\rho^{(1)}$ and $\rho^{(2)}$ are measured in the X and Z bases, respectively. The party i with color A obtains the outcomes $(-1)^{\xi_i^{(1)}}$ and $(-1)^{\xi_i^{(2)}}$, while the party j with color B obtains the outcomes $(-1)^{\zeta_j^{(1)}}$ and $(-1)^{\zeta_j^{(2)}}$, where $\xi,\ \zeta=0,\ 1$.

(v) They keep $\rho^{(0)}$ if for all of them (i and j) $\xi_i^{(2)} \oplus \Sigma_{\{k,i\}\in E}\zeta_k^{(2)}=0$, and $\zeta_j^{(1)} \oplus \Sigma_{\{k,j\}\in E}\xi_k^{(1)}=0$, which implies $\boldsymbol{\mu}_B^{(1)} \oplus \boldsymbol{\mu}_B^{(2)}=\mathbf{0}$ and $\boldsymbol{\mu}_A^{(0)} \oplus \boldsymbol{\mu}_A^{(1)} \oplus \boldsymbol{\mu}_A^{(2)}=\mathbf{0}$, respectively, where $\oplus$ denotes bitwise addition modulo 2.

They iterate procedures (ii)–(v) by using the output states which survive the selection in procedure (v) as the input states for the next round where the X and Z bases of their reference frames are exchanged with a Hadamard transformation. Note in Fig. 7 that the source state $\rho^{(0)}$ and the two ancilla states $\rho^{(1)}$ and $\rho^{(2)}$ are connected by the two multilateral CNOT gates in the same way as the bipartite case for the double selection to remove fully the detectable errors on $\rho^{(0)}$ in the first order. This setup is distinct from that of Ref. [12].

We apply this double-selection protocol specifically to the Steane seven-qubit code state (a CSS code state) as an example of two-colorable graph states and compare it in performance with the Aschauer-Dür-Briegel (ADB) protocol of single selection [11]. We consider a multiparty communication situation, where the N-qubit two-colorable graph states of $|\mathbf{0}_A,\mathbf{0}_B\rangle$ are shared through N identical noisy channels $\mathcal{C}^{\otimes N}$. Then, the noisy copies of $\rho_{\rm in}=\mathcal{C}^{\otimes N}(|\mathbf{0}_A,\mathbf{0}_B\rangle\langle\mathbf{0}_A,\mathbf{0}_B|)$ are purified with the noisy CNOT gates and measurements. We have simulated directly the noisy operations on the code states in the communication channels and the purification procedures by using the Monte Carlo method. (It is very complicated in the high-dimensional space to provide the purification map in terms of the transition probability tensor.) The fidelity of the purified state ρ' is measured by

$$F(\rho',|\mathbf{0}_A,\mathbf{0}_B\rangle)=\langle\mathbf{0}_A,\mathbf{0}_B|\rho'|\mathbf{0}_A,\mathbf{0}_B\rangle. \tag{25}$$

If the initial fidelity

$$F_{\rm in}\equiv F(\rho_{\rm in},|\mathbf{0}_A,\mathbf{0}_B\rangle)=F_{\rm ch}^7+O((1-F_{\rm ch})^3) \tag{26}$$

is higher than $F_{\rm min}$, we can achieve the fidelity $F_{\rm max}$ by iterating the purification procedure.

The resultant maximum achievable fidelity $F_{\rm max}$ and the minimum required initial fidelity $F_{\rm min}$ are plotted in Fig. 8 for the Steane seven-qubit code state $|\mathbf{0}_A,\mathbf{0}_B\rangle=|0_L\rangle$ as functions of the error probability $p=p_g=p_m$, where $r_i=1/3$ is taken typically for the error probabilities of the noisy communication channel $\mathcal{C}$ in Eq. (13). As expected, the double selection achieves the considerably higher fidelity $F_{\rm max}$ with lower minimum required initial fidelity $F_{\rm min}$ in comparison with the single selection [11]. It really saturates the upper bound $F_{\rm max}^{\mathcal{D}}\approx F_{\rm upper}=1-7(4/15)p_g$ for $N=7$ with $p_{ij}=p_g/15$ $(ij\neq 0)$ of Eq. (17) in the low-noise regime. The noise threshold for the local operations is also improved from 5.9% (single) to 8.2% (double) for $p=p_g=p_m$. It is also seen in Fig. 9 ($F_{\rm in}\simeq 0.48$ for $F_{\rm ch}=0.9$ typically) that both schemes provide comparable yields, similar to the bipartite case. The yields are, however, significantly lower than those of the bipartite case. This is because the coincidence of the more measurement outcomes is required in the multipartite case so that the success probability of postselection is reduced.

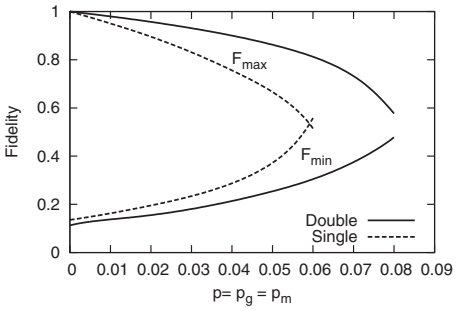

FIG. 8. Maximum achievable fidelity $F_{\rm max}$ (upper curves) and minimum required initial fidelity $F_{\rm min}$ (lower curves) for the Steane seven-qubit code state $|0_L\rangle$ are plotted as functions of the error probability $p=p_g=p_m$ for the single and double selections.

The two-colorable graph states, including CSS code states and cluster states, play important roles in quantum computation as well as quantum communication. Then, these results really indicate that the double selection is profitable also in quantum computation. In fact, encoded ancilla qubits are used to stabilize a computation in a fault-tolerant way, and the performance of computation highly depends on the fidelity of these ancilla qubits [20,21]. In the usual fault-tolerant context [21–23], these encoded ancilla qubits are prepared through the single selection. Thus, the double selection has a good potential to improve the noise threshold of fault-tolerant computation. The verification process with double selection is used in fault-tolerant computation with concat-

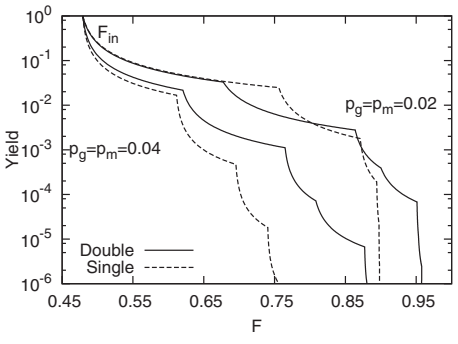

FIG. 9. The yield $Y_{\mathcal{A}}(F,F_{\rm ch}=0.9)$ is plotted as a function of the target fidelity F for each protocol with $p_g=p_m=0.02$ (upper curves) and $p_g=p_m=0.04$ (lower curves).

enated construction of verified logical cluster states, where a considerably high noise threshold of ~3% is achieved [24]. We will discuss elsewhere further applications of the double selection for quantum computation.

V. CONCLUSION

We have investigated entanglement purification with double selection under imperfect local operations. It has been shown that the double-selection protocol improves significantly the purification performance compared with the usual protocol with single selection. That is, the double-selection protocol has higher noise thresholds for the local operations and communication channels and achieves higher fidelity of purified states. It also provides a reasonable yield comparable to or even better than that of the single selection. It has been shown that the purification fidelity is limited by the intrinsically undetectable errors, which are introduced by the final gate operations. The double selection is a simple method to remove certainly all the detectable errors in the first order so that it achieves the upper bound on the fidelity in the low-noise regime. The double selection has been further applied to the purification of multipartite entanglement, specifically two-colorable graph states. The improvement of the fidelity and noise threshold has been shown for the Steane seven-qubit code state as a typical example. The double selection can be extended for various graph states in the same way. These results really indicate that the double selection is profitable for entanglement-based protocols. Since multipartite entangled states, such as CSS codes and cluster states, play important roles in quantum computation as well as quantum communication, the double selection has a good potential to improve the performance of quantum computation.

ACKNOWLEDGMENT

This work was supported by the JSPS Grant No. 20.2157.

APPENDIX: TRANSITION PROBABILITY TENSORS

The transition probability tensors to characterize the purification maps are calculated by tracing the linear transformations of Bell states through the purification procedures. In the single-selection protocol the linear transformation $\tilde{\mathcal{S}}$ of two Bell states $\phi_i^{(0)}\otimes\phi_j^{(1)}$ before the postselection is given as

$$\tilde{\mathcal{S}}(\phi_i^{(0)}\otimes\phi_j^{(1)})=\tilde{S}_{kl}^{ij}\phi_k^{(0)}\otimes\phi_l^{(1)}, \tag{A1}$$

which provides $\tilde{\mathcal{S}}(\rho^{(0)}\otimes\rho^{(1)})=F_iF_j\tilde{S}_{kl}^{ij}\phi_k^{(0)}\otimes\phi_l^{(1)}$. This map consists of the noisy bilateral CNOT gate $\mathcal{G}(\phi_i^{(0)}\otimes\phi_j^{(1)})=G_{ab}^{ij}\phi_a^{(0)}\otimes\phi_b^{(1)}$, the error effect on the ancilla $\phi_b^{(1)}$ in the bilateral Z measurement $\mathcal{M}(\phi_b^{(1)})=M_l^b\phi_l^{(1)}$, and the bilateral Hadamard operation $\mathcal{H}(\phi_a^{(0)})=H_k^a\phi_k^{(0)}$ to describe mathematically (perfect by itself) the change in the reference frames for the next round,

$$\tilde{S}_{kl}^{ij}=H_k^aM_l^bG_{ab}^{ij}. \tag{A2}$$

The noisy bilateral CNOT gate G_{km}^{ij} is decomposed into the ideal one U_{ab}^{ij} and the bilateral combination $N_{km}^{cd}N_{cd}^{ab}$ of the noises as follows:

$$G_{km}^{ij}=N_{km}^{cd}N_{cd}^{ab}U_{ab}^{ij}. \tag{A3}$$

The ideal bilateral CNOT gate operation $\mathcal{U}^{\otimes 2}\equiv\mathcal{U}_A\otimes\mathcal{U}_B$ with the local operations at Alice (A) and Bob (B) induces the permutation U_{ab}^{ij} among $\phi_i^{(0)}\otimes\phi_j^{(1)}$'s. To find U_{ab}^{ij} we use suitably the graph-state representation as

$$|\phi_i\rangle\equiv(I\otimes H)|\mu_A^i,\mu_B^i\rangle, \tag{A4}$$

where

$$\boldsymbol{\mu}^i=(\mu_A^i,\mu_B^i)=(0,0),(1,0),(1,1),(0,1) \tag{A5}$$

for $i=0,1,2,3$, respectively. The action of bilateral CNOT gate on the graph states, $|\mu_A^i,\mu_B^i\rangle^{(0)}|\mu_A^j,\mu_B^j\rangle^{(1)}\rightarrow|\mu_A^i,\mu_B^i\oplus\mu_B^j\rangle^{(0)}|\mu_A^i\oplus\mu_A^j,\mu_B^j\rangle^{(1)}$, is denoted simply as

$$\tilde{\mathcal{U}}(\boldsymbol{\mu}^i\otimes\boldsymbol{\mu}^j)=(\mu_A^i,\mu_B^i\oplus\mu_B^j)\otimes(\mu_A^i\oplus\mu_A^j,\mu_B^j). \tag{A6}$$

Then, the permutation is read as

$$U_{ab}^{ij}=\begin{cases}1 & [\boldsymbol{\mu}^i\otimes\boldsymbol{\mu}^j=\tilde{\mathcal{U}}(\boldsymbol{\mu}^a\otimes\boldsymbol{\mu}^b)]\\ 0 & [\boldsymbol{\mu}^i\otimes\boldsymbol{\mu}^j\neq\tilde{\mathcal{U}}(\boldsymbol{\mu}^a\otimes\boldsymbol{\mu}^b)].\end{cases} \tag{A7}$$

For example, $U_{22}^{13}=1$ for $\tilde{\mathcal{U}}[\boldsymbol{\mu}^2\otimes\boldsymbol{\mu}^2=(1,1)\otimes(1,1)]=\boldsymbol{\mu}^1\otimes\boldsymbol{\mu}^3=(1,0)\otimes(0,1)$, and $U_{ij}^{13}=0$ for the others, providing $\mathcal{U}^{\otimes 2}(\phi_1^{(0)}\otimes\phi_3^{(1)})=U_{ij}^{13}\phi_i^{(0)}\otimes\phi_j^{(1)}=\phi_2^{(0)}\otimes\phi_2^{(1)}$. The noise map of the CNOT gate at one party in Eq. (4) is specified for the basis states $\phi_a^{(0)}\otimes\phi_b^{(1)}$ as

$$\begin{aligned}\mathcal{N}(\phi_a^{(0)}\otimes\phi_b^{(1)})&=\sum_{ij}p_{ij}(\sigma_i\phi_a^{(0)}\sigma_i)\otimes(\sigma_j\phi_b^{(1)}\sigma_j)\\&=N_{cd}^{ab}\phi_c^{(0)}\otimes\phi_d^{(1)},\end{aligned} \tag{A8}$$

where σ_i and σ_j act on the control and target qubits at the party, respectively. This formula is applied equally to the CNOT gate operations by Alice and Bob. The operations by σ_i and σ_j in Eq. (A8) induce the permutations among the Bell states as $\mathcal{P}_{\sigma_i}(\phi_a)=\sigma_i\phi_a\sigma_i=\phi_c$, which are given explicitly by

$$\mathcal{P}_{\sigma_0}=\begin{pmatrix}0&1&2&3\\0&1&2&3\end{pmatrix},\quad \mathcal{P}_{\sigma_1}=\begin{pmatrix}0&1&2&3\\1&0&3&2\end{pmatrix},$$

$$\mathcal{P}_{\sigma_2}=\begin{pmatrix}0&1&2&3\\2&3&0&1\end{pmatrix},\quad \mathcal{P}_{\sigma_3}=\begin{pmatrix}0&1&2&3\\3&2&1&0\end{pmatrix}, \tag{A9}$$

e.g., $\sigma_1\phi_2\sigma_1=\phi_3$ is given as $2\rightarrow 3$ in $\mathcal{P}_{\sigma_1}$, and so on. This reads

$$N_{cd}^{ab}=p_{ij}[(ac)\in\mathcal{P}_{\sigma_i},(bd)\in\mathcal{P}_{\sigma_j}], \tag{A10}$$

e.g., $N_{10}^{00}=p_{10}$ for $(ac)=(01)$ and $(bd)=(00)$, and so on. Then, the bilateral combination of the deporalizing errors is given by

$$\mathcal{N}_B[\mathcal{N}_A(\phi_a^{(0)}\otimes\phi_b^{(1)})]=N_{km}^{cd}N_{cd}^{ab}\phi_k^{(0)}\otimes\phi_m^{(1)}, \tag{A11}$$

where $\mathcal{N}_A$ and $\mathcal{N}_B$ represent the noise maps of Eq. (A8) at Alice and Bob, respectively.

The imperfect Z measurement by each party can be described equivalently as a sequence of a noise map

$$\mathcal{M}_e(\rho) = (1-p_m)\sigma_0\rho\sigma_0 + p_m\sigma_1\rho\sigma_1, \tag{A12}$$

and the ideal measurement with the projection operators $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. This is because the action of the POVM operators E_k in Eqs. (5) and (6) is reproduced by $|k\rangle\langle k|\mathcal{M}_e$ as $\mathrm{Tr}(E_k\rho)=\mathrm{Tr}[\mathcal{M}_e(|k\rangle\langle k|)\rho]=\mathrm{Tr}[|k\rangle\langle k|\mathcal{M}_e(\rho)]$ $(k=0,1)$ [4]. Then, the noise effect in the bilateral Z measurement is given by

$$M_l^b = m_l^f m_f^b \tag{A13}$$

as a product of the single ones $\mathcal{M}_e(\phi_b)=m_f^b\phi_f$ in Eq. (A12) with

$$m_f^b = \begin{cases} 1-p_m & [(bf)\in\mathcal{P}_{\sigma_0}] \\ p_m & [(bf)\in\mathcal{P}_{\sigma_1}] \\ 0 & [(bf)\in\mathcal{P}_{\sigma_2},\mathcal{P}_{\sigma_3}]. \end{cases} \tag{A14}$$

The bilateral Hadamard operation is given by

$$H_k^a = h_k^e h_e^a, \tag{A15}$$

where the single operation $H|\phi_a\rangle=h_e^a|\phi_e\rangle$ is given with $h_0^0=h_3^1=h_2^2=h_1^3=1$ and $h_e^a=0$ for the others. This operation provides mathematically the inversion of the direction (control and target) of the CNOT gate in the next round, and the permutation of the error parameters is induced accordingly as

$$p_{ij} \to p'_{i'j'}[\sigma_{i'} = H\sigma_j H, \sigma_{j'} = H\sigma_i H], \tag{A16}$$

that is, the components are exchanged as $i\leftrightarrow j$ and then $1\leftrightarrow 3$ round by round. The uniform error distribution is specifically invariant as $p_{ij}=p'_{i'j'}=p_g/15$ $(ij\neq 00)$.

After all the transition probability tensor S_i^{jk} of the single selection is obtained by picking up the right states $\phi_0^{(1)}$ and $\phi_3^{(1)}$ $(l=0,3)$ from $\tilde{\mathcal{S}}(\rho^{(0)}\otimes\rho^{(1)})=F_jF_k\tilde{S}_{il}^{jk}\phi_i^{(0)}\otimes\phi_l^{(1)}$, which pass the postselection after the Z measurement,

$$S_i^{jk} = \tilde{S}_{i0}^{jk} + \tilde{S}_{i3}^{jk}, \tag{A17}$$

where the error parameters p_{ij} and p_m are included as seen so far. By taking the uniform error distribution $p_{ij}=p_g/15$ $(ij\neq 00)$ and then setting $p_g=p_m=0$, this formula of S_i^{jk} for the single selection really reproduces the purification maps presented in the preceding studies with imperfect [4] and perfect [8,9] local operations, respectively.

Similarly, the purification procedure of the double selection before the postselection is described as a linear map $\tilde{\mathcal{D}}$ of $\phi_i^{(0)}\otimes\phi_j^{(1)}\otimes\phi_k^{(2)}$ as

$$\tilde{D}_{lmn}^{ijk} = H_l^a M_m^c \tilde{M}_n^d G_{dc}^{kb} G_{ab}^{ij}, \tag{A18}$$

where

$$\tilde{M}_n^d = H_n^f M_f^e H_e^d \tag{A19}$$

provides the noise effect in the bilateral X measurement. Then, the transition probability tensor of the double selection is obtained by the postselection after the Z and X measurements as

$$D_i^{jkl} = \sum_{m=0,3;n=0,1} \tilde{D}_{imn}^{jkl}. \tag{A20}$$

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998); W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[5] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001); R. Raussendorf, D. E. Browne, and H.-J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[6] P. W. Shor, *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1996), p. 56.
[7] K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).
[8] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[9] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[10] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, R4075 (1998).
[11] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003); H. Aschauer, W. Dür, and H.-J. Briegel, Phys. Rev. A **71**, 012319 (2005).
[12] K. Goyal, A. McCauley, and R. Raussendorf, Phys. Rev. A **74**, 032318 (2006).
[13] S. Glancy, E. Knill, and H. M. Vasconcelos, Phys. Rev. A **74**, 032319 (2006).
[14] C. Kruszynska, A. Miyake, H.-J. Briegel, and W. Dür, Phys. Rev. A **74**, 052316 (2006).
[15] A. Miyake and H.-J. Briegel, Phys. Rev. Lett. **95**, 220501 (2005).
[16] C. Kruszynska, S. Anders, W. Dür, and H.-J. Briegel, Phys. Rev. A **73**, 062328 (2006).
[17] E. N. Maneva and J. A. Smolin, *Quantum Computation and Quantum Information*, AMS Contemporary Mathematics Vol. 305, edited by J. Samuel and J. Lomonaco (American Mathematical Society, Providence, RI, 2002).
[18] A. Kay, Phys. Rev. A **77**, 052319 (2008).
[19] W. Dür and H.-J. Briegel, Rep. Prog. Phys. **70**, 1381 (2007).
[20] B. Eastin, Phys. Rev. A **75**, 022301 (2007).
[21] E. Knill, Nature (London) **434**, 39 (2005).
[22] A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997).
[23] A. Cross, D. DiVincenzo, and B. Terhal, e-print arXiv:0711.1556.
[24] K. Fujii and K. Yamamoto, *Proceedings of the 9th International Conference of QCMC* (AIP, Melville, NY, 2009), p. 141.