Tight bound on coherent-state-based entanglement generation over lossy channels

Koji Azuma,* Naoya Sota, Masato Koashi, and Nobuyuki Imoto
Division of Materials Physics, Department of Materials Engineering Science, Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan
(Received 3 December 2009; published 25 February 2010)

The first stage of the hybrid quantum repeaters is entanglement generation based on transmission of pulses in coherent states over a lossy channel. Protocols to make entanglement with only one type of error are favorable for rendering subsequent entanglement distillation efficient. Here we provide the tight upper bound on performances of these protocols that is determined only by the channel loss. In addition, we show that this bound is achievable by utilizing a proposed protocol [K. Azuma, N. Sota, R. Namiki, Ş. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **80**, 060303(R) (2009)] composed of a simple combination of linear optical elements and photon-number-resolving detectors.

DOI: 10.1103/PhysRevA.81.022325 PACS number(s): 03.67.Hk, 42.50.Pq, 03.67.Mn

I. INTRODUCTION

The transmission of quantum information is important to accomplish applications such as quantum teleportation [1], quantum key distribution [2], and distributed quantum computation [3]. To achieve such quantum communication, optical pulses are used as the carrier of quantum information. In a practical communication channel, the pulses inevitably suffer from photon losses that increase exponentially with channel length, which makes it inefficient to conduct long-distance quantum communication by direct transmission of photons. One way to achieve efficient long-distance quantum communication against the photon losses is to invoke a quantum repeater protocol [4] utilizing quantum memories. In fact, there are many works suggesting that long-distance quantum communication can be efficiently achieved by repeater protocols based on realizable quantum memories [5–14].

A type of the repeater protocols we focus on here is the so-called hybrid quantum repeater protocol [15–19]. These protocols are based on a simple interaction between a qubit quantum memory A and an optical pulse a prepared in a coherent state, which is

$$\begin{aligned}\hat{V}|0\rangle_A|\alpha\rangle_a &= |0\rangle_A|\alpha_0\rangle_a,\\ \hat{V}|1\rangle_A|\alpha\rangle_a &= |1\rangle_A|\alpha_1\rangle_a,\end{aligned} \tag{1}$$

where $\hat{V}$ is a unitary operator and $|\alpha\rangle_a$ and $\{|\alpha_j\rangle_a\}_{j=0,1}$ are coherent states. Quantum memories with this type of interaction are considered to be implementable by individual Λ-type atoms, single electrons trapped in quantum dots, nitrogen-vacancy (NV) centers in a diamond with a nuclear spin degree of freedom, or neutral donor impurities in semiconductors [15,16,18]. As an advantage of the hybrid quantum repeater protocols, all the stages in the repeater protocol—entanglement generation, entanglement distillation [20–22], and entanglement swapping [23]—are shown to be implementable [15,16,24] only by the unitary operations in the form of Eq. (1). In the stream of the stages in the repeaters, an undoubted method to achieve higher efficiencies is to find a good entanglement generation protocol, leaving the quantum memories in entanglement that is efficiently distillable at the distillation stage and efficiently connectable at the entanglement swapping stage. Since realistic entanglement distillation protocols [20–22] and entanglement swapping [23] work more efficiently against a restricted type of errors, entanglement generation protocols yielding entanglement with only one type of error are favorable for a high performance of the hybrid quantum repeaters. Actually, a number of protocols [17–19] have been proposed for generating the single-error-type entanglement, which raises a fundamental question of how the amount of the channel loss imposes an ultimate bound on the efficiency of generating single-error-type entanglement. The answer to this question not only clarifies the possibility of further improvement of the entanglement generation protocols in hybrid quantum repeaters but also gives a fundamental benchmark enabling us to compare other types of quantum repeaters to hybrid quantum repeaters.

Reference [17] can be regarded as one of the first attempts to derive such a limit of performance of single-error-type entanglement generation. There, van Loock *et al.* have considered the cases where a single probe pulse interacts with the sender's quantum memory and with the receiver's quantum memory in exactly the same manner, as in the protocols in Refs. [17,18]. The question was the best performance among arbitrary choices of the measurement on the probe pulse after the interactions. They have given an upper bound on the performance, but it remains to be open whether the bound is achievable by optimizing the measurement. On the other hand, in Ref. [19], we have presented a protocol using two probe pulses that interact with the quantum memories of the sender and of the receiver independently, and we have shown that the protocol has a higher performance than the single-probe protocols in Refs. [17,18]. At this point, it became clear that we need a more general bound that encompasses both one-probe and two-probe protocols. Toward this goal, we have given a preliminary result in Ref. [19], which was limited to the cases where the sender begins with a symmetric state $(|0\rangle_A + |1\rangle_A)/\sqrt{2}$.

In this article, we solve the final piece of the puzzle about the limit of single-error-type entanglement generation protocols by providing the tight upper bound encompassing all the protocols starting from interaction (1) by the sender.

*azuma@qi.mp.es.osaka-u.ac.jp

The bound is stated in terms of the average singlet fraction of generated entanglement and by the success probability, and it is determined only by the channel loss, that is, the length of the channel. Moreover, the general bound is shown to be achievable by using the proposed protocol [19] that is realizable by a simple combination of linear optical elements and photon-number-resolving detectors.

This article is organized as follows. In Sec. II, we define protocols to generate entanglement with only one type of error and we define the measure of its performance. We derive an upper bound on those performances in Sec. III, which is the main theorem in this article. In Sec. IV, we show that the upper bound is achievable by convex combination of the protocol proposed in Ref. [19] and a trivial protocol. In Sec. V, we derive an explicit expression of the tight upper bound as a function of the transmittance of the channel loss. Section VI concludes the article.

II. SINGLE-ERROR-TYPE ENTANGLEMENT GENERATION AND THE MEASURE OF ITS PERFORMANCE

Let us define the family of single-error-type entanglement generation protocols considered in this article. We require Alice and Bob to make an entangled state with only one type of error. More precisely, Alice and Bob are required to make qubits AB in an entangled state that can be transformed into a state contained in the subspace spanned by Bell states $\{|\Phi^{\pm}\rangle_{AB}\}$ via local unitary operations, where $|\Phi^{\pm}\rangle_{AB} := (|00\rangle_{AB} \pm |11\rangle_{AB})/\sqrt{2}$.

To generate such an entangled state, Alice and Bob execute the following steps (Fig. 1): (i) Alice prepares qubit A in her desired state $|\phi\rangle_A = \sum_{j=0,1} e^{i\Theta_j}\sqrt{q_j}|j\rangle_A$ with real parameters Θ_j, $q_j \geqslant 0$, and $\sum_j q_j = 1$, and she makes it interact with a pulse in a coherent state $|\alpha\rangle_a = e^{-|\alpha|^2/2} e^{\alpha\hat{a}^\dagger}|0\rangle_a$ via a unitary operation $\hat{V}$ of Eq. (1). (ii) Alice sends the pulse a to Bob, through a lossy channel described by an isometry,

$$\hat{N}|\alpha\rangle_a = |\sqrt{T}\alpha\rangle_b|\sqrt{1-T}\alpha\rangle_E, \tag{2}$$

where $0 < T < 1$ is the transmittance of the channel and system E is the environment. (iii) Upon receiving the pulse in mode b, Bob may perform arbitrary operations and measurements involving pulse b and his memory qubit B and declare success outcome k occurring with a probability p_k or failure. (iv) If Step (iii) succeeds, depending on the outcome k, Alice and Bob apply a local unitary operation $\hat{U}_k^A \otimes \hat{U}_k^B$ to the obtained state, in order to satisfy that the final state $\hat{\tau}_k^{AB}$ is contained in the subspace spanned by $\{|\Phi^{\pm}\rangle_{AB}\}$ and also that the nearest Bell state to the state $\hat{\tau}_k^{AB}$ is $|\Phi^{+}\rangle_{AB}$.

We evaluate the performance of the protocols by the total success probability,

$$P_s = \sum_k p_k, \tag{3}$$

and the averaged fidelity of the obtained entangled states,

$$F = \frac{1}{P_s}\sum_k p_k F_k, \tag{4}$$

where F_k is

$$F_k := \langle\Phi^{+}|\hat{\tau}_k^{AB}|\Phi^{+}\rangle. \tag{5}$$

Thanks to the choice of the unitary operation in Step (iv), F_k is equivalent to the so-called *singlet fraction* [22]. Since $\hat{\tau}_k^{AB}$ is contained in the subspace spanned by $\{|\Phi^{\pm}\rangle_{AB}\}$, $F_k \geqslant 1/2$ holds. This means

$$F \geqslant 1/2. \tag{6}$$

We also allow Alice and Bob to switch among two or more protocols probabilistically. The performance of such a mixed protocol is determined as follows. Suppose that Alice and Bob can execute a protocol with performance $(P_s^{(1)}, F^{(1)})$ and a protocol with performance $(P_s^{(2)}, F^{(2)})$. Then, by choosing these protocols with probabilities $\{r, 1-r\}$, Alice and Bob can achieve performance (P_s', F') determined by

$$\begin{pmatrix} P_s' \\ P_s'F' \end{pmatrix} = r\begin{pmatrix} P_s^{(1)} \\ P_s^{(1)}F^{(1)} \end{pmatrix} + (1-r)\begin{pmatrix} P_s^{(2)} \\ P_s^{(2)}F^{(2)} \end{pmatrix}. \tag{7}$$

It is thus convenient to describe the performance of a protocol by point (P_s, P_sF). Then, the set of achievable points (P_s, P_sF) forms a convex set.

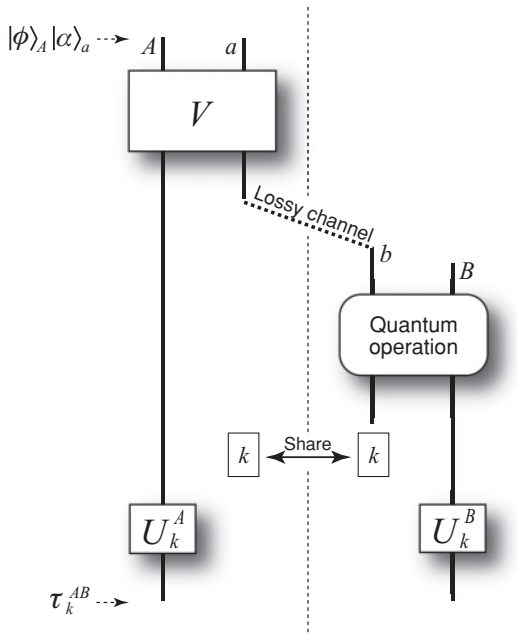

FIG. 1. The scenario of entanglement generation protocols. $|\phi\rangle_A := \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j}|j\rangle_A$. Bob's quantum operation returns qubit B in a state depending on outcome k, and he shares the outcome with Alice by using classical communication.

III. AN UPPER BOUND ON THE PERFORMANCE OF A SINGLE-ERROR-TYPE ENTANGLEMENT GENERATION PROTOCOL

We first introduce a protocol equivalent to the single-error-type entanglement generation protocol. Steps (i) and (ii) indicate that, when the pulse arrives at Bob, the state of the total system AbE is written in the form of

$$|\psi\rangle_{AbE} = \sum_{j=0,1}\sqrt{q_j}|j\rangle_A|u_j\rangle_b|v_j\rangle_E, \tag{8}$$

with $0 \leqslant q_0 \leqslant 1$, $q_0 + q_1 = 1$, and

$$|\langle u_1|u_0\rangle|^{1-T} = |\langle v_1|v_0\rangle|^T > 0. \tag{9}$$

Let us define a phase-flip channel Λ_A on qubit A by

$$\Lambda_A(\hat{\rho}) := f\hat{\rho} + (1-f)\hat{\sigma}_z^A \hat{\rho} \hat{\sigma}_z^A, \tag{10}$$

with

$$f := \frac{1 + |\langle v_1|v_0\rangle|}{2} = \frac{1 + |\langle u_1|u_0\rangle|^{\frac{1-T}{T}}}{2} \tag{11}$$

and $\hat{\sigma}_z^A := |0\rangle\langle 0|_A - |1\rangle\langle 1|_A$. From Eqs. (8), (10), and (11), we have

$$\mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AbE}] = \Lambda_A(|\psi'\rangle\langle\psi'|_{Ab}), \tag{12}$$

where

$$|\psi'\rangle_{Ab} := \sum_{j=0,1} \sqrt{q_j} e^{i(-1)^j\varphi} |j\rangle_A |u_j\rangle_b, \tag{13}$$

with $2\varphi := \arg[\langle v_1|v_0\rangle]$. The effect of the lossy channel is thus equivalently described as preparation of $|\psi'\rangle_{Ab}$ followed by Λ_A. Since any operation of Bob commutes with Λ_A, the protocol is equivalent to the following sequence (Fig. 2): (1) System Ab is prepared in $|\psi'\rangle_{Ab}$; (2) Bob's successful measurement leaves system AB in a state $\hat{\rho}_k^{AB}$; (3) Λ_A is applied on qubit A.

In what follows, according to the equivalent protocol of Fig. 2, we show that, for fixed T and $|\langle u_1|u_0\rangle|$, the performance $(P_s, P_s F)$ of an arbitrary protocol must be in the triangle with the apexes,

$$X_0 := (0,0),$$
$$X_1 := \left(1 - |\langle u_1|u_0\rangle|, (1 - |\langle u_1|u_0\rangle|)\frac{1 + |\langle u_1|u_0\rangle|^{\frac{1-T}{T}}}{2}\right),$$
$$X_2 := (1, 1/2). \tag{14}$$

The proof is divided into two cases.

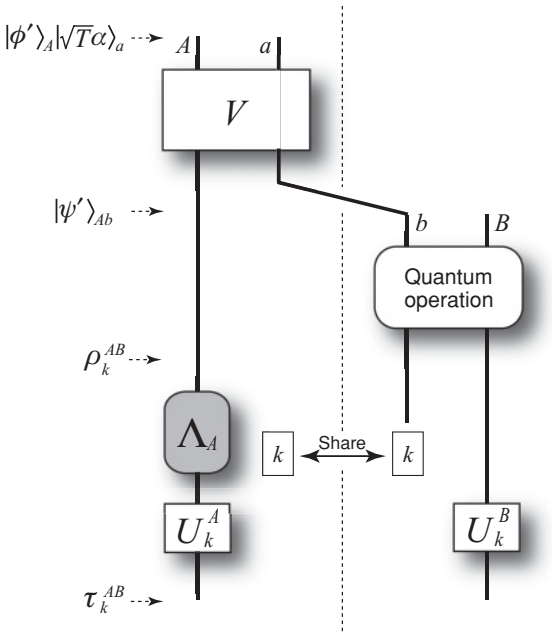

FIG. 2. An imaginary protocol equivalent to the real protocol in Fig. 1. $|\phi'\rangle_A := \sum_{j=0,1} \sqrt{q_j} e^{i\Theta_j + i(-1)^j\varphi}|j\rangle_A$. Channel $a \to b$ becomes ideal at the expense of the application of a phase-flip channel Λ_A.

(a) $|q_0 - q_1| = 1$ *or* $|\langle u_1|u_0\rangle| = 1$. In these cases, from Eq. (13), $|\psi'\rangle_{Ab}$ is a product state between system A and b. This implies that $\hat{\tau}_k^{AB}$ is a separable state, which means $F_k \leqslant 1/2$. From Eq. (6), $F = 1/2$. Thus, in this case, the performance $(P_s, P_s F)$ of protocols must be on the segment X_0X_2.

(b) $|q_0 - q_1| < 1$ *and* $|\langle u_1|u_0\rangle| < 1$. As stated in Step (iv), whenever Bob declares success outcome k, the state $\hat{\tau}_k^{AB}$ of their qubits satisfies

$$\langle\Psi^\pm|\hat{\tau}_k^{AB}|\Psi^\pm\rangle = \langle\Psi_k'^\pm|\Lambda_A(\hat{\rho}_k^{AB})|\Psi_k'^\pm\rangle = 0, \tag{15}$$

with $|\Psi_k'^\pm\rangle_{AB} := \hat{U}_k^{A\dagger} \otimes \hat{U}_k^{B\dagger}|\Psi^\pm\rangle_{AB} = (|x_k^0\rangle_A|y_k^1\rangle_B \pm |x_k^1\rangle_A|y_k^0\rangle_B)/\sqrt{2}$, $|\Psi^\pm\rangle_{AB} := (|01\rangle_{AB} \pm |10\rangle_{AB})/\sqrt{2}$, $|x_k^j\rangle_A := \hat{U}_k^{A\dagger}|j\rangle_A$ and $|y_k^j\rangle_B := \hat{U}_k^{B\dagger}|j\rangle_B$ $(j = 0, 1)$. Since $\hat{\rho}_k^{AB}$ is positive and $0 < f < 1$, Eq. (15) indicates

$$\sqrt{\hat{\rho}_k^{AB}}|\Psi_k'^\pm\rangle_{AB} = 0, \tag{16}$$

$$\sqrt{\hat{\rho}_k^{AB}}\hat{\sigma}_z^A|\Psi_k'^\pm\rangle_{AB} = 0, \tag{17}$$

for both $\pm$. Note that Eq. (16) implies

$$\hat{\rho}_k^{AB} = \frac{1+a_k}{2}|\Phi_k'^+\rangle\langle\Phi_k'^+|_{AB} + \frac{1-a_k}{2}|\Phi_k'^-\rangle\langle\Phi_k'^-|_{AB} + \frac{b_k}{2}|\Phi_k'^+\rangle\langle\Phi_k'^-|_{AB} + \frac{b_k^*}{2}|\Phi_k'^-\rangle\langle\Phi_k'^+|_{AB}, \tag{18}$$

where $|\Phi_k'^\pm\rangle_{AB} := \hat{U}_k^{A\dagger} \otimes \hat{U}_k^{B\dagger}|\Phi^\pm\rangle_{AB} = (|x_k^0\rangle_A|y_k^0\rangle_B \pm |x_k^1\rangle_A|y_k^1\rangle_B)/\sqrt{2}$, and the positivity of $\hat{\rho}_k^{AB}$ implies

$$a_k^2 + |b_k|^2 \leqslant 1. \tag{19}$$

Note that $0 \leqslant a_k \leqslant 1$ is satisfied by the choice of the unitary operation $\hat{U}_k^A \otimes \hat{U}_k^B$ in Step (iv). Adding and subtracting Eqs. (16) and (17), we obtain

$$\sqrt{\hat{\rho}_k^{AB}}|x_k^0\rangle_A|y_k^1\rangle_B = \sqrt{\hat{\rho}_k^{AB}}\hat{\sigma}_z^A|x_k^0\rangle_A|y_k^1\rangle_B = \sqrt{\hat{\rho}_k^{AB}}|x_k^1\rangle_A|y_k^0\rangle_B = \sqrt{\hat{\rho}_k^{AB}}\hat{\sigma}_z^A|x_k^1\rangle_A|y_k^0\rangle_B = 0. \tag{20}$$

Since $\hat{\rho}_k^{AB} \neq 0$, the four states, $|x_k^0\rangle_A|y_k^1\rangle_B$, $\hat{\sigma}_z^A|x_k^0\rangle_A|y_k^1\rangle_B$, $|x_k^1\rangle_A|y_k^0\rangle_B$, and $\hat{\sigma}_z^A|x_k^1\rangle_A|y_k^0\rangle_B$, must be linearly dependent, which only happens when $\{|x_k^j\rangle_A\}_{j=0,1}$ is a set of eigenvectors of $\hat{\sigma}_z^A$. Combining this fact with Eq. (18), we obtain

$$\hat{\rho}_k^A := \mathrm{Tr}_B\left[\hat{\rho}_k^{AB}\right] = \frac{\hat{1}^A + z_k\hat{\sigma}_z^A}{2}, \tag{21}$$

where $z_k := \pm\mathrm{Re}(b_k)$.

The fidelity F_k of the final state is given by $F_k = \langle\Phi^+|\hat{\tau}_k^{AB}|\Phi^+\rangle = \langle\Phi_k'^+|\Lambda_A(\hat{\rho}_k^{AB})|\Phi_k'^+\rangle$. Since $\{|x_k^j\rangle_A\}_{j=0,1}$ is an eigenbasis of $\hat{\sigma}_z^A$, we have $\hat{\sigma}_z^A|\Phi_k'^+\rangle = \pm|\Phi_k'^-\rangle$, which means $F_k = f\langle\Phi_k'^+|\hat{\rho}_k^{AB}|\Phi_k'^+\rangle + (1-f)\langle\Phi_k'^-|\hat{\rho}_k^{AB}|\Phi_k'^-\rangle$. From Eqs. (18) and (11), the fidelity F_k is rewritten as

$$F_k = \tfrac{1}{2}(1 + |\langle v_1|v_0\rangle|a_k). \tag{22}$$

Combining this equation, Eq. (19), and the definition of z_k, we have

$$\left(\frac{2F_k-1}{|\langle v_1|v_0\rangle|}\right)^2+z_k^2\leqslant 1. \tag{23}$$

Let us consider the success probability of the protocol. Suppose that Bob's failure measurement returns a state $\hat{\rho}_f^{AB}$ with probability $1-P_s$. Since Alice does nothing until the end of Bob's generalized measurement, Alice's averaged density operator is unchanged through the measurement, that is,

$$\hat{\psi}'^A=P_s\hat{\rho}_s^A+(1-P_s)\hat{\rho_f}^A, \tag{24}$$

where $\hat{\psi}'^A:=\mathrm{Tr}_b[|\psi'\rangle\langle\psi'|_{Ab}]$, $\hat{\rho}_s^A:=(\sum_k p_k\hat{\rho}_k^A)/P_s$ and $\hat{\rho_f}^A:=\mathrm{Tr}_B[\hat{\rho_f}^{AB}]$. Equation (13) indicates that $\hat{\psi}'^A$ is in the form of

$$\hat{\psi}'^A=\frac{\hat{1}^A+x_0\hat{\sigma}_x^A+y_0\hat{\sigma}_y^A+z_0\hat{\sigma}_z^A}{2}, \tag{25}$$

where $\hat{\sigma}_x^A:=|0\rangle\langle 1|_A+|1\rangle\langle 0|_A$, $\hat{\sigma}_y^A:=-i|0\rangle\langle 1|_A+i|1\rangle\langle 0|_A$ and x_0, y_0, and z_0 satisfy

$$\begin{aligned} z_0&=q_0-q_1,\\ x_0^2+y_0^2&=4q_0q_1|\langle u_1|u_0\rangle|^2=\left(1-z_0^2\right)|\langle u_1|u_0\rangle|^2. \end{aligned} \tag{26}$$

On the other hand, $\hat{\rho}_s^A$ is written as

$$\hat{\rho}_s^A=\frac{1}{P_s}\sum_k p_k\hat{\rho}_k^A=\frac{\hat{1}+z_s\hat{\sigma}_z^A}{2}, \tag{27}$$

where $z_s:=(\sum_k p_kz_k)/P_s$, and it satisfies

$$\left(\frac{2F-1}{|\langle v_1|v_0\rangle|}\right)^2+z_s^2\leqslant 1 \tag{28}$$

from Eq. (23) and the convexity of function x^2. Note that this inequality implies

$$F\leqslant\frac{1+|\langle v_1|v_0\rangle|}{2}=\frac{1+|\langle u_1|u_0\rangle|^{\frac{1-T}{T}}}{2}, \tag{29}$$

where we used Eq. (9). We also decompose $\hat{\rho}_f^A$ as

$$\hat{\rho}_f^A=\frac{\hat{1}^A+x_f\hat{\sigma}_x^A+y_f\hat{\sigma}_y^A+z_f\hat{\sigma}_z^A}{2} \tag{30}$$

with real numbers x_f, y_f, z_f satisfying

$$x_f^2+y_f^2+z_f^2\leqslant 1. \tag{31}$$

From Eq. (24), we have

$$\begin{aligned} x_0&=(1-P_s)x_f,\\ y_0&=(1-P_s)y_f,\\ z_0&=P_sz_s+(1-P_s)z_f. \end{aligned} \tag{32}$$

From these equations, Eqs. (26) and (31), we obtain

$$\begin{aligned} g(P_s):=&P_s^2\left(1-z_s^2\right)-2P_s(1-z_0z_s)\\ &+(1-|\langle u_1|u_0\rangle|^2)\left(1-z_0^2\right)\geqslant 0, \end{aligned} \tag{33}$$

or, equivalently, we have

$$\begin{aligned} &[(1-|\langle u_1|u_0\rangle|^2)z_0-P_sz_s]^2\\ &\leqslant\left[1-\left(1-z_s^2\right)|\langle u_1|u_0\rangle|^2\right]\left(P_s-\frac{1-|\langle u_1|u_0\rangle|^2}{1-|\langle u_1|u_0\rangle|\sqrt{1-z_s^2}}\right)\\ &\quad\times\left(P_s-\frac{1-|\langle u_1|u_0\rangle|^2}{1+|\langle u_1|u_0\rangle|\sqrt{1-z_s^2}}\right). \end{aligned} \tag{34}$$

Since $z_0^2<1$ and $0<|\langle u_1|u_0\rangle|<1$, we have

$$\begin{aligned} g(1-|\langle u_1|u_0\rangle|^2)=&-(1-|\langle u_1|u_0\rangle|^2)\left[\left(1-z_s^2\right)|\langle u_1|u_0\rangle|^2\right.\\ &\left.+(z_0-z_s)^2\right]<0, \end{aligned} \tag{35}$$

and

$$g(1)=-\left(1-z_0^2\right)|\langle u_1|u_0\rangle|^2-(z_0-z_s)^2<0, \tag{36}$$

which means $g(P_s)<0$ for $P_s\geqslant 1-|\langle u_1|u_0\rangle|^2$ because $g(P_s)$ is linear or convex. Thus, Eq. (33) implies

$$P_s<1-|\langle u_1|u_0\rangle|^2. \tag{37}$$

To satisfy inequality (34), the right-hand side of the inequality should be nonnegative, which occurs only when

$$P_s\leqslant\frac{1-|\langle u_1|u_0\rangle|^2}{1+|\langle u_1|u_0\rangle|\sqrt{1-z_s^2}} \tag{38}$$

under the condition of Eq. (37). Combining Eq. (28), we have

$$P_s\leqslant\frac{1-|\langle u_1|u_0\rangle|^2}{1+|\langle u_1|u_0\rangle|\left(\frac{2F-1}{|\langle v_1|v_0\rangle|}\right)}, \tag{39}$$

which can be rewritten as

$$\begin{aligned} P_sF&\leqslant\frac{1}{2}\left(1-\frac{|\langle v_1|v_0\rangle|}{|\langle u_1|u_0\rangle|}\right)P_s\\ &\quad+\frac{1}{2}(1-|\langle u_1|u_0\rangle|^2)\frac{|\langle v_1|v_0\rangle|}{|\langle u_1|u_0\rangle|} \end{aligned} \tag{40}$$

$$\begin{aligned} &=\frac{1}{2}\left(1-|\langle u_1|u_0\rangle|^{\frac{1-2T}{T}}\right)P_s\\ &\quad+\frac{1}{2}(1-|\langle u_1|u_0\rangle|^2)|\langle u_1|u_0\rangle|^{\frac{1-2T}{T}}, \end{aligned} \tag{41}$$

where we used Eq. (9).

Since Eqs. (6), (29), and (41) must be satisfied at the same time, the performance (P_s, P_sF) of an arbitrary protocol must be in the triangle with the apexes X_0, X_1, and

$$X_3:=\left(1-|\langle u_1|u_0\rangle|^2,\tfrac{1}{2}(1-|\langle u_1|u_0\rangle|^2)\right), \tag{42}$$

which is included in the triangle $X_0X_1X_2$. This completes the proof.

IV. SIMULATABILITY OF AN ARBITRARY PROTOCOL VIA SYMMETRIC PROTOCOLS

Here we show that the performance of an arbitrary protocol, which is in the triangle defined by Eq. (14) with fixed T and $|\langle u_1|u_0\rangle|$, is simulatable by utilizing a protocol in Ref. [19]. In the protocol in Ref. [19], Alice starts with preparing system A in a symmetric state $|\phi\rangle_A=(|0\rangle_A+|1\rangle_A)/\sqrt{2}$, and, upon receiving pulses from Alice, Bob carries out a measurement that is composed of a simple combination of linear optical

elements and photon-number-resolving detectors. Let us call it symmetric protocol in what follows. With a proper choice of the intensity of pulse a, the symmetric protocol can achieve (P_s, P_sF) with

$$\begin{aligned} P_s &= 1-u, \\ F &= \frac{1+u^{\frac{1-T}{T}}}{2}, \end{aligned} \tag{43}$$

for any u with $0 < u \leqslant 1$ [19]. This indicates that the symmetric protocol can achieve performance $(P_s, P_sF) = X_0$ by choosing $u = 1$ and performance $(P_s, P_sF) = X_1$ by choosing $u = |\langle u_1|u_0\rangle|$. On the other hand, performance $(P_s, P_sF) = X_2$ is also achievable by a trivial protocol in which Alice and Bob prepare their memories in state $|00\rangle_{AB}$ and declare success all the time. The achievability of points X_0, X_1, and X_2 indicates that all the points in the triangle $X_0X_1X_2$ are achievable by mixing. Since this fact holds for any $|\langle u_1|u_0\rangle|$, we conclude that, for given T, the performance of an arbitrary protocol is simulatable by combining symmetric protocols and the trivial protocol.

V. OPTIMAL PERFORMANCE OF SINGLE-ERROR-TYPE ENTANGLEMENT GENERATION

Here we calculate the optimal performance of the mixture of arbitrary single-error-type entanglement generation protocols for given T. As shown in the preceding section, for any T, the performance (P_s, P_sF) of an arbitrary protocol is achievable by mixing symmetric protocols and the trivial protocol. Since the performance achieved by a symmetric protocol or the trivial protocol can be described by a point $(P_s, P_sF) = \mathbf{(}P_s, P_sF^{\mathrm{sym}}(P_s)\mathbf{)}$ with

$$F^{\mathrm{sym}}(P_s) := \frac{1+(1-P_s)^{\frac{1-T}{T}}}{2}, \quad (0 \leqslant P_s \leqslant 1), \tag{44}$$

the performance of the mixture of arbitrary protocols must be in the convex hull of the region $\mathcal{S} := \{(P_s, P_sF) \mid 0 \leqslant P_s \leqslant 1,\ 1/2 \leqslant F \leqslant F^{\mathrm{sym}}(P_s)\}$. In what follows, we show that the convex hull, $\mathrm{Conv}(\mathcal{S})$, is given by the region $\mathcal{C}_{\mathcal{S}} := \{(P_s, P_sF) \mid 0 \leqslant P_s \leqslant 1,\ 1/2 \leqslant F \leqslant F^{\mathrm{opt}}(P_s)\}$ with $F^{\mathrm{opt}}(P_s)$ defined by

$$F^{\mathrm{opt}}(P_s) := \begin{cases} \frac{1+(1-P_s)^{\frac{1-T}{T}}}{2} & \left(P_s \leqslant \frac{T}{1-T}\right), \\ \frac{1}{2} + \frac{1-P_s}{2P_s}\frac{T}{1-2T}\left(\frac{1-2T}{1-T}\right)^{\frac{1-T}{T}} & \left(P_s > \frac{T}{1-T}\right). \end{cases} \tag{45}$$

Note that $P_s > T/(1-T)$ holds only when $T < 1/2$. The tight upper bound $F^{\mathrm{opt}}(P_s)$ is depicted in Fig. 3.

Let us proceed to the proof of $\mathcal{C}_{\mathcal{S}} = \mathrm{Conv}(\mathcal{S})$. From Eq. (44), we have

$$\frac{\mathrm{d}P_sF^{\mathrm{sym}}(P_s)}{\mathrm{d}P_s} = \frac{1}{2}\left[1+\left(1-\frac{P_s}{T}\right)(1-P_s)^{\frac{1-2T}{T}}\right], \tag{46}$$

$$\frac{\mathrm{d}^2P_sF^{\mathrm{sym}}(P_s)}{\mathrm{d}{P_s}^2} = \frac{1}{2}\frac{1-T}{T}\left(\frac{P_s}{T}-2\right)(1-P_s)^{\frac{1-3T}{T}}. \tag{47}$$

The latter equation indicates

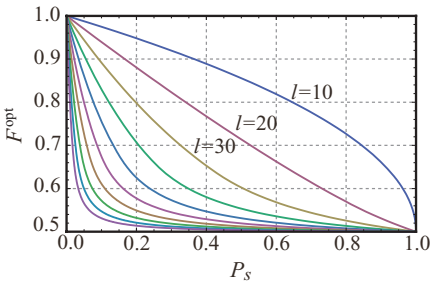

FIG. 3. (Color online) The optimal performances of single-error-type entanglement generation for $10 \leqslant l \leqslant 100$ km at intervals of 10 km, where we assume $T = e^{-l/l_0}$ and $l_0 = 25$ km (corresponding to ~0.17 dB/km attenuation).

$$\begin{aligned} \frac{\mathrm{d}^2P_sF^{\mathrm{sym}}(P_s)}{\mathrm{d}{P_s}^2} &> 0 \quad (P_s > 2T), \\ \frac{\mathrm{d}^2P_sF^{\mathrm{sym}}(P_s)}{\mathrm{d}{P_s}^2} &\leqslant 0 \quad (P_s \leqslant 2T). \end{aligned} \tag{48}$$

(a) $T \geqslant 1/2$. In this case, $F^{\mathrm{opt}}(P_s) = F^{\mathrm{sym}}(P_s)$, and hence $\mathcal{S} = \mathcal{C}_{\mathcal{S}}$. In addition, Eq. (48) indicates that $P_sF^{\mathrm{sym}}(P_s)$ is concave for $0 \leqslant P_s \leqslant 1$. These facts imply that $\mathrm{Conv}(\mathcal{S})$ is equivalent to $\mathcal{S}$, namely, to $\mathcal{C}_{\mathcal{S}}$.

(b) $T < 1/2$. Let P_s^* be $P_s^* := T/(1-T)$. The proof begins with noting the following facts: (i) $F^{\mathrm{opt}}(P_s) = F^{\mathrm{sym}}(P_s)$ for $0 \leqslant P_s < P_s^*$; (ii) $F^{\mathrm{opt}}(P_s^*) = F^{\mathrm{sym}}(P_s^*)$; (iii) $F^{\mathrm{opt}}(1) = F^{\mathrm{sym}}(1)$; (iv) $P_sF^{\mathrm{opt}}(P_s)$ and $[\mathrm{d}P_sF^{\mathrm{opt}}(P_s)]/(\mathrm{d}P_s)$ are continuous at $P_s = P_s^*$;

$$\text{(v)}\quad \frac{\mathrm{d}^2P_sF^{\mathrm{opt}}(P_s)}{\mathrm{d}{P_s}^2}\begin{cases} < 0, & (0 \leqslant P_s < P_s^*), \\ = 0, & (P_s^* < P_s); \end{cases} \tag{49}$$

(vi) $F^{\mathrm{opt}}(P_s) > F^{\mathrm{sym}}(P_s)$ for $P_s^* < P_s < 1$. Facts (i)–(v) are easily confirmed from Eqs. (44)–(45). Fact (vi) is proven by facts (ii)–(iii),

$$\frac{\mathrm{d}P_sF^{\mathrm{opt}}(P_s^*)}{\mathrm{d}P_s} = \frac{\mathrm{d}P_sF^{\mathrm{sym}}(P_s^*)}{\mathrm{d}P_s}, \tag{50}$$

and by Eqs. (48)–(49). Facts (iv)–(v) show that $\mathcal{C}_{\mathcal{S}}$ is convex. Facts (i)–(iii) and (vi) imply $\mathcal{S} \subset \mathcal{C}_{\mathcal{S}}$. From facts (i)–(v), we have $\mathcal{C}_{\mathcal{S}} \subset \mathrm{Conv}(\mathcal{S})$. Therefore, we conclude $\mathrm{Conv}(\mathcal{S}) = \mathcal{C}_{\mathcal{S}}$.

VI. SUMMARY

In conclusion, we have provided the tight upper bound on the performances of protocols that generate entanglement with only one type of error by transmitting pulses in coherent states through a lossy channel. As represented by Eq. (45), the tight upper bound is stated in terms of the success probability P_s and the average singlet fraction F of generated entanglement and is determined only by the transmittance T of the channel. In addition, we have shown that the upper bound is achievable without large-scale quantum operations, namely, by utilizing a simple protocol [19] composed of linear optical elements and photon-number-resolving detectors.

The method enabling us to derive such a general bound can be summarized as follows. The proof begins with replacing the real protocol in Fig. 1 by an equivalent (virtual) protocol

in Fig. 2. Thanks to the replacement, the effect of the optical loss in the practical channel is reduced to a *local* phase-flip channel acting on Alice's memory, and the quality of final entanglement is bounded by the form of the local density operator of the memory A fed to the phase-flip channel [see Eqs. (21) and (23)]. Since the local density operator can only be altered by Bob remotely at the expense of a failure probability, we are led to Eq. (24) relating the change in Alice's local density operator and the success probability. This relation enables us to derive a trade-off relation, Eq. (41), between the success probability P_s and the average singlet fraction F, which leads to the tight upper bound of arbitrary protocols.

Throughout this article, we have focused on the entanglement generation protocols with only one type of error, based on the fact that the known simple distillation protocols and swapping protocols work more efficiently against such a restricted type of errors. In addition, since the efficiencies of the entanglement distillation protocols and swapping protocols for the single-error-type entanglement are usually characterized by the singlet fraction, we have adopted a specific set of measures, the total probability P_s and the singlet fraction F. In order to treat the entanglement generation protocols separately from distillation protocols and swapping protocols, we have considered the average of the singlet fractions, which has an operational meaning of treating all the success events in the same manner in the subsequent steps of distillation and swapping. If we look into the properties of the distillation protocols in more detail, there is a possibility that accepting multiple types of errors for higher success probability in the generation protocol could lead to a better result if there exists a distillation protocol with a lesser penalty on the multiple types of errors. It is also better to postpone the averaging until the end of the whole protocol. Pursuing such possibilities is important for implementation of quantum repeaters and is also interesting in connection with the fundamental question of what is the best way of distributing entanglement against an optical loss in the channel. We expect that the methods introduced here may be also useful in solving such general problems in the search for good entanglement generation protocols in hybrid quantum repeaters.

ACKNOWLEDGMENTS

We would like to thank Şahin Kaya Özdemir, Ryo Namiki, Takashi Yamamoto, and Hitoshi Takeda for valuable discussions. We acknowledge the support of a MEXT Grant-in-Aid for Scientific Research on Innovative Areas, No. 21102008 and No. 20104003; a MEXT Grant-in-Aid for the Global COE Program; and a JSPS Grant-in-Aid for Scientific Research (C), No. 20540389. K.A. is supported by JSPS.

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] L. K. Grover, e-print arXiv:quant-ph/9704012.
[4] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[5] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[7] B. Zhao, Z.-B. Chen, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, Phys. Rev. Lett. **98**, 240502 (2007).
[8] Z.-B. Chen, B. Zhao, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, Phys. Rev. A **76**, 022329 (2007).
[9] L. Jiang, J. M. Taylor, and M. D. Lukin, Phys. Rev. A **76**, 012301 (2007).
[10] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **98**, 190503 (2007).
[11] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, Phys. Rev. A **76**, 050301(R) (2007).
[12] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).
[13] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. A **72**, 052330 (2005).
[14] N. Sangouard, R. Dubessy, and C. Simon, Phys. Rev. A **79**, 042340 (2009).
[15] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).
[16] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New J. Phys. **8**, 184 (2006).
[17] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).
[18] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, Phys. Rev. Lett. **101**, 040502 (2008).
[19] K. Azuma, N. Sota, R. Namiki, Ş. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **80**, 060303(R) (2009).
[20] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[21] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[22] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[23] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[24] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn, New J. Phys. **8**, 30 (2006).