Optimal supplier of single-error-type entanglement via coherent-state transmission

Koji Azuma,[1,2,*] Nobuyuki Imoto,[3,4] and Masato Koashi[5]

[1] *NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[2] *NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[3] *Institute for Photon Science and Technology, School of Science, University of Tokyo, Tokyo 113-0033, Japan*
[4] *Center for Quantum Information and Quantum Biology, Osaka University, Osaka 560-8531, Japan*
[5] *Photon Science Center, University of Tokyo, Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

(Received 31 March 2022; accepted 27 May 2022; published 21 June 2022)

Compared with entanglement with multiple types of noise, entanglement including only one type of error is a favorable fundamental resource not only for quantum communication but also for distributed quantum computation. We consider protocols that present single-error-type entanglement for distant qubits via coherent-state transmission over a lossy channel. Such a protocol is regarded as a subroutine to serve entanglement for larger protocol to yield a final output, such as ebits or pbits. In this paper, we provide a subroutine protocol which achieves the *global* optimal for typical jointly convex yield functions monotonically nondecreasing with respect to the singlet fraction, such as an arbitrary convex function of a singlet fraction, two-way distillable entanglement, and two-way distillable key. Entanglement generation based on remote nondestructive parity measurement protocol [K. Azuma *et al.*, Phys. Rev. A **85**, 062309 (2012)] is identified as such an optimal subroutine.

DOI: 10.1103/PhysRevA.105.062432

I. INTRODUCTION

Generating entanglement between distant qubits is a fundamental building block not only for quantum communication but also for distributed quantum computation. In quantum key distribution (QKD), private bits (pbits) are distilled from the (virtually) generated entangled states through error correction and privacy amplification [1–5], while Bell pairs (ebits) are through entanglement distillation [6–8] for more general scenarios such as quantum teleportation [9] and controlled-not operations [10–12] for spatially distant qubits and chips in distributed fault-tolerant quantum computation [13–18]. If entanglement generation protocol is run in parallel between nearest-neighboring nodes in a quantum network, ebits and pbits are served for arbitrary clients in the network efficiently [19–21], through aggregation [21] of quantum repeaters [19,20] with entanglement distillation and entanglement swapping [22]. Therefore, entanglement generation protocol is regarded in general as a subroutine to serve entanglement for larger protocol to yield a final output, such as ebits or pbits.

Entanglement generation protocol is normally based on transmission of flying bosonic systems, such as photons, over a communication channel, such as an optical fiber, a mode in free space, or a microwave transmission line. The dominant noise in the channel is the photon loss. Recently, excellent upper bounds on the two-way quantum and private capacities of a point-to-point pure-loss bosonic channel are derived [23,24] (indeed, one of which, now called PLOB bound [24], coincides with the capacities). These bounds show that there is no gap in the rate-loss scaling between the upper bounds and the rates of existing point-to-point entanglement generation protocols [25–30] or QKD protocols [31–40] based on the transmission of polarized (or time-bin) single-photon states, Fock states, and coherent states (or cat states) over a pure-loss channel. Entanglement generation protocols [41–43] and QKD protocols [44–57] working with an intermediate node between communicators also have the same rate-loss scaling with upper bounds [21,58–60] on the quantum and private capacities of the corresponding quantum network. Besides, if such an entanglement generation protocol, which can provide ebits with the same rate-loss scaling as the upper bounds for a point-to-point pure-loss channel (by being combined with optimal entanglement distillation if necessary), is adopted in the aggregated quantum repeater protocol [21], its rate-loss scaling essentially has no gap with that given by the quantum and private capacity of a pure-loss bosonic channel network [21,59,60], irrespective of its topology (see, e.g., a review article [61] for detail). These facts suggest that there is not much room to improve further existing entanglement generation protocols in terms of scaling. In other words, it is rather important in practice to design a protocol by considering a balance between easiness of the implementation and its specific performance.

Especially, a protocol based on coherent-state encoding is an example of protocol with such a good balance. In B92 QKD protocol [35,37,38], a bit is encoded into phases of a coherent state, and it is sent from a sender, Alice, to a receiver, Bob, directly through an optical channel. In the twin-field

[*] koji.azuma.ez@hco.ntt.co.jp

(TF) QKD protocol [47–54], Alice and Bob send coherent states with information of bits to an intermediate node, called Claire, which is supposed to perform a Bell measurement based on single-photon interference. Entanglement generation protocol [25–28,30,42,43,62] is also based on coherent-state encoding to generate entanglement between Alice's qubit and Bob's qubit, as such an encoding can be established through a dispersive Jaynes-Cummings Hamiltonian between a coherent state and a matter qubit, such as a superconducting qubit, a quantum dot, a single ion, a nitrogen-vacancy center in a diamond, or a single atom. Therefore, protocols based on coherent-state encoding constitute an important category as practical entanglement generation and QKD.

In this paper, we consider protocols that present entanglement with only one type of error (such as a phase error) for distant qubits via coherent-state transmission over a lossy channel, as well as local operations and classical communication (LOCC). On regarding this as a subroutine to serve single-error-type entanglement for larger protocol to yield a final output, we identify a protocol which achieves the *global* optimal for typical jointly convex yield functions monotonically nondecreasing with respect to the singlet fraction [63], such as an arbitrary convex function of a singlet fraction, two-way distillable entanglement, and two-way distillable key. In particular, entanglement generation protocol based on remote nondestructive parity measurement (RNPM) protocol [27,43] is identified as such an optimal subroutine.

This paper is organized as follows. In Sec. II, we define the yield function for single-error-type entanglement and show its several properties. We consider point-to-point protocol in Sec. III and three-party protocol working with the help of an intermediate node in Sec. IV. Section V concludes this paper.

II. SINGLE-ERROR-TYPE ENTANGLEMENT AND THE YIELD BASED ON IT

In this paper, we consider entanglement generation protocols which provide single-error-type entanglement $\hat{\tau}^{AB}$ for distant qubits A and B, i.e., a state in the Hilbert subspace spanned by two orthogonal Bell states, with the free use of LOCC. Since two orthogonal Bell states can be transformed into $|\Phi^+\rangle_{AB} := (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$ and $|\Phi^-\rangle_{AB} := (|00\rangle_{AB} - |11\rangle_{AB})/\sqrt{2}$ via a local unitary operation [7], we can assume that the state is described as

$$\hat{\tau}^{AB}(\zeta,\chi,\upsilon) = \frac{1+\zeta}{2}|\Phi^+\rangle\langle\Phi^+|_{AB} + \frac{1-\zeta}{2}|\Phi^-\rangle\langle\Phi^-|_{AB} + \frac{\chi - i\upsilon}{2}|\Phi^+\rangle\langle\Phi^-|_{AB} + \frac{\chi + i\upsilon}{2}|\Phi^-\rangle\langle\Phi^+|_{AB} \tag{1}$$

with three real parameters ζ, χ, and υ satisfying $\zeta^2 + \chi^2 + \upsilon^2 \leqslant 1$. By noting that $\hat{X}^A \otimes \hat{X}^B|\Phi^{\pm}\rangle_{AB} = \pm|\Phi^{\pm}\rangle_{AB}$ and $\hat{Z}^A|\Phi^+\rangle_{AB} = |\Phi^-\rangle_{AB}$ and that the application of a unitary operation $e^{-i\theta\hat{Z}^A/2}$ is closed in the Hilbert subspace spanned by $\{|\Phi^{\pm}\rangle_{AB}\}$, where $\hat{X}^A := |0\rangle\langle 1|_A + |1\rangle\langle 0|_A$ and $\hat{Z}^A := |0\rangle\langle 0|_A - |1\rangle\langle 1|_A$, the state $\hat{\tau}^{AB}$ can always be transformed into a standard form

$$\begin{aligned}\hat{\gamma}^{AB}(z,x) &:= \frac{1+z}{2}|\Phi^+\rangle\langle\Phi^+|_{AB} + \frac{1-z}{2}|\Phi^-\rangle\langle\Phi^-|_{AB} + \frac{x}{2}(|\Phi^+\rangle\langle\Phi^-|_{AB} + |\Phi^-\rangle\langle\Phi^+|_{AB})\\ &= \frac{1+x}{2}|00\rangle\langle 00|_{AB} + \frac{1-x}{2}|11\rangle\langle 11|_{AB} + \frac{z}{2}(|00\rangle\langle 11|_{AB} + |11\rangle\langle 00|_{AB}),\end{aligned} \tag{2}$$

via a local unitary operation, where

$$x = |\chi|, \quad z = \sqrt{\zeta^2 + \upsilon^2} \tag{3}$$

are non-negative parameters satisfying $x^2 + z^2 \leqslant 1$. Note that z is related with the *singlet fraction* F of $\hat{\tau}^{AB}$ [64], defined by $F := \max_{\hat{U}^A \otimes \hat{V}^B} {}_{AB}\langle\Phi^+|(\hat{U}^A \otimes \hat{V}^B)\hat{\tau}^{AB}(\hat{U}^{A\dagger} \otimes \hat{V}^{B\dagger})|\Phi^+\rangle_{AB}$ with unitary operators $\hat{U}^A$ and $\hat{V}^B$, as

$$z = 2F - 1. \tag{4}$$

This implies that any single-error-type state $\hat{\tau}^{AB}$ whose standard form $\hat{\gamma}^{AB}(z,x)$ has nonzero z is entangled, which can thus be called a single-error-type entangled state.

We consider a scenario where a single-error-type entangled state $\hat{\tau}^{AB}$ generated through an entanglement generation protocol can be used as an input for a subsequent protocol such as entanglement distillation, secret-key distillation, entanglement swapping [22], or their combination. In particular, we assume that the subsequent protocol accepts only the standard form $\hat{\gamma}^{AB}(z,x)$ and its yield Y is a function of z and x, i.e., $Y = Y(\hat{\gamma}^{AB}(z,x)) = Y(z,x)$. Using the yield function $Y(z,x)$ of a subsequent protocol as a reference, we may define a measure of entanglement in general single-error-type state $\hat{\tau}^{AB}(\zeta,\chi,\upsilon)$, which we also denote by Y as $Y = Y(\hat{\tau}^{AB}(\zeta,\chi,\upsilon)) = Y(\sqrt{\zeta^2+\upsilon^2}, |\chi|)$.

For $Y(\hat{\tau}^{AB})$ to be a proper measure, the yield function $Y(z,x)$ must satisfy several properties as follows. Since $Y(\hat{\tau}^{AB})$ should be zero for any separable state $\hat{\tau}^{AB}$, the yield Y is zero for separable states $\hat{\gamma}^{AB}(0,x)$, i.e.,

$$Y(0,x) = 0. \tag{5}$$

From the monotonicity of $Y(\hat{\tau}^{AB})$ under LOCC as an entanglement measure, if Alice and Bob can deterministically convert a state $\hat{\gamma}^{AB}(z,x)$ to another state $\hat{\gamma}^{AB}(z',x')$ by LOCC, entanglement in $\hat{\gamma}^{AB}(z,x)$ is no smaller than that in $\hat{\gamma}^{AB}(z',x')$, namely,

$$Y(z,x) \geqslant Y(z',x'). \tag{6}$$

For example, if Alice inputs a qubit pair AB in a state $\hat{\gamma}^{AB}(z,x)$ into a phase-flip channel

$$\Lambda_v^A(\hat{\rho}) := \frac{1+v}{2}\hat{\rho} + \frac{1-v}{2}\hat{Z}^A\hat{\rho}\hat{Z}^A \tag{7}$$

with $0 \leqslant v \leqslant 1$, the state of the qubit pair becomes $\hat{\gamma}^{AB}(vz,x)$ and, thus,

$$Y(z,x) \geqslant Y(vz,x), \tag{8}$$

implying monotonically nondecreasing of $Y(z,x)$ with respect to z. Similarly, since Alice and Bob can convert state $\hat{\gamma}^{AB}(z,x)$

into state $\hat{\gamma}^{AB}(z, \upsilon x)$ by inputting the qubit pair into a channel

$$\mathcal{E}_{\upsilon}^{AB}(\hat{\rho}) := \frac{1+\upsilon}{2}\hat{\rho} + \frac{1-\upsilon}{2}(\hat{X}^A \otimes \hat{X}^B)\hat{\rho}(\hat{X}^A \otimes \hat{X}^B) \quad (9)$$

with $0 \leqslant \upsilon \leqslant 1$, we have

$$Y(z, x) \geqslant Y(z, \upsilon x), \quad (10)$$

implying monotonically nondecreasing of $Y(z, x)$ over x.

In this paper, we impose two assumptions on the function $Y(z, x)$. That is to say, the results derived in the subsequent sections are true for any yield function $Y(z, x)$ as long as it satisfies those assumptions. The first assumption is that $Y(z, x)$ is a jointly convex function. This means that Y is also a convex function over single-error-type states $\hat{\tau}^{AB}(\zeta, \chi, \upsilon)$, which can be seen as follows. Consider a convex mixture of a single-error-type state $\hat{\tau}^{AB}(\zeta', \chi', \upsilon')$ and a single-error-type state $\hat{\tau}^{AB}(\zeta'', \chi'', \upsilon'')$ and denote it by a single-error-type state $\hat{\tau}^{AB}(\zeta, \chi, \upsilon)$. Then,

$$(\zeta, \chi, \upsilon) = p(\zeta', \chi', \upsilon') + (1-p)(\zeta'', \chi'', \upsilon'') \quad (11)$$

holds for $0 \leqslant p \leqslant 1$. The measure for the mixture $\hat{\tau}^{AB}(\zeta, \chi, \upsilon)$ then satisfies

$$\begin{aligned} Y(\hat{\tau}^{AB}(\zeta, \chi, \upsilon)) &= Y(\sqrt{\zeta^2+\upsilon^2}, |\chi|) \leqslant Y(p\sqrt{\zeta'^2+\upsilon'^2} \\ &\quad + (1-p)\sqrt{\zeta''^2+\upsilon''^2}, p|\chi'| + (1-p)|\chi''|) \\ &\leqslant pY(\sqrt{\zeta'^2+\upsilon'^2}, |\chi'|) \\ &\quad + (1-p)Y(\sqrt{\zeta''^2+\upsilon''^2}, |\chi''|) \\ &= pY(\hat{\tau}^{AB}(\zeta', \chi', \upsilon')) \\ &\quad + (1-p)Y(\hat{\tau}^{AB}(\zeta'', \chi'', \upsilon'')), \end{aligned} \quad (12)$$

where we used the convexity of norms and the monotonicity of Eqs. (8) and (10) to have the first inequality, and we used the joint convexity of the yield $Y(z, x)$ to have the second inequality.

The second assumption we make is an inequality

$$Y(\upsilon z, \sqrt{1-z^2}) \leqslant zY(\upsilon, 0) \quad (13)$$

for any $0 \leqslant \upsilon \leqslant 1$ and $0 \leqslant z \leqslant 1$. The left-hand side of this inequality corresponds to the case where the output of the phase-flip channel Λ_{υ}^{A} with the input of a pure state $\hat{\gamma}^{AB}(z, \sqrt{1-z^2})$ is sent to the subsequent protocol. On the other hand, the right-hand side corresponds to the case where a maximally entangled state $\hat{\gamma}^{AB}(1, 0)$ given with probability z is input to the phase-flip channel Λ_{υ}^{A}, followed by being sent to the subsequent protocol. The inequality (13) requires the latter case to give an average overall yield to be no smaller than the former. Typical yield functions satisfy the inequality (13), as inferred from the following examples.

As an example, let us consider a subsequent protocol whose yield function Y depends only on the singlet fraction of $\hat{\gamma}^{AB}(z, x)$, i.e., $Y(z, x) = Y(z)$ for any x and is convex over z. In this case, the convexity of $Y(z)$ and Eq. (5) implies

$$pY(z) \geqslant Y(pz) \quad (14)$$

for any $0 \leqslant p \leqslant 1$, leading to Eq. (13). For instance, when we execute a quantum repeater protocol composed of single-error-type entanglement generation, the recurrence method [6–8], and the entanglement swapping, it is conventional to start by converting initial entangled states $\hat{\gamma}^{AB}(z, x)$ between neighboring repeater stations into a Bell-diagonal one, $\hat{\gamma}^{AB}(z, 0)$. Then, the yield function of the overall protocol would naturally depend only on the singlet fraction of the initial state, namely, $Y(z)$.

Another example of the yield function having convexity and satisfying Eq. (13) is the distillable entanglement E_{D}. The analytic formula of the distillable entanglement for general mixed states has not yet been found, but it has been derived for maximally correlated states $\hat{\rho}^{AB} := \sum_{i,j} a_{ij}|ii\rangle\langle jj|_{AB}$ [63,65]. The formula is described by

$$E_{\mathrm{D}}(\hat{\rho}^{AB}) = S(\hat{\rho}^{A}) - S(\hat{\rho}^{AB}), \quad (15)$$

where $\hat{\rho}^{A} := \mathrm{Tr}_B[\hat{\rho}^{AB}]$ and S is the von Neumann entropy defined by $S(\hat{\rho}) := -\mathrm{Tr}[\hat{\rho}\, \log_2 \hat{\rho}]$. This quantity coincides with the two-way distillable key, in this case [65–67]. Since the single-error-type entangled states $\hat{\gamma}^{AB}(z, x)$ are examples of the maximally correlated states, the distillable entanglement for $\hat{\gamma}^{AB}(z, x)$ is

$$E_{\mathrm{D}}(\hat{\gamma}^{AB}(z, x)) = h\left(\frac{1+x}{2}\right) - h\left(\frac{1+\sqrt{z^2+x^2}}{2}\right), \quad (16)$$

where h is the binary entropy function $h(x) := -x\, \log_2 x - (1-x)\log_2(1-x)$. A direct calculation shows that E_{D} is convex over (z, x) and also satisfies Eq. (13).

III. TIGHT BOUND ON SINGLE-ERROR-TYPE ENTANGLEMENT GENERATION

In this section, we derive a tight bound on entanglement generation protocols that are based on coherent-state transmission from a sender to a receiver, followed by arbitrary LOCC operations. We start by defining the protocols and their yield as the measure of the performance (Sec. III A). In Sec. III B, instead of considering an LOCC protocol that is generally complex, we consider separable operations and show the requisites for producing single-error-type entanglement. In Sec. III C, we derive an upper bound on the yield that could be given by the separable operations. Finally, in Sec. III D, we show that a protocol of Ref. [27] achieves the upper bound. In Sec. III E, we explicitly show how efficient the optimal protocol is.

A. 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 paper. Suppose that separated parties called Alice and Bob have qubits A and B, respectively, and their goal is to make the qubits AB in a single-error-type entangled state. In general, a protocol is described as follows (Fig. 1): (i) Alice prepares qubit A in her desired state $|\phi\rangle_A = \sum_{j=0,1} \sqrt{q_j} e^{i\Theta_j}|j\rangle_A$ with real parameters Θ_j, $q_j > 0$, 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

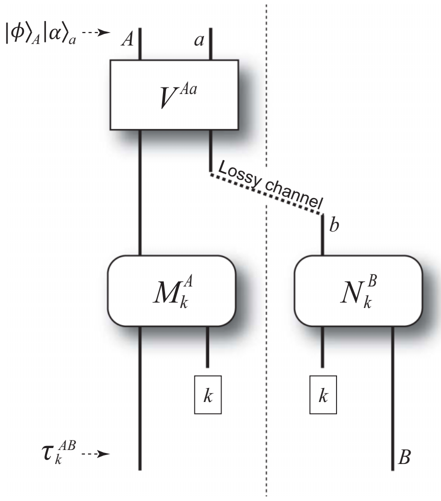

FIG. 1. Scenario of single-error-type entanglement generation. $|\phi\rangle_A := \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j}|j\rangle_A$. An outcome k corresponds to the application of a separable operator $\hat{M}_k^A \otimes \hat{N}_k^B$. If the final entanglement $\hat{\tau}_k^{AB}$ includes only one type of error, Alice and Bob may declare the success of the protocol.

operation $\hat{V}^{Aa}$ defined by

$$\hat{V}^{Aa}|0\rangle_A|\alpha\rangle_a = |0\rangle_A|\alpha_0\rangle_a,$$
$$\hat{V}^{Aa}|1\rangle_A|\alpha\rangle_a = |1\rangle_A|\alpha_1\rangle_a, \tag{17}$$

where the possible output states $\{|\alpha_j\rangle_a\}_{j=0,1}$ are also coherent states. (ii) Alice sends the pulse a to Bob, through a lossy channel described by an isometry

$$\hat{L}^{a\to bE}|\alpha\rangle_a = |\sqrt{T}\alpha\rangle_b|\sqrt{1-T}\alpha\rangle_E, \tag{18}$$

where $0 < T < 1$ is the transmittance of the channel and system E is the environment. At this point, Alice and Bob share a quantum state described by

$$|\psi\rangle_{AbE} = \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j}|j\rangle_A|\sqrt{T}\alpha_j\rangle_b|\sqrt{1-T}\alpha_j\rangle_E. \tag{19}$$

(iii) Alice and Bob manipulate system Ab through LOCC, and may declare outcome k with probability p_k to herald the success of the generation of qubits AB in a single-error-type entangled state $\hat{\tau}_k^{AB}$. The correction of the success events k is denoted by $\mathcal{S}$. We assume that for successful events with $k \in \mathcal{S}$, the state $\hat{\tau}_k^{AB}$ is given by the standard form in Eq. (2), namely,

$$\hat{\tau}_k^{AB} = \hat{\gamma}^{AB}(z_k, x_k) \tag{20}$$

with $z_k > 0$ and $x_k \geqslant 0$.

Let us define a method for evaluating single-error-type entanglement generation protocols. Typically, following such an entanglement generation, a subsequent protocol that works with the obtained entanglement $\hat{\tau}_k^{AB}$, such as entanglement distillation, secret-key distillation, or entanglement swapping [22], is executed. This implies that the value of the entanglement generation cannot be determined by itself, namely, it depends on the protocol to be performed after the entanglement generation. In this paper, using the yield function Y defined in Sec. II, the performance of the overall protocol is evaluated by the average overall yield $\bar{Y}$, which is defined by

$$\bar{Y} := \sum_{k\in\mathcal{S}} p_k Y\left(\hat{\tau}_k^{AB}\right) = \sum_{k\in\mathcal{S}} p_k Y(\hat{\gamma}^{AB}(z_k, x_k))$$
$$= \sum_{k\in\mathcal{S}} p_k Y(z_k, x_k). \tag{21}$$

B. Requisites for separable operations

We start by considering the description of the LOCC in step (iii) of the protocol in Sec. III A. In general, it is known that any LOCC operation can be described by a separable operation $\{\hat{M}_\kappa^A \otimes \hat{N}_\kappa^B\}$ (although the converse is not true, that is, there are separable operations [68–71] that are not implementable by LOCC). Here κ stands for the record of all the communication between Alice and Bob. The definition of the protocol in Sec. III A allows the possibility of discarding part of the record, in which case the output state $\hat{\tau}_k^{AB}$ in step (iii) is a probabilistic mixture $\sum_\kappa q_{\kappa|k}\hat{\rho}_\kappa^{AB}$ over the output states $\{\hat{\rho}_\kappa^{AB}\}_\kappa$ for various values of κ. Since $\hat{\tau}_k^{AB}$ is a single-error-type state in the form of Eq. (1), all the states $\{\hat{\rho}_\kappa^{AB}\}_\kappa$ should also be such single-error-type states. Then, due to the assumed convexity of the yield function Y in Eq. (12), the optimum value of the average overall yield $\bar{Y}$ is always achieved by maintaining all the record. Hence, we here assume that the state $\hat{\tau}_k^{AB}$ obtained in step (iii) is written by a single term as

$$\hat{\tau}_k^{AB} = \frac{1}{p_k}\left(\hat{M}_k^A \otimes \hat{N}_k^B\right)\mathrm{Tr}_E(|\psi\rangle\langle\psi|_{AbE})\left(\hat{M}_k^A \otimes \hat{N}_k^B\right)^\dagger \tag{22}$$

with separable operators $\{\hat{M}_k^A \otimes \hat{N}_k^B\}$ satisfying

$$\sum_{k\in\mathcal{S}} \hat{M}_k^{A\dagger}\hat{M}_k^A \otimes \hat{N}_k^{B\dagger}\hat{N}_k^B \leqslant \hat{1}^{AB}, \tag{23}$$

where $\hat{M}_k^A$ is an operator on the qubit A while operator $\hat{N}_k^B$ maps state vectors for the system b to those for the qubit B. Since $\hat{\tau}_k^{AB}$ with $k \in \mathcal{S}$ is entangled by definition, the ranks of operators $\hat{M}_k^A$ and $\hat{N}_k^B$ are 2 for any $k \in \mathcal{S}$.

We rewrite the state of Eq. (19) as

$$|\psi\rangle_{AbE} = \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j}|j\rangle_A|u_j\rangle_b|v_j\rangle_E \tag{24}$$

with $0 < q_0 < 1$, $q_0 + q_1 = 1$, and

$$1 > |\langle u_1|u_0\rangle|^{1-T} = |\langle v_1|v_0\rangle|^T > 0 \tag{25}$$

from a property $|\langle\sqrt{T}\alpha_1|\sqrt{T}\alpha_0\rangle| = |\langle\alpha_1|\alpha_0\rangle|^T$ of coherent states $\{|\alpha_j\rangle\}_{j=0,1}$. From Eqs. (24) and (7), we have a simplified representation [27]

$$\mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AbE}] = \Lambda^A_{|\langle v_1|v_0\rangle|}(|\psi'\rangle\langle\psi'|_{Ab}), \tag{26}$$

where

$$|\psi'\rangle_{Ab} := \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j + i(-1)^j\varphi}|j\rangle_A|u_j\rangle_b \tag{27}$$

with $2\varphi := \arg[\langle v_1|v_0\rangle]$. Thus, Eq. (22) is rewritten as

$$\hat{\tau}_k^{AB} = \frac{1}{p_k}\left(\hat{M}_k^A \otimes \hat{N}_k^B\right)\Lambda^A_{|\langle v_1|v_0\rangle|}(|\psi'\rangle\langle\psi'|_{Ab})\left(\hat{M}_k^A \otimes \hat{N}_k^B\right)^\dagger. \tag{28}$$

Let us consider requisites for $\{\hat{M}_k^A \otimes \hat{N}_k^B\}_{k\in\mathcal{S}}$, stemming from the assumption that $\hat{\tau}_k^{AB}$ is in the standard form of Eq. (2).

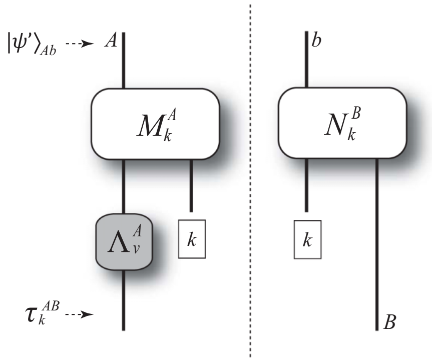

FIG. 2. An imaginary protocol equivalent to the real protocol in Fig. 1. $|\psi'\rangle_{Ab} := \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j+i(-1)^j\varphi}|j\rangle_A|u_j\rangle_b$, where $\varphi := \arg[\langle v_1|v_0\rangle]/2$. Channel $a\to b$ becomes ideal at the expense of the application of a phase-flip channel Λ_v^A with $v = |\langle v_1|v_0\rangle|$.

Since Eq. (2) implies ${}_{AB}\langle 01|\hat{\tau}_k^{AB}|01\rangle_{AB} = 0$, the separable operator $\hat{M}_k^A\otimes\hat{N}_k^B$ must satisfy

$$0 = {}_{AB}\langle 01|\hat{M}_k^A\Lambda^A_{|\langle v_1|v_0\rangle|}\big(\hat{\sigma}_k^{AB}\big)\hat{M}_k^{A\dagger}|01\rangle_{AB}, \tag{29}$$

where

$$\hat{\sigma}_k^{AB} := \hat{N}_k^B(|\psi'\rangle\langle\psi'|_{Ab})\hat{N}_k^{B\dagger}. \tag{30}$$

From $0 < |\langle v_1|v_0\rangle| < 1$ and the positivity of $\hat{\sigma}_k^{AB}$, we have

$$\sqrt{\hat{\sigma}_k^{AB}}|1\rangle_B\big(\hat{M}_k^{A\dagger}|0\rangle_A\big) = \sqrt{\hat{\sigma}_k^{AB}}|1\rangle_B\big(\hat{Z}^A\hat{M}_k^{A\dagger}|0\rangle_A\big) = 0. \tag{31}$$

If $\hat{M}_k^{A\dagger}|0\rangle_A$ and $\hat{Z}^A\hat{M}_k^{A\dagger}|0\rangle_A$ were linearly independent, $\sqrt{\hat{\sigma}_k^{AB}}|1\rangle_B = 0$, which would imply that $\hat{\sigma}_k^{AB}$ is a separable state. This would, in turn, mean the separability of $\hat{\tau}_k^{AB}$. To avoid this contradiction, $\hat{M}_k^{A\dagger}|0\rangle_A$ and $\hat{Z}^A\hat{M}_k^{A\dagger}|0\rangle_A$ must be linearly dependent, which implies that the state $\hat{M}_k^{A\dagger}|0\rangle_A$ is an eigenstate of $\hat{Z}^A$. Similarly, from ${}_{AB}\langle 10|\hat{\tau}_k^{AB}|10\rangle_{AB} = 0$, i.e.,

$$0 = {}_{AB}\langle 10|\hat{M}_k^A\Lambda^A_{|\langle v_1|v_0\rangle|}\big(\hat{\sigma}_k^{AB}\big)\hat{M}_k^{A\dagger}|10\rangle_{AB}, \tag{32}$$

we have

$$\sqrt{\hat{\sigma}_k^{AB}}|0\rangle_B\big(\hat{M}_k^{A\dagger}|1\rangle_A\big) = \sqrt{\hat{\sigma}_k^{AB}}|0\rangle_B\big(\hat{Z}^A\hat{M}_k^{A\dagger}|1\rangle_A\big) = 0, \tag{33}$$

meaning that the state $\hat{M}_k^{A\dagger}|1\rangle_A$ must also be an eigenstate of $\hat{Z}^A$. Combined with $\mathrm{rank}(M_k^{A\dagger}) = 2$, these conclude that $\hat{M}_k^{A\dagger}|0\rangle_A$ and $\hat{M}_k^{A\dagger}|1\rangle_A$ are different eigenstates of $\hat{Z}^A$. By letting $k\in\mathcal{S}_l$ for $l = 0, 1$ denote the subset of outcomes $k\in S$ such that $\hat{M}_k^{A\dagger}|0\rangle_A \propto (\hat{X}^A)^l|0\rangle_A$ and $\hat{M}_k^{A\dagger}|1\rangle_A \propto (\hat{X}^A)^l|1\rangle_A$, where $\mathcal{S} = \mathcal{S}_0\cup\mathcal{S}_1$ with $\mathcal{S}_0\cap\mathcal{S}_1 = \emptyset$, this implies

$$\hat{M}_k^A = \begin{cases} m_k^0|0\rangle\langle 0|_A + m_k^1|1\rangle\langle 1|_A & (k\in\mathcal{S}_0),\\ m_k^0|1\rangle\langle 0|_A + m_k^1|0\rangle\langle 1|_A & (k\in\mathcal{S}_1),\end{cases} \tag{34}$$

with nonzero m_k^j. This equation shows that $\hat{M}_k^A$ commutes with the phase-flip channel $\Lambda^A_{|\langle v_1|v_0\rangle|}$. Hence, the considered protocol is simulatable by a protocol of Fig. 2 where the separable operation $\{\hat{M}_k^A\otimes\hat{N}_k^B\}_{k\in\mathcal{S}}$ is applied to the state $|\psi'\rangle_{Ab}$ before the phase-flip channel $\Lambda^A_{|\langle v_1|v_0\rangle|}$.

Let us consider the form of $\hat{N}_k^B$. From Eq. (34), Eqs. (31) and (33) are reduced to

$$\begin{aligned}\sqrt{\hat{\sigma}_k^{AB}}|01\rangle_{AB} &= \sqrt{\hat{\sigma}_k^{AB}}|10\rangle_{AB} = 0 \quad (k\in\mathcal{S}_0),\\ \sqrt{\hat{\sigma}_k^{AB}}|00\rangle_{AB} &= \sqrt{\hat{\sigma}_k^{AB}}|11\rangle_{AB} = 0 \quad (k\in\mathcal{S}_1).\end{aligned} \tag{35}$$

From the definition (30) of $\hat{\sigma}_k^{AB}$, $\hat{N}_k^B$ should satisfy

$$\begin{aligned}\hat{N}_k^B|u_0\rangle_b &= n_k^0|0\rangle_B,\ \hat{N}_k^B|u_1\rangle_b = n_k^1|1\rangle_B \quad (k\in\mathcal{S}_0),\\ \hat{N}_k^B|u_0\rangle_b &= n_k^0|1\rangle_B,\ \hat{N}_k^B|u_1\rangle_b = n_k^1|0\rangle_B \quad (k\in\mathcal{S}_1),\end{aligned} \tag{36}$$

with nonzero n_k^j. Let $\{{}_b\langle\tilde{u}_i|\}_{i=0,1}$ be a dual basis in the Hilbert subspace spanned by ${}_b\langle u_0|$ and ${}_b\langle u_1|$ for the basis $\{|u_i\rangle_b\}_{i=0,1}$, which satisfies

$$\langle\tilde{u}_i|u_j\rangle = \delta_{ij}. \tag{37}$$

By using this dual basis, $\hat{N}_k^B$ can be described by

$$\hat{N}_k^B = \begin{cases} n_k^0|0\rangle_{Bb}\langle\tilde{u}_0| + n_k^1|1\rangle_{Bb}\langle\tilde{u}_1| & (k\in\mathcal{S}_0),\\ n_k^0|1\rangle_{Bb}\langle\tilde{u}_0| + n_k^1|0\rangle_{Bb}\langle\tilde{u}_1| & (k\in\mathcal{S}_1).\end{cases} \tag{38}$$

As a result of Eqs. (34) and (38), $\hat{\tau}_k^{AB}$ of Eq. (28) is described as $\hat{\tau}_k^{AB} = \Lambda^A_{|\langle v_1|v_0\rangle|}(|\psi_k'\rangle\langle\psi_k'|_{AB})$ with

$$\begin{aligned}|\psi_k'\rangle_{AB} &:= \frac{1}{\sqrt{p_k}}\big(\hat{M}_k^A\otimes\hat{N}_k^B\big)|\psi'\rangle_{Ab}\\ &= \frac{1}{\sqrt{p_k}}\sum_{j=0,1} m_k^j n_k^j\sqrt{q_j}e^{i\Theta_j+i(-1)^j\varphi}(\hat{X}^A\hat{X}^B)^l|jj\rangle_{AB}\end{aligned} \tag{39}$$

for $k\in\mathcal{S}_l$ $(l = 0, 1)$, where

$$p_k = \sum_{j=0,1} q_j\big|m_k^j n_k^j\big|^2. \tag{40}$$

Since $\hat{\tau}_k^{AB} = \Lambda^A_{|\langle v_1|v_0\rangle|}(|\psi_k'\rangle\langle\psi_k'|_{AB})$ is in the standard form $\hat{\gamma}^{AB}(z_k, x_k)$, so is the state $|\psi_k'\rangle_{AB}$, namely, $|\psi_k'\rangle\langle\psi_k'|_{AB} = \hat{\gamma}^{AB}(z_k', \sqrt{1-z_k'^2})$, where z_k' is obtained from Eqs. (2) and (39) as

$$z_k' = \frac{2\sqrt{q_0q_1}\big|m_k^0m_k^1n_k^0n_k^1\big|}{p_k}. \tag{41}$$

Considering the action of the phase-flip channel $\Lambda^A_{|\langle v_1|v_0\rangle|}$, we have

$$\begin{aligned} z_k &= |\langle v_1|v_0\rangle| z_k',\\ x_k &= \sqrt{1-z_k'^2}.\end{aligned} \tag{42}$$

Note that we cannot freely choose parameters p_k and z_k'. In particular, in order to make the operators $\{\hat{M}_k^A\otimes\hat{N}_k^B\}$ achievable, the operators should satisfy Eq. (23). From Eqs. (34), (38), and (37), this condition is shown to be equivalent to

$$\begin{aligned}&\left(1-\sum_{k\in\mathcal{S}}\big|m_k^0n_k^0\big|^2\right)^{1/2}\left(1-\sum_{k\in\mathcal{S}}\big|m_k^0n_k^1\big|^2\right)^{1/2} \geqslant |\langle u_1|u_0\rangle|,\\ &\left(1-\sum_{k\in\mathcal{S}}\big|m_k^1n_k^0\big|^2\right)^{1/2}\left(1-\sum_{k\in\mathcal{S}}\big|m_k^1n_k^1\big|^2\right)^{1/2} \geqslant |\langle u_1|u_0\rangle|.\end{aligned} \tag{43}$$

One way to derive these inequalities is to take a representation of $\hat{N}_k^{B\dagger}\hat{N}_k^B$ with (orthonormal) cat states $|c_\pm\rangle_b := (e^{-i\phi}|u_0\rangle_b \pm e^{i\phi}|u_1\rangle_b)/\sqrt{2(1\pm|\langle u_1|u_0\rangle|)}$, where $2\phi := \arg[\langle u_1|u_0\rangle]$, and to notice that Eq. (23) means $\hat{1}^B - \sum_{k\in\mathcal{S}} m_k^j \hat{N}_k^{B\dagger}\hat{N}_k^B \geqslant 0$ for $j = 0, 1$.

C. An upper bound on separable operations

Let us derive an upper bound on the average overall yield $\bar{Y}$ defined in Eq. (21) assuming that Y satisfies Eq. (13). From Eq. (42), we have

$$\begin{aligned}\bar{Y} &= \sum_{k\in\mathcal{S}} p_k Y\left(|\langle v_1|v_0\rangle| z_k', \sqrt{1-z_k'^2}\right)\\ &\leqslant Y(|\langle v_1|v_0\rangle|, 0)\sum_{k\in\mathcal{S}} p_k z_k'. \end{aligned}\tag{44}$$

On the other hand, since conditions of Eq. (43) imply

$$\frac{1}{4}\sum_{k\in\mathcal{S}}\sum_{i,j=0,1}\left|m_k^i n_k^j\right|^2 \leqslant 1 - |\langle u_1|u_0\rangle|,\tag{45}$$

we have

$$\begin{aligned}\sum_{k\in\mathcal{S}} p_k z_k' &= 2\sqrt{q_0 q_1}\sum_{k\in\mathcal{S}}\left|m_k^0 n_k^0 m_k^1 n_k^1\right|\\ &\leqslant \sum_{k\in\mathcal{S}}\left|m_k^0 n_k^0 m_k^1 n_k^1\right| \leqslant \frac{1}{4}\sum_{k\in\mathcal{S}}\sum_{i,j=0,1}\left|m_k^i n_k^j\right|^2\\ &\leqslant 1 - |\langle u_1|u_0\rangle|. \end{aligned}\tag{46}$$

Therefore, substituting Eq. (46) for the bound of Eq. (44), we obtain an upper bound described by

$$\bar{Y} \leqslant Y(|\langle v_1|v_0\rangle|, 0)(1 - |\langle u_1|u_0\rangle|).\tag{47}$$

If we use Eq. (25), this bound is rewritten as

$$\bar{Y} \leqslant Y\left(|\langle u_1|u_0\rangle|^{\frac{1-T}{T}}, 0\right)(1 - |\langle u_1|u_0\rangle|),\tag{48}$$

which gives an upper bound,

$$\bar{Y} \leqslant \max_{0<u<1} Y\left(u^{\frac{1-T}{T}}, 0\right)(1-u).\tag{49}$$

D. An optimal protocol and the optimal performance

Conversely, here we show that the bound of Eq. (49) is achievable by an entanglement generation protocol introduced in Ref. [27]. This protocol uses a dispersive Jaynes-Cummings Hamiltonian between a matter qubit and a coherent state $|\alpha\rangle_a$ leading to the assumption of $|\alpha_0\rangle_a = |\alpha e^{i\theta/2}\rangle_a$ and $|\alpha_1\rangle_a = |\alpha e^{-i\theta/2}\rangle_a$ with a constant $\theta > 0$ in Eq. (17) for unitary operation $\hat{V}^{Aa}$, and it is regarded as a specific example of the protocol of Sec. III A, based only on Bob's local operation composed of linear optical elements and ideal photon-number-resolving detectors. In particular, in the protocol, Alice first makes a probe pulse a in a coherent state $|\alpha/\sqrt{T}\rangle_a$ interact with her qubit A in state $|+\rangle_A := (|0\rangle_A + |1\rangle_A)/\sqrt{2}$ with the unitary operation $\hat{V}^{Aa}$ and then sends it to Bob together with a local-oscillator (LO) pulse. On receiving the pulse a and the LO pulse, Bob generates a probe pulse b in a coherent state $|\alpha\rangle_b$ from the LO pulse, and makes it interact with his qubit B in state $|+\rangle_B$ with the unitary operation $\hat{V}^{Bb}$. Then, he inputs the pulses a and b to a 50:50 beam splitter, followed by a displacement operation $\hat{D}[-\sqrt{2}\alpha\cos(\theta/2)]$ (using a remaining LO pulse) on the pulse having experienced the constructive interference. Finally, he measures two output pulses with photon-number-resolving detectors.

The protocol provides [27] single-error-type entangled states when it succeeds (i.e., when the photon detectors find nonzero photons), all of which can be transformed to $\hat{\gamma}^{AB}(2F-1, 0)$ with fidelity

$$F = \frac{1 + u^{\frac{1-T}{T}}}{2},\tag{50}$$

and the total success probability $P_{\rm s} = \sum_{k\in\mathcal{S}} p_k$ is

$$P_{\rm s} = 1 - u,\tag{51}$$

where $u := |\langle\alpha e^{i\theta/2}|\alpha e^{-i\theta/2}\rangle|^T$ is controllable by choosing α. Hence, with the entanglement generation protocol, the average overall yield $\bar{Y}$ is given by

$$\begin{aligned}\bar{Y} &= \sum_{k\in\mathcal{S}} p_k Y(2F-1, 0) = Y(2F-1, 0)P_{\rm s}\\ &= Y\left(u^{\frac{1-T}{T}}, 0\right)(1-u). \end{aligned}\tag{52}$$

Since the parameter u can be chosen freely in the protocol, the protocol can achieve

$$\bar{Y} = \max_{0<u<1} Y\left(u^{\frac{1-T}{T}}, 0\right)(1-u),\tag{53}$$

which coincides with the upper bound (49). Therefore, for the yield function Y satisfying Eq. (13), the entanglement generation protocol of Ref. [27] is concluded to give the maximum yield of the single-error-type entanglement generation protocols.

E. Comparison with the quantum and private capacity

To see how efficient the optimal protocol in Sec. III D is, let us consider the asymptotic yield of an overall protocol, by assuming that the single-error-type entangled states successfully generated by the protocol are collectively input to the optimal two-way entanglement distillation protocol, implying the assumption of $Y = E_{\rm D}$. In this case, from Eqs. (16) and (53), the overall performance is

$$\bar{E}_{\rm D,max} := \max_{0<u<1}(1-u)\left[1 - h\left(\frac{1+u^{\frac{1-T}{T}}}{2}\right)\right].\tag{54}$$

This quantity represents how many ebits are obtained per use of the entanglement generation protocol, i.e., per channel use, in an asymptotically faithful scenario. The overall yield $\bar{E}_{\rm D,max}$ is plotted by Fig. 3(b). On the other hand, the two-way quantum and private capacity of a pure-loss channel with the transmittance T is $-\log_2(1-T)$ [24], represented by Fig. 3(a). We also describe the success probabilities to obtain single-error-type entanglement with $F = 99.4\%$ and with $F = 99.8\%$ by using the optimal entanglement generation in Sec. III D as Figs. 3(c) and 3(d), respectively. As shown in Fig. 3, the overall yield $\bar{E}_{\rm D,max}$ based on the optimal two-way entanglement distillation [Fig. 3(b)] is one order of magnitude

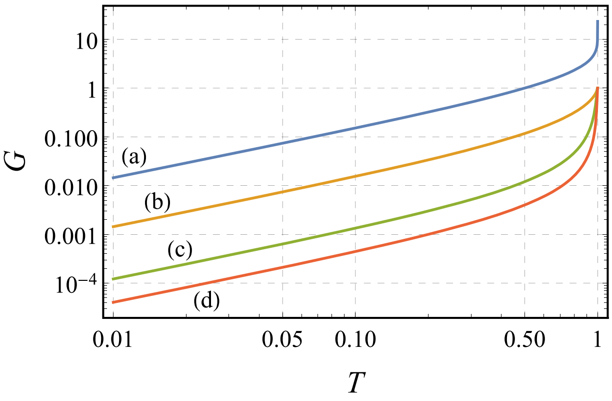

FIG. 3. Performance of the point-to-point optimal supplier of single-error-type entanglement over coherent-state transmission over a lossy channel with the transmittance T. Curve (a) describes the quantum and private capacity of the lossy channel as a reference. Curve (b) describes $\bar{E}_{\mathrm{D,max}}$ which is the two-way distillable entanglement of the single-error-type entanglement generated by the optimal supplier, per channel use. Curves (c) and (d) represent the success probabilities to obtain single-error-type entanglement with $F = 99.4\%$ and with $F = 99.8\%$ by using the optimal supplier, respectively.

less than the quantum and private capacity of the lossy channel [Fig. 3(a)], and one order of magnitude better than direct generation of 99.4%-fidelity entanglement with the optimal protocol in Sec. III D [Fig. 3(c)].

IV. TIGHT BOUND ON SINGLE-ERROR-TYPE ENTANGLEMENT GENERATION BY THREE PARTIES

In this section, we derive a tight bound on the entanglement generation protocols based on three parties. We start by defining the protocols in Sec. IV A. Using the results in Secs. III B and III C, we derive an upper bound on the performance of protocols based on separable operations in Sec. IV B. In Sec. IV C, we show that a protocol based on the remote nondestructive parity measurement of Ref. [43] achieves the upper bound. In Sec. IV D, we explicitly show how efficient the optimal protocol is.

A. Single-error-type entanglement generation by three parties

To generate a single-error-type entangled state between Alice and Bob, they can ask another party called Claire for help. In fact, single-error-type entanglement generation found in Ref. [43] adopts such a three-party protocol. This kind of protocol proceeds as follows (Fig. 4): (i) Alice prepares qubit A in her desired state $|\phi\rangle_A = \sum_{j=0,1}\sqrt{q_j^A}e^{i\Theta_j^A}|j\rangle_A$ with real parameters Θ_j^A, $q_j^A > 0$, and $\sum_j q_j^A = 1$, 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 $\hat{V}^{Aa}$ of Eq. (17). (ii) Similarly, by using a unitary operation $\hat{V}^{Bb}$, Bob makes a pulse in coherent state $|\beta\rangle_b$ interact with his qubit B prepared in his desired state $|\varphi\rangle_B = \sum_{j=0,1}\sqrt{q_j^B}e^{i\Theta_j^B}|j\rangle_B$. (iii) Alice and Bob send the pulses a and b to Claire through lossy channels described by isometries $\hat{L}^{a\to c_aE_a}$ and $\hat{L}^{b\to c_bE_b}$,

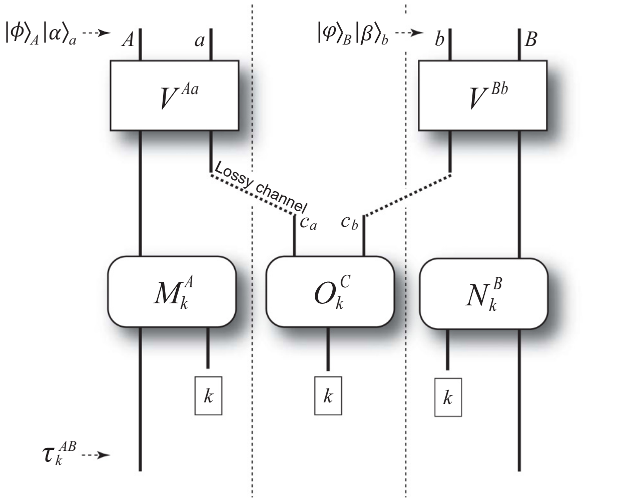

FIG. 4. Scenario of single-error-type entanglement generation by three parties. $|\phi\rangle_A := \sum_{j=0,1}\sqrt{q_j^A}e^{i\Theta_j^A}|j\rangle_A$ and $|\varphi\rangle_B := \sum_{j=0,1}\sqrt{q_j^B}e^{i\Theta_j^B}|j\rangle_B$. An outcome k corresponds to the application of a separable operator $\hat{M}_k^A \otimes \hat{N}_k^B \otimes {}_C\langle O_k|$. If the final entanglement $\hat{\tau}_k^{AB}$ includes only one type of error, Alice, Bob, and Claire may declare the success of the protocol.

$$\hat{L}^{x\to c_xE_x}|\alpha\rangle_x = |\sqrt{T_x}\alpha\rangle_{c_x}|\sqrt{1-T_x}\alpha\rangle_{E_x} \tag{55}$$

for $x = a, b$, respectively, where c_x is the pulse at Claire's location, $0 < T_x < 1$ is the transmittance of the channel for pulse x, and E_x is the environment. At this point, Alice, Bob, and Claire share a quantum state $|\xi\rangle_{Ac_aE_a} \otimes |\zeta\rangle_{Bc_bE_b}$ with

$$|\xi\rangle_{Ac_aE_a} = \sum_{j=0,1}\sqrt{q_j^A}e^{i\Theta_j^A}|j\rangle_A|\sqrt{T_a}\alpha_j\rangle_{c_a}|\sqrt{1-T_a}\alpha_j\rangle_{E_a},$$
$$|\zeta\rangle_{Bc_bE_b} = \sum_{j=0,1}\sqrt{q_j^B}e^{i\Theta_j^B}|j\rangle_B|\sqrt{T_b}\beta_j\rangle_{c_b}|\sqrt{1-T_b}\beta_j\rangle_{E_b}. \tag{56}$$

(iv) Alice, Bob, and Claire manipulate system ABc_ac_b through LOCC, and may declare outcome k with probability p_k to herald the success of the generation of qubits AB in a single-error-type entangled state $\hat{\tau}_k^{AB}$ in the form of Eq. (20) for $k \in \mathcal{S}$.

This protocol is evaluated by the same way as in Sec. III A, namely, by Eq. (21).

B. An upper bound on single-error-type entanglement generation by three parties

Similar to Sec. III B, we consider a separable operation $\{\hat{M}_k^A \otimes \hat{N}_k^B \otimes {}_C\langle O_k|\}$, instead of the LOCC operation executed by Alice, Bob, and Claire at step (iv), based on the fact that separable operations compose a class of operations (strictly) larger than the set of LOCC operations. Here, through finding the form of separable operators $\hat{M}_k^A \otimes \hat{N}_k^B \otimes {}_C\langle O_k|$ that successfully return single-error-type entanglement $\hat{\tau}_k^{AB}$ in the form of Eq. (20), we associate the three-party protocol with a two-party protocol as in Fig. 2.

For simplicity, let us rewrite the states of Eq. (56) as

$$|\xi\rangle_{Ac_aE_a} = \sum_{j=0,1}\sqrt{q_j^A}e^{i\Theta_j^A}|j\rangle_A\big|u_j^a\big\rangle_{c_a}\big|v_j^a\big\rangle_{E_a},$$
$$|\zeta\rangle_{Bc_bE_b} = \sum_{j=0,1}\sqrt{q_j^B}e^{i\Theta_j^B}|j\rangle_B\big|u_j^b\big\rangle_{c_b}\big|v_j^b\big\rangle_{E_b}, \qquad (57)$$

where $0 < q_0^X < 1$ and $q_0^X + q_1^X = 1$ for $X = A, B$, and

$$1 > \big|\big\langle u_1^a\big|u_0^a\big\rangle\big|^{1-T_a} = \big|\big\langle v_1^a\big|v_0^a\big\rangle\big|^{T_a} > 0,$$
$$1 > \big|\big\langle u_1^b\big|u_0^b\big\rangle\big|^{1-T_b} = \big|\big\langle v_1^b\big|v_0^b\big\rangle\big|^{T_b} > 0. \qquad (58)$$

From Eqs. (57) and (7), we have

$$\mathrm{Tr}_{E_a}[|\xi\rangle\langle\xi|_{Ac_aE_a}] = \Lambda^A_{|\langle v_1^a|v_0^a\rangle|}(|\xi'\rangle\langle\xi'|_{Ac_a}),$$
$$\mathrm{Tr}_{E_b}[|\zeta\rangle\langle\zeta|_{Bc_bE_b}] = \Lambda^B_{|\langle v_1^b|v_0^b\rangle|}(|\zeta'\rangle\langle\zeta'|_{Bc_b}), \qquad (59)$$

where

$$|\xi'\rangle_{Ac_a} := \sum_{j=0,1}\sqrt{q_j^A}e^{i\Theta_j^A+i(-1)^j\varphi_a}|j\rangle_A\big|u_j^a\big\rangle_{c_a},$$
$$|\zeta'\rangle_{Bc_b} := \sum_{j=0,1}\sqrt{q_j^B}e^{i\Theta_j^B+i(-1)^j\varphi_b}|j\rangle_B\big|u_j^b\big\rangle_{c_b} \qquad (60)$$

with $2\varphi_x := \arg[\langle v_1^x|v_0^x\rangle]$ for $x = a, b$. Hence, a separable operation $\{\hat{M}_k^A \otimes \hat{N}_k^B \otimes {}_C\langle O_k|\}$ to the system ABc_ac_b in state $|\xi\rangle_{Ac_aE_a} \otimes |\zeta\rangle_{Bc_bE_b}$ is equivalent to that in state $\Lambda^A_{|\langle v_1^a|v_0^a\rangle|}(|\xi'\rangle\langle\xi'|_{Ac_a}) \otimes \Lambda^B_{|\langle v_1^b|v_0^b\rangle|}(|\zeta'\rangle\langle\zeta'|_{Bc_b})$.

Suppose that Alice, Bob, and Claire apply a separable operator $\hat{M}_k^A \otimes \hat{N}_k^B \otimes {}_C\langle O_k|$ to the state $\Lambda^A_{|\langle v_1^a|v_0^a\rangle|}(|\xi'\rangle\langle\xi'|_{Ac_a}) \otimes \Lambda^B_{|\langle v_1^b|v_0^b\rangle|}(|\zeta'\rangle\langle\zeta'|_{Bc_b})$, and they return an entangled state $\hat{\tau}_k^{AB}$ in the form (2). The separable operator $\hat{M}_k^A \otimes \hat{N}_k^B \otimes {}_C\langle O_k|$ must satisfy

$${}_{AB}\langle 01|\hat{M}_k^A\Lambda^A_{|\langle v_1^a|v_0^a\rangle|}\big(\hat{\mu}_k^{AB}\big)\hat{M}_k^{A\dagger}|01\rangle_{AB} = 0,$$
$${}_{AB}\langle 10|\hat{M}_k^A\Lambda^A_{|\langle v_1^a|v_0^a\rangle|}\big(\hat{\mu}_k^{AB}\big)\hat{M}_k^{A\dagger}|10\rangle_{AB} = 0, \qquad (61)$$

with

$$\hat{\mu}_k^{AB} := \hat{N}_k^B{}_C\langle O_k|\big[|\xi'\rangle\langle\xi'|_{Ac_a} \otimes \Lambda^B_{|\langle v_1^b|v_0^b\rangle|}(|\zeta'\rangle\langle\zeta'|_{Bc_b})\big]|O_k\rangle_C\hat{N}_k^{B\dagger}. \qquad (62)$$

Note that Eq. (61) is in the same form as Eqs. (29) and (32). In addition, $\hat{\mu}_k^{AB}$ is a positive operator and $0 < |\langle v_1^a|v_0^a\rangle| < 1$. Thus, similar to considerations from Eqs. (29) to (34), $\hat{M}_k^A$ can be assumed to be in the form of

$$\hat{M}_k^A = \begin{cases} m_k^0|0\rangle\langle 0|_A + m_k^1|1\rangle\langle 1|_A & \big(k \in \mathcal{S}_0^A\big), \\ m_k^0|1\rangle\langle 0|_A + m_k^1|0\rangle\langle 1|_A & \big(k \in \mathcal{S}_1^A\big), \end{cases} \qquad (63)$$

with nonzero m_k^j, where $\mathcal{S}_0^A$ and $\mathcal{S}_1^A$ are two disjoint subsets of set $\mathcal{S}$, i.e., satisfying $\mathcal{S} = \mathcal{S}_0^A \cup \mathcal{S}_1^A$ and $\mathcal{S}_0^A \cap \mathcal{S}_1^A = \emptyset$, and $\hat{\mu}_k^{AB}$ satisfies

$$\sqrt{\hat{\mu}_k^{AB}}|01\rangle_{AB} = \sqrt{\hat{\mu}_k^{AB}}|10\rangle_{AB} = 0 \quad \big(k \in \mathcal{S}_0^A\big),$$
$$\sqrt{\hat{\mu}_k^{AB}}|00\rangle_{AB} = \sqrt{\hat{\mu}_k^{AB}}|11\rangle_{AB} = 0 \quad \big(k \in \mathcal{S}_1^A\big). \qquad (64)$$

This implies

$${}_{AB}\langle 01|\hat{N}_k^B\Lambda^B_{|\langle v_1^b|v_0^b\rangle|}\big(\hat{\nu}_k^{AB}\big)\hat{N}_k^B|01\rangle_{AB} = 0,$$
$${}_{AB}\langle 10|\hat{N}_k^B\Lambda^B_{|\langle v_1^b|v_0^b\rangle|}\big(\hat{\nu}_k^{AB}\big)\hat{N}_k^B|10\rangle_{AB} = 0 \qquad (65)$$

for any $k \in \mathcal{S}_0^A$ and

$${}_{AB}\langle 00|\hat{N}_k^B\Lambda^B_{|\langle v_1^b|v_0^b\rangle|}\big(\hat{\nu}_k^{AB}\big)\hat{N}_k^B|00\rangle_{AB} = 0,$$
$${}_{AB}\langle 11|\hat{N}_k^B\Lambda^B_{|\langle v_1^b|v_0^b\rangle|}\big(\hat{\nu}_k^{AB}\big)\hat{N}_k^B|11\rangle_{AB} = 0 \qquad (66)$$

for any $k \in \mathcal{S}_1^A$, with

$$\hat{\nu}_k^{AB} := {}_C\langle O_k|(|\xi'\rangle\langle\xi'|_{Ac_a} \otimes |\zeta'\rangle\langle\zeta'|_{Bc_b})|O_k\rangle_C. \qquad (67)$$

Similar to considerations from Eqs. (29) to (34), combined with $0 < |\langle v_1^b|v_0^b\rangle| < 1$, Eqs. (65) and (66) conclude that $\hat{N}_k^B$ can be assumed to be in the form of

$$\hat{N}_k^B = \begin{cases} n_k^0|0\rangle\langle 0|_B + n_k^1|1\rangle\langle 1|_B & \big(k \in \mathcal{S}_0^B\big), \\ n_k^0|1\rangle\langle 0|_B + n_k^1|0\rangle\langle 1|_B & \big(k \in \mathcal{S}_1^B\big), \end{cases} \qquad (68)$$

where $\mathcal{S}_0^B$ and $\mathcal{S}_1^B$ are two disjoint subsets of set $\mathcal{S}$, with nonzero n_k^j, and $\hat{\nu}_k^{AB}$ satisfies

$$\sqrt{\hat{\nu}_k^{AB}}|01\rangle_{AB} = \sqrt{\hat{\nu}_k^{AB}}|10\rangle_{AB} = 0 \quad \big(k \in \textstyle\bigcup_{i=0,1}\mathcal{S}_i^A \cap \mathcal{S}_i^B\big),$$
$$\sqrt{\hat{\nu}_k^{AB}}|00\rangle_{AB} = \sqrt{\hat{\nu}_k^{AB}}|11\rangle_{AB} = 0 \quad \big(k \in \textstyle\bigcup_{i=0,1}\mathcal{S}_i^A \cap \mathcal{S}_{i\oplus 1}^B\big). \qquad (69)$$

At this point, we have obtained two facts: (i) $\hat{M}_k^A \otimes \hat{N}_k^B$ commutes with the phase-flip channel $\Lambda^A_{|\langle v_1^a|v_0^a\rangle|} \otimes \Lambda^B_{|\langle v_1^b|v_0^b\rangle|}$; (ii) the range of $\hat{\nu}_k^{AB}$ is either the two-dimensional Hilbert subspace spanned by states $\{|00\rangle_{AB}, |11\rangle_{AB}\}$ or that by states $\{|01\rangle_{AB}, |10\rangle_{AB}\}$. The fact (i) implies that the considered protocol is simulatable by a protocol of Fig. 5 where the separable operation $\{\hat{M}_k^A \otimes \hat{N}_k^B \otimes {}_C\langle O_k|\}$ is applied to the state $|\xi'\rangle_{Ac_a} \otimes |\zeta'\rangle_{Bc_b}$ before the phase-flip channel $\Lambda^A_{|\langle v_1^a|v_0^a\rangle|} \otimes \Lambda^B_{|\langle v_1^b|v_0^b\rangle|}$. In addition, combined with Eqs. (63), (68), and (69), the fact (ii) indicates that $\hat{M}_k^A\hat{N}_k^B{}_C\langle O_k||\xi'\rangle_{Ac_a}|\zeta'\rangle_{Bc_b}$ belongs to the subspace spanned by states $\{|00\rangle_{AB}, |11\rangle_{AB}\}$. This implies that the effect of the phase-flip channel $\Lambda^B_{|\langle v_1^b|v_0^b\rangle|}$ $(\Lambda^A_{|\langle v_1^a|v_0^a\rangle|})$ on the entangled state $\hat{M}_k^A\hat{N}_k^B{}_C\langle O_k||\xi'\rangle_{Ac_a}|\zeta'\rangle_{Bc_b}$ is equivalent to that of a phase-flip channel $\Lambda^A_{|\langle v_1^b|v_0^b\rangle|}$ $(\Lambda^B_{|\langle v_1^a|v_0^a\rangle|})$. Hence, in the success cases, the protocol works equivalently to a virtual protocol A (B) in Fig. 5 where Alice, Bob, and Claire prepare unnormalized state $\hat{M}_k^A\hat{N}_k^B{}_C\langle O_k||\xi'\rangle_{Ac_a}|\zeta'\rangle_{Bc_b}$ to be input into a series of phase-flip channels $\Lambda^A_{|\langle v_1^b|v_0^b\rangle|}\Lambda^A_{|\langle v_1^a|v_0^a\rangle|} = \Lambda^A_{|\langle v_1^a|v_0^a\rangle||\langle v_1^b|v_0^b\rangle|}$ $(\Lambda^B_{|\langle v_1^a|v_0^a\rangle|}\Lambda^B_{|\langle v_1^b|v_0^b\rangle|} = \Lambda^B_{|\langle v_1^a|v_0^a\rangle||\langle v_1^b|v_0^b\rangle|})$.

Let us relate the virtual protocol A in Fig. 5 to the two-party protocol depicted in Fig. 2 by regarding Claire and Bob in the former as a single party, which is Bob in the latter. Since Alice's operator $\hat{M}_k^A$ takes the same form [see Eqs. (63) and

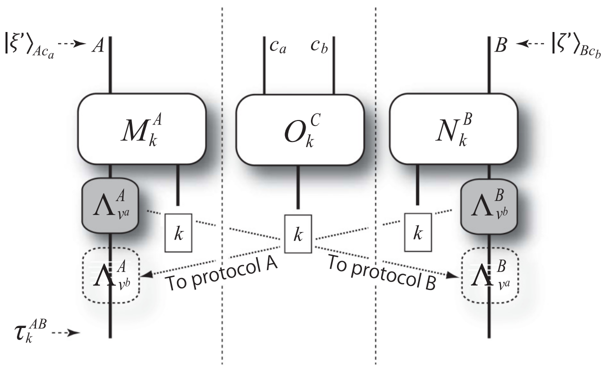

FIG. 5. An imaginary protocol equivalent to the real protocol in Fig. 4. $|\xi'\rangle_{Ac_a} := \sum_{j=0,1}\sqrt{q_j^A}e^{i\Theta_j^A+i(-1)^j\varphi_a}|j\rangle_A|u_j^a\rangle_{c_a}$ and $|\zeta'\rangle_{Bc_b} := \sum_{j=0,1}\sqrt{q_j^B}e^{i\Theta_j^B+i(-1)^j\varphi_b}|j\rangle_B|u_j^b\rangle_{c_b}$. Channels $a \to c_a$ and $b \to c_b$ become ideal at the expense of the application of phase-flip channels $\Lambda_{\nu^a}^A$ with $\nu^a = |\langle v_1^a|v_0^a\rangle|$ and $\Lambda_{\nu^b}^B$ with $\nu^b = |\langle v_1^b|v_0^b\rangle|$, respectively. If the protocol returns success outcome k, the effect of phase-flip channel $\Lambda_{\nu^b}^B$ ($\Lambda_{\nu^a}^A$) is equivalent to that of $\Lambda_{\nu^b}^A$ ($\Lambda_{\nu^a}^B$). We define virtual protocol A (B) as the modified protocol where $\Lambda_{\nu^b}^B$ ($\Lambda_{\nu^a}^A$) is converted to $\Lambda_{\nu^b}^A$ ($\Lambda_{\nu^a}^B$).

(34)], we notice that the protocol A is a special case of the protocol in Fig. 2 with the following substitutions:

$$\begin{aligned} q_j &\mapsto q_j^A, \\ \Theta_j &\mapsto \Theta_j^A, \\ |u_j\rangle_b &\mapsto |u_j^a\rangle_{c_a}, \\ |\langle v_1|v_0\rangle| &\mapsto |\langle v_1^a|v_0^a\rangle||\langle v_1^b|v_0^b\rangle|, \\ \hat{N}_k^B &\mapsto ({}_C\langle O_k| \otimes \hat{N}_k^B)|\zeta'\rangle_{Bc_b}. \end{aligned} \tag{70}$$

Therefore, derivation of requisites starting from Eqs. (35) to (47) is also applicable here under the above substitution. We thus obtain a bound

$$\bar{Y} \leqslant Y(|\langle v_1^a|v_0^a\rangle||\langle v_1^b|v_0^b\rangle|, 0)(1 - |\langle u_1^a|u_0^a\rangle|) \tag{71}$$

for the virtual protocol A. Similarly, by exchanging the roles of Alice and Bob in the above argument, we also obtain a bound

$$\bar{Y} \leqslant Y(|\langle v_1^a|v_0^a\rangle||\langle v_1^b|v_0^b\rangle|, 0)(1 - |\langle u_1^b|u_0^b\rangle|) \tag{72}$$

for the virtual protocol B. Let $u := \max\{|\langle u_1^a|u_0^a\rangle|, |\langle u_1^b|u_0^b\rangle|\}$. Since both inequalities (71) and (72) hold, use of Eqs. (58) and (8) leads to

$$\begin{aligned} \bar{Y} &\leqslant Y(|\langle v_1^a|v_0^a\rangle||\langle v_1^b|v_0^b\rangle|, 0)(1 - u) \\ &\leqslant Y(u^{\frac{1-T_a}{T_a}+\frac{1-T_b}{T_b}}, 0)(1 - u). \end{aligned} \tag{73}$$

This gives an upper bound on $\bar{Y}$,

$$\bar{Y} \leqslant \max_{0<u<1} Y(u^{\frac{1-T_a}{T_a}+\frac{1-T_b}{T_b}}, 0)(1 - u). \tag{74}$$

C. An optimal protocol and the optimal performance for three-party protocols

Conversely, here we show that the bound of Eq. (74) for protocols based on separable operations is achievable by a protocol based on the remote nondestructive parity measurement proposed in Ref. [43], which is a three-party implementation of the optimal protocol [27] (employed in Sec. III D) for executing projective measurement $\hat{Z}^A \otimes \hat{Z}^B$. In particular, similar to the protocol [27], this protocol uses unitary interaction $\hat{V}^{Aa}$ of Eq. (17) with the assumption of $|\alpha_0\rangle_a = |\alpha e^{i\theta/2}\rangle_a$ and $|\alpha_1\rangle_a = |\alpha e^{-i\theta/2}\rangle_a$ for the coherent-state input $|\alpha\rangle_a$ with a constant $\theta > 0$, and it is based only on Claire's local operation composed of linear optical elements and ideal photon-number-resolving detectors. More precisely, in the protocol, Alice (Bob) first makes probe pulse a (b) in a coherent state $|\alpha/\sqrt{T_a}\rangle_a$ ($|\alpha/\sqrt{T_b}\rangle_b$) interact with her qubit A (his qubit B) in state $|+\rangle_A$ ($|+\rangle_B$) with the unitary operation $\hat{V}^{Aa}$ ($\hat{V}^{Bb}$) and then sends it to Claire. On receiving the pulse a from Alice and the pulse b from Bob, Claire makes them interfere via a 50:50 beam splitter, and applies a displacement operation $\hat{D}[-\sqrt{2}\alpha\cos(\theta/2)]$ on the pulse having experienced the constructive interference. Finally, Claire measures two output pulses with photon-number-resolving detectors.

The protocol provides [43] single-error-type entangled states when it succeeds (i.e., when Claire's photon detectors find nonzero photons), all of which can be transformed to $\hat{\gamma}^{AB}(2F-1, 0)$ with fidelity

$$F = \frac{1 + u^{\frac{1-T_a}{T_a}+\frac{1-T_b}{T_b}}}{2}, \tag{75}$$

and the total success probability $P_{\rm s} = \sum_{k\in\mathcal{S}} p_k$ is

$$P_{\rm s} = 1 - u, \tag{76}$$

where $u := |\langle\alpha e^{i\theta/2}|\alpha e^{-i\theta/2}\rangle|^{T_a}$ is a parameter controllable by choosing α. Therefore, with the entanglement generation protocol, the yield $\bar{Y}$ is

$$\begin{aligned} \bar{Y} &= \sum_{k\in\mathcal{S}} p_k Y(2F-1, 0) = Y(2F-1, 0)P_{\rm s} \\ &= Y(u^{\frac{1-T_a}{T_a}+\frac{1-T_b}{T_b}}, 0)(1 - u). \end{aligned} \tag{77}$$

Since u can freely be chosen in the entanglement generation protocol of Ref. [43], it can achieve the bound of (74), i.e.,

$$\bar{Y} = \max_{0<u<1} Y(u^{\frac{1-T_a}{T_a}+\frac{1-T_b}{T_b}}, 0)(1 - u). \tag{78}$$

D. Comparison with the quantum and private capacity

Similar to Sec. III D, to see how efficient the optimal protocol in Sec. IV C is, let us consider an asymptotic yield with $Y = E_{\rm D}$, by assuming that the single-error-type entangled states successfully generated by the protocol are collectively input to the optimal two-way entanglement distillation protocol. In this case, from Eqs. (16) and (78), the overall performance is

$$\bar{E}_{\rm D,max} := \max_{0<u<1}(1 - u)\left[1 - h\left(\frac{1 + u^{\frac{1-T_a}{T_a}+\frac{1-T_b}{T_b}}}{2}\right)\right]. \tag{79}$$

For simplicity, let $T_a = T_b = \sqrt{T}$, where T represents the transmittance of a series of lossy channels between Alice and Claire and between Claire and Bob. Then, the yield $\bar{E}_{\rm D,max}$ is described by Fig. 6(b). On the other hand, the two-way quantum and private capacity (per use of the pair of

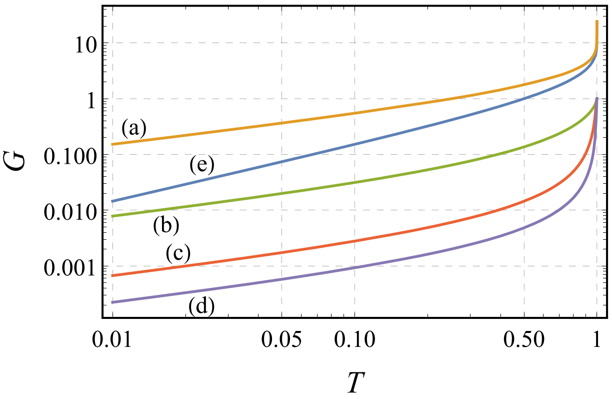

FIG. 6. Performance of the optimal supplier of single-error-type entanglement with a middle measuring station. This middle station is connected with Alice and Bob by a lossy channel with transmittance $\sqrt{T}$, respectively (i.e., $T_a = T_b = \sqrt{T}$). Curve (a) describes the quantum and private capacity of this network. Curve (b) describes $\bar{E}_{\mathrm{D,max}}$ which is the two-way distillable entanglement of the single-error-type entanglement generated by the optimal supplier, per use of the pair of channels between AC and CB. Curves (c) and (d) represent the success probabilities to obtain single-error-type entanglement with $F = 99.4\%$ and with $F = 99.8\%$ by using the optimal supplier, respectively. Curve (e) describes the quantum and private capacity of a lossy channel with transmittance T (which can directly connect Alice and Bob).

channels between A and C and between C and B) of the considered network is $-\log_2(1-\sqrt{T})$ [21,59–61], represented by Fig. 6(a). We also describe the success probabilities to obtain single-error-type entanglement with $F = 99.4\%$ and with $F = 99.8\%$ by using the optimal entanglement generation in Sec. IV D as Figs. 6(c) and 6(d), respectively. As a reference, we also describe the quantum and private capacity $-\log_2(1-T)$ of a lossy channel with transmittance T (which can directly connect Alice and Bob) as Fig. 6(e). As shown in Fig. 6, the yield $\bar{E}_{\mathrm{D,max}}$ based on the optimal two-way entanglement distillation [Fig. 6(b)] is one order of magnitude less than the quantum and private capacity of the network [Fig. 6(a)], and one order of magnitude better than direct generation of 99.4%-fidelity entanglement with the RNPM protocol in Sec. IV C [Fig. 6(c)].

V. DISCUSSION

In this paper, we have identified entanglement generation based on the RNPM as the optimal supplier of single-error-type entanglement over coherent-state transmission, for arbitrary subsequent protocol with a jointly convex yield function satisfying Eq. (13). Notice that although the RNPM is designed to distribute entanglement (or, more generally, to implement the projective measurement $\hat{Z}^A \otimes \hat{Z}^B$), it is closely related with QKD as well. In fact, the RNPMs for the two-party scenario in Sec. III D and for the three-party scenario in Sec. IV C can be regarded as coherent versions of the B92 QKD and of the TF QKD, respectively. Besides, note that they have a slight difference in the implementation, as described in Secs. III D and IV C. In particular, the receiver can use a transmitted LO pulse to generate a coherent state with a properly locked phase in the former scenario, while both of the communicators need their own local LOs phase-locked to each other in the latter. Nevertheless, even in the latter scenario, we would be able to lock the phases properly in the near future, by considering recent progress of the related technology in the context of realization of TF QKD (see, e.g., [73]).

The condition (13) is satisfied by typical yield functions, such as arbitrary convex functions of the singlet fraction, two-way distillable entanglement, and two-way distillable key. If the distillable entanglement or key is adopted as a measure of the performance, its overall yield is only one order of magnitude less than the quantum and private capacity [21,24,59,60] of the associated pure-loss bosonic channel network, and merely one order of magnitude better than direct generation of high-fidelity (in particular, 99.4%-fidelity) entanglement with the RNPM, as represented by Fig. 3 for the two-party protocol and by Fig. 6 for the three-party protocol. Considering that the overall yield cannot be achieved without the use of the optimal entanglement distillation in an asymptotic scenario, the latter gap implies that if entanglement generation protocol is efficient like one based on the RNPM, entanglement distillation protocol may not be necessary to achieve controlled-not operations in distributed quantum computation, in contrast to what one may infer from existing schemes [13–16]. This suggests that performance of entanglement generation protocol affects the overall design of a distributed quantum computing architecture. On the other hand, considering that the quantum and private capacity [21,24,59,60] of the associated pure-loss bosonic channel network is achieved with the use of two-mode infinitely squeezed vacuum states [72], the former gap implies that it is reasonable in practice to adopt protocol based on coherent-state transmission, like the RNPM protocol. Indeed, in the field of QKD, TF QKD protocol [47–54] based on coherent-state encoding has already been identified as an important class of protocol to beat the repeaterless bounds [23,24] in a practical manner (see, e.g., [73]).

ACKNOWLEDGMENTS

We would like to thank K. Fujii, G. Kato, W. J. Munro, N. Sota, and H. Takeda for valuable discussions. We acknowledge the support from Moonshot R&D, JST Grant No. JPMJMS2061, in part, from CREST, JST Grant No. JP-MJCR1671, from PREST, JST Grant No. JP-MJPR1861, and from JSPS KAKENHI Grant No. 21H05183 JP.

[1] D. Mayers, J. ACM **48**, 351 (2001).
[2] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] M. Koashi, New J. Phys. **11**, 045018 (2009).

[5] R. Renner, Int. J. Quantum Inf. **06**, 1 (2008).
[6] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[7] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[9] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[10] D. Gottesman, in *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32–43.
[11] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).
[12] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).
[13] A. G. Fowler, A. M. Stephens, and P. Groszkowski, Phys. Rev. A **80**, 052312 (2009).
[14] K. Fujii, T. Yamamoto, M. Koashi, and N. Imoto, arXiv:1202.6588.
[15] Y. Li and S. C. Benjamin, New J. Phys. **14**, 093008 (2012).
[16] N. H. Nickerson, Y. Li, and S. C. Benjamin, Nat. Commun. **4**, 1756 (2013).
[17] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim, Phys. Rev. A **89**, 022317 (2014).
[18] K. Nemoto, M. Trupke, S. J. Devitt, A. M. Stephens, B. Scharfenberger, K. Buczak, T. Nöbauer, M. S. Everitt, J. Schmiedmayer, and W. J. Munro, Phys. Rev. X **4**, 031022 (2014).
[19] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[20] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[21] K. Azuma and G. Kato, Phys. Rev. A **96**, 032332 (2017).
[22] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[23] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. **5**, 5235 (2014).
[24] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[25] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).
[26] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, Phys. Rev. Lett. **101**, 040502 (2008).
[27] K. Azuma, N. Sota, R. Namiki, Ş. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **80**, 060303(R) (2009).
[28] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, Nat. Photonics **4**, 792 (2010).
[29] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, Nat. Photonics **6**, 777 (2012).
[30] K. Azuma and G. Kato, Phys. Rev. A **85**, 060303(R) (2012).
[31] C. H. Bennett and G. Brassard, in *Proceedings of International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), 175.
[32] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[33] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[34] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[35] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[36] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[37] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[38] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, Phys. Rev. A **80**, 032302 (2009).
[39] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).
[40] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
[41] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[42] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).
[43] K. Azuma, H. Takeda, M. Koashi, and N. Imoto, Phys. Rev. A **85**, 062309 (2012).
[44] S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 012301 (2014).
[45] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, New J. Phys. **16**, 043005 (2014).
[46] K. Azuma, K. Tamaki, and W. J. Munro, Nat. Commun. **6**, 10171 (2015).
[47] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).
[48] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X **8**, 031043 (2018).
[49] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Applied **11**, 034053 (2019).
[50] J. Lin and N. Lütkenhaus, Phys. Rev. A **98**, 042332 (2018).
[51] M. Curty, K. Azuma, and H.-K. Lo, npj Quantum Inf. **5**, 64 (2019).
[52] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Phys. Rev. A **98**, 062323 (2018).
[53] K. Maeda, T. Sasaki, and M. Koashi, Nat. Commun. **10**, 3140 (2019).
[54] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, npj Quantum Inf. **7**, 22 (2021).
[55] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, Appl. Phys. B **122**, 96 (2016).
[56] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, Quantum Sci. Technol. **3**, 034002 (2018).
[57] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, Phys. Rev. A **99**, 052330 (2019).
[58] K. Azuma, A. Mizutani, and H.-K. Lo, Nat. Commun. **7**, 13523 (2016).
[59] L. Rigovacca, G. Kato, S. Bäuml, M. Kim, W. J. Munro, and K. Azuma, New J. Phys. **20**, 013033 (2018).
[60] S. Pirandola, Commun. Phys. **2**, 51 (2019).
[61] K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li, AVS Quantum Science **3**, 014101 (2021).
[62] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).
[63] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[64] P. Badziąg, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **62**, 012311 (2000).

[65] E. M. Rains, Phys. Rev. A **60**, 179 (1999).

[66] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[67] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[68] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).

[69] M. Koashi, F. Takenaga, T. Yamamoto, and N. Imoto, arXiv:0709.3196.

[70] E. Chitambar and R. Duan, Phys. Rev. Lett. **103**, 110502 (2009).

[71] M. Koashi, K. Azuma, S. Nakamura, and N. Imoto, arXiv:1303.1269.

[72] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).

[73] M. Curty, K. Azuma, and H.-K. Lo, Phys. Today **74** (3), 36 (2021).