PHYSICAL REVIEW A **85**, 060303(R) (2012)

Optimal entanglement manipulation via coherent-state transmission

Koji Azuma[1,*] and Go Kato[2,†]

[1]*NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[2]*NTT Communication Science Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

(Received 8 August 2011; published 26 June 2012)

We derive an optimal bound for arbitrary entanglement manipulation based on the transmission of a pulse in coherent states over a lossy channel followed by local operations and unlimited classical communication (LOCC). This stands on a theorem to reduce LOCC via a local unital qubit channel to local filtering. We also present an optimal protocol based on beam splitters and a quantum nondemolition (QND) measurement on photons. Even if we replace the QND measurement with photon detectors, the protocol can achieve near-optimal performance, outperforming known entanglement generation schemes.

DOI: 10.1103/PhysRevA.85.060303 PACS number(s): 03.67.Hk, 03.65.Ud, 03.67.Bg, 03.67.Mn

Entanglement is now well known as an essential resource for quantum communication [1] despite its being found in an attempt to point out a paradoxical nature of quantum mechanics [2]. In fact, it is known that any quantum communication [including quantum key distribution (in the sense of Ref. [3])] can never be accomplished by distant parties who are not capable of sharing entangled pairs. This implies the importance of evaluating the potential to share entanglement through a given communication channel, which determines its value as a quantum channel. If we look at practical quantum communication such as fiber-based quantum key distribution, free-space quantum communication, entanglement generation in quantum repeaters, quantum communication via superconducting transmission lines, and a quantum memory for bosons (transmission in time), we become aware that all the protocols rely on a lossy bosonic channel. Thus, quantum communication based on this channel is practically the most important class (cf. [4]).

One of the most fundamental protocols in this class is the family of coherent-state-based protocols represented by Bennett's quantum key distribution (called B92 QKD) [5] and entanglement generation protocols in quantum repeaters [6–11]. These protocols are based on the transmission of a pulse in coherent states over a lossy channel, and they are dominated by the following paradigm: (i) A sender prepares an entangled state composed of computational basis states of a qubit A and coherent states of a pulse a. (ii) The sender then sends the pulse a to the mode b at the receiver's site through a lossy channel. (iii) Then, the sender and the receiver manipulate the shared system Ab through their local operations and unlimited two-way classical communication (LOCC) in order to convert the initial entangled state to a more entangled state. Since entanglement does not increase on average under LOCC from its definition, in order to increase entanglement at step (iii), the sender and the receiver need to take a risk of failure of their LOCC manipulation. Hence, the potential of the coherent-state-based protocols is determined by optimizing the LOCC manipulation for obtaining more entanglement for a fixed failure probability, representing the latent ability of the initial entanglement itself. But, the analysis for such an "entanglement manipulation" for a single entangled pair Ab in a mixed state has remained a long-standing open problem, in contrast to that for pure-state inputs [12]. In addition, the LOCC manipulation is beyond the paradigms in Refs. [8,10,13]. Therefore, grasping the potential of such coherent-state-based protocols must be a key step in the practical and theoretical evolution of quantum communication.

In this paper, we present a theoretical limit of the performance of arbitrary coherent-state-based protocols, as well as a simple protocol that achieves the limit. Since even arbitrary LOCC follows this bound, the limit corresponds to a single-shot distillable entanglement of the initial one prepared via coherent-state transmission, bounding all types of quantum communication regarded as an entanglement manipulation (such as B92 QKD). The derivation of the bound is based on a general proposition to reduce LOCC manipulation via a local unital qubit channel to local filtering. The derived limit is represented in terms of the total success probability and an average entanglement monotone [14] of the generated entangled states, and it is determined only by the transmittance of the channel. The bound is shown to be accomplished by a simple protocol composed only of beam splitters and a quantum nondemolition (QND) measurement [15] on photons. If we substitute photon detectors for the QND measurement, the protocol can entangle distant qubits with near-optimal performance, which is shown to outperform known protocols [6–10]. Since these protocols are simple as in Fig. 1(a) but comparable to any complicated LOCC, the protocols will play important roles in constructing various quantum communication schemes.

Coherent-state-based protocols. We start by defining the protocols considered here: (A-i) A sender called Alice prepares a qubit A and a pulse a in her desired state in the form of $\sum_{j=0,1} e^{i\Theta_j}\sqrt{q_j}|j\rangle_A|\alpha_j\rangle_a$ for a computational basis $\{|j\rangle_A\}_{j=0,1}$, coherent states $\{|\alpha_j\rangle_a\}_{j=0,1}$, real parameters Θ_j, and $q_j \geqslant 0$ with $\sum_{j=0,1} q_j = 1$; (A-ii) Alice sends the pulse a to a receiver called Bob, through a lossy channel described by an isometry $|\alpha\rangle_a \to |\sqrt{T}\alpha\rangle_b|\sqrt{1-T}\alpha\rangle_e$, where T is the transmittance, b is a mode at Bob's place, and e is the environment; (A-iii) then, Alice and Bob manipulate the system Ab through LOCC to obtain an entangled state $\hat{\tau}_k^{A'B}$ between Alice's system A' and Bob's system B, and declare

*azuma.koji@lab.ntt.co.jp
†kato.go@lab.ntt.co.jp

whether they obtain a success outcome k occurring with a probability p_k or a failure outcome. Note that the output systems $A'B$ are not limited to qubits [16]. In what follows, the set of all the success events k is denoted by $\mathcal{S}$.

As a measure of the performance of the protocols, we take the total success probability, i.e., $P_s = \sum_{k\in\mathcal{S}} p_k$. We also need to choose an entanglement measure for estimating the value of the obtained entangled states $\{\hat{\tau}_k^{A'B}\}_{k\in\mathcal{S}}$. Since the output system $A'B$ has no restrictions, in contrast to those described in Refs. [8,10,13], the singlet fraction may be unsuitable. Thus, we take an entanglement monotone E applicable to any bipartite system $A'B$, which does not increase, on average, under any local pure operation and is convex [14]. In addition, here we require it to be a convex monotonically nondecreasing function of the concurrence C [17] at least for qubits, which is satisfied by various entanglement measures (cf. [18]). Based on such an E, as another measure of the protocols, we adopt the average $\bar{E}$ of the obtained entangled states $\{\hat{\tau}_k^{A'B}\}_{k\in\mathcal{S}}$, namely, $\bar{E} = [\sum_{k\in\mathcal{S}} p_k E(\hat{\tau}_k^{A'B})]/P_s$. We also allow Alice and Bob to switch among two or more protocols probabilistically. This corresponds [13] to taking the convex hull of achievable points $(P_s, P_s\bar{E})$.

Virtual protocol. For an actual protocol, we define the virtual protocol [10] that works in the same way as the actual protocol but simplifies the analysis significantly. Steps (A-i) and (A-ii) indicate that when the pulse arrives at Bob's site, the state of the total system Abe is written in the form $|\psi\rangle_{Abe} = \sum_{j=0,1} \sqrt{q_j}|j\rangle_A|u_j\rangle_b|v_j\rangle_e$ for states $\{|u_j\rangle\}_{j=0,1}$ and $\{|v_j\rangle\}_{j=0,1}$ with $|\langle u_1|u_0\rangle|^{1-T} = |\langle v_1|v_0\rangle|^T > 0$. Thus, for a state

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

with $2\xi := \arg[\langle v_1|v_0\rangle]$, and for a phase-flip channel

$$\Lambda_u^A(\hat{\rho}) := \frac{1+u^{\frac{1-T}{T}}}{2}\hat{\rho} + \frac{1-u^{\frac{1-T}{T}}}{2}\hat{Z}^A\hat{\rho}\hat{Z}^A, \tag{2}$$

with $\hat{Z}^A := |0\rangle\langle 0|_A - |1\rangle\langle 1|_A$, we have $\mathrm{Tr}_e[|\psi\rangle\langle\psi|_{Abe}] = \Lambda^A_{|\langle u_1|u_0\rangle|}(|\psi'\rangle\langle\psi'|_{Ab})$. Hence, we can consider any protocol to have the following sequence: (V-i) System Ab is prepared in $|\psi'\rangle_{Ab}$; (V-ii) $\Lambda^A_{|\langle u_1|u_0\rangle|}$ is applied on qubit A; (V-iii) Alice and Bob perform an LOCC, which provides $\hat{\tau}_k^{A'B}$. We call this sequence "the virtual protocol." We next introduce a proposition that enables us to derive an optimal bound in more general settings.

Proposition. Let $(P_s, \bar{E})$ be the performance of an LOCC protocol starting with qubits AB in state $\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB})$, where $\mathcal{E}^A$ is a random local unitary channel [19] defined by $\mathcal{E}^A(\hat{\rho}^{AB}) := \sum_l q_l \hat{U}_l^A\hat{\rho}^{AB}\hat{U}_l^{A\dagger}$. Then, there is a protocol that is not less efficient than $(P_s, \bar{E})$ but that is based only on Bob's measurement (cf. [20]). In addition, for Schmidt coefficients λ_0 and $\lambda_1(\leqslant\lambda_0)$ of $|\varphi\rangle_{AB}$, The performance $(P_s, \bar{E})$ must be in the region of $\{(P_s, \bar{E}) \mid 0 \leqslant P_s \leqslant 1, 0 \leqslant \bar{E} \leqslant E(C^{\max}(P_s))\}$ with $C^{\max}(P_s) := (2\sqrt{\lambda_0\lambda_1})^{-1}C(\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB}))$ for $P_s < 2\lambda_1$ and $C^{\max}(P_s) := P_s^{-1}\sqrt{(P_s-\lambda_1)/\lambda_0}C(\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB}))$ for $P_s \geqslant 2\lambda_1$.

Proof. Let Kraus operators $\{\hat{M}_k^A \otimes \hat{N}_k^B\}_{k\in\mathcal{S}}$ be Alice and Bob's successful measurement in step (V-iii), where the index k refers to a branch of the tree of all possible outcomes of their LOCC operation. Without loss of generality, the input spaces of $\hat{M}_k^A$ and $\hat{N}_k^B$ can be assumed to be qubit spaces. If Alice and Bob can achieve the measurement $\{\hat{M}_k^A \otimes \hat{N}_k^B\}_{k\in\mathcal{S}}$, they can always, in principle, obtain a state $\hat{\tau}_k^{AB} := (\hat{M}_k^A \otimes \hat{N}_k^B)\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB})(\hat{M}_k^A \otimes \hat{N}_k^B)^\dagger/p_k$. From the convexity of the entanglement monotone E [14], the performance of this protocol based on local pure operations is not less than protocols where, for a set $\mathcal{S}' \subset \mathcal{S}$, they provide a mixture of the states $(\sum_{k\in\mathcal{S}'} p_k\hat{\tau}_k^{AB})/(\sum_{k\in\mathcal{S}'} p_k)$ instead of states $\{\hat{\tau}_k^{AB}\}_{k\in\mathcal{S}'}$. Thus, we can assume that Alice and Bob return the state $\hat{\tau}_k^{AB}$ with probability p_k. Note that the range of $\hat{\tau}_k^{AB}$ can be assumed to be qubit spaces.

For fixed $\hat{U}_l^A$ and branch k, by applying Proposition 1 in Ref. [21] to every round of Alice with retaining the causality of the branch [22], we can compose unitary operators $\{\hat{V}_{k|l}^A\}_k$ and Kraus operators $\{\hat{O}_{k|l}^B\}_k$ that satisfy

$$\left(\hat{M}_k^A\hat{U}_l^A \otimes \hat{N}_k^B\right)|\varphi\rangle_{AB} = \left(\hat{V}_{k|l}^A\hat{U}_l^A \otimes \hat{O}_{k|l}^B\right)|\varphi\rangle_{AB}, \tag{3}$$

with $d_k := \det(\hat{M}_k^{A\dagger}\hat{M}_k^A)\det(\hat{N}_k^{B\dagger}\hat{N}_k^B) = \det(\hat{O}_{k|l}^{B\dagger}\hat{O}_{k|l}^B)$. On the other hand, using the formula in [17], we can show that the concurrence C for the state $\hat{\tau}_k^{AB}$ is described by $p_kC(\hat{\tau}_k^{AB}) = \sqrt{d_k}C(\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB}))$. Thus, if Bob performs $\{\hat{O}_{k|l}^B\}_k$, he obtains a state $\hat{\tau}_{k|l}^{AB} := \hat{O}_{k|l}^B\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB})\hat{O}_{k|l}^{B\dagger}/p_{k|l}$ with probability $p_{k|l} := \langle\varphi|\hat{O}_{k|l}^{B\dagger}\hat{O}_{k|l}^B|\varphi\rangle$ and concurrence $C(\hat{\tau}_{k|l}^{AB}) = \sqrt{d_k}C(\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB}))/p_{k|l} = p_kC(\hat{\tau}_k^{AB})/p_{k|l}$. Since $\sum_l q_l p_{k|l} = p_k$ holds from Eq. (3) and $\sum_l q_l p_{k|l}E(\hat{\tau}_{k|l}^{AB}) \geqslant p_kE(\hat{\tau}_k^{AB})$ is implied by $\sum_l q_l p_{k|l}C(\hat{\tau}_{k|l}^{AB}) = p_kC(\hat{\tau}_k^{AB})$ and the convexity of $E(C)$, the original LOCC protocol is concluded to be outperformed by a protocol that performs only Bob's measurement $\{\hat{O}_{k|l}^B\}_k$ with probability q_l and returns k and l as the outcome.

Thus, we focus on a protocol that is based on Bob's measurement $\{\hat{O}_k^B\}_k$ and returns state $\hat{\rho}_k^{AB} := \hat{O}_k^B\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB})\hat{O}_k^{B\dagger}/p_k$ with probability p_k. We note that there are Kraus operators $\hat{\Omega}^B$ and $\{\hat{L}_k^B\}_{k\in\mathcal{S}}$ satisfying $\hat{L}_k^B\hat{\Omega}^B = \hat{O}_k^B$. In fact, if we define them as $\hat{\Omega}^B := (\sum_{k\in\mathcal{S}} \hat{O}_k^{B\dagger}\hat{O}_k^B)^{1/2}$ and $\hat{L}_k^B := \hat{O}_k^B(\hat{\Omega}^B)^{-1}$, where $\hat{\Omega}^{-1}$ is the inverse of $\hat{\Omega}$ in its range, the operators satisfy $\hat{\Omega}^{B\dagger}\hat{\Omega}^B \leqslant \hat{1}^B$ and $\sum_{k\in\mathcal{S}} \hat{L}_k^{B\dagger}\hat{L}_k^B \leqslant \hat{1}^B$ from $\sum_{k\in\mathcal{S}} \hat{O}_k^{B\dagger}\hat{O}_k^B \leqslant \hat{1}^B$. Hence, we can regard Bob's measurement $\{\hat{O}_k^B\}_k$ as a sequential measurement of $\hat{\Omega}^B$ followed by $\{\hat{L}_k^B\}_{k\in\mathcal{S}}$. On the other hand, the entanglement monotone E of the state $\hat{\tau}_s^{AB} := \hat{\Omega}^B\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB})\hat{\Omega}^B/P_s$ with $P_s = \sum_{k\in\mathcal{S}} p_k$ is not less than $[\sum_{k\in\mathcal{S}} p_kE(\hat{\rho}_k^{AB})]/P_s$, because the entanglement monotone E does not increase through a local operation on average [14]. Therefore, we can assume that Bob merely applies a filter $\hat{\Omega}^B$ to qubits AB.

Let us proceed to the optimization of $(P_s, E(\hat{\tau}_s^{AB}))$ over the filter $\hat{\Omega}^B$. From the monotonicity of $E(C)$, our attention is concentrated on the maximization of $C(\hat{\tau}_s^{AB})$ for a fixed P_s. On the other hand, for the Schmidt decomposition of $|\varphi\rangle_{AB} = \sum_{j=0,1}\sqrt{\lambda_j}|jj\rangle_{AB}$, we have $P_s = \langle\varphi|\hat{\Omega}^{B\dagger}\hat{\Omega}^B|\varphi\rangle = \sum_{j=0,1}\lambda_j\langle j|\hat{\Omega}^{B\dagger}\hat{\Omega}^B|j\rangle$ and $P_sC(\hat{\tau}_s^{AB}) = [\det(\hat{\Omega}^{B\dagger}\hat{\Omega}^B)]^{1/2}C(\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB})) \leqslant (\Pi_{j=0,1}\langle j|\hat{\Omega}^{B\dagger}\hat{\Omega}^B|j\rangle)^{1/2}C(\mathcal{E}^A(|\varphi\rangle\langle\varphi|_{AB}))$, where the equalities hold by choosing $\hat{\Omega}^B$ with $\langle 0|\hat{\Omega}^{B\dagger}\hat{\Omega}^B|1\rangle = 0$. Combined with

$\hat{\Omega}^{B\dagger}\hat{\Omega}^{B} \leqslant \hat{1}^{B}$, this shows that $C^{\max}(P_s)$ is the maximum of $C(\hat{\tau}_s^{AB})$, which concludes the proposition.

Optimal bound. Let us apply the proposition to our problem. Schmidt coefficients of $|\psi'\rangle_{Ab}$ are $\lambda_{\pm} := [1 \pm \sqrt{1-x^2}]/2$, and the concurrence of the input state is $C(\Lambda^{A}_{|\langle u_1|u_0\rangle|}(|\psi'\rangle\langle\psi'|_{Ab})) = |\langle u_1|u_0\rangle|^{\frac{1-T}{T}}x$ from Ref. [23], where $x := 2\sqrt{q_0 q_1(1-|\langle u_1|u_0\rangle|^2)}$. Hence, $C^{\max}(P_s) = |\langle u_1|u_0\rangle|^{\frac{1-T}{T}}$ for $P_s < 1-\sqrt{1-x^2}$ and $C^{\max}(P_s) = P_s^{-1}|\langle u_1|u_0\rangle|^{\frac{1-T}{T}}x[1-2(1-P_s)/(1+\sqrt{1-x^2})]^{1/2}$ for $P_s \geqslant 1-\sqrt{1-x^2}$. Since $C^{\max}(P_s)$ is a monotonically nondecreasing function of x, the choice of $q_0 = q_1 = 1/2$ gives the maximum value of $C^{\max}(P_s)$, which is further bounded by an achievable concurrence $C^{\rm opt}_{u^*}(P_s)$ with

$$C^{\rm opt}_{u}(P_s) := \frac{u^{\frac{1-T}{T}}\sqrt{(1-u)(2P_s+u-1)}}{P_s} \tag{4}$$

for

$$u^* := \tfrac{1}{2}\big[(1-P_s)(2-T) + \sqrt{4P_s^2(1-T)+(1-P_s)^2T^2}\big], \tag{5}$$

satisfying $1-P_s \leqslant u^* \leqslant 1$. Therefore, the performance of any protocol must be in the convex hull of $\{(P_s, P_s\bar{E}) \mid 0 \leqslant P_s \leqslant 1, 0 \leqslant \bar{E} \leqslant E(C^{\rm opt}_{u^*}(P_s))\}$.

Optimal protocol. We have shown that the achievable region of an arbitrary protocol is described by Eqs. (4) and (5). Here we present a specific protocol achieving the optimal bound $C^{\rm opt}_{u^*}(P_s)$ except for a trivial point $P_s = 1$. We allow Alice and Bob to use an implementable [7] interaction between an off-resonance laser pulse in a coherent state $|\alpha\rangle_a$ and a matter qubit A, which is described by a unitary operation $\hat{U}_\theta|j\rangle_A|\alpha\rangle_a = |j\rangle_A|\alpha e^{i(-1)^j\theta/2}\rangle_a$ for $j = 0,1$. θ depends on the strength of the interaction ($\theta \sim 0.01$ [7]). Let us consider the following protocol [see Fig. 1 (a)]: (1) Alice makes a probe pulse in a coherent state $|\alpha/\sqrt{T}\rangle_a$ ($\alpha \geqslant 0$) interact with her qubit A in a state $(\sum_{j=0,1} e^{-i(-1)^j\zeta_{\alpha/\sqrt{T}}}|j\rangle_A)/\sqrt{2}$ with $\zeta_\alpha := (1/2)\alpha^2\sin\theta$ by $\hat{U}_\theta$, and she applies a displacement operation $\hat{D}_{-(\alpha/\sqrt{T})\cos(\theta/2)}$ to the pulse a; (2) Alice sends the pulse to Bob through a lossy channel $a \to b_1$ (with transmittance T) together with the local oscillator (LO); (3) on receiving the pulse b_1 and the LO, Bob generates a second probe pulse b_2 in a coherent state $|\beta\rangle_{b_2}$ with $\beta \geqslant \alpha$ from the LO, and he makes the pulse b_2 interact with his qubit B in state $(\sum_{j=0,1} e^{-i(-1)^j\zeta_\beta}|j\rangle_B)/\sqrt{2}$ by $\hat{U}_\theta$; (4) Bob applies a displacement operation $\hat{D}_{-\beta\cos(\theta/2)}$ to the pulse b_2; (5) Bob further applies a 50:50 beam splitter described by $|\alpha_1\rangle_{b_1}|\alpha_2\rangle_{b_2} \to |(\alpha_1+\alpha_2)/\sqrt{2}\rangle_{b_3}|(\alpha_1-\alpha_2)/\sqrt{2}\rangle_{b_4}$ to the pulses in modes b_1 and b_2; (6) Bob applies a QND measurement to pulses b_3 and b_4 in order to execute a projective measurement $\{\hat{Q}_s^{b_3b_4}, \hat{1}^{b_3b_4} - \hat{Q}_s^{b_3b_4}\}$ with $\hat{Q}_s^{b_3b_4} := \hat{1}^{b_3b_4} - \sum_{n=0}^{\infty}|n\rangle\langle n|_{b_3}\otimes|n\rangle\langle n|_{b_4}$; (7) if Bob receives an outcome corresponding to the projection $\hat{Q}_s^{b_3b_4}$, Bob declares the success of the protocol.

In the virtual protocol for this scheme, since Bob's operations in steps (3)–(7) commute with the phase-flip channel $\Lambda^{A}_{|\langle u_1|u_0\rangle|}$, the operations are assumed to be directly applied to the state $|\psi'\rangle_{Ab}$. In this frame, the state after step (5) is

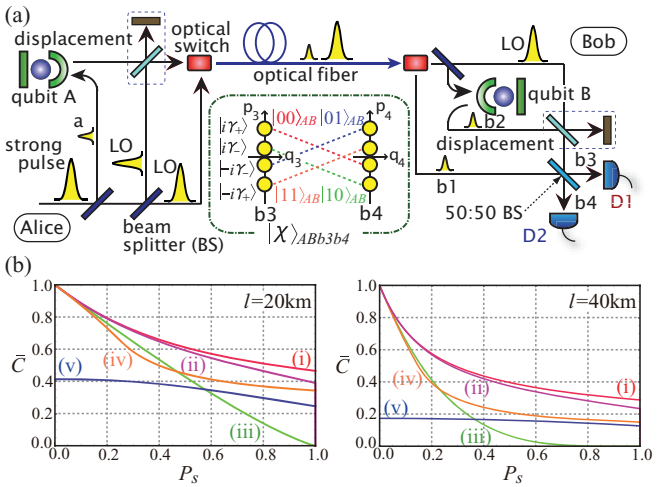

FIG. 1. (Color online) (a) Schematic of near-optimal protocol. If we replace the photon detectors D1 and D2 with the QND measurement to perform the projection $\hat{Q}_s^{b_3b_4}$, we can reduce the protocol to the optimal one. (b) Performance of various protocols. The average concurrence $\bar{C}$ as a function of the success probability P_s when $T = e^{-l/l_0}$ with $l_0 = 25$ km (~ 0.17 dB/km attenuation) and $\theta = 0.01$, for (i) the optimal protocol, (ii) the near-optimal protocol, (iii) a photon-detector-based two-probe protocol [10] that achieves a tight bound [13] for single-error-type entanglement generation, (iv) an optimized photon-detector-based single-probe protocol [8,9], and (v) a homodyne-detection-based single-probe protocol [7].

described by

$$\begin{aligned}|\chi\rangle_{ABb_3b_4} = \tfrac{1}{2}[&|00\rangle_{AB}|i\gamma_+\rangle_{b_3}|-i\gamma_-\rangle_{b_4}\\ &+|01\rangle_{AB}|-i\gamma_-\rangle_{b_3}|i\gamma_+\rangle_{b_4}+|10\rangle_{AB}|i\gamma_-\rangle_{b_3}|-i\gamma_+\rangle_{b_4}\\ &+|11\rangle_{AB}|-i\gamma_+\rangle_{b_3}|i\gamma_-\rangle_{b_4}],\end{aligned} \tag{6}$$

with $\gamma_\pm := [(\beta \pm \alpha)\sin(\theta/2)]/\sqrt{2}$. This state can be represented, in the respective phase spaces of modes b_3 and b_4, by $|\chi\rangle_{ABb_3b_4}$ in Fig. 1(a). This figure suggests an intuitive reason why this protocol can generate entanglement between qubits AB: If there are more photons in mode b_3 (b_4) than in mode b_4 (b_3), the possibility that the state has lived in the subspace spanned by $\{|00\rangle_{AB}, |11\rangle_{AB}\}$ ($\{|01\rangle_{AB}, |10\rangle_{AB}\}$) is higher. A direct calculation shows $||_A\langle j|\hat{Q}_s^{b_3b_4}|\chi\rangle_{ABb_3b_4}||^2 = [1-e^{-\gamma_+^2-\gamma_-^2}I_0(2\gamma_+\gamma_-)]/2$ for $j = 0,1$ and ${}_{ABb_3b_4}\langle\chi|(|1\rangle\langle 0|_A \otimes \hat{Q}_s^{b_3b_4})|\chi\rangle_{ABb_3b_4} = [e^{-(\gamma_+-\gamma_-)^2} - e^{-\gamma_+^2-\gamma_-^2}I_0(2\gamma_+\gamma_-)]/2$, where $I_0(x) := \sum_{n=0}^{\infty}(x/2)^{2n}/(n!)^2$ is a modified Bessel function. Thus, the success probability P_s is

$$P_s = 1 - e^{-(\beta^2+\alpha^2)\sin^2(\theta/2)}I_0((\beta^2-\alpha^2)\sin^2(\theta/2)). \tag{7}$$

Combined with the fact that the final state is written $\Lambda^{A}_{u_\alpha}(|\phi\rangle\langle\phi|_{ABb_3b_4})$ with $|\phi\rangle_{ABb_3b_4} := \hat{Q}_s^{b_3b_4}|\chi\rangle_{ABb_3b_4}/\sqrt{P_s}$ and $u_\alpha := e^{-2\alpha^2\sin^2(\theta/2)}$, the calculation results also show that the concurrence C between A and Bb_3b_4 satisfies $C(\Lambda^{A}_{u_\alpha}(|\phi\rangle\langle\phi|_{ABb_3b_4})) = C^{\rm opt}_{u_\alpha}(P_s)$ from Ref. [23]. On the other hand, for any α and P satisfying $1-u_\alpha \leqslant P < 1$, there is a choice of β for making $P_s = P$ hold. Hence, fixing $P_s = P$, we can choose α such that u_α is equivalent to u^* of Eq. (5). Thus, the present protocol attains the optimal performance $C^{\rm opt}_{u^*}(P_s)$.

Near-optimal protocol. We have shown that a protocol employing the QND measurement on incoming pulses can optimally generate entanglement between Alice's qubit A and Bob's entire system Bb_3b_4 including pulses b_3b_4. However, in practice, it is difficult to achieve such a QND measurement, and the pulses b_3b_4 are unsuitable for storing the entangled state for a long time. Therefore, it is important to find a protocol that does not need to use a QND measurement and produces entanglement between Alice and Bob's qubits AB instead of A and Bb_3b_4. One such protocol can be obtained by replacing steps (6) and (7) in the optimal protocol with the following steps [see Fig. 1 (a)]: (6′) Bob counts the number of photons by using photon-number-resolving detectors in modes b_3 and b_4, respectively, and (7′) if the outcomes m and n of the two detectors are different, Bob declares the success of the protocol. Note that the significant recent progress [24] of photon detector technologies is allowing us to use photon-number-resolving detectors. However, the usage of the photon-number-resolving detectors assumed here is only for simplicity. That is, our protocol works even if we replace those detectors with more realistic ones such as threshold detectors, as seen in Ref. [10].

Let us consider the modified protocol. From the definition, the success probability P_s must be the same as Eq. (7). In the virtual protocol for this scheme, with probability $P_{mn} := e^{-\gamma_+^2-\gamma_-^2}(\gamma_+^{2m}\gamma_-^{2n} + \gamma_-^{2m}\gamma_+^{2n})/(2m!n!)$, the protocol returns outcomes m and n, and provides a final state $\Lambda^A_{u_\alpha}(|\phi_{mn}\rangle\langle\phi_{mn}|_{AB})$ for state $|\phi_{mn}\rangle_{AB} := {}_{b_3}\langle m|_{b_4}\langle n||\chi\rangle_{ABb_3b_4}/\sqrt{P_{mn}}$ with concurrence $C(\Lambda^A_{u_\alpha}(|\phi_{mn}\rangle\langle\phi_{mn}|_{AB})) = u_\alpha^{\frac{1-T}{T}} e^{-\gamma_+^2-\gamma_-^2}|\gamma_+^{2m}\gamma_-^{2n} - \gamma_-^{2m}\gamma_+^{2n}|/(2m!n!P_{mn})$ from Ref. [23]. Hence, for an entanglement monotone E with $E(C)$, the average of the entanglement monotones is determined by $\bar{E} = [\sum_{m,n\geqslant 0}(1-\delta_{mn})\, P_{mn} E(C(\Lambda^A_{u_\alpha}(|\phi_{mn}\rangle\langle\phi_{mn}|_{AB})))]/P_s$. Parameters α and β (determining $\gamma_\pm$) should be chosen to maximize $\bar{E}$ with P_s fixed.

In Fig. 1(b), we show the performance of several known protocols [7–10] as well as the optimal and near-optimal protocols in terms of the average concurrence $\bar{C}$. For comparison, we assume that all the devices used in the protocols are ideal. From the figures, we can confirm that the near-optimal protocol performs similarly to the optimal protocol and it outperforms the existing protocols [6–10]. Such a superiority of our protocol remains even if we assume the usage of more realistic photon detectors. Through the relation $E = E(C)$ for qubits, one could also easily estimate the performance even in terms of the entanglement monotone E.

In conclusion, we have provided an optimal bound $E(C^{\rm opt}_{u^*}(P_s))$ defined by Eqs. (4) and (5) for arbitrary LOCC entanglement manipulation via coherent-state transmission. In addition, we have presented a simple optimal scheme and its practical version [Fig. 1(a)] with almost optimal performance. This suggests that quantum optical devices in quantum communication can become as powerful as arbitrary operations for distilling entanglement from the state prepared via coherent-state transmission. The setting of the problem respects a shared nature of known realistic schemes [5–11], but we believe that our solution to the problem will provide new insights into fundamental theories such as those in Refs. [4,12,17,21] and into limits on other quantum communication protocols as in Refs. [25,26].

We thank M. Koashi, who pointed out the possibility of simplifying the proof of our proposition, W. J. Munro, M. Owari, and K. Tamaki, whose comments helped us to improve this paper, and K. Igeta, N. Matsuda, F. Morikoshi, N. Sota, and Y. Tokura for helpful discussions. K.A. is supported by a MEXT Grant-in-Aid for Scientific Research on Innovative Areas 21102008.

[1] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] M. M. Wolf, D. Pérez-García, and G. Giedke, Phys. Rev. Lett. **98**, 130501 (2007).
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] L. Childress, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).
[7] P. van Loock *et al.*, Phys. Rev. Lett. **96**, 240501 (2006).
[8] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).
[9] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, Phys. Rev. Lett. **101**, 040502 (2008).
[10] K. Azuma *et al.*, Phys. Rev. A **80**, 060303(R) (2009).
[11] K. Azuma, H. Takeda, M. Koashi, and N. Imoto, Phys. Rev. A **85**, 062309 (2012).
[12] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999); G. Vidal, *ibid.* **83**, 1046 (1999); D. Jonathan and M. B. Plenio, *ibid.* **83**, 1455 (1999).
[13] K. Azuma, N. Sota, M. Koashi, and N. Imoto, Phys. Rev. A **81**, 022325 (2010).
[14] G. Vidal, J. Mod. Opt. **47**, 355 (2000); M. Horodecki, Quantum Inf. Comput. **1**, 3 (2001).
[15] V. B. Branginsky, Y. I. Vorontosov, and K. S. Thorne, Science **209**, 547 (1980).
[16] Even if a system includes an observable with a continuous spectrum, the measurement outcomes from the system can be regarded as discrete by dividing the spectrum into intervals, and the following proof for an optimal bound is valid as long as we can take a proper entanglement monotone applicable to infinite dimensional systems.
[17] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[18] The entanglement of formation, the geometric measure of entanglement, the Bures measure of entanglement, and the Groverian measure of entanglement are examples of such an entanglement monotone E [cf. A. Streltsov, H. Kampermann, and D. Bruß, New J. Phys. **12**, 123004 (2010)].
[19] Random unitary channels on a qubit are equivalent to unital qubit channels. See M. Gregoratti and R. F. Werner, J. Mod. Opt. **50**, 915 (2003).

[20] In this proposition, Bob can be regarded as a sender who prepares qubits AB in a state $|\varphi\rangle_{AB}$ and sends qubit A to Alice through a unital qubit channel $\mathcal{E}^A$. In this regard, since Bob's measurement merely corresponds to a modification of the prepared state $|\varphi\rangle_{AB}$, this proposition implies that his state preparation is rather important.

[21] H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).

[22] Suppose that the state $\hat{U}_l^A|\varphi\rangle_{AB}$ becomes $|\varphi_{k_1,\ldots,k_{2n}|l}\rangle_{AB}$ for the measurement outcomes $k_1,\ldots,k_{2n}$ at the $2n$-th round, and Alice applies a Kraus operator $\hat{M}^A_{k_{2n+1}|k_1,\ldots,k_{2n}}$ at the $(2n+1)$-th round. Then, Proposition 1 in Ref. [21] presents a Kraus operator $\hat{O}^B_{k_{2n+1}|l,k_1,\ldots,k_{2n}}$ and a unitary operator $\hat{V}^A_{k_{2n+1}|l,k_1,\ldots,k_{2n}}$ such that $\hat{M}^A_{k_{2n+1}|k_1,\ldots,k_{2n}}|\varphi_{k_1,\ldots,k_{2n}|l}\rangle_{AB} = \hat{V}^A_{k_{2n+1}|l,k_1,\ldots,k_{2n}}\hat{O}^B_{k_{2n+1}|l,k_1,\ldots,k_{2n}}|\varphi_{k_1,\ldots,k_{2n}|l}\rangle_{AB}$, which holds for every round of Alice. We can thus define $\hat{O}^B_{k|l} := \cdots \hat{N}^B_{k_4|k_1,k_2,k_3}\hat{O}^B_{k_3|l,k_1,k_2}\hat{N}^B_{k_2|k_1}\hat{O}^B_{k_1|l}$.

[23] If we input $|\omega\rangle_{AB} = \sum_{j=0,1}\sqrt{p_j}|j\rangle_A|\phi_j\rangle_B$ to a phase flip channel $\Lambda^A(\hat{\rho}) := f\hat{\rho} + (1-f)\hat{Z}^A\hat{\rho}\hat{Z}^A$ with $1/2 \leqslant f \leqslant 1$, the concurrence C of the output state $\Lambda^A(|\omega\rangle\langle\omega|_{AB})$ is $2(2f-1)\sqrt{p_0p_1(1-|\langle\phi_1|\phi_0\rangle|^2)}$ from the formula in [17].

[24] R. H. Hadfield, Nat. Photon. **3**, 696 (2009).

[25] L. Praxmeyer and P. van Loock, Phys. Rev. A **81**, 060303(R) (2010).

[26] N. Sangouard *et al.*, Rev. Mod. Phys. **83**, 33 (2011).