Quantum repeaters and computation by a single module: Remote nondestructive parity measurement

Koji Azuma,[1,2,*] Hitoshi Takeda,[2] Masato Koashi,[2,3] and Nobuyuki Imoto[2]

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

[2]*Department of Materials Engineering Science, Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan*

[3]*Photon Science Center, The University of Tokyo, Hongo, Tokyo 113-8656, Japan*

(Received 10 June 2010; revised manuscript received 7 May 2012; published 12 June 2012)

We introduce a simple photonic probing scheme of remote nondestructive parity measurement (RNPM) on a pair of matter qubits. The protocol works as a single module for key operations such as entanglement generation, Bell measurement, and parity check measurement, which are sufficient not only for building up a quantum repeater but also for equipping it with entanglement distillation. Moreover, the RNPM protocol can also be used for generating cluster states toward measurement-based quantum computation.

DOI: 10.1103/PhysRevA.85.062309 PACS number(s): 03.67.Hk, 03.67.Lx

I. INTRODUCTION

In quantum mechanics, measuring a property of a system may cause a backaction on its state, but sometimes a backaction can be useful for quantum information processing. A simple nontrivial example of such a measurement is the nondestructive parity (NP) measurement on two qubits AB, which is the projection measurement to the subspace with even parity spanned by $\{|00\rangle_{AB},|11\rangle_{AB}\}$ and to the odd one spanned by $\{|01\rangle_{AB},|10\rangle_{AB}\}$. When the qubits are in state $|\varphi\rangle_{AB}$ initially, the un-normalized postmeasurement state is ideally either $\hat{P}^{AB}_{\rm even}|\varphi\rangle_{AB}$ or $\hat{P}^{AB}_{\rm odd}|\varphi\rangle_{AB}$, where $\hat{P}^{AB}_{\rm even}$ ($\hat{P}^{AB}_{\rm odd}$) is the projection onto the even (odd) subspace. This measurement provides a powerful tool when the two qubits are quantum memories located far apart. For example, if we prepare each qubit in state $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$, the NP measurement leaves the pair in maximally entangled state (Bell state) $\sqrt{2}\hat{P}^{AB}_{\rm even}|{+}{+}\rangle_{AB} = |\Phi^{+}\rangle_{AB}$ or $\sqrt{2}\hat{P}^{AB}_{\rm odd}|{+}{+}\rangle_{AB} = |\Psi^{+}\rangle_{AB}$, where $|\Phi^{\pm}\rangle_{AB} := (|00\rangle_{AB} \pm |11\rangle_{AB})/\sqrt{2}$ and $|\Psi^{\pm}\rangle_{AB} := (|01\rangle_{AB} \pm |10\rangle_{AB})/\sqrt{2}$. Various other nontrivial operations are also derived from the NP measurement [see Figs. 1(d)–1(f) below].

In this paper, we provide a simple protocol to implement the NP measurement, which we call remote nondestructive parity measurement (RNPM) protocol. The protocol is based on an off-resonant coupling of light pulses with the quantum memories, and it works even if the quantum memories are distant. The deviation of the RNPM protocol from the ideal NP measurement mainly comes from the loss in the optical channel, whose transmission depends on its length L as $\eta_L := e^{-L/L_{\rm att}}$ with an attenuation length $L_{\rm att}$. This makes the RNPM protocol probabilistic and noisy, but these imperfections behave in a controlled way, even with the use of threshold detectors that cannot distinguish one from two or more photons. As a result, the RNPM protocol constitutes a viable module which can be singly used to build a quantum repeater, in contrast to the other known repeater protocols [1–14]. Moreover, the local use of highly efficient RNPM protocols will also allow us to generate cluster states even when they are located sparsely to make single-qubit addressing easier and to reduce decoherence, which helps implementation of measurement-based quantum computation.

This paper is organized as follows. In Sec. II, we introduce the RNPM protocol and prove its working principle. In Sec. III, we show the possibilities of the various applications of the RNPM protocol. Section IV concludes this paper.

II. RNPM PROTOCOL

The requirement on the memory qubit for the RNPM protocol is as follows. The qubit is assumed to allow us to apply phase flip $\hat{Z} := |0\rangle\langle 0| - |1\rangle\langle 1|$, Hadamard gate $\hat{H} := |+\rangle\langle 0| + |-\rangle\langle 1|$ with $|-\rangle := \hat{Z}|+\rangle$, and Z-basis measurement. The qubit is also assumed to interact with an off-resonant laser pulse a in a coherent state $|\alpha\rangle_a := e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}(\alpha^n/\sqrt{n!})|n\rangle_a$ according to a unitary operation $\hat{U}_\theta|j\rangle|\alpha\rangle_a = e^{-i(-1)^j\phi_\alpha/2}|j\rangle|\alpha e^{i(-1)^j\theta/2}\rangle_a$ ($j = 0,1$), where $\{|n\rangle_a\}$ are the number states of the mode a, $\phi_\alpha = \alpha^2\sin\theta$, and θ is a fixed parameter for the strength of the interaction. Since this interaction is an off-resonant coupling based on a basic Hamiltonian, Jaynes-Cummings Hamiltonian, it will be feasible with various qubits such as an individual Λ-type atom, a trapped ion, a single electron trapped in quantum dots, a nitrogen-vacancy (NV) center in a diamond with a nuclear spin degree of freedom, and a neutral donor impurity in semiconductors [6].

We now describe our RNPM protocol in detail. Suppose that the qubits A and B are respectively held by Alice and Bob, who are distance L_0 apart [see Fig. 1(a)]. Claire is located in between, connected to Alice and Bob with optical channels $a \to c_1$ and $b \to c_2$ with lengths $L_A(\leqslant L_0)$ and $L_B := L_0 - L_A$, respectively. Let $T_A := \tau\eta_{L_A}$ and $T_B := \tau\eta_{L_B}$ be the overall transmittance of the channels, where τ stands for the local loss. The RNPM protocol proceeds as follows. (i) Alice (Bob) prepares pulse a (pulse b) in a coherent state $|\alpha/\sqrt{T_A}\rangle_a$ ($|\alpha/\sqrt{T_B}\rangle_b$) with $\alpha \geqslant 0$, and lets it interact with qubit A (qubit B) by $\hat{U}_\theta$. (ii) Alice (Bob) sends Claire the pulse a (the pulse b) through the optical channel $a \to c_1$ ($b \to c_2$). (iii) On receiving the pulses c_1c_2, Claire makes

*azuma.koji@lab.ntt.co.jp

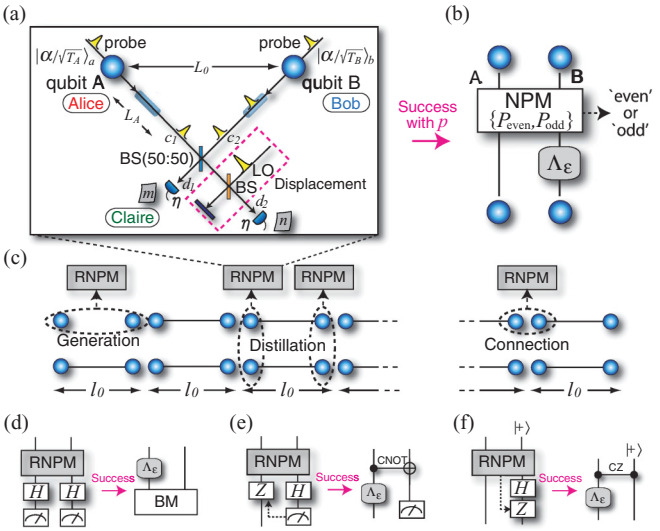

FIG. 1. (Color online) The RNPM protocol and its applications. (a) The RNPM protocol. (b) A circuit equivalent to the successful RNPM protocol, where a phase-flip channel $\Lambda_\epsilon(\hat{\rho}) := (1-\epsilon)\hat{\rho} + \epsilon\hat{Z}\hat{\rho}\hat{Z}$ with phase error probability ϵ is applied as the penalty of photon losses. ϵ may depend on the outcome returned by photon detectors. In the lossless limit, the RNPM protocol works as the ideal NP measurement. (c) Quantum repeaters based on the RNPM protocols. (d)–(f) Applications of the RNPM protocol: (d) Bell measurement (BM), (e) parity check measurement, and (f) a gate for extending one-dimensional cluster states, where the measurement instrument means Z-basis measurement and the dashed arrow implies the transmission of the measurement outcome.

the pulses interfere by a 50:50 beam splitter. (iv) On the mode receiving the constructive interference, Claire applies displacement operation $\hat{D}[-\sqrt{2}\alpha\cos(\theta/2)]$ by using a local oscillator (LO). (v) Claire counts photons of the output modes d_1d_2 by two photon detectors, and she announces the outcome (m,n). (vi) If $m+n$ is odd, Bob applies phase flip $\hat{Z}$ to qubit B. Events with $m>0$ and $n=0$ ($m=0$ and $n>0$) indicate outcome "odd" ("even"), which are regarded as the success events of this protocol.

To see the backactions in the success events, we use the fact that the RNPM protocol works equivalently if we omit step (iv) and replace step (i) with the following: (i′) After making pulse a (pulse b) in a coherent state $|\alpha/\sqrt{T_A}\rangle_a$ ($|\alpha/\sqrt{T_B}\rangle_b$) interact with qubit A (qubit B), Alice (Bob) applies displacement operation $\hat{D}[-(\alpha/\sqrt{T_A})\cos(\theta/2)]$ ($\hat{D}[-(\alpha/\sqrt{T_B})\cos(\theta/2)]$) on the pulse. In this protocol, through steps (i′)–(iii), qubits AB are transformed as

$$\begin{aligned}
|00\rangle_{AB} &\xrightarrow{\text{(i')}} |00\rangle_{AB}|i\beta_A\rangle_a|i\beta_B\rangle_b \to |00\rangle_{AB}|0\rangle_{d_1}|i\sqrt{2}\beta\rangle_{d_2},\\
|01\rangle_{AB} &\xrightarrow{\text{(i')}} |01\rangle_{AB}|i\beta_A\rangle_a|-i\beta_B\rangle_b \to |01\rangle_{AB}|-i\sqrt{2}\beta\rangle_{d_1}|0\rangle_{d_2},\\
|10\rangle_{AB} &\xrightarrow{\text{(i')}} |10\rangle_{AB}|-i\beta_A\rangle_a|i\beta_B\rangle_b \to |10\rangle_{AB}|i\sqrt{2}\beta\rangle_{d_1}|0\rangle_{d_2},\\
|11\rangle_{AB} &\xrightarrow{\text{(i')}} |11\rangle_{AB}|-i\beta_A\rangle_a|-i\beta_B\rangle_b \to |11\rangle_{AB}|0\rangle_{d_1}|-i\sqrt{2}\beta\rangle_{d_2},
\end{aligned} \tag{1}$$

where $\beta := \alpha\sin(\theta/2)$ and $\beta_X := \beta/\sqrt{T_X}$ ($X = A,B$). Since this protocol does not use LO after (i′), we are allowed to assume that the total number k of photons in modes ab was measured after step (i′), without affecting the protocol at all.

We start with the ideal case where $T_A = T_B = 1$ and the detectors at modes d_1d_2 are the ideal photon-number-resolving detectors. Then, the k photons in modes ab are preserved throughout steps (ii) and (iii), which leads to $m+n=k$. Combined with Eq. (1), this suggests that all the k photons are captured by one of the detectors. Hence, if photon detector d_1 (d_2) announces the arrival of $k(>0)$ photons, from $\langle k|0\rangle = 0$ and $\langle k|-i\sqrt{2}\beta\rangle = (-1)^k\langle k|i\sqrt{2}\beta\rangle$, we see that the backaction of the RNPM protocol is $\hat{P}^{AB}_{\text{odd}}$ ($\hat{P}^{AB}_{\text{even}}$) after Bob's phase flip at step (vi).

We can easily describe the backactions of the RNPM protocol with practical channels and detectors, as long as the dark counting are negligible, namely, $|0\rangle_{d_1}$ always produces $m=0$. This guarantees that the success outcome still gives the correct parity, but $l := m+n$ is no longer equal to k. Since the backaction depends only on $(-1)^k$, we see the following. If $l \equiv k \pmod 2$, the final state is the same as the ideal case. Otherwise, the final state suffers from a phase flip error $\hat{Z}^B$. This observation means that the RNPM protocol effectively works as the circuit described in Fig. 1(b), where the success probability p and the phase error probability ϵ (conditioned on the success) are solely determined from the joint probability $Q(k,l)$ as follows:

$$p = \sum_{l\geqslant 1}\chi_l^+, \quad \epsilon = \frac{1}{2p}\sum_{l\geqslant 1}(\chi_l^+ - \chi_l^-), \tag{2}$$

with $\chi_l^\pm := \sum_k(\pm 1)^{k-l}Q(k,l)$.

Let us derive the explicit forms of (p,ϵ) with various types of detectors with quantum efficiency η. Here we consider the case $T_A = T_B(=T)$ for simplicity, and the general cases are treated in Appendix A. Since k is the total number of photons in two coherent states with amplitude $i\beta/\sqrt{T}$, it follows the Poissonian distribution $P_\lambda(k) := (e^{-\lambda}\lambda^k)/k!$ with $\lambda = 2\beta^2/T$. When photon-number-resolving detectors are used, $l = m+n$ is the number of photons that have passed through a channel with transmittance ηT. Hence, we have $Q(k,l) = Q_\infty(k,l) := B_{\eta T}(l|k)P_{2\beta^2/T}(k)$ with a binomial distribution $B_p(l|k) := [p^l(1-p)^{k-l}k!]/[l!(k-l)!]$. Using Eq. (2), we have $p(\beta) = 1-e^{-2\beta^2\eta}$ and $\epsilon(\beta,T) = (1-e^{-2\beta^2\eta[2(\eta T)^{-1}-2]})/2$. When we use single-photon detectors, we are informed of the detection of exactly one photon. Hence, we have $Q(k,1) = Q_\infty(k,1)$ and $Q(k,0) = Q_\infty(k,0) + \sum_{l\geqslant 2}Q_\infty(k,l)$, leading to $p(\beta) = P_{2\eta\beta^2}(1)$ and $\epsilon(\beta,T) = (1-e^{-2\beta^2\eta[2(\eta T)^{-1}-2]})/2$. When threshold detectors are used, from $Q(k,1) = \sum_{l\geqslant 1}Q_\infty(k,l)$, we obtain $p(\beta) = 1-e^{-2\beta^2\eta}$ and $\epsilon(\beta,T) = (1-e^{-2\beta^2\eta[2(\eta T)^{-1}-1]})/2$.

As seen in the above examples, the success probability p and the phase error probability ϵ of the RNPM protocol are under a trade-off relation, which is controllable by β, namely by α. For a fixed L_0, the choice of $L_A = L_B = L_0/2$ gives the best performance of (p,ϵ). On the other hand, the choice $L_A = L_0$ has a technical merit in stabilizing the relative phase between pulses c_1 and c_2 (see Appendix B). The RNPM protocol can also be used for interacting quantum memories located in a single site, in which case L_0 is nearly zero and only the local loss τ determines the trade-off relation.

III. APPLICATIONS OF RNPM PROTOCOL

As we have seen, the performance of the RNPM protocol is determined by the local and channel losses as well as the resolution of photon detectors, implying that the effectiveness of the RNPM protocol increases in accordance with the progress of available devices. In what follows, we explore how such a progress enables us to accomplish applications ranging from quantum repeaters to quantum computation.

A. Long-distance quantum communication over lossy channels

The goal here is to share an entangled pair of qubits between two end stations separated by distance L. With direct transmission of single photons, the communication time would increase exponentially with distance L according to $e^{L/L_{\rm att}}$. Disposition of relaying stations with quantum memories helps to avoid the exponential increase by using a quantum repeater protocol [1]. Suppose that the stations are placed at $l_0 := L/2^n$ intervals [see Fig. 1(c)]. Each station has at least two qubits.

The first step is entanglement generation between neighboring stations separated by l_0. The RNPM protocol is applied to the two qubits in state $|+\rangle|+\rangle$ and is repeated until it is successful. Assuming the communication time l_0/c required for each trial, it takes the time $(l_0/c)p(\beta_g)^{-1}$ on average, and the Bell state is produced with phase error probability $\epsilon_0 := \epsilon(\beta_g, \tau\eta_{l_0/2})$. The parameter β_g can be freely chosen by adjusting the intensity of the light pulses. Here we consider the case with $L_A = L_B = l_0/2$ for simplicity of the notations (the cases with $L_A = l_0$ are found in Appendix B).

Next, the repeater protocol proceeds to entanglement connection [15]. Suppose that two stations separated by $2^j l_0$ ($j = 0, 1, \ldots, n-1$) can share a qubit pair in the Bell state with phase error probability ϵ_j and with average time t_j. After creating two such pairs connecting three stations, the middle one executes the Bell measurement by locally applying the RNPM protocol as in Fig. 1(d), which succeeds with probability $p(\beta_s)$ and produces entangled qubits $2^{j+1}l_0$ apart. Adding up the contribution of the phase errors in the two initial pairs and in the Bell measurement, we have $1 - 2\epsilon_{j+1} = (1 - 2\epsilon_j)^2[1 - 2\epsilon(\beta_s, \tau)]$. Since it approximately takes time $(3/2)t_j$ per trial [11], we have $t_{j+1} \sim (3/2)t_j\, p(\beta_s)^{-1}$ for the average time for success. Solving these recursive relations, we see that the average total time $T = t_n$ is approximately written as

$$T \sim \frac{l_0}{c}\left(\frac{3}{2}\right)^{\log_2(L/l_0)} p(\beta_g)^{-1}\, p(\beta_s)^{-\log_2(L/l_0)}, \qquad (3)$$

and the final state is $\hat{\rho}^{AB} = F|\Phi^+\rangle\langle\Phi^+|_{AB} + (1 - F)|\Phi^-\rangle\langle\Phi^-|_{AB}$, with

$$2F - 1 = [1 - 2\epsilon(\beta_g, \tau\eta_{l_0/2})]^{L/l_0}[1 - 2\epsilon(\beta_s, \tau)]^{L/l_0 - 1}. \qquad (4)$$

For large L, it should be chosen as $\beta_g^2 \sim \beta_s^2 \sim O(l_0/L)$. Then, noticing that $p(\beta) \sim O(\beta^2)$ and $\epsilon(\beta, T) \sim O(\beta^2)$ hold regardless of the types of the photon detectors, we have $F \sim O(1)$ and $T \sim O[(3/2)^{\log_2(L/l_0)}(L/l_0)^{\log_2(L/l_0)+1}]$. Hence, T increases only subexponentially with L. We also numerically optimized T over n, β_g, and β_s for fixed values of final fidelity F and the distance L, which are shown in Fig. 2. In contrast to Refs. [1,4,6,8,9,11–13], this figure shows that the protocol works even only with threshold detectors.

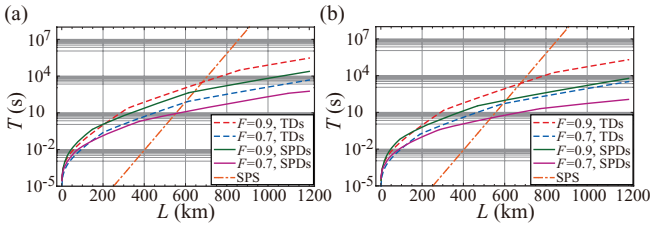

FIG. 2. (Color online) The minimum time T needed to generate entanglement with $F = 0.9$, 0.7 over distance L under the use of threshold detectors (TDs) and single-photon detectors (SPDs): (a) $\tau = 0.95$ and $\eta = 0.9$; (b) $\tau = 0.98$ and $\eta = 0.95$. $c = 2 \times 10^8$ m/s and $L_{\rm att} = 22$ km. The direct transmission time $(f\eta T_L)^{-1}$ of the photon from 10 GHz ($f = 10^{10}$) single-photon source (SPS) is also shown as a reference.

We stress that, since the produced state $\hat{\rho}^{AB}$ includes only one type of error, for fixed fidelity F, this entanglement has higher quality than ones generated by the other repeaters. This feature relieves us of targeting a high fidelity. For example, $F > 1/2$ is sufficient for distilling secret key from the entanglement $\hat{\rho}^{AB}$ [16], and three or four pairs of $F = 0.7$ with single-type errors have the same ability as one pair of $F = 0.9$ with general errors.

B. Entanglement distillation

While the optical losses considered above are the dominant obstacle in long-distance communication, other types of small noises will also be inevitable. For example, practical quantum memories will decohere with time. To overcome such general noises, quantum repeaters require to be equipped with entanglement distillation [19]. Entanglement distillation not only helps to counter such general errors, but also, even under such a situation, reduces the scaling of the communication time to be polynomial [1] in distance L. While all the known repeaters have needed additional complicated operations for entanglement distillation [1,4,6,8,9,11–14], our repeater can be easily equipped with it by using the same module, that is, the RNPM protocol.

In a simple method of distillation called the recurrence method [20], Alice and Bob first transform each pair of qubits locally into the so-called Werner state while keeping the fidelity F to a Bell state. Suppose that they have two such pairs A_1B_1 and A_2B_2 with $F > 1/2$. Alice applies a controlled-NOT gate on her qubit A_1 as the control and on A_2 as the target, and measures A_2 on Z basis (the whole process is called parity check measurement). Bob also applies the same measurement on his qubits. Their outcomes will agree with probability $P_{\rm rec}(F) = (8F^2 - 4F + 5)/9$, and then the remaining pair A_1B_1 will have improved fidelity $F' = [(2F + 1)^2 + (4F - 1)^2]/[18P_{\rm rec}(F)]$.

Since the outcome of each party is the parity of the two qubits, it can also be obtained via the RNPM protocol. In addition, if the RNPM protocol succeeds, by subsequently measuring A_2 on X basis to produce outcome x and then by applying $\hat{Z}^x$ on A_1, the postmeasurement state of A_1 is also simulated except the phase error $\epsilon(\beta, \tau)$ [see Fig. 1(e)]. The overall success probability is $P_s := P_{\rm rec}(F)p^2(\beta)$, which is in a trade-off relation with the fidelity $F' = \{(2F + 1)^2 +$

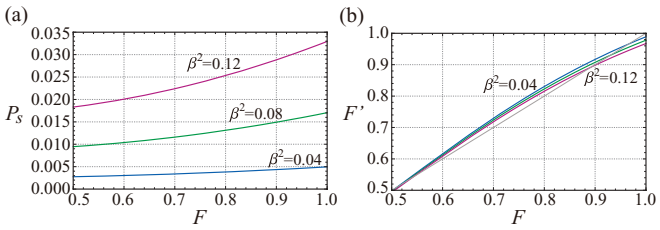

FIG. 3. (Color online) For $\beta^2 = 0.04, 0.08, 0.12$ with $\tau = 0.98$ and $\eta = 0.95$, the efficiencies of the recurrence method based on the RNPM protocols with single-photon detectors as a function of fidelity F of the initial Werner states to a Bell state. (a) The success probability $P_s = P_{\rm rec}(F)[P_{2\eta\beta^2}(1)]^2$. (b) The fidelity F' of the final pair.

$(4F-1)^2[1-2\epsilon(\beta,\tau)]^2\}/[18P_{\rm rec}(F)]$ of the final state and is controllable through β. In Fig. 3 we give numerical examples with single-photon detectors.

C. Generation of cluster states

One promising way for implementing quantum computing is the so-called measurement-based quantum computation, where computation proceeds with sequential one-qubit measurements on a system in a highly entangled state, the cluster state [21]. The addressing of individual qubits is easier when they are located not so close to each other. Such a sparse configuration also helps to reduce correlated errors from the environment. In this case, the RNPM protocol works as an entangler for qubits that are not in close proximity. In fact, the gate shown in Fig. 1(f) can be used for extending one-dimensional cluster states, and the parity check measurement in Fig. 1(e) can be used for fusing two cluster states [22,23]. The combination of these two types of gates enables us to build up a large cluster state. Despite the use of a single interaction per qubit, our scheme has no fundamental limitation on the success probability, which is in striking contrast to the other known entanglers [24–26]. Hence, with future development of good detectors and reduction of internal losses, the RNPM protocol will also work as a useful tool for implementing quantum computing.

IV. SUMMARY

We have proposed a versatile protocol, called the RNPM protocol, for measuring the parity of two separated qubits in a nondestructive way. The performance of the RNPM protocol is simply related to the optical loss and the characteristics of photon detectors. We have shown that, even with threshold detectors, the protocol can be used as a module to build up quantum repeaters for long-distance quantum communication. Efficient single-photon detectors will allow us to equip the repeaters with entanglement distillation, a countermeasure against arbitrary types of noises. With further improvement of the performance, more general quantum computation will be made possible through the generation of cluster states via the RNPM protocol. We believe that the existence of such a versatile tool provides an attractive route toward realization of quantum communication and computation, in which efforts can be focused on development and improvement of that particular tool.

ACKNOWLEDGMENTS

We thank N. Sota for valuable discussions. We acknowledge the support of a MEXT Grant-in-Aid for Scientific Research on Innovative Areas (Grants No. 21102008 and No. 20104003), a MEXT Grant-in-Aid for the Global COE Program, and a JSPS Grant-in-Aid for Scientific Research (C) 20540389. K.A. was supported by JSPS.

APPENDIX A: THE PERFORMANCE OF THE RNPM PROTOCOL

Here, for arbitrary values of T_A and T_B, we derive the performance (p,ϵ) of the RNPM protocol with various types of detectors. As shown in the main body of this paper, the performance is determined by calculating the joint probability $Q(k,l)$ with which modes ab have k photons in total and the arrival of l photons is announced by photon detectors $d_1 d_2$ in total. Let k_a and k_b be the numbers of photons in modes a and b, respectively. Since mode a is in a coherent state with amplitude $i\beta/\sqrt{T_A}$, k_a follows the Poissonian distribution $P_{\beta^2/T_A}(k_a)$ with $P_\lambda(k) := (e^{-\lambda}\lambda^k)/k!$. Similarly, k_b obeys the Poissonian distribution $P_{\beta^2/T_B}(k_b)$.

Suppose that we use photon-number-resolving detectors with quantum efficiency η for the detectors d_1 and d_2. Each of the k_a photons will then be detected with probability ηT_A. Hence, the probability of detecting l_a photons among k_a photons in mode a is given by $B_{\eta T_A}(l_a|k_a)P_{\beta^2/T_A}(k_a)$, where $B_p(l|k) := [p^l(1-p)^{k-l}k!]/[l!(k-l)!]$ is the binomial distribution. Similarly, the probability of detecting l_b photons among k_b photons in mode b is given by $B_{\eta T_B}(l_b|k_b)P_{\beta^2/T_B}(k_b)$. Since $Q(k,l)$ is given by the sum of all probabilities with $k = k_a + k_b$ and $l = l_a + l_b$, we have

$$
\begin{aligned}
Q(k,l) = Q_\infty(k,l) &:= \sum_{l_a=0}^{l}\sum_{k_a=l_a}^{l_a+(k-l)} B_{\eta T_A}(l_a|k_a)P_{\beta^2/T_A}(k_a) \\
&\quad\times B_{\eta T_B}(l-l_a|k-k_a)P_{\beta^2/T_B}(k-k_a) \\
&= e^{-\beta^2(\frac{1}{T_A}+\frac{1}{T_B})}(\eta\beta^2)^l \sum_{l_a=0}^{l}\frac{1}{l_a!(l-l_a)!} \\
&\quad\times \sum_{k_a=l_a}^{l_a+(k-l)} \frac{\left(\frac{1-\eta T_A}{T_A}\beta^2\right)^{k_a-l_a}\left(\frac{1-\eta T_B}{T_B}\beta^2\right)^{k-l-(k_a-l_a)}}{(k_a-l_a)![k-l-(k_a-l_a)]!} \\
&= e^{-\beta^2(\frac{1}{T_A}+\frac{1}{T_B})}(\eta\beta^2)^l \frac{1}{(k-l)!} \\
&\quad\times \left[\left(\frac{1-\eta T_A}{T_A}+\frac{1-\eta T_B}{T_B}\right)\beta^2\right]^{k-l}\sum_{l_a=0}^{l}\frac{1}{l_a!(l-l_a)!} \\
&= \frac{e^{-\beta^2(\frac{1}{T_A}+\frac{1}{T_B})}}{l!(k-l)!}(2\beta^2\eta)^l \\
&\quad\times \left[\left(\frac{1-\eta T_A}{T_A}+\frac{1-\eta T_B}{T_B}\right)\beta^2\right]^{k-l}, \qquad \text{(A1)}
\end{aligned}
$$

where we used the binomial theorem

$$(a+b)^n = \sum_{m=0}^{n} \frac{n!}{m!(n-m)!} a^m b^{n-m} \tag{A2}$$

for any $a,b \in \boldsymbol{R}$ and $n \in \boldsymbol{N}$. From the expression of $Q(k,l)$, $\chi_l^{\pm}$ are calculated to be

$$\chi_l^{+} = \sum_k Q(k,l) = \sum_{k=l}^{\infty} Q_\infty(k,l) = \frac{(2\beta^2\eta)^l}{l!} e^{-2\beta^2\eta}, \tag{A3}$$

$$\begin{aligned}\chi_l^{-} &= \sum_k (-1)^{k-l} Q(k,l) = \sum_{k=l}^{\infty} (-1)^{k-l} Q_\infty(k,l) \\ &= \frac{(2\beta^2\eta)^l}{l!} e^{-2\beta^2\eta(\frac{1}{\eta T_A}+\frac{1}{\eta T_B}-1)},\end{aligned} \tag{A4}$$

by noting $e^x = \sum_{m=0}^{\infty} x^m/m!$. Hence, the success probability p and the phase error probability ϵ of the RNPM protocol with photon-number-resolving detectors are

$$p(\beta) = \sum_{l\geqslant 1} \chi_l^{+} = \sum_{l=1}^{\infty} \chi_l^{+} = 1 - e^{-2\beta^2\eta}, \tag{A5}$$

$$\begin{aligned}\epsilon(\beta,T_A,T_B) &= \frac{1}{2p} \sum_{l\geqslant 1} (\chi_l^{+} - \chi_l^{-}) = \frac{1}{2p} \sum_{l=1}^{\infty} (\chi_l^{+} - \chi_l^{-}) \\ &= \frac{1}{2}\left(1 - e^{-2\beta^2\eta(\frac{1}{\eta T_A}+\frac{1}{\eta T_B}-2)}\right).\end{aligned} \tag{A6}$$

Note that the above expressions are reduced to the ones in the main body of the paper for $T_A = T_B (= T)$. By substituting $T_A = \tau\eta_{L_A} = \tau e^{-L_A/L_{\rm att}}$ and $T_B = \tau\eta_{L_0-L_A} = \tau e^{-(L_0-L_A)/L_{\rm att}}$ into Eqs. (A5) and (A6), one can easily confirm that, for a fixed L_0, the choice of $L_A = L_B = L_0/2$ gives the best performance. In other words, the RNPM protocol works best when Claire is located at the middle point between Alice and Bob.

1. Use of single-photon detectors

Here we assume the use of single-photon detectors with quantum efficiency η, which announce the detection of photons only when receiving exactly one photon. In this case, $Q(k,l)$ is described by

$$Q(k,1) = Q_\infty(k,1), \tag{A7}$$

$$Q(k,0) = Q_\infty(k,0) + \textstyle\sum_{l\geqslant 2} Q_\infty(k,l). \tag{A8}$$

Then, $\chi_1^{\pm}$ are calculated to be

$$\chi_1^{+} = \sum_k Q(k,1) = \sum_{k=1}^{\infty} Q_\infty(k,1) = 2\beta^2\eta e^{-2\beta^2\eta}, \tag{A9}$$

$$\begin{aligned}\chi_1^{-} &= \sum_k (-1)^{k-1} Q(k,1) = \sum_{k=1}^{\infty} (-1)^{k-1} Q_\infty(k,1) \\ &= 2\beta^2\eta e^{-2\beta^2\eta(\frac{1}{\eta T_A}+\frac{1}{\eta T_B}-1)},\end{aligned} \tag{A10}$$

from the last equations in Eqs. (A3) and (A4). Hence, we conclude

$$p(\beta) = \sum_{l\geqslant 1} \chi_l^{+} = \chi_1^{+} = 2\beta^2\eta e^{-2\beta^2\eta}, \tag{A11}$$

$$\begin{aligned}\epsilon(\beta,T_A,T_B) &= \frac{1}{2p} \sum_{l\geqslant 1} (\chi_l^{+} - \chi_l^{-}) = \frac{1}{2p} (\chi_1^{+} - \chi_1^{-}) \\ &= \frac{1}{2}\left(1 - e^{-2\beta^2\eta(\frac{1}{\eta T_A}+\frac{1}{\eta T_B}-2)}\right).\end{aligned} \tag{A12}$$

2. Use of threshold detectors

Here we consider the case of threshold detectors with quantum efficiency η. Since this type of detector clicks only when receiving nonzero photons, we have

$$Q(k,1) = \sum_{l\geqslant 1} Q_\infty(k,l), \tag{A13}$$

$$Q(k,0) = Q_\infty(k,0). \tag{A14}$$

From this, $\chi_1^{\pm}$ are calculated to be

$$\begin{aligned}\chi_1^{+} &= \sum_k Q(k,1) = \sum_{k=1}^{\infty} \sum_{l=1}^{k} Q_\infty(k,l) = \sum_{l=1}^{\infty} \sum_{k=l}^{\infty} Q_\infty(k,l) \\ &= \sum_{l=1}^{\infty} \frac{(2\beta^2\eta)^l}{l!} e^{-2\beta^2\eta} = 1 - e^{-2\beta^2\eta},\end{aligned} \tag{A15}$$

$$\begin{aligned}\chi_1^{-} &= \sum_k (-1)^{k-1} Q(k,1) = \sum_{k=1}^{\infty} \sum_{l=1}^{k} (-1)^{k-1} Q_\infty(k,l) \\ &= \sum_{l=1}^{\infty} (-1)^{l-1} \sum_{k=l}^{\infty} (-1)^{k-l} Q_\infty(k,l) \\ &= \sum_{l=1}^{\infty} (-1)^{l-1} \frac{(2\beta^2\eta)^l}{l!} e^{-2\beta^2\eta(\frac{1}{\eta T_A}+\frac{1}{\eta T_B}-1)} \\ &= \left(1 - e^{-2\beta^2\eta}\right) e^{-2\beta^2\eta(\frac{1}{\eta T_A}+\frac{1}{\eta T_B}-1)},\end{aligned} \tag{A16}$$

from the last equations in Eqs. (A3) and (A4). Hence, the success probability p and the phase error probability ϵ are

$$p(\beta) = \sum_{l\geqslant 1} \chi_l^{+} = \chi_1^{+} = 1 - e^{-2\beta^2\eta}, \tag{A17}$$

$$\begin{aligned}\epsilon(\beta,T_A,T_B) &= \frac{1}{2p} \sum_{l\geqslant 1} (\chi_l^{+} - \chi_l^{-}) = \frac{1}{2p} (\chi_1^{+} - \chi_1^{-}) \\ &= \frac{1}{2}\left(1 - e^{-2\beta^2\eta(\frac{1}{\eta T_A}+\frac{1}{\eta T_B}-1)}\right).\end{aligned} \tag{A18}$$

APPENDIX B: A MODIFIED RNPM PROTOCOL

Although the RNPM protocol has the best performance when Claire is halfway between Alice and Bob, the choice with $L_A = L_0$ is also worth mentioning since the stabilization of the relative phase between the relevant pulses can be easier. To clarify this fact, here we introduce a modified RNPM protocol where Claire's task in the original RNPM protocol is executed by Bob.

Suppose that the qubits A and B are respectively held by Alice and Bob, who are distance L_0 apart and share an optical channel $a \to b_1$ (see Fig. 4). Let $T_A := \tau\eta_{L_0}$ and $T_B := \tau$ be the overall transmittance of the channels, where

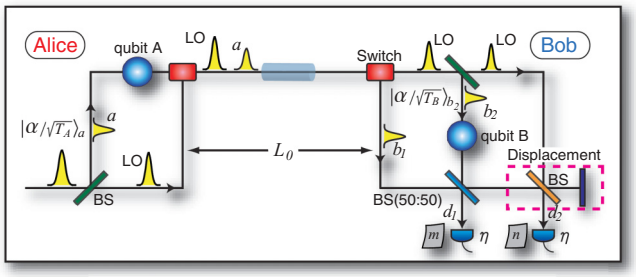

FIG. 4. (Color online) A modified RNPM protocol. This protocol is executed only by Alice and Bob through an optical channel between them. The performance of this protocol is equivalent to that of the original RNPM protocol with $L_A = L_0$, but the stabilization of the relative phase between pulses b_1 and b_2 is easier.

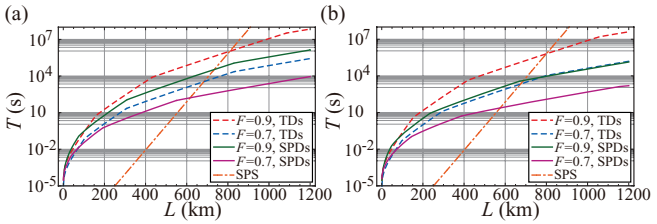

FIG. 5. (Color online) For $L_A = l_0$ and $L_B = 0$, the minimum time T needed to generate entanglement with $F = 0.9$, 0.7 over distance L under the use of threshold detectors (TDs) and single-photon detectors (SPDs): (a) $\tau = 0.95$ and $\eta = 0.9$; (b) $\tau = 0.98$ and $\eta = 0.95$. $c = 2 \times 10^8$ m/s and $L_{\rm att} = 22$ km. The direct transmission time $(f\eta T_L)^{-1}$ of the photon from a 10-GHz ($f = 10^{10}$) single-photon source (SPS) is also described as a reference.

τ stands for the local loss. The modified RNPM protocol proceeds as follows. (i.1) Alice prepares pulse a in a coherent state $|\alpha/\sqrt{T_A}\rangle_a$ with $\alpha \geqslant 0$, and lets it interact with qubit A by $\hat{U}_\theta$. (i.2) Alice sends Bob the probe pulse a and a LO through the same optical channel $a \to b_1$, with a short time delay. (ii) On receiving the probe pulse b_1 and the LO, Bob generates an independent probe pulse b_2 in a coherent state $|\alpha/\sqrt{T_B}\rangle_{b_2}$ from the LO, and lets it interact with qubit B by $\hat{U}_\theta$. (iii) Bob makes the pulses $b_1 b_2$ interfere by a 50:50 beam splitter. (iv) On the mode receiving the constructive interference, Bob applies displacement operation $\hat{D}[-\sqrt{2}\alpha\cos(\theta/2)]$ by using the LO. (v) Bob counts photons of the output modes $d_1 d_2$ by two photon detectors, which produces the outcome (m,n). (vi) If $m+n$ is odd, Bob applies phase flip $\hat{Z}$ to qubit B.

In this case, Bob does not need to use his own LO, and all the pulses are generated from the same LO held by Alice. Any slow phase fluctuation on the probe pulse during the travel over distance L_0 will be automatically compensated since the LO goes through the same fluctuation.

1. The performance of long-distance quantum communication over lossy channels

Here we calculate the performance of quantum repeaters with the modified RNPM protocol. More specifically, we use the modified RNPM protocols with $L_0 = l_0 = L/2^n$ for the entanglement generation. In this case, the average total time T and the fidelity F are described by

$$T \sim \frac{l_0}{c}\left(\frac{3}{2}\right)^{\log_2(L/l_0)} p(\beta_g)^{-1} p(\beta_s)^{-\log_2(L/l_0)}, \quad \text{(B1)}$$

$$F = \frac{1 + [1-2\epsilon(\beta_g, \tau\eta_{l_0}, \tau)]^{L/l_0}[1-2\epsilon(\beta_s,\tau,\tau)]^{L/l_0-1}}{2}. \quad \text{(B2)}$$

By substituting Eqs. (A11) and (A12) [or Eqs. (A17) and (A18)] into these equations, we numerically optimized T over n, β_g, and β_s for fixed values of final fidelity F and the distance L, which are shown in Fig. 5.

[1] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[2] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[3] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (Lodnon) **414**, 413 (2001).

[4] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).

[5] L. I. Childress, J. M. Taylor, A. Sørensen, and M. D. Lukin, Phys. Rev. A **72**, 052330 (2005).

[6] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).

[7] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New J. Phys. **8**, 164 (2006).

[8] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, Phys. Rev. Lett. **101**, 040502 (2008).

[9] K. Azuma, N. Sota, R. Namiki, Ş. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **80**, 060303(R) (2009).

[10] K. Azuma, N. Sota, M. Koashi, and N. Imoto, Phys. Rev. A **81**, 022325 (2010).

[11] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[12] J. B. Brask, I. Rigas, E. S. Polzik, U. L. Andersen, and A. S. Sørensen, Phys. Rev. Lett. **105**, 160501 (2010).

[13] N. Sangouard, C. Simon, N. Gisin, J. Laurat, R. Tualle-Brouri, and P. Grangier, J. Opt. Soc. Am. B **27**, A137 (2010).

[14] N. Sangouard, R. Dubessy, and C. Simon, Phys. Rev. A **79**, 042340 (2009).

[15] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[16] This is because, for a single-error-type state like $\hat{\rho}^{AB}$, the formula of secure key rate of the entanglement-based protocol [17,18] is proportional to $1 - h(F)$ with the binary entropy function $h(x) := -x\log_2 x - (1-x)\log_2(1-x)$.

[17] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[18] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[19] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).
[20] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[21] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[22] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
[23] L.-M. Duan and R. Raussendorf, Phys. Rev. Lett. **95**, 080503 (2005).
[24] S. D. Barrett and P. Kok, Phys. Rev. A **71**, 060310(R) (2005).
[25] Y. L. Lim, A. Beige, and L. C. Kwek, Phys. Rev. Lett. **95**, 030505 (2005).
[26] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn, New J. Phys. **8**, 30 (2006).