

Nearly deterministic Bell measurement with multiphoton entanglement for efficient quantum-information processing

Seung-Woo Lee,¹ Kimin Park,^{1,2} Timothy C. Ralph,³ and Hyunseok Jeong¹¹*Center for Macroscopic Quantum Control, Department of Physics and Astronomy, Seoul National University, Seoul 151-742, Korea*²*Department of Optics, Palacký University, 17. listopadu 1192/12, 77146 Olomouc, Czech Republic*³*Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

(Received 21 July 2015; published 19 November 2015)

We present a detailed analysis of the Bell measurement scheme proposed in Lee *et al.* [*Phys. Rev. Lett.* **114**, 113603 (2015)] based on a logical qubit using Greenberger-Horne-Zeilinger entanglement of photons. The success probability of the proposed Bell measurement can be made arbitrarily high using only linear optics as the number of photons in a logical qubit increases. We compare our scheme with all the other proposals, using single-photon qubits, coherent-state qubits, or hybrid qubits, suggested to enhance the efficiency of the Bell measurement. As a remarkable advantage, our scheme requires only photon on-off measurements, while photon number resolving detectors are necessary for all the other proposals. We find that the scheme based on coherent-state qubits shows the best performance with respect to the attained success probability in terms of the average number of photons used in the process, while our scheme outperforms the schemes using single-photon qubits. We finally show that efficient quantum communication and fault-tolerant quantum computation can be realized using our approach.

DOI: [10.1103/PhysRevA.92.052324](https://doi.org/10.1103/PhysRevA.92.052324)

PACS number(s): 42.50.Ex, 03.67.Hk, 03.67.Lx

I. INTRODUCTION

Bell measurement is a crucial element of quantum communication and quantum computation protocols. It discriminates between four entangled states known as Bell states,

$$\begin{aligned} |\Phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|0_L\rangle|0_L\rangle \pm |1_L\rangle|1_L\rangle), \\ |\Psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|0_L\rangle|1_L\rangle \pm |1_L\rangle|0_L\rangle), \end{aligned} \quad (1)$$

where $|0_L\rangle$ and $|1_L\rangle$ are the logical qubit bases. In optical implementations, single photons with their polarization degree of freedom are typically employed to construct logical qubits [1–3]. For a single-photon qubit, the Bell measurement can be implemented using linear optics and photodetectors [4,5], which we shall refer to as the standard Bell-measurement scheme. This scheme, in effect, projects two photons onto a complete measurement basis of two Bell states and two product states so that only two of the Bell states can be unambiguously identified. Due to this reason, the success probability of the standard Bell measurement is limited to 50% [4,5], and it has been a fundamental hindrance to the implementation of a deterministic quantum teleportation and scalable quantum computation with linear optics [1,2].

In order to enhance the success probability of the Bell measurement, several schemes have been proposed based on single-photon qubits using either ancillary entangled states [6,7] or additional squeezing operations [8]. Instead of using single photons, different types of physical degrees of freedom of light can also be employed to construct logical qubits, for example, using superpositions of coherent states [9,10] or hybrid entanglement of single photons and coherent states [11,12]. Although each of these schemes has its own merit, there exist several features to overcome in the implementation of those schemes, such as the requirement of ancillary

resource entanglement [6,7] or the limited success probabilities [8]. Moreover, all aforementioned schemes suffer from the requirement of photon number resolving detection [6–11].

In this paper, we discuss a scheme for implementing a nearly deterministic Bell measurement with linear optics and photon on-off measurements [13]. The logical qubit is defined as a Greenberger-Horne-Zeilinger (GHZ)-type multiphoton entangled state. It is shown that the logical Bell states can be efficiently discriminated by performing N times of standard Bell measurements, where N is the number of photons in a logical qubit. The limited success probability of the standard Bell measurement $1/2$ is overcome by the fact that each of the four logical Bell states is characterized by the number of contributions from two Bell states of single-photon qubits, that can be identified by the standard Bell measurement performed on photon pairs. As a result, the logical Bell measurement fails only when none of the N pairs is a detectable Bell state, resulting in a success probability of $1 - 2^{-N}$ that rapidly approaches unity as N increases. A detailed review of our scheme will be presented in Sec. II.

In Sec. III, we compare our scheme with other well-known Bell measurement schemes proposed based on linear optics; our scheme outperforms the previous proposals employing single-photon qubits [6–8] in its efficiency against the number of photons used in the measurement process. The other schemes employing coherent state [9,10] or optical hybrid qubits [11,12] enable us to achieve even higher success probability than ours with the same average photon number usage. However, all the other schemes except ours require photon number resolving detection, while our scheme can be performed with linear optics and photon on-off measurements only.

In Sec. IV, we discuss the applications of our scheme to quantum communication and computations. We will show that a qubit in an N photon GHZ-type entanglement can be

teleported with an arbitrarily high success probability with a $2N$ photon GHZ-type entangled channel as N becomes large. It will be shown that in our approach a complete set of universal gate operations can be constructed using only linear optics, on-off measurements, and multiphoton entanglement. We investigate the effect of photon losses, a major factor of errors, and demonstrate a fault-tolerant quantum computation in our approach. We expect our scheme to be a competitive approach to photonic quantum-information processing.

II. LINEAR OPTICAL BELL MEASUREMENT SCHEME WITH MULTIPHOTON ENCODING

A. Standard Bell measurement scheme

We first consider the standard Bell measurement technique for single-photon qubits. The logical basis of single-photon qubits are typically defined with the photon polarization degree of freedom, in terms of either the horizontal and vertical polarization states, i.e., $\{|H\rangle, |V\rangle\}$, or the diagonal states $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$. Here we assume the Bell states of single-photon qubits in the diagonal basis,

$$\begin{aligned} |\Phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|+\rangle \pm |-\rangle|-\rangle), \\ |\Psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|-\rangle \pm |-\rangle|+\rangle). \end{aligned} \quad (2)$$

The standard Bell measurement scheme for single-photon qubits employs linear optical elements such as polarizing beam splitter (PBS), wave plates, and photon detection [5]. It projects two photons onto a complete measurement basis of two Bell states and two product states so that only two of the Bell states can be identified. For example, one can identify $|\Phi^-\rangle$ and $|\Psi^-\rangle$ using three PBS and four on-off photodetectors as illustrated in Fig. 1(a). For $|\Phi^-\rangle$ or $|\Psi^-\rangle$ states, two photons are separated into different modes at the first PBS, resulting in one click from the upper two and another from lower two detectors. If the separated clicks have the different polarization output, i.e., (H, V) or (V, H) , the result is $|\Phi^-\rangle$, while for the same polarization output, i.e., (H, H) or (V, V) , the result is $|\Psi^-\rangle$. On the other hand, two photons of the state $|\Phi^+\rangle$ or $|\Psi^+\rangle$ proceed together via the first PBS either way to the upper or lower two detectors. All possible clicks at the detectors from $|\Phi^+\rangle$ can equally be yielded from $|\Psi^+\rangle$ so that it is impossible to discriminate them. Therefore, the success

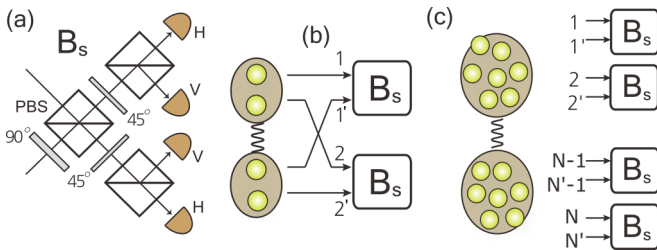


FIG. 1. (Color online) (a) Standard Bell measurement B_s for single-photon qubits using linear optical elements and photon on-off detectors. (b) Logical Bell measurement for the qubits encoded with two photons. (c) Logical Bell measurement for N -photon qubits through N times of B_s measurements.

probability of the standard Bell measurement scheme is limited to $1/2$ [4,5]. Which two Bell states are successfully identified can be selected by putting appropriate wave plates at the input modes of the first PBS. We will refer to the standard Bell measurement in Fig. 1(a) as B_s hereafter.

B. Our proposal: Bell measurement with multiphoton encoding

Here we introduce a scheme for discriminating four Bell states by using linear optics and qubits with multiphoton encoding [13]. We define the logical basis of qubits with N photons as

$$\begin{aligned} |0_L\rangle &\equiv |+\rangle^{\otimes N} = |+\rangle_1|+\rangle_2|+\rangle_3 \cdots |+\rangle_N, \\ |1_L\rangle &\equiv |-\rangle^{\otimes N} = |-\rangle_1|-\rangle_2|-\rangle_3 \cdots |-\rangle_N. \end{aligned} \quad (3)$$

Thus, a logical qubit is generally written in the form of a GHZ-type state as $\alpha|+\rangle^{\otimes N} + \beta|-\rangle^{\otimes N}$. The encoding of a logical qubit into N photons can be realized, for example, by the teleportation scheme between an encoded single photon and N photons. For this purpose, the GHZ state of $N + 1$ photons is used as the teleportation channel and the encoded single photon as the input state.

Let us first explain our proposal with the simplest case, i.e., two-photon encoding ($N = 2$), where the logical qubit bases are $|0_L\rangle \equiv |+\rangle \otimes |+\rangle$ and $|1_L\rangle \equiv |-\rangle \otimes |-\rangle$. The logical Bell states in this encoding are written by

$$\begin{aligned} |\Phi_{(2)}^\pm\rangle &= \frac{1}{\sqrt{2}}(|+\rangle_1|+\rangle_2|+\rangle_{1'}|+\rangle_{2'} \pm |-\rangle_1|-\rangle_2|-\rangle_{1'}|-\rangle_{2'}), \\ |\Psi_{(2)}^\pm\rangle &= \frac{1}{\sqrt{2}}(|+\rangle_1|+\rangle_2|-\rangle_{1'}|-\rangle_{2'} \pm |-\rangle_1|-\rangle_2|+\rangle_{1'}|+\rangle_{2'}), \end{aligned} \quad (4)$$

where the first logical qubit is of photonic modes 1 and 2 while the second is of $1'$ and $2'$. If we simply rearrange the order of photon modes $1'$ and 2 , and by using the fact that $|\pm\rangle|\pm\rangle = (|\Phi^\pm\rangle \pm |\Phi^\mp\rangle)/\sqrt{2}$ and $|\pm\rangle|\mp\rangle = (|\Psi^\pm\rangle \pm |\Psi^\mp\rangle)/\sqrt{2}$, these Bell states can be represented in terms of the Bell states in Eq. (2) as

$$\begin{aligned} |\Phi_{(2)}^\pm\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{11'}|\Phi^\pm\rangle_{22'} + |\Phi^-\rangle_{11'}|\Phi^\mp\rangle_{22'}), \\ |\Psi_{(2)}^\pm\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{11'}|\Psi^\pm\rangle_{22'} + |\Psi^-\rangle_{11'}|\Psi^\mp\rangle_{22'}). \end{aligned} \quad (5)$$

Interestingly, these four Bell states can be thus identified by means of two independent standard Bell measurements for single-photon qubits (B_s) performed on two photons; one is from the first and the other from the second qubit as illustrated in Fig. 1(b). Note that the photons in each qubit are indistinguishable so that any single photon can be selected arbitrarily to perform each independent B_s measurement.

Let us now explain how one can discriminate the four logical Bell states, keeping in mind that the B_s measurement defined in the previous section can unambiguously identify $|\Phi^-\rangle$ and $|\Psi^-\rangle$ out of the four Bell states of single photons. From the results of two B_s measurements, one can identify the

Bell states encoded with two photons as follows:

$$\begin{aligned} |\Phi_{(2)}^+\rangle &: \text{both } B_s \text{ succeed with } |\Phi^-\rangle, \\ |\Phi_{(2)}^-\rangle &: \text{one } B_s \text{ succeeds with } |\Phi^-\rangle, \\ |\Psi_{(2)}^+\rangle &: \text{both } B_s \text{ succeed with } |\Psi^-\rangle, \\ |\Psi_{(2)}^-\rangle &: \text{one } B_s \text{ succeed with } |\Psi^-\rangle, \\ \text{Failure} &: \text{both } B_s \text{ fail.} \end{aligned}$$

As the failure occurs only when both B_s measurements fail (i.e., neither $|\Phi^-\rangle$ nor $|\Psi^-\rangle$ is obtained), the four Bell states $|\Phi_{(2)}^\pm\rangle$ and $|\Psi_{(2)}^\pm\rangle$ can be discriminated with 75% success probability, i.e., $P_s = 3/4$. Note that our scheme employs only linear optics and on-off photodetectors as it can be implemented by means of two separate B_s measurements.

Our scheme can be generalized for the case of arbitrary N photon encoding. From Eq. (3), the logical Bell states $|\Phi_{(N)}^\pm\rangle = (|0_L\rangle|0_L\rangle \pm |1_L\rangle|1_L\rangle)/\sqrt{2}$ and $|\Psi_{(N)}^\pm\rangle = (|0_L\rangle|1_L\rangle \pm |1_L\rangle|0_L\rangle)/\sqrt{2}$ encoded with N photons can be written by

$$\begin{aligned} |\Phi_{(N)}^\pm\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|+\rangle)^{\otimes N} \pm (|-\rangle|-\rangle)^{\otimes N} \\ &= \frac{1}{\sqrt{2^{N+1}}}((|\Phi^+\rangle + |\Phi^-\rangle)^{\otimes N} \pm (|\Phi^+\rangle - |\Phi^-\rangle)^{\otimes N}), \\ |\Psi_{(N)}^\pm\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|-\rangle)^{\otimes N} \pm (|-\rangle|+\rangle)^{\otimes N} \\ &= \frac{1}{\sqrt{2^{N+1}}}((|\Psi^+\rangle + |\Psi^-\rangle)^{\otimes N} \pm (|\Psi^+\rangle - |\Psi^-\rangle)^{\otimes N}), \end{aligned} \quad (6)$$

by using $|\pm\rangle|\pm\rangle = (|\Phi^+\rangle \pm |\Phi^-\rangle)/\sqrt{2}$ and $|\pm\rangle|\mp\rangle = (|\Psi^+\rangle \pm |\Psi^-\rangle)/\sqrt{2}$. After some calculations, we can rewrite these in the form of

$$\begin{aligned} |\Phi_{(N)}^+\rangle &= \frac{1}{\sqrt{2^{N-1}}} \sum_{j=0}^{[N/2]} \mathcal{P}[|\Phi^+\rangle^{\otimes N-2j} |\Phi^-\rangle^{\otimes 2j}], \\ |\Phi_{(N)}^-\rangle &= \frac{1}{\sqrt{2^{N-1}}} \sum_{j=0}^{[(N-1)/2]} \mathcal{P}[|\Phi^+\rangle^{\otimes N-2j-1} |\Phi^-\rangle^{\otimes 2j+1}], \\ |\Psi_{(N)}^+\rangle &= \frac{1}{\sqrt{2^{N-1}}} \sum_{j=0}^{[N/2]} \mathcal{P}[|\Psi^+\rangle^{\otimes N-2j} |\Psi^-\rangle^{\otimes 2j}], \\ |\Psi_{(N)}^-\rangle &= \frac{1}{\sqrt{2^{N-1}}} \sum_{j=0}^{[(N-1)/2]} \mathcal{P}[|\Psi^+\rangle^{\otimes N-2j-1} |\Psi^-\rangle^{\otimes 2j+1}], \end{aligned} \quad (7)$$

where $[x]$ denotes the largest integer less than or equal to x (i.e., $\leq x$), and $\mathcal{P}[\cdot]$ is the permutation function for N elements of photon pairs. For example, we can rewrite the logical Bell state for $N = 3$ as

$$\begin{aligned} |\Phi_{(3)}^+\rangle &= \frac{1}{4}((|\Phi^+\rangle + |\Phi^-\rangle)^{\otimes 3} + (|\Phi^+\rangle - |\Phi^-\rangle)^{\otimes 3}) \\ &= \frac{1}{2}(|\Phi^+\rangle|\Phi^+\rangle|\Phi^+\rangle + |\Phi^+\rangle|\Phi^-\rangle|\Phi^-\rangle \\ &\quad + |\Phi^-\rangle|\Phi^+\rangle|\Phi^-\rangle + |\Phi^-\rangle|\Phi^-\rangle|\Phi^+\rangle) \\ &= \frac{1}{2}(|\Phi^+\rangle^{\otimes 3} + \mathcal{P}[|\Phi^+\rangle|\Phi^-\rangle^{\otimes 2}]), \end{aligned} \quad (8)$$

where $\mathcal{P}[|\Phi^+\rangle|\Phi^-\rangle^{\otimes 2}] = |\Phi^+\rangle|\Phi^-\rangle^{\otimes 2} + |\Phi^-\rangle|\Phi^+\rangle|\Phi^-\rangle + |\Phi^-\rangle^{\otimes 2}|\Phi^+\rangle$. Likewise, all other Bell states for $N = 3$ can be represented in this way.

Therefore, the four logical Bell states with arbitrary N photon encoding can be discriminated via N times of separated B_s measurements as illustrated in Fig. 1(c). Here, each B_s is performed on two photons; one is arbitrarily selected from the first and the other is from the second qubit. One can identify the logical Bell states from the results of N independent B_s measurements as follows:

$$\begin{aligned} |\Phi_{(N)}^+\rangle &: \text{even number of } B_s \text{ succeed with } |\Phi^-\rangle, \\ |\Phi_{(N)}^-\rangle &: \text{odd number of } B_s \text{ succeed with } |\Phi^-\rangle, \\ |\Psi_{(N)}^+\rangle &: \text{even number of } B_s \text{ succeed with } |\Psi^-\rangle, \\ |\Psi_{(N)}^-\rangle &: \text{odd number of } B_s \text{ succeed with } |\Psi^-\rangle, \\ \text{Failure} &: \text{all } B_s \text{ fail.} \end{aligned}$$

As the failure occurs only when none of the N times B_s measurements succeed, the four logical Bell states $|\Phi_{(N)}^\pm\rangle$ and $|\Psi_{(N)}^\pm\rangle$ can be discriminated with a success probability $P_s = 1 - 2^{-N}$. It is remarkable that the success probability rapidly approaches unity as N increases. For example, the success rate up to 99.6% can be achieved with $N = 8$ encoding. We note that our scheme for N photon encoding can be performed effectively via either spatially or temporally distributed N times of B_s measurements, irrespectively of the order of measurements. We will compare the efficiency of our scheme with other proposals in the following section.

III. COMPARISON WITH OTHER PROPOSALS

A. Other schemes to beat the 1/2 limit

Besides our proposal, many efforts have been devoted so far to improve the success probability of Bell measurement based on linear optics. We here consider several recent proposals employing single-photon qubits [6–8], and calculate its success probability in terms of the total number of photons (\bar{n}) used in the process for the comparison with our scheme. We will take into account the photons contained in the constructed logical qubits to be measured and in the ancillary states used in the measurement process as well as the increase of the average photon number by squeezing operation used in the process.

Grice's scheme. A scheme proposed by Grice [6] enhances the success probability of Bell-state discrimination employing ancillary entangled states of photons and photon number resolving detection in the Bell measurement process (see Ref. [6] for details). It increases the success probability up to $P_s = 1 - 2^{-N_a}$ by using $2^{N_a} - 2$ additional photons. Here N_a is the number of ancillary entangled states $|\Gamma_j\rangle$ with $j = 1, \dots, N_a - 1$, each of which contains 2^j photons. The total number of photons used in the Bell measurement process can be thus obtained by counting all photons in two logical qubits and the ancillary states. As we here consider single-photon encoding, two photons are used in two logical qubits. Thus, the total number of photons counted is $\bar{n} = 2 + 2^{N_a} - 2 = 2^{N_a}$, by which we can rewrite the success probability as $P_s = 1 - 1/\bar{n}$.

Zaidi and van Loock's scheme. Zaidi and van Loock proposed a scheme to improve the success probability of Bell

measurement for single photons in terms of inline squeezing operations accompanied by photon number resolving detections [8]. With this approach, the success probability up to 64.3% is achieved for dual-rail encoding (photon polarization encoding) and to 62.5% for single rail encoding (vacuum and single-photon state encoding). Let us here consider this scheme with dual-rail encoding in order to compare it with other schemes using single-photon polarization. In this scheme, each mode of Bell states is squeezed by a squeezing operator $\hat{S}(r) = \exp[-r(\hat{a}^{\dagger 2} - \hat{a}^2)/2]$ to improve the success probability of Bell discrimination. Here, r is the squeezing parameter and $\hat{a}^{\dagger}(\hat{a})$ is the creation (annihilation) operator. Suppose that Bell states, here assumed to be as $|\phi^{\pm}\rangle = (|HH\rangle \pm |VV\rangle)/\sqrt{2}$, pass through a beam splitter as $U_{\text{BS}}|\phi^{\pm}\rangle$ and then are squeezed. They can be written in the dual-rail representation as

$$\frac{i}{2}(|2'0'0'0'\rangle + |0'0'0'2'\rangle \pm |0'2'0'0'\rangle \pm |0'0'2'0'\rangle), \quad (9)$$

where $|n'\rangle = \hat{S}(r)|n\rangle$. The average photon number \bar{n} in all four modes can be calculated by

$$\langle \phi^{\pm} | \hat{S}_{1,2,3,4}(-r)(\hat{n}_1 + \hat{n}_2 + \hat{n}_3 + \hat{n}_4)\hat{S}_{1,2,3,4}(r) | \phi^{\pm} \rangle, \quad (10)$$

where \hat{n}_i is the photon number operator in the i th mode and $\hat{S}_{1,2,3,4}(r) = \hat{S}_1(r)\hat{S}_2(r)\hat{S}_3(r)\hat{S}_4(r)$. If we use the relation

$$\hat{S}(-r)\hat{n}\hat{S}(r) = (\hat{a}^{\dagger} \cosh r - \hat{a} \sinh r)(\hat{a} \cosh r - \hat{a}^{\dagger} \sinh r), \quad (11)$$

the total average photon number in all four modes can be obtained as

$$\bar{n} = \langle \hat{n}_1 + \hat{n}_2 + \hat{n}_3 + \hat{n}_4 \rangle = 2 \cosh 2r + 4 \sinh^2 r. \quad (12)$$

The best value of r to achieve the highest success probability is investigated in Ref. [8] and given as $r = 0.6585$. With this value, the average photon number in the Bell state after the squeezing is obtained as $\bar{n} = 6.00029$, which yields the success probability of the Bell measurement as $P_s = 0.643$.

Ewert and van Loock's scheme 1. Ewert and van Loock proposed a scheme to discriminate the Bell states of single-photon qubits by using ancillary multiphoton entanglement [7]. This employs a similar method used in Grice's scheme [6] and photon number resolving detection to increase the success probability. In the proposed Bell measurement setup, the total number of photons used in a single process can be counted as $\bar{n} = 4N_m + 2$ where N_m is the number of ancillary states. The success probability achieved using N_m ancillary entangled states is given by $P_s = 1 - 2^{-N_m - 1}$. Thus, we can rewrite the success probability by the average total photon number used in the process \bar{n} as $P_s = 1 - 2^{-\bar{n}/4 - 1/2}$.

Ewert and van Loock's scheme 2. Recently, another scheme of linear optical Bell measurement was proposed [14] by employing parity-state encoding with multiphotons [15]. The logical qubit is constructed with n blocks each containing m photons. It was shown that the success probability reaches up to $P_s = 1 - 2^{-n}$ similarly with our scheme. As the number of photons contained in each logical Bell state is $2 \times n \times m$, we can write the success probability of Bell measurement by using the average photon number used in the process $\bar{n} = 2nm$ as $P_s = 1 - 2^{-\bar{n}/2m}$.

B. Bell measurement with other physical qubits

Instead of single photons, other optical degrees of freedom can be used to construct the logical qubit in linear optical quantum-information processing. We will here consider two previous proposals employing other optical qubits to compare with our scheme.

Coherent-state qubits. One of the well-known approaches employs two coherent states $|\alpha\rangle$ and $|\alpha\rangle$ with amplitudes $\pm\alpha$, or alternatively their superposed states $|\alpha\rangle \pm |\alpha\rangle$, as a qubit basis. It was shown that a nearly deterministic Bell-state measurement is possible in this approach [9,10]. Quantum teleportation [16] and quantum computation schemes [9,10,17,18] based on the coherent-state encoding have been proposed and investigated. A drawback of this approach is that one cannot easily perform the local unitary transforms such as \hat{Z} operation due to nonorthogonality of two coherent states.

In this approach, the Bell measurement can be implemented as follows. If the four Bell states

$$\begin{aligned} |\Phi^{\pm}\rangle &= \mathcal{N}_{\pm}(|\alpha\rangle|\alpha\rangle \pm |\alpha\rangle|\alpha\rangle), \\ |\Psi^{\pm}\rangle &= \mathcal{N}_{\pm}(|\alpha\rangle|\alpha\rangle \pm |\alpha\rangle|\alpha\rangle), \end{aligned} \quad (13)$$

where $\mathcal{N}_{\pm} = (2 \pm 2e^{-4|\alpha|^2})^{-1/2}$, pass through a 50:50 beam splitter (BS), the resulting states are

$$\begin{aligned} |\alpha\rangle|\alpha\rangle \pm |\alpha\rangle|\alpha\rangle &\xrightarrow{\text{BS}} (|\sqrt{2}\alpha\rangle \pm |-\sqrt{2}\alpha\rangle)|0\rangle, \\ |\alpha\rangle|\alpha\rangle \pm |\alpha\rangle|\alpha\rangle &\xrightarrow{\text{BS}} |0\rangle(|\sqrt{2}\alpha\rangle \pm |-\sqrt{2}\alpha\rangle). \end{aligned} \quad (14)$$

As $|\sqrt{2}\alpha\rangle + |-\sqrt{2}\alpha\rangle$ and $|\sqrt{2}\alpha\rangle - |-\sqrt{2}\alpha\rangle$ contain respectively an even and odd number of photons, two parity measurements acting on two output modes discriminate between the four Bell states. Here, the even number state $|\sqrt{2}\alpha\rangle + |-\sqrt{2}\alpha\rangle$ yields the case when no photon is detected in both detectors, due to the nonzero overlap of $\langle 0 | \pm \sqrt{2}\alpha \rangle = e^{-\alpha^2}$, which is counted as a failure. Assuming equal input probabilities of four Bell states, we can then calculate the average success probability of the Bell measurement as $P_s = 1 - \mathcal{N}_{\pm}^2 \langle 0 | (|\sqrt{2}\alpha\rangle + |-\sqrt{2}\alpha\rangle)^2 / 2 = 1 - (2 \cosh 2\alpha^2)^{-1}$. We can also obtain the average photon number included in the Bell states, by averaging $\langle \hat{n}_1 + \hat{n}_2 \rangle$ for all four Bell states, resulting in

$$\bar{n} = |\alpha|^2 \left(\frac{1 - e^{-2\alpha^2}}{1 + e^{-4\alpha^2}} + \frac{1 + e^{-2\alpha^2}}{1 - e^{-4\alpha^2}} \right), \quad (15)$$

which we will use later to compare our scheme with respect to the success probability for the average photon number used in the process.

Optical hybrid qubits. Recently, a hybrid approach was proposed by combining both approaches for single photons and coherent-state qubits [11,12]. The logical qubit is constructed based on the orthonormal basis, $\{|0_L\rangle = |+\rangle|\alpha\rangle, |1_L\rangle = |-\rangle|\alpha\rangle\}$, where $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$. It was shown that this approach enables a near-deterministic quantum teleportation as well as deterministic \hat{X} and \hat{Z} operations using linear optics. In this scheme, the logical Bell-state measurement can be performed using two independent Bell-state measurements, the standard Bell measurement (B_s) for the single-photon part and the coherent-state Bell

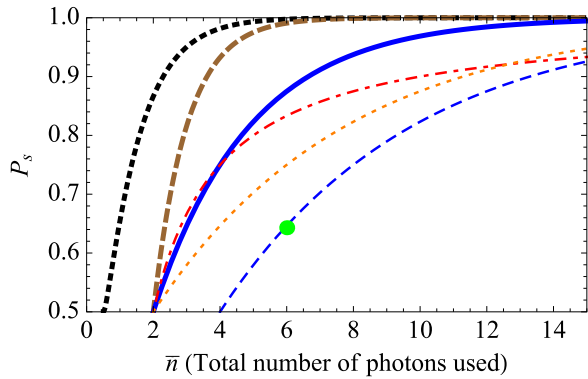


FIG. 2. (Color online) The success probability of Bell measurements against the average photon number (\bar{n}) used in the process. The black thick dotted curve is for the coherent-state qubits, the brown thick dashed curve for optical hybrid qubits, the blue thick curve for our scheme. The blue dashed curve is for Zaidi and van Loock's scheme 2 when $m = 2$ (it is the same with ours when $m = 1$). The red dot-dashed curve is for Grice's scheme, the orange dotted curve is for Ewert and van Loock's scheme, and the green circle at $P_s = 0.643$ and $\bar{n} = 6.00029$ is for Zaidi and van Loock's scheme 1.

measurement described above for the coherent-state part. The logical Bell measurement can be successfully performed unless both Bell measurements on each part fail so that its success probability is given as $P_s = 1 - e^{-2\alpha^2}/2$. As the average number of photons contained in any single Bell state is obtained as $\bar{n} = 2 + 2\alpha^2$, we can rewrite the success probability by \bar{n} as $P_s = 1 - e^{-\bar{n}+2}/2$.

C. Comparison with our scheme

In our scheme, the single Bell measurement process consumes a total of $2N$ photons as each logical Bell state contains $2N$ photons and no additional photons are used in the process. Thus, the success probability of Bell measurement can be written as $P_s = 1 - 2^{-\bar{n}/2}$ with the average photon number $\bar{n} = 2N$ used in the process. We plot P_s against \bar{n} for our scheme and all other above-mentioned schemes in Fig. 2. We will present some observations about the results and comparisons of our scheme with others as below:

(i) Our scheme shows the best performance among the schemes employing single-photon qubits, with respect to the attained success probability against the average photon number (\bar{n}) used in the process. For example, our scheme can reach $P_s = 0.996$ by using total $\bar{n} = 16$ photons for the Bell measurement. On the other hand, the attained success probabilities by other Bell measurement schemes suggested by Grice [6], Zaidi and van Loock [8], and Ewert and van Loock [7] are much lower than ours with the same number of photon usage. Moreover, our scheme does not require photon number resolving detectors in contrast to these schemes [6–8].

(ii) The scheme recently proposed by Ewert *et al.* [14], similarly with ours, employs multiphoton entanglement encoding. The logical qubit is constructed in the form of the parity-state encoding [15], devised to tolerate photon losses by containing n blocks of m photons, i.e., total nm photons. It also enables one to perform near-deterministic Bell measurement with the

success probability, $1 - 2^{-n}$, similarly with ours. However, in order to achieve $P_s = 1 - 2^{-n}$, it uses total $2nm$ photons. The attained success probability against the average photon number usage is the same as ours when $m = 1$, and becomes worse with increasing m (see the blue dashed line in Fig. 2 for the case when $m = 2$). It was also pointed out in Ref. [14] that, under the effects of photon losses, increasing n yields higher success probability than increasing m .

(iii) The schemes with coherent-state encoding [9,10] or optical hybrid encoding [11,12] yield higher success probabilities than ours for the same average photon number usage as we can see in Fig. 2. This is due to the fact that the success probability of coherent-state Bell measurement, employed in both (coherent-state encoding and hybrid encoding) schemes, dramatically increases as the amplitude of the coherent states gets higher. However, it requires the exact discrimination of even and odd number of photons, which becomes more difficult to realize for higher amplitudes. We stress again that, in contrast, our scheme only requires photon on-off detectors, which is a considerable advantage to realize.

IV. APPLICATION TO QUANTUM-INFORMATION PROCESSING

In this section, we will consider the application of our scheme to quantum communication and all-optical quantum computation. We will also investigate the effects of photon loss, which is the major detrimental factor of errors for the optical implementation of quantum-information processing [2].

In our analysis, we have made some assumptions as follows. The resource states required for logical qubits or entangled channels for gate teleportation, e.g., GHZ entanglement of multiphotons, are assumed to be prepared by off-line processes. The evolution of optical quantum states in a lossy environment is obtained by solving the master equation [19]

$$\frac{d\rho}{dt} = \gamma(\hat{J} + \hat{L})\rho, \quad (16)$$

where $\hat{J}\rho = \sum_i \hat{a}_i \rho \hat{a}_i^\dagger$, $\hat{L}\rho = -\sum_i (\hat{a}_i^\dagger \hat{a}_i \rho + \rho \hat{a}_i^\dagger \hat{a}_i)/2$, and \hat{a}_i (\hat{a}_i^\dagger) is the annihilation (creation) operator for the i th mode. Here, γ is the decay constant, and the loss rate is defined as $\eta = 1 - e^{-\gamma t}$. It is assumed that all optical systems, from the logical qubits to teleportation channels, experience the same loss effects with rate η . During the generation process of entangled quantum channel, loss also occurs with rate η so that some imperfect resource states in which photons may be lost at one or more modes are possibly supplied into in-line communication or computation. The logical qubits are assumed to be prepared in ideal pure states when they are first supplied into the in-line process. During the in-line process, the same loss rate η is applied to each photonic mode of the qubits for each gate operation and corresponding time in quantum memory. Details of our analysis will be presented in the following subsections.

A. Quantum communication

Our Bell measurement scheme is useful for the implementation of quantum communications. At first, it immediately enhances the success probability of the standard quantum teleportation [20]. In our approach, an unknown qubit is prepared with N photon encoding as $|\phi_N\rangle_A = a|+\rangle_A^{\otimes N} + b|-\rangle_A^{\otimes N}$ at site A . The channel state $|+\rangle_A^{\otimes N}|+\rangle_B^{\otimes N} + |-\rangle_A^{\otimes N}|-\rangle_B^{\otimes N}$ is distributed between site A and B . Here, both the qubit and channel states are in the form of GHZ entanglement. First, the sender located at site A carries out our Bell measurement scheme, i.e., N times of B_s measurements, where each B_s is acting on two photons, one from $|\phi_N\rangle_A$ and the other from the site A of the channel state. The receiver at site B can then retrieve the input state $|\phi_N\rangle$ by performing appropriate unitary transforms, either Pauli X (bit flip) or Z (phase flip) or both operations, which can be implemented deterministically as we will explain in the following Sec. IV B. The success probability of quantum teleportation with N photon encoding is just given as $P_s = 1 - 2^{-N}$, equal to that of the logical Bell measurement. Therefore, a near-deterministic quantum teleportation can be achieved by employing only linear optics and photon on-off detectors. For example, if four-photon entangled logical qubit and eight-photon entangled channel states are used, the success probability of quantum teleportation becomes higher than 90%.

In the realization of quantum communications, photon loss is unavoidable. An arbitrarily encoded qubit $|\phi_N\rangle = a|+\rangle^{\otimes N} + b|-\rangle^{\otimes N}$ evolves under a lossy environment into a mixed state in the form of

$$(1-\eta)^N |\phi_N\rangle\langle\phi_N| + \frac{1}{2} \sum_{k=1}^N \binom{N}{k} (1-\eta)^{N-k} \eta^k \times (|\phi_{N-k}\rangle\langle\phi_{N-k}| + |\phi_{N-k}^-\rangle\langle\phi_{N-k}^-|), \quad (17)$$

where $\binom{N}{k}$ denotes the binomial coefficient and η is the loss rate on each photonic mode. As one can see here, the total loss probability of each logical qubit is given by $P = 1 - (1-\eta)^N$. The probability that k photons are lost out of N is $\binom{N}{k} (1-\eta)^{N-k} \eta^k$ and its possible resulting state is either $|\phi_{N-k}\rangle = a|+\rangle^{\otimes N-k} + b|-\rangle^{\otimes N-k}$, or $|\phi_{N-k}^-\rangle = a|+\rangle^{\otimes N-k} - b|-\rangle^{\otimes N-k}$. Note that there is no logical error in the former state, while the latter contains a Pauli- Z error. Therefore, if a photon is lost from any single mode of a logical qubit, it experiences a Pauli- Z error with probability $1/2$.

The logical Bell measurement is also affected by photon losses. During the quantum teleportation process, losses occur possibly at both the input qubit and the channel states. We thus here consider the Bell measurements performed on two qubits in the assumption that they both experience photon losses with the same rate η . In our Bell measurement scheme [see Fig. 1(c)], N times of B_s measurements are performed independently on two photons; one is from the qubit and the other is from the channel. If either of the two photons are lost, the B_s fails. The probability that losses occur at k times of B_s can be written by

$$\binom{N}{k} \{(1-\eta)^2\}^{(N-k)} \{1 - (1-\eta)^2\}^k = \binom{N}{k} (1-\eta)^{2(N-k)} \eta^k (2-\eta)^k. \quad (18)$$

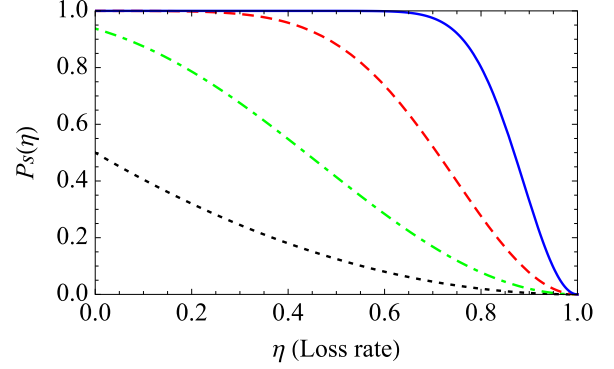


FIG. 3. (Color online) The success probabilities of quantum teleportation under the effect of photon losses (η) based on our Bell measurement scheme with N -photon encoding; the black dotted curve for single photon ($N = 1$), the green dot-dashed curve for $N = 4$, the red dashed curve for $N = 16$, and the blue curve for $N = 80$ photon encoding.

Therefore, we can obtain the total success probability of Bell measurements under losses as

$$P_s(\eta) = 1 - \sum_{k=0}^N \binom{N}{k} (1-\eta)^{2(N-k)} \eta^k (2-\eta)^k \left(\frac{1}{2}\right)^{N-k} = 1 - \left(\frac{1+\eta(2-\eta)}{2}\right)^N, \quad (19)$$

which becomes $P_s(0) = 1 - 2^{-N}$ when there is no loss $\eta = 0$ and $P_s(1) = 0$ for $\eta = 1$. Assuming that no additional operational errors occur during the Bell measurement and feedforward operations, the success probability of teleportation under a lossy environment is obtained as $P_s(\eta)$. We plot $P_s(\eta)$ against the loss rate η for different encoding numbers N in Fig. 3. It shows us that in principle quantum teleportation can be implemented with arbitrary high success probability under a lossy environment by increasing the encoding number N in our scheme. Note that here we do not consider the Pauli Z error caused by losses, which can be propagated to the teleported qubit with probability $1/2$. Such a Pauli logical error should be corrected by employing error correction codes, details of which will be considered in the following subsections.

For a long-distance quantum communication, the distance between the sender and receiver is limited by the effects of photon losses and quantum repeaters are necessary at intermediated locations [21]. As quantum repeaters typically require Bell measurements to complete the protocol [14,22], our scheme can be possibly employed to enhance the performance of such a protocol, which will be a possible future work.

B. Universal gate operations

In order to realize universal quantum computation, a set of logical quantum gates is necessary, by which any logical operation is in principle possible to construct. For example, Pauli X , arbitrary Z (phase) rotation, Hadamard, and a controlled- Z (CZ) operations constitute such a universal set. In our framework, Pauli X and arbitrary Z (phase) operations are straightforward to implement using linear optical elements.

The Pauli X (bit flip) operation can be performed by flipping $|+\rangle \leftrightarrow |-\rangle$ implemented by a polarization rotator at all photon modes. An arbitrary Z (phase) operation can be performed by applying the phase-shift operation only a single photonic mode: $\{|+\rangle, |-\rangle\} \rightarrow \{|+\rangle, e^{i\theta}|-\rangle\}$, and no operation is required for the other modes. Thus, both the Pauli X and arbitrary Z (phase) operations are deterministic in our approach.

In order to realize the Hadamard and CZ gates, we here employ the gate teleportation protocol with specific types of entangled states [23]. For the Hadamard operation, the entangled state $|Z\rangle \approx |0_L\rangle|0_L\rangle + |0_L\rangle|1_L\rangle + |1_L\rangle|0_L\rangle - |1_L\rangle|1_L\rangle$ should be used as the quantum channel for teleportation. If one performs a standard teleportation of unknown qubit $|\phi\rangle$ with the channel $|Z\rangle$, the output state is given as the $\hat{H}|\phi\rangle$ where \hat{H} indicates the Hadamard gate. Likewise, one can realize the CZ gate operation by performing two-qubit teleportation with $|Z'\rangle \approx |0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle$ where $|0000\rangle = |0_L\rangle|0_L\rangle|0_L\rangle|0_L\rangle$ and so on, as the quantum channel for teleportation. In this case, the cost is the preparation of multiphoton entanglement as resource states. As the success probability of the Hadamard or CZ gates is the same as the success probability of the logical Bell measurements, it is possible to implement these operations nearly deterministically by increasing the number of photons N in a logical qubit.

Alternatively, other approaches for the realization of the Hadamard and CZ gates, such as the Knill-Laflamme-Milburn (KLM) scheme [3] or the parity encoded scheme used in Refs. [15,24,25], may be considered: Such approaches may possibly reduce the resource requirements in gate operations in comparison to gate teleportation in which many resources are consumed to prepare the channel states $|Z\rangle$ and $|Z'\rangle$ (details will be discussed in Sec. IV C), however it may require more feedforward operations than gate teleportation.

The effects of photon losses should be also considered for the implementations of quantum computing. A logically encoded qubit with N photons may be affected by losses during the in-line process, resulting in the same form as Eq. (17), which contains some logical errors. When performing gate teleportation for the Hadamard and CZ gate operations, the success probability of Bell measurement is also deteriorated by photon losses. Here we assume that the resource channels $|Z\rangle$ and $|Z'\rangle$ are prepared off-line and immediately used such that only the input qubits are subjected to losses. In this case, the Bell measurement fails with rate $(1/2)^{N-k}$ when k photons are lost in the qubit. Thus, we can calculate the success probability of the gate teleportation with loss rate η as

$$\begin{aligned} P'_s(\eta) &= 1 - \sum_{k=0}^N \binom{N}{k} (1-\eta)^{N-k} \eta^k \left(\frac{1}{2}\right)^{N-k} \\ &= 1 - \left(\frac{1+\eta}{2}\right)^N, \end{aligned} \quad (20)$$

where $\binom{N}{k}$ represents the binomial coefficient. It becomes $P'_s(0) = 1 - 2^{-N}$ when there is no loss $\eta = 0$, and $P'_s(1) = 0$ for $\eta = 1$. It is higher than the one obtained in Eq. (18) as we assumed here that loss occurs only at the input qubit modes (no loss at the channel states).

During the computation process, several errors are caused by photon losses. Some of the errors are detectable by measurements during the gate operations, which are called “locatable” [2], while other errors propagate and can only be corrected by an error correction code. This latter kind are called “unlocatable.” As we can see in Eq. (17), losses occur with the rate P in quantum memory or gate operations. If any single photon is lost, the logical qubit experiences a Pauli Z error with probability $1/2$. The loss errors in quantum memory as well as deterministic operations, such as the Pauli X or arbitrary Z rotation, are unlocatable. On the other hand, the errors in Hadamard or CZ gates caused by losses are in fact immediately detectable by missing photons at the detectors during the logical Bell measurement. Moreover, as the gate teleportation scheme is used here, missing photons in the input qubit are compensated at the output qubit as far as the teleportation succeeds.

C. Fault-tolerant quantum computation

In order to build arbitrary large-scale quantum computers, it should be justified that they can be implemented with tolerance to small errors: so-called fault-tolerance [26]. For this, the amount of noise per operation with appropriate error corrections should be below a fault-tolerant threshold. We thus carried out numerical simulations to obtain the threshold for our scheme with a given loss rate η . We here employ the seven qubit STEANE code [27] with several levels of concatenation based on the circuit-based telecorrection [28], in order to directly compare its performance with previous other schemes employing the same correction code and circuit [11,18,25,28]. Note that the STEANE code can correct arbitrary logical or unlocatable errors, but for the purpose of this calculation we assume that the other errors are negligible compared to the loss errors.

We will employ the modified telecorrection circuit composed of CZcz, Hadamard, $|+\rangle$ state, and X -basis measurement [18]. Let us define the error model for our approach as follows: When Hadamard or CZ gates fail, the output qubit is assumed to experience depolarization, which can be modeled by a random Pauli operation, i.e., Pauli Z and X operation independently act on the logical qubit with the equal probability $1/2$. For the other loss errors in quantum memory or gate operations, Pauli Z operation is applied to the qubit with probability $1/2$. We use this error model for the lowest level of concatenation, while the same error model described in Ref. [28] is used for higher levels of concatenation. Based on this approach, we performed a series of Monte Carlo simulation (using C++) to obtain the corrected error rates for a range of η with different N . The resulting corrected error rates in a lower level are used for the error rates for the elements used in the next level of error correction. If the error rates tend to zero in the limit of many levels of concatenation, it is guaranteed that in principle the fault-tolerant quantum computation is possible with those certain η and N .

In this way, the noise thresholds of our scheme with different N are obtained as shown in Table I. Interestingly, the largest threshold is obtained when the logical qubit is encoded with four photons ($N = 4$). Note that a further increase of N lowers the threshold, which may be due to unlocatable

TABLE I. Fault-tolerant noise thresholds (η) for different numbers of photons in a logical qubit (N) using the seven-qubit STEANE code and the telecorrection protocol [28]. The highest threshold is obtained when $N = 4$.

N	Noise threshold η	N	Noise threshold η
3	1.3×10^{-3}	7	1.1×10^{-3}
4	1.7×10^{-3}	8	0.9×10^{-3}
5	1.5×10^{-3}	9	0.7×10^{-3}
6	1.3×10^{-3}	10	0.6×10^{-3}

errors becoming dominant for larger N encoding. Let us then compare the result with those obtained by other schemes. The threshold obtained by our scheme ($\sim 1.7 \times 10^{-3}$) is much higher than those for coherent-state qubits ($\sim 2 \times 10^{-4}$) [9,10,17,18] and optical hybrid qubits ($\sim 5 \times 10^{-4}$) [11]. On the other hand, it is almost equivalent to the one using parity-states encoding with entangled photons [15,25]. Even much higher thresholds may be attainable by employing recently proposed topological error codes [31,32], which will be a possible future work.

The number of resources required for one round of error correction is another important factor to analyze the scalability of quantum computation. One can estimate the resource requirements of the telecorrection scheme by the following estimation. The total number of operations in one round of telecorrection is about 1000 [2] and the element operations are used with the following fractions [18,28]: memory 0.284, Hadamard 0.098, CZ 0.343, diagonal state 0.164, and X -basis measurement 0.111. If we assume that the number N_H , N_{CZ} , and $N_{|+\rangle}$ of resources are consumed to prepare the Hadamard, CZ gate, and the diagonal state, respectively, and none for the others. Then, the total resource requirements for one round of error corrections is obtained by

$$98N_H + 343N_{CZ} + 164N_{|+\rangle}.$$

In fact, it depends on the form of the required entangled states and the efficiency of their generation methods. In our scheme, as explained in Sec. IV B, the entangled states $|Z\rangle$ and $|Z'\rangle$ are used as the channel for gate teleportation to realize Hadamard and CZ gate, respectively. If we assume conditional generation of $|Z\rangle$ and $|Z'\rangle$ from entangled photon pairs, e.g., using the fusion gate operation [33], the resource cost increases exponentially with increasing N the number of photon in a logical qubit. On the other hand, any on-demand or efficient generation scheme for such multiphoton entanglement will be able to reduce dramatically the resource requirements. Recently, such multiphoton entanglement has been experimentally produced [34]. For example, GHZ entanglement up to eight photons [29,30] and cluster states up to eight photons [31] have been successfully generated. Several on-demand generation schemes were proposed theoretically [35,36] and are expected to be realized, e.g., based on semiconductor quantum dots [37].

V. CONCLUSIONS

We have presented a detailed scheme for nearly deterministic Bell measurement using multiphoton entanglement

and linear optics proposed in Ref. [13]. The limitation that only two of four Bell states can be identified by the standard Bell measurement B_s is overcome by the GHZ type of multiphoton entanglement and N times of B_s measurements, where N is the number of photons in a logical qubit. The logical Bell measurement is performed through N times of B_s measurements, and it fails only when none of those N times of B_s measurements succeeds. Therefore, the success probability of the logical Bell measurement is given as $1 - 2^{-N}$, which rapidly approaches unity as N increases.

We have compared the efficiency of our scheme with those of other previous schemes proposed to improve the success probabilities of Bell measurement based on linear optics; several schemes were proposed based on single-photon qubits [6–8,14] or other optical qubits such as coherent state [9,10] and optical hybrid qubits [11]. We showed that our scheme outperforms other schemes employing single-photon qubits, with respect to the attained success probability in terms of the average number of photons used in the process. Although the scheme using coherent-state or optical hybrid qubits achieves a higher success probability than ours by consuming the same number of photons on average, a considerable advantage of our scheme over all the other schemes is that it does not require photon number resolving detections but only photon on-off detection suffices.

We have demonstrated that our scheme can be effectively used for the implementation of quantum teleportation and all-optical quantum computation. The success probability of quantum teleportation increases rapidly to unity as increasing N , the number of photons in the qubit and channel states. We showed that in our approach fault-tolerant quantum computation is possible under photon losses. It is remarkable that the highest noise threshold is obtained with four-photon encoded qubits and eight-photon entangled channels that are accessible within current technologies [34]. For example, eight-photon GHZ entangled states have been recently generated successfully in optics laboratories [29,30].

Interestingly, our Bell measurement scheme can be implemented via either spatially or temporally distributed and independent N times B_s measurements. Such an experiment may be considered not only with spatially separated N -mode entangled states but also with temporal mode entanglement as done in Refs. [38–40]. For a temporally distributed implementation, only one standard Bell measurement device, illustrated in Fig. 1(a) [4], will be sufficient to perform independent N times of B_s measurements for a logical Bell measurement. We finally note that our idea for a distributed Bell measurement scheme, in principle, is not limited to photonic qubits but can be applied to any multipartite systems with other physical degrees of freedom. Our work reveals the possibility of using multipartite entanglement for efficient quantum communication and computation.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (Grant No. 2010-0018295). K.P. acknowledges financial support from Grant No. GA14-36681G

of the Czech Science Foundation. T.C.R. was supported by the Australian Research Council Centre of Excellence

for Quantum Computation and Communication Technology (Project No. CE110001027).

-
- [1] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Rev. Mod. Phys.* **79**, 135 (2007).
- [2] T. C. Ralph and G. J. Pryde, *Prog. Opt.* **54**, 209 (2010).
- [3] E. Knill, R. Laflamme, and G. J. Milburn, *Nature (London)* **409**, 46 (2001).
- [4] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, *Phys. Rev. A* **59**, 3295 (1999).
- [5] J. Calsamiglia and N. Lütkenhaus, *Appl. Phys. B* **72**, 67 (2001).
- [6] W. P. Grice, *Phys. Rev. A* **84**, 042331 (2011).
- [7] F. Ewert and P. van Loock, *Phys. Rev. Lett.* **113**, 140403 (2014).
- [8] H. A. Zaidi and P. van Loock, *Phys. Rev. Lett.* **110**, 260501 (2013).
- [9] H. Jeong, M. S. Kim, and J. Lee, *Phys. Rev. A* **64**, 052308 (2001).
- [10] H. Jeong and M. S. Kim, *Phys. Rev. A* **65**, 042305 (2002); *Quantum Inf. Comput.* **2**, 208 (2002).
- [11] S.-W. Lee and H. Jeong, *Phys. Rev. A* **87**, 022326 (2013).
- [12] S.-W. Lee and H. Jeong, in *Proceedings of the First International Workshop on Entangled Coherent States and Its Application to Quantum Information Science* (Tamagawa University, Tokyo, 2012), pp. 41–46.
- [13] S.-W. Lee, K. Park, T. C. Ralph, and H. Jeong, *Phys. Rev. Lett.* **114**, 113603 (2015).
- [14] F. Ewert, M. Bergmann, and P. van Loock, [arXiv:1503.06777](https://arxiv.org/abs/1503.06777).
- [15] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, *Phys. Rev. Lett.* **95**, 100501 (2005).
- [16] S. J. van Enk and O. Hirota, *Phys. Rev. A* **64**, 022313 (2001).
- [17] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, *Phys. Rev. A* **68**, 042319 (2003).
- [18] A. P. Lund, T. C. Ralph, and H. L. Haselgrove, *Phys. Rev. Lett.* **100**, 030503 (2008).
- [19] S. J. D. Phoenix, *Phys. Rev. A* **41**, 5132 (1990).
- [20] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [21] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature (London)* **414**, 413 (2001).
- [22] K. Azuma, K. Tamaki, and H.-K. Lo, *Nat. Commun.* **6**, 6787 (2015).
- [23] D. Gottesman and I. L. Chuang, *Nature (London)* **402**, 390 (1999).
- [24] A. Gilchrist, A. J. Hayes, and T. C. Ralph, *Phys. Rev. A* **75**, 052328 (2007).
- [25] A. J. F. Hayes, H. L. Haselgrove, A. Gilchrist, and T. C. Ralph, *Phys. Rev. A* **82**, 022323 (2010).
- [26] P. W. Shor, in *Proceedings of the 37th Annual Symposium on Fundamentals of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1996), pp. 56–65.
- [27] A. M. Steane, *Phys. Rev. A* **54**, 4741 (1996).
- [28] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen, *Phys. Rev. A* **73**, 052306 (2006).
- [29] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, *Nat. Photon.* **6**, 225 (2012).
- [30] Y.-F. Huang, B.-H. Liu, L. Peng, Y.-H. Li, L. Li, C.-F. Li, and G.-C. Guo, *Nat. Commun.* **2**, 546 (2011).
- [31] X.-C. Yao, T.-X. Wang, H.-Z. Chen, W.-B. Gao, A. G. Fowler, R. Raussendorf, Z.-B. Chen, N.-L. Liu, C.-Y. Lu, Y.-J. Deng, Y.-A. Chen, and J.-W. Pan, *Nature (London)* **482**, 489 (2012).
- [32] S. D. Barrett and T. M. Stace, *Phys. Rev. Lett.* **105**, 200502 (2010).
- [33] D. E. Browne and T. Rudolph, *Phys. Rev. Lett.* **95**, 010501 (2005).
- [34] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Zukowski, *Rev. Mod. Phys.* **84**, 777 (2012).
- [35] C. Schön, E. Solano, F. Verstraete, J. I. Cirac, and M. M. Wolf, *Phys. Rev. Lett.* **95**, 110503 (2005).
- [36] N. H. Lindner and T. Rudolph, *Phys. Rev. Lett.* **103**, 113602 (2009).
- [37] R. J. Young, R. M. Stevenson, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields, *New J. Phys.* **8**, 29 (2006).
- [38] A. Zavatta, M. D’Angelo, V. Parigi, and M. Bellini, *Phys. Rev. Lett.* **96**, 020502 (2006).
- [39] M. D’Angelo, A. Zavatta, V. Parigi, and M. Bellini, *J. Mod. Opt.* **53**, 2259 (2006).
- [40] H. Jeong, A. Zavatta, M. Kang, S.-W. Lee, L. S. Costanzo, S. Grandi, T. C. Ralph, and M. Bellini, *Nat. Photon.* **8**, 564 (2014).