HOKKAIDO UNIVERSITY

| | |
|---|---|
| Title | Analog Quantum Computation and Communication with Digitized Continuous Variables [an abstract of entire text] |
| Author(s) | 福井, 浩介 |
| Description | この博士論文全文の閲覧方法については、以下のサイトをご参照ください。<br>https://www.lib.hokudai.ac.jp/dissertations/copy-guides/ |
| Degree Grantor | 北海道大学 |
| Degree Name | 博士(工学) |
| Dissertation Number | 甲第13299号 |
| Issue Date | 2018-09-25 |
| Doc URL | https://hdl.handle.net/2115/71849 |
| Type | doctoral thesis |
| File Information | Kosuke_Fukui_summary.pdf |

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

学位論文内容の要約

博士の専攻分野の名称　博士（工学）　氏名　福井　浩介

学位論文題名

**Analog Quantum Computation and Communication with Digitized Continuous Variables**

**(連続量状態を用いたアナログ量子情報処理に関する研究)**

Big data analytics is valuable for text analytics, machine learning, predictive analytics, data mining, statistics, businesses, and so on. Nowadays size of world's data in is growing exponentially. The exploding volume of data growth has led to several challenges: data center power, cooling, storage, data movement, and management complexity, and so on. Quantum computation (QC) is an attractive tool to perform faster processing speed for big data analytics, since QC has been shown to solve efficiently some hard problems for conventional computers. For the conventional computers, a simulation of the many-body physical systems is generally inefficient, since the computer memory to simulate the systems is required exponentially in proportion to the increasing of the size of the systems. In 1982, Richard Feynman came up with the idea of a quantum computer that bring out the advantage of quantum mechanics, which can simulate quantum systems efficiently. In 1985, David Deutsch proposed the quantum Turing machine. In the quantum Turing machine, a "*qubit*", which can hold a quantum superposition of 0 and 1, enable us to encode many inputs to a logic circuit simultaneously, and then it can make calculations on all the inputs at the same time. In 1994, Peter Shor showed that his proposed algorithm for integer factorization can be performed exponentially less operations than the most efficient known algorithm[1]. Shor's algorithm, processing on a quantum computer, can factorize even integers of orders exceeding 1000 used for RSA-encryption in reasonable time. In 1996, Grover proposed a database search algorithm to perform a polynomial speedup over the best classical algorithm. In Grover's algorithm, amplitude amplification of the intended quantum state is employed, which is an important techique in quatum algorithm [2].

Today, in several candidates for a element of quantum computer, the accuracy of quantum gates have made progress toward a goal of the threshold value required by large-scale QC. For example, in the superconducting and trapped-ion qubit, the error probability of a two-qubit gate has been less than 1%. However, these prototype systems of quantum computer are small; none of them contain as many as 20 qubits, since cracking RSA Encrypt that requires a 100-million-qubit system can not be achievable in presence technology.

Unfortunately, a large-scale quantum circuit that requires scalable entangled states is still a significant experimental challenge for most candidates of qubits. Among the candidates, in QC with the continuous variables, squeezed vacuum states with the optical setting have shown great potential to generate scalable entangled states because the entanglement is generated by only beam splitter coupling between two squeezed vacuum states [3]. However, scalable computation with squeezed vacuum states has been shown to be difficult to achieve because of the accumulation of errors during the QC process, even though the states are created with perfect experimental apparatus [4]. Therefore, fault-tolerant protection from noise is required that uses the quantum error correcting code. Because noise accumulation originates from the "continuous" nature of the continuous variable, it can be circumvented by encoding continuous variables into digitized variables using an appropriate code, such as Gottesman–Kitaev–Preskill (GKP) code [5], which are referred to as GKP qubits. In 2014, Menicucci showed that large-scale QC with continuous variables is possible within the framework of measurement-based QC using squeezed vacuum states with GKP qubits [4]. Moreover, GKP qubits keep the advantage of squeezed vacuum states on optical implementation that they can be entangled by only a beam splitter coupling. Hence, GKP qubits offer a promising element for the implementation of FTQC with continuous variables. Regarding the generation of the GKP qubit, a promising proposal [6] exists to prepare a good GKP qubit in circuit quantum electrodynamics with the squeezing level around 10 dB [7] within the reach of near-term experimental set-up. This implies that large-scale QC is possible, if the required squeezing level of the initial single qubit for FTQC is less than 10 dB.

To be practical, the squeezing level required for large-scale QC should be experimentally achievable. Unfortunately, the required squeezing level is still high, and it is highly desirable to reduce the required squeezing level to

around 10 dB to realize the large-scale QC. Thus, another twist is necessary to reduce the required squeezing level. It is analog information contained in the GKP qubit that has been overlooked. The effect of noise on continuous variable states is observed as a deviation in an analog measurement outcome, which includes beneficial information for quantum error correction. Despite this, the analog information from the GKP qubit has been wasted because the GKP qubit has been treated as only a discrete variable qubit, for which the measurement outcomes are described by bits, when we identify the bit value. Harnessing the wasted information for the QEC will improve the error tolerance compared with using the conventional method based on only bit information.

To alleviate the required squeezing level for large-scale QC with the GKP qubits, we propose the analog quantum error correction in chapter 3 and high-threshold QC in chapter 4, where the analog quantum error correction is applied to the surface code and the resource state for QC is constructed with a low error accumulation with the help of analog information. In chapter 5, we also present a novel method to reduce the number of qubits required for the quantum error correction during large-scale QC, where the logical-qubit level quantum error correction is partially substituted for the single-qubit level quantum error correction. In chapters 6 and 7, in addition to the implementation of large-scale QC, toward long-distance quantum communication, we present several novel methods that offer the way of long-distance quantum communication with the GKP qubit. Chapter 8 is devoted to summary and conclusions. In this thesis based on the works in Refs. [8–10] and the works in preparation.

Chapter 3 contains an introduction to the analog quantum error correction and the application for several quantum error correcting codes such as the repetition codes, the concatenated code, and the surface code.

Because quantum states has intrinsically continuous nature, the measurement outcome is also analog information using an appropriate detector such as homodyne and hetelodyne detectors. In the measurement of the GKP qubit using a homodyne detector, we make a decision on the bit value $k(=0,1)$, digital information, from the measurement outcome of the GKP qubit $q_{\rm m} = q_k + \Delta_{\rm m}$ to minimize the deviation $|\Delta_{\rm m}|$, where $q_k(k=0,1)$ is defined as $(2t+k)\sqrt{\pi}(t=0,\pm1,\pm2,\cdots.)$ as shown in Fig. 1(a). If we consider only digital information $k$, as in conventional QEC, we waste the analog information contained in $\Delta_{\rm m}$. To utilize the analog information, in this chapter, we consider a likelihood function and propose a maximum-likelihood method to improve the QEC performance.

We here define the true deviation $|\bar{\Delta}|$ as the difference between the measurement outcome and true peak value $\bar{q}_k$, that is, $|\bar{\Delta}| = |\bar{q}_k - q_m|$. We consider the following two possible events: one is the correct decision, where the true deviation value $|\bar{\Delta}|$ is less than $\sqrt{\pi}/2$ and equals to $|\Delta_{\rm m}|$ as shown in Fig. 1(b). The other is the incorrect decision, where $|\bar{\Delta}|$ is greater than $\sqrt{\pi}/2$ and satisfies $|\bar{\Delta}| + |\Delta_m| = \sqrt{\pi}$, as shown in Fig. 1(c). Because the true deviation value obeys the Gaussian distribution function $f(\bar{\Delta})$, we can evaluate the probabilities of the two events by

$$f(\bar{\Delta}) = \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{-\bar{\Delta}^2/(2\sigma^2)}. \tag{1}$$

In our method, we regard function $f(\bar{\Delta})$ as a likelihood function. Using this function, the likelihood of the correct decision is calculated by

$$f(\bar{\Delta}) = f(\Delta_{\rm m}). \tag{2}$$

The likelihood of the incorrect decision, whose $|\bar{\Delta}|$ is $\sqrt{\pi} - |\Delta_{\rm m}|$, is calculated by

$$f(\bar{\Delta}) = f(\sqrt{\pi} - |\Delta_{\rm m}|). \tag{3}$$

We can reduce the decision error on the entire code word by considering the likelihood of the joint event and choosing the most likely candidate.

To provide an insight into our method, we apply the analog QEC to the repetition code. As a simple example, we focus on the three-qubit bit-flip code. In this code, a single logical qubit $|\widetilde{\psi}\rangle_{\rm L}$=$\alpha\,|\widetilde{0}\rangle_{\rm L} + \beta\,|\widetilde{1}\rangle_{\rm L}$, where $|\alpha|^2 + |\beta|^2 = 1$, is encoded into three GKP qubits. The two logical basis states $|\widetilde{0}\rangle_{\rm L}$ and $|\widetilde{1}\rangle_{\rm L}$ are defined as

$$|\widetilde{0}\rangle_{\rm L} = |\widetilde{0}\rangle_1 |\widetilde{0}\rangle_2 |\widetilde{0}\rangle_3, \qquad |\widetilde{1}\rangle_{\rm L} = |\widetilde{1}\rangle_1 |\widetilde{1}\rangle_2 |\widetilde{1}\rangle_3, \tag{4}$$

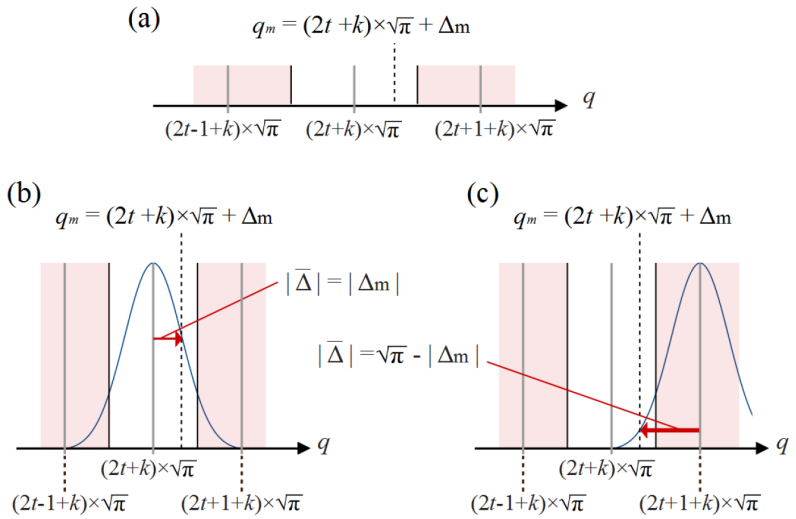


FIG. 1. Introduction of a likelihood function. (a) Measurement outcome and deviation from the peak value in $q$ quadrature. The dotted line shows the measurement outcome $q_m$ equal to $(2t+k)\sqrt{\pi}+\Delta_m$ $(t=0,\pm1,\pm2,\cdots,\ k=0,1)$, where $k$ is defined as the bit value that minimizes the deviation $\Delta_m$. The red areas indicate the area that yields code word $(k+1)$ mod 2, whereas the white area denotes the area that yields the codeword $k$. (b) and (c) Gaussian distribution functions as likelihood functions of the true deviation value $\overline{\Delta}$represented by the arrows. (b) refers to the case of the correct decision, where the amplitude of the true deviation value is $|\overline{\Delta}| < \sqrt{\pi}/2$, whereas (c) the case of the incorrect decision $\sqrt{\pi}/2 < |\overline{\Delta}| < \sqrt{\pi}$.

respectively. In the QEC with the three-qubit bit-flip code, the error identification for the GKP qubits is substantially different from that for QEC using only digital information. While the parity of the code qubits is transcribed on the ancilla qubit in QEC using only digital information, the deviation of the physical GKP qubits is projected onto the deviation of the ancillae.

We explain how the deviation of the physical GKP qubits is projected onto the deviation of the ancillae in the following. Fig.2 shows a quantum circuit for the QEC with the three-qubit bit-flip code. This circuit looks almost the same as the circuit for digital information apart from the third ancilla qubit. However, the error identification for the GKP qubits is substantially different from that for QEC using only digital information. In this circuit, the sum of deviations of the physical GKP qubits $i$ and $i+1$ $(i=1,2)$ are projected onto the ancilla $i$. The deviation of the physical GKP qubit 3 is projected onto ancilla 3. First, a single logical qubit $|\widetilde{\psi}\rangle_{\rm L}$ is prepared by two controlled-not (CNOT) gates acting on the data qubit $|\widetilde{\psi}\rangle_1 = \alpha\,|\widetilde{0}\rangle_1 + \beta\,|\widetilde{1}\rangle_1$ and two ancillae $|\widetilde{0}\rangle_i$ ( $i$ = 2, 3). The CNOT gate, which corresponds to the operator $\exp(-i\hat{q}_{\rm L}\hat{p}_{\rm A})$, transforms

$$\hat{q}_{\rm L} \to \hat{q}_{\rm L}, \qquad \hat{p}_{\rm L} \to \hat{p}_{\rm L} - \hat{p}_{\rm A}\ , \tag{5}$$

$$\hat{q}_{\rm A} \to \hat{q}_{\rm A} + \hat{q}_{\rm L}, \qquad \hat{p}_{\rm A} \to \hat{p}_{\rm A}, \tag{6}$$

where $\hat{q_{\rm L}}$ ($\hat{q_{\rm A}}$) and $\hat{p_{\rm L}}$ ($\hat{p_{\rm A}}$) are the $q$ and $p$ quadrature operators of the logical (ancilla) qubit, respectively. Then, the Gaussian quantum channel displaces the $q$ and $p$ quadratures randomly and independently, and increases the variance of the three physical GKP qubits. After the Gaussian quantum channel, the bit-flip error correction is implemented using the three ancillae $|\widetilde{0}\rangle_{{\rm A}j}$ ($j$=1, 2) and $|\widetilde{+}\rangle_{\rm A3}$. Before the CNOT gates in the error correction circuit, the true deviation values of the physical GKP qubits and ancillae in the $q$ quadrature, which obey Gaussian distribution with mean zero, are denoted by $\overline{\Delta}_j$ and $\overline{\Delta}_{{\rm A}j}$ ($j$=1, 2, 3), respectively. For simplicity, because the ancilla qubits are fresh, we assume that the initial variance is much smaller than that of the physical qubits of the logical qubit. Then, the CNOT gates change the true deviation values of three ancillae $\overline{\Delta}_{{\rm A}j}$ in $q$ quadrature as follows:

$$\begin{aligned}
&\overline{\Delta}_{\rm A1} \to \overline{\Delta}_{\rm A1} + \overline{\Delta}_1 + \overline{\Delta}_2 = \overline{\Delta}_1 + \overline{\Delta}_2\ ,\\
&\overline{\Delta}_{\rm A2} \to \overline{\Delta}_{\rm A2} + \overline{\Delta}_2 + \overline{\Delta}_3 = \overline{\Delta}_2 + \overline{\Delta}_3\ ,\\
&\overline{\Delta}_{\rm A3} \to \overline{\Delta}_{\rm A3} + \overline{\Delta}_3 = \overline{\Delta}_3\ .
\end{aligned} \tag{7}$$

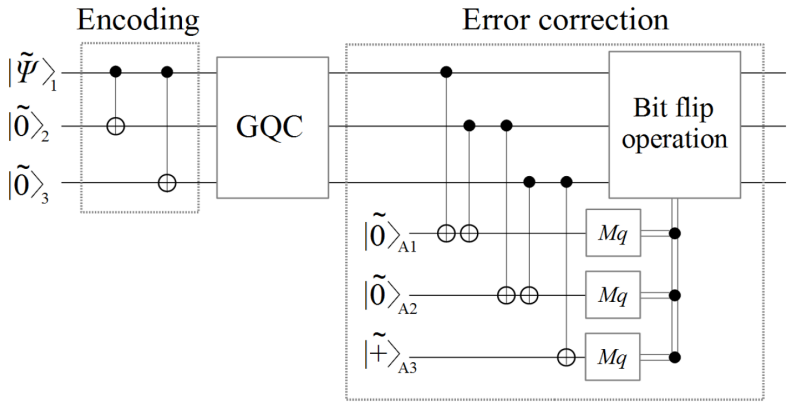


FIG. 2. A quantum circuit of the QEC for the three-qubit bit-flip code with GKP qubits using the proposed method. The data qubit $|\widetilde{\psi}\rangle_1$ and two GKP qubits $|\widetilde{0}\rangle_2$ and $|\widetilde{0}\rangle_3$ encode a single logical qubit. $|\widetilde{0}\rangle_{A1}$, $|\widetilde{0}\rangle_{A2}$, and $|\widetilde{+}\rangle_{A3}$ denote ancilla qubits for the QEC. The Gaussian quantum channel and $M_q$ denote the Gaussian quantum channel and measurements of ancillae in $q$ quadrature, respectively.

Therefore, the sum of deviations of the physical GKP qubits $i$ and $i+1$ ($i = 1,2$) are projected onto the ancilla $i$. The deviation of physical GKP qubit 3 is projected onto ancilla 3.

From the measurement of the three ancillae in $q$ quadrature, we obtain the outcome $q_{\mathrm{m,A}i} = q_0 + \Delta_{\mathrm{m,A}i}$ ($i$ = 1, 2) from ancillae 1 and 2, and $q_{\mathrm{m,A3}} = q_k + \Delta_{\mathrm{m,A3}}$ ($k$ = 0, 1) from ancilla 3, under the conditions $\Delta_{\mathrm{m,A}i} \in [-\sqrt{\pi}, \sqrt{\pi}]$ and $\Delta_{\mathrm{m,A3}} \in [-\sqrt{\pi}/2, \sqrt{\pi}/2]$. We then define the values $\delta_1 = \Delta_{\mathrm{m,A1}} - \Delta_{\mathrm{m,A2}} + \Delta_{\mathrm{m,A3}}$ and $\delta_2 = \Delta_{\mathrm{m,A2}} - \Delta_{\mathrm{m,A3}}$. For $i$ = 1, 2, if $\delta_i \in [-\sqrt{\pi}, \sqrt{\pi}]$, then we define the values $M_i$=$\delta_i$. Otherwise, if $\delta_i \in [\sqrt{\pi}, 2\sqrt{\pi}]$, we define the values $M_i$=$\delta_i - 2\sqrt{\pi}$, and if $\delta_i \in [-2\sqrt{\pi}, -\sqrt{\pi}]$, we define the values $M_i$= $2\sqrt{\pi} + \delta_i$. Error identification is executed from $M_1$ and $M_2$ as follows. If both $|M_1|$ and $|M_2|$ are smaller than $\sqrt{\pi}/2$, we decide that no error occurs on the logical qubits. Otherwise, we consider two error patterns: one containing a single error, and the other containing double errors. For the first pattern, we presume that the true deviation values $\overline{\Delta}_i$ ($i$ = 1, 2) and $\overline{\Delta}_3$ of the qubits in the logical qubit are $M_i$ and $\Delta_{\mathrm{m,A3}}$, respectively. Then, the likelihood of the first pattern $F_1$ is given by

$$F_1 = f(M_1) f(M_2) f(\Delta_{\mathrm{m,A3}}). \tag{8}$$

For the second pattern, if $M_i \in [0, \sqrt{\pi}]$, we presume that $\overline{\Delta}_i$ is $M_i{}^* = M_i - \sqrt{\pi}$, and if $M_i \in [-\sqrt{\pi}, 0]$, we presume that $\overline{\Delta}_i$ is $M_i{}^* = M_i + \sqrt{\pi}$. If $\Delta_{\mathrm{m,A3}} \in [0, \sqrt{\pi}/2]$, we presume $\overline{\Delta}_3$ to be $\Delta^*_{\mathrm{m,A3}} = \Delta_{\mathrm{m,A3}} - \sqrt{\pi}$, and if $\Delta_{\mathrm{m,A3}} \in [-\sqrt{\pi}/2, 0]$, we presume that $\overline{\Delta}_3$ is $\Delta^*_{\mathrm{m,A3}} = \Delta_{\mathrm{m,A3}} + \sqrt{\pi}$. Then, the likelihood of the second pattern $F_2$ is given by

$$F_2 = f(M_1{}^*) f(M_2{}^*) f(\Delta^*_{\mathrm{m,A3}}). \tag{9}$$

Hence, we can use the likelihood functions $f(|\Delta_{\mathrm{m}}|)$ and $f(\sqrt{\pi} - |\Delta_{\mathrm{m}}|)$ to compare the two error patterns and decide the more likely pattern. For example, if $M_1$ is in the range $[\sqrt{\pi}/2, \sqrt{\pi}]$, and both $M_2$ and $\Delta_{\mathrm{m,A3}}$ are in the range $[0, \sqrt{\pi}/2]$, we consider the first error pattern as a single error on qubit 1 of the logical qubit and the second error pattern as double errors on qubits 2 and 3. If $F_1 > F_2$, we decide that the first error pattern occurs, and vice versa. In error identification, the likelihood that $|\overline{\Delta}_i|$ is greater than $\sqrt{\pi}$ is not taken into account because it is always less than $\sqrt{\pi}$ provided $|\overline{\Delta}_i|$ is less than $\sqrt{\pi}$. In the conventional manner, based on majority voting with binary measurement outcomes, the first error pattern is invariably selected because an estimation using only digital information yields a larger probability for a single error than that for double errors.

We numerically simulated the QEC for the three-qubit bit-flip code using the Monte Carlo method. In this simulation, it is assumed that the encoded data qubit is prepared perfectly, that is, the initial variances of the data qubit and ancillae are zero, and the variances of the GKP qubits of the encoded data qubit increase independently in the Gaussian quantum channel. These assumptions are set to allow a clear comparison between the conventional and proposed methods. The numerical results confirm that our method suppresses errors more effectively than the conventional method that uses only digital information. To obtain a failure probability less than $10^{-9}$, the standard

deviation should be less than 0.25 for the proposed method, whereas it needs to be less than 0.21 for the conventional method, which corresponds to the squeezing level of 9.0 dB and 10.6 dB, respectively. This improvement comes from the fact, as mentioned before, that our method can correct double errors, whereas the conventional method corrects only a single error.

In addition to the three-qubit the three-qubit bit-flip code, we have numerically simulated the QEC process using the $C_4/C_6$ code [11] and the surface code [12, 13]. In the decoding of the QEC process with the $C_4/C_6$ code, we applied the analog QEC to a maximum likelihood method for a concatenated code proposed with a message-passing algorithm by Poulin [14], and later Goto and Uchikawa [15] for Knill's $C_4/C_6$ code [11]. We refer to the full paper (Ref. [9]) for the detailed explanation of our method. In the decoding of the QEC proces with the surface code, we employ the minimum distance decoding, which can be done efficiently by a minimum-wight perfect matching algorithm [16, 17] employed to find the most likely location of the errors according to the error syndrome. We refer to the full paper (Ref. [8]) for the detailed explanation of our method. Numerical results have shown that the QEC using the $C_4/C_6$ code and the surface code with the analog QEC can achieve the hashing bound close to the quantum capacity of the Gaussian quantum channel, that is, our method provides a optimal performance against the Gaussian quantum channel. On the other hand, the $C_4/C_6$ code and the surface code without analog QEC provides suboptimal performance, where the QEC is performed using only digital information.

In chapter 4, we propose high-threshold large-scale QC to alleviate the required squeezing level for large-scale QC by harnessing analog information contained in the GKP qubit. The proposed method consists of two parts (We refer to the full paper Ref. [9] for the detailed explanation of our method). One part of our method is to apply analog QEC [8] to topologically protected measurement based QC [12, 13, 18, 19], which is one of the best candidates among all quantum computation models and allows us to implement the high-threshold large-scale QC.

The other part of our method is highly-reliable measurement with the help of analog information, and its application to the construction of the 3D cluster state for topologically protected measurement based QC with a low error accumulation using the proposed highly-reliable measurement, which we call it HRM. In general, the errors on a qubit, which causes degradation of the threshold, is accumulated as the number of the entangling gate increases. To avoid this accumulation of errors, we develop the HRM described as below. In the HRM, we introduce an upper limit $v_{\mathrm{up}}$ and give the maximum deviation that will not cause incorrect measurement of the bit value as shown in

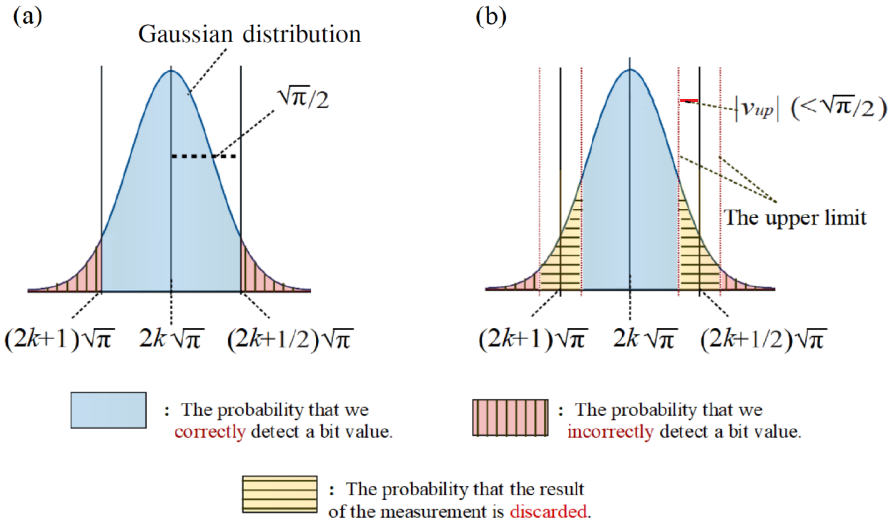


FIG. 3. Introduction of the highly-reliable measurement (HRM). (a) The conventional measurement of the GKP qubit, where the Gaussian distribution followed by the deviation of the GKP qubit that has variance $\sigma^2$. The plain (blue) region and the region with vertical (red) line represent the different code word $(k-1)$ mod 2 and $(k+1)$ mod 2, respectively. The vertical line regions correspond to the probability of incorrect decision of the bit value. (b) The highly-reliable measurement. The shown dot line represents a upper limit $v_{\mathrm{up}}$. The horizontal line areas show the probability that the results of the measurement is discarded by introducing $v_{\mathrm{up}}$. The vertical line areas show the probability that our method fails.

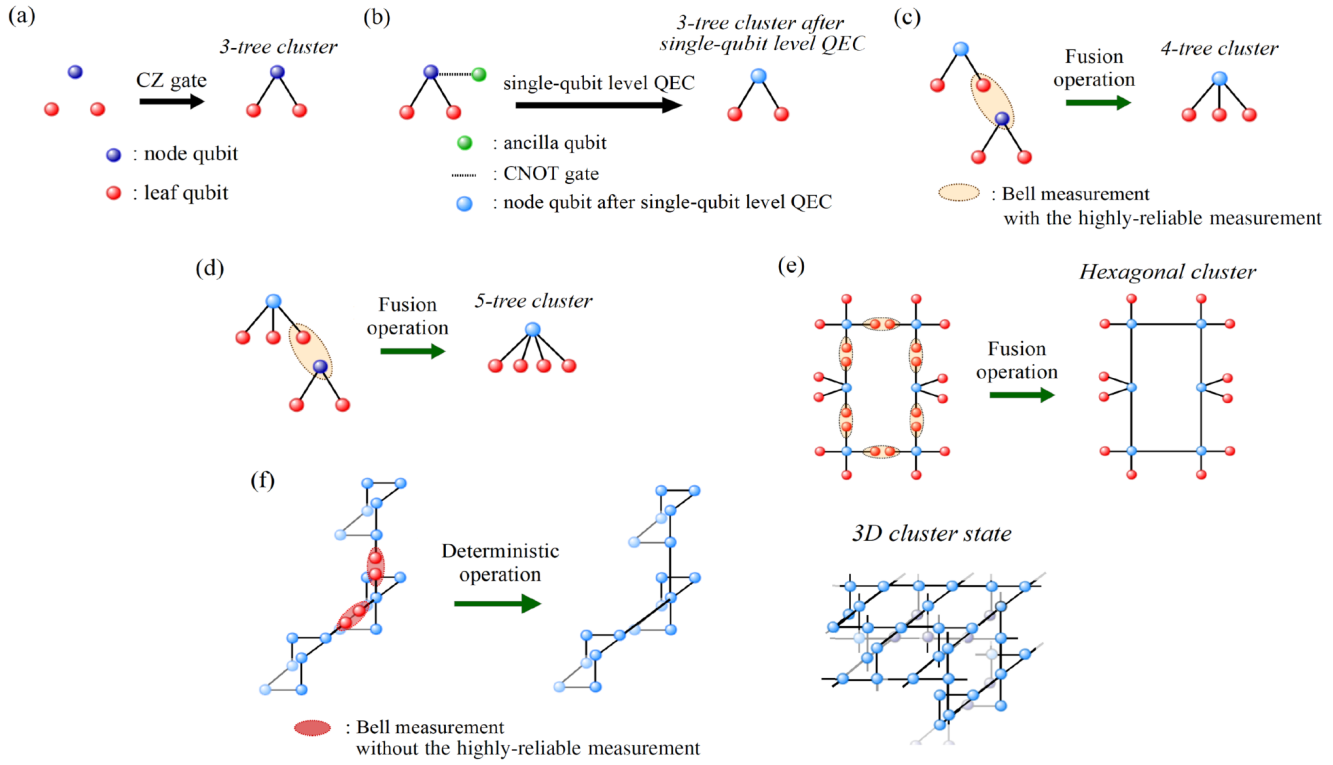


FIG. 4. The 3D cluster state construction. (a) The preparation of the 3-tree cluster state by using the CZ gate. (b) The single-qubit level QEC using the additional ancilla qubit with the HRM. (c)–(e) The construction of the hexagonal cluster state from the 3-tree qubit with the HRM. (f) The construction of the 3D cluster state from the hexagonal cluster states, where the entanglement is generated between the neighboring hexagonal cluster states without the HRM.

Fig. 4 (b). As a result, the error probability decreases at the cost of the success probability of the measurement. In this work, we apply the HRM to the 3D cluster state construction to generate the 3D cluster state with a high fidelity. In the proposed 3D cluster state construction, there are four steps, where the HRM is used to prevent the noise of the deviation of the GKP qubit from propagating between the GKP qubits during the construction of the 3D cluster state.

In step 1, we prepare a node qubit and two leaf qubits of the variance $\sigma^2$ in the $q$ and $p$ quadrature (Fig. 4 (a)). By using the CZ gate, we obtain a 3-tree cluster state composed of a node qubit and two leaf qubits, where the variance of the node and leaf qubits in the $p$ quadrature increase from $\sigma^2$ to $3\sigma^2$ and $2\sigma^2$ , respectively. On the other hand, the variance of the node and leaf qubits in the $q$ quadrature keep $\sigma^2$. In step 2, we operate the single-qubit level QEC [5]with the HRM (Fig. 4 (b)). The single-qubit level QEC can reduce the variance of the node qubit in the $p$ quadrature from $3\sigma^2$ to $\sigma^2$, if the true deviation of the ancilla qubit in $p$ quadrature $\overline{\Delta}_p$ is less than $\sqrt{\pi}/2$. On the other hand, if $\overline{\Delta}_p$ is more than $\sqrt{\pi}/2$, the bit error in the $p$ quadrature occurs after the single-qubit level QEC. In our method, this error can be considerably reduced by the HRM on the ancilla. The reduction of the variance of the node qubit to $\sigma^2$ effectively improves the required squeezing level for FTQC. In step 3, we increase the number of the leaf qubits of the tree cluster state by using the fusion gate with the HRM. The fusion gate can avoid the deviation of the GKP qubit from increasing and the HRM can prevent the qubit-level error from propagating during constructing the 6-tree cluster state (Fig. 4(c)-(e)), which we call the hexagonal cluster state. As an example, we describe the construction of the 4-tree cluster state as follows. By using the fusion gate, we construct the 4-tree cluster state from the two 3-tree cluster states, one of which is corrected by the single-qubit level QEC and the other is uncorrected (Fig. 4 (c)). In the fusion gate, the Bell measurement with the HRM is implemented. If the misidentification of the bit value in the Bell measurement occurs, the feedforward operation according to Bell measurement propagates the qubit-level error in the 4-tree cluster. This unheralded qubit-level error can be considerably reduced by using the HRM.

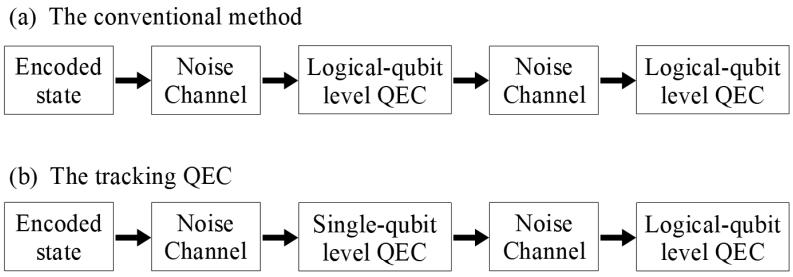


FIG. 5. Introduction of the tracking QEC. (a) The conventional QEC with the two QECs cycle, where the QECs are performed with the only logical-qubit level QEC. (b) The tracking QEC with the two QECs cycle, where the first logical-qubit level QEC in the conventional method is substituted for the single-qubit level QEC.

We simulated the QEC for topologically protected measurement-base quantum com by using the minimum-weight perfect matching algorithm. The numerical results confirm that our method can also suppress errors with the independent error model, and the threshold for the standard deviation can be improved from 0.208 to 0.228, which corresponds to squeezing level from 10.6 dB to 9.8 dB. In the numerical calculation, we set the upper limit $v_{\rm up}$ to $2\sqrt{\pi}/5$ in order to adopt the independent error model. Therefore, continuous variable large-scale QC with analog QEC and the HRM can improve the required squeezing level for topologically protected measurement-base quantum com by 6.2 dB in comparison to the existing scheme for continuous variable large-scale QC [4]. This improvement results of the required squeezing level corresponds to the reduction of the error probability to misidentify the single GKP qubit in $q$ and $p$ quadrature from $2.7 \times 10^{-15}$ to $7.4 \times 10^{-5}$. By the reduction of the squeezing level around 10 dB, we believe this work considerably take us closer to the realization of CV-FTQC, and will be indispensable to construct CV-FTQC. Furthermore, our method will provide highly versatile QEC with CV states, because our method can be applied to the GKP qubit, a cat code, binomial codes, and other various codes used to digitize

Chapter 5 contains a novel method to reduce the number of qubits required for the quantum error correction during large-scale QC. In large scale quantum computation, a large number of physical qubits is needed to obtain the highly accurate results of quantum computation. This required number of physical qubits is one issue that we should struggle toward the implementation of large scale quantum computation. In this chapter, we propose the method to reduce the number of qubits required for the QEC during large scale quantum computation, where the logical-qubit level QEC is partially substituted for the single-qubit level QEC. Since the single-qubit level QEC can not correct the qubit-level errors, the bit and phase flip errors, we just *track* the measurement outcomes in the single-qubit level QEC. Then, the QEC is performed by using a set of *tracked* measurement outcomes in QECs to correct the qubit-level errors.

We explain the method that the logical-qubit level QEC is partially substituted for the single-qubit level QEC [5] in the repeated QEC process as shown in Fig. 5 (b). In our method, we apply analog QEC [8] to the tracking QEC to improve the QEC performance. Since the single-qubit level QEC can reduce the error probability and the number of qubits required for the single-qubit level QEC is less than that for the logical-qubit level one, the substitution of the logical-qubit QEC for the single-qubit level one will reduce the required number of qubits.

To provide an insight into our method, we focus on the tracking QEC with the two QECs cycle, where the QEC after the Gaussian quantum channel is repeated twice as shown in Fig. 5. In the QEC, we obtain the measurement outcomes of bit values $m_{pi}$ and $m_{qi}$ for the $i$-th physical GKP qubit of the encoded data qubit and encoded qubit, respectively. In addition to bit values, we also obtain deviation values $\Delta_{\rm pmi}$ and $\Delta_{\rm qmi}$ for the $i$-th physical GKP qubit. In our method, the first and second QECs are performed by the single- and logical-qubit level QEC, respectively. Since the single-qubit level QEC can not correct the qubit-level error, we just *track* the measurement outcomes in the first QEC. After the two QECs, we obtain a set of the likelihoods are obtained from the results of the first and second QECs. From the set of the likelihoods in the two QECs, we consider the following two possible events: one is the correct decision, where the no qubit-level error occurs in both QECs. In this case, both true deviation values

of the first and second QECs, $|\overline{\Delta}^{(1)}|$ and $|\overline{\Delta}^{(2)}|$, are less than $\sqrt{\pi}/2$ or more than $\sqrt{\pi}/2$. When both true deviation values are less than $\sqrt{\pi}/2$, $|\overline{\Delta}^{(1)}|$ and $|\overline{\Delta}^{(2)}|$ are equal to $|\Delta_{\rm m}^{(1)}|$ and $|\Delta_{\rm m}^{(2)}|$, respectively. When both true deviation values are more than $\sqrt{\pi}/2$, $|\overline{\Delta}^{(1)}|$ and $|\overline{\Delta}^{(2)}|$ are equal to $\sqrt{\pi}-|\Delta_{\rm m}^{(1)}|$ and $\sqrt{\pi}-|\Delta_{\rm m}^{(2)}|$, respectively. The other is the incorrect decision, where the single error occurs in one of two QECs. In this case, one of two true deviation values of the first and second QECs are greater than $\sqrt{\pi}/2$, and satisfies $|\bar{\Delta}^{(1)}| = |{\Delta_{\rm m}}^{(1)}|$ and $|\bar{\Delta}^{(2)}|+|\Delta_{\rm m}^{(2)}| = \sqrt{\pi}$, or satisfies $|\bar{\Delta}^{(1)}|+|\Delta_{\rm m}^{(1)}| = \sqrt{\pi}$ and $|\bar{\Delta}^{(2)}| = |\Delta_{\rm m}^{(2)}|$, respectively. Hence, the likelihoods for the correct decision without and with analog QEC are calculated by

$$F_{\rm corr} = {p_{\rm corr}}^2 + (1-p_{\rm corr})^2, \tag{10}$$

$$F_{\rm corr}^{\rm ana} = f(|\Delta_{\rm m}^{(1)}|)f(|\Delta_{\rm m}^{(2)}|) + f(\sqrt{\pi}-|\Delta_{\rm m}^{(1)}|)f(\sqrt{\pi}-|\Delta_{\rm m}^{(2)}|), \tag{11}$$

respectively, where $p_{\rm corr}$ is given by Eq. (2.77). The likelihoods for the incorrect decision without and with analog QEC are calculated by

$$F_{\rm in} = 2(1-p_{\rm corr})p_{\rm corr}, \tag{12}$$

$$F_{\rm in}^{\rm ana} = f(|\Delta_{\rm m}^{(1)}|)f(\sqrt{\pi}-|\Delta_{\rm m}^{(2)}|) + f(\sqrt{\pi}-|\Delta_{\rm m}^{(1)}|)f(|\Delta_{\rm m}^{(2)}|), \tag{13}$$

respectively. By considering these likelihoods of the joint event and choosing the most likely candidate, we can reduce the decision error on the entire code word in the second logical-qubit level QEC. By contrast, in the conventional method, the two QECs are independently performed by the only logical-qubit level QEC. Although we focus on the tracking QEC with the GKP qubits, we note that the tracking QEC with the discrete variables can be also performed, where the likelihoods are given by only Eqs. (10) and (12). In our method, we utilize analog QEC using Eqs. (11) and (13) to transform the QEC performance of the single-qubit level QEC into that of the approximately logical-qubit level QEC as shown in the numerical calculations.

We here estimate the required number of physical qubits to implement the two QECs. In the $C_4/C_6$ code with the concatenation level $l$ ($l \geq 1$) and the $n$-QEC cycle, the number of the physical qubits for the conventional method $R_{\rm con}^{(n,l)}$ and proposed method $R_{\rm pro}^{(n,l)}$ are described as

$$R_{\rm con}^{(n,l)} = n \times 16 \times 12^{l-1}, \tag{14}$$

$$R_{\rm pro}^{(n,l)} = 2(n-1)4 \times 3^{l-1} + 16 \times 12^{l-1}, \tag{15}$$

respectively. Hence, the proposed method for the $n$-QEC cycle can reduce $R_{\rm con}^{(n,l)} - R_{\rm pro}^{(n,l)} = (n-1) \times \left\{ R_{\rm con}^{(2,l)} - R_{\rm pro}^{(2,l)} \right\}$ physical qubits, where the single- and logical-qubit level QECs are performed in the first $(n-1)$-QECs and the $n$-th QEC, respectively. We describe the reduction rate of the number of physical qubits per $n$-QEC cycle. For the $n$-QEC cycle using $C_4/C_6$ code with the level $l$, the reduction rate is obtained by

$$\frac{R_{\rm con}^{(n,l)} - R_{\rm pro}^{(n,l)}}{R_{\rm con}^{(n,l)}} = \frac{2(n-1) \times 4^{l-1} - n + 1}{2n \times 4^{l-1}}. \tag{16}$$

We simulate the QEC after the Gaussian quantum channel is repeated twice. In this simulation, we use the Knill's $C_4/C_6$ code [11] for the concatenation and assume that the encoded data qubit, encoded Bell state, and the physical qubits are prepared perfectly, and the variance of the GKP qubits of the encoded data qubit is increased to $\sigma^2$ only by the Gaussian quantum channel. In the noise channel of the Gaussian quantum channel with $n$-cycles, the logical-qubit suffers from each of $n$-noise channels independently by the same amount of the noise. For the 2-QEC cycle, numerical results have shown that the proposed method with analog QEC in the practical noise level can achieve efficient resource reduction by $16 \times 12^{l-1} - 8 \times 3^{l-1}$ physical qubits with the concatenation level $l$ with only a small impact on the QEC performance, where the reduction rate for the 2-QEC cycle is $(2 \times 4^{l-1} - 1)/(4 \times 4^{l-1}) = 1/2 - 1/(4 \times 4^{l-1})$. Hence, the reduction rate becomes close to 50 % for larger $l$, where the reduction rates are 25, 43.8, 48.4, 49.6 and 49.9 for the level 1, 2, 3, 4, and 5, respectively. Furthermore,

it has been shown that the analog QEC makes the performances of the single-qubit level QEC almost identical to those of the logical-qubit level QEC under the condition of a practical noise level. To the best of our knowledge, this approach is the first practical attempt to utilize both the single- and standard logical-qubit level QECs to alleviate the requirement of the number of qubits. Hence, the proposed method has a great advantage in implementing large-scale quantum computation with continuous variables and will open a new way to practical quantum computers.

In chapters 6 and 7, we propose the method to implement long-distance quantum communication with GKP qubits. The GKP qubits will be recognized as an important technological element to implement long-distance quantum communication with continuous variables, which is an important ingredient of the secure quantum internet [20] to implement secure communications [21, 22], distributed quantum cryptographic protocols, and so on. There are two reasons for the advantage of the implementation of quantum communication. One is that the GKP qubit has a superb error tolerance against the disturbance of a noise channel, comparing with the other continuous variable code such as the cat code and the binomial code. In fact, we have shown that the GKP qubit can provide an optimal performance against the Gaussian quantum channel in this thesis [8]. Furthermore, the GKP qubit can significantly outperform all other continuous variable codes, with respect to the bosonic pure-loss channel (i.e. photon loss channel) after the optimal recovery operation [23]. The other is that the ability to deterministically generate the entanglement generation is useful for a quantum repeater that is indispensable element, where quantum repeaters between the sender Alice and the receiver Bob are needed to achieve the polynomial scaling of the efficiency with the total distance between Alice and Bob. This advantage of the GKP qubit regarding the entanglement generation leads to achieve the high secret key rate as compared with the repeater protocol using only photon qubits, since the protocol using only photon qubits needs numerous photon qubits to succeed entanglement generation in all of quantum repeaters between Alice and Bob.

Chapter 6 contains the entanglement distillation protocol with the GKP qubit using analog information to improve the entanglement distillation performance toward long-distance quantum communication. The entanglement distillation protocol is an essential tool to distribute the entangled states with a high-fidelity between a distant party, which is used to implement quantum information processing such as quantum key distribution, quantum communication based on quantum repeaters, teleportation, dense coding, distributed quantum computation, and so on. In this chapter, we focus on a so-called quantum privacy amplification protocol [24]. Firstly, we model the quantum privacy amplification protocol for ideal and approximate GKP qubits. Next, we propose the quantum privacy amplification protocol with the GKP qubit using analog information to improve the entanglement distillation performance. In the proposed method, the HRM is applied to the conventional entanglement distillation protocol. We numerically calculated the performance of the quantum privacy amplification protocol to valid our method. The numerical results have shown that the proposed method has a great advantage in enhancing the performance of a quantum privacy amplification even with a very noisy channel, where the conventional method can not work. Hence, our method will bring up virtue of the HRM with continuous variables in quantum communication with continuous variables, and open up a promising avenue to quantum communication with continuous variables.

In chapter 7, we present a method to implement long-distance quantum communication with GKP qubits. In this chapter, we propose the method to implement long-distance and resource-efficient quantum repeater protocol using analog information contained in the GKP qubit. In the proposed method, we apply the HRM using GKP qubits to "all photonic quantum repeater protocol" based on photon qubits to enhance tolerance against photon loss. To evaluate our method based on the GKP qubit, we compare our method with the method based on photon qubit such as Azuma *et al*.'s method [25]. For example as numerical results, our method can achieve the value ($L_{\mathrm{AB}}$, $E^X_{AB}$, $P_{\mathrm{suc}}$, $N_{\mathrm{qubit}}$) = (800 km, 4.7%, 49%, 130) for the upper limit $v_{up}$=0.214 $\sqrt{\pi}$, where $L_{\mathrm{AB}}$, $E^X_{AB}$, $P_{\mathrm{suc}}$, and $N_{\mathrm{qubit}}$ are the distance Alice and Bob, the $X$ (bit flip) error probability of entanglement shared by Alice and Bob, the success probability of the entanglement generation between Alice and Bob, and the number of photons prepared at each node for each blind cluster state, respectively. By contrast, Azuma *et al*.'s method achieve the value ($L_{\mathrm{AB}}$, $E^X_{AB}$, $P_{\mathrm{suc}}$, $N_{\mathrm{qubit}}$) = (800 km, 4.1%, 60%, 24,440). Therefore, our method can achieve the comparative performance with

the conventional methods based on photon qubits. Furthermore, our method can reduce the number of the GKP qubits required for quantum communication by several orders of magnitude less than the conventional method. In addition, we have obtained the results that our analog quantum error correction can improve the performance of our method. Furthermore, our method can be not limited to the GKP qubit but widely applicable to improve the performance of the quantum repeater protocols, which can incorporate with GKP qubit, cat code, and other various codes used to digitize continuous variable states. Hence, we believe the proposed method will open up a new approach to quantum repeater protocol with digitized continuous variable states, which will be indispensable to construct quantum communication with continuous variables.

Chapter 8 is devoted to summary and conclusions.

---


[1] P. W. Shor. SIAM J. Comp. **26**, 1484 (1997) .
[2] L. K. Grover. Phys. Rev. Lett. **79**, 325 (1997).
[3] J. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa. APLPhotonics **1** 060801 (2016) .
[4] N. C. Menicucci. Phys. Rev. Lett. **112**, 120504 (2014) .
[5] D. Gottesman, A. Kitaev, and J. Preskill. Phys. Rev. A **64**, 012310 (2001).
[6] B. M. Terhal and D. Weigand. Phys. Rev. A **93**, 012315 (2016).
[7] M. A. Castellanos-Beltran, K. D. Irwin, G. C. Hilton, L. R. Vale, and K. W. Lehnert. Nat. Physics **4**, 929-931 (2008) .
[8] K. Fukui, A. Tomita, and A. Okamoto. Phys. Rev. Lett. 119, 180507 (2017).
[9] K. Fukui, A. Tomita, A. Okamoto, and K. Fujii. Phys. Rev. X. **8**, 021054 (2018).
[10] K. Fukui, A. Tomita, and A. Okamoto. Phys. Rev. A, **98**, 022326 (2018) .
[11] E. Knill. Nature, **434**, 39-44 (2005) .
[12] A. Y. Kitaev. Ann. Phys. **303**, 2 (2003).
[13] R. Raussendorf and J. Harrington. Phys. Rev. Lett. **98**, 190504 (2007) .
[14] D. Poulin. Phys. Rev. A **74**, 052333 (2006) .
[15] H. Goto and H. Uchikawa. Sci. Rep. **3**, 2044 (2013 .
[16] J. Edmonds. Canadian Journal of mathematics **17**, 449 (1965).
[17] V. Kolmogorov. Mathematical Programming Computation**1**, 43 (2009) .
[18] R. Raussendorf, J. Harrington, and K. Goyal. New J. Phys. **9**, 199 (2007) .
[19] R. Raussendorf, J. Harrington, and K. Goyal. *A fault-tolerant one-way quantum computer,*Annals of Physics **321**, 2242 (2006) .
[20] H. J. Kimble. Nature **453**, 1023 (2008).
[21] C. H. Bennett and G. Brassard. in *Proceeding of the IEEE International Conference on Computers, Systems,and Signal Processing, Bangalore, India* 175-179 (IEEE,New York, 1984).
[22] A. K. Ekert. Phys. Rev. Lett. **67**, 661 (1991).
[23] V. V. Albert, K. Noh, K. Duivenvoorden, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang. arXiv: 1708.05010 (2017) .
[24] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Phys. Rev. Lett. **77**, 2818 (1998) .
[25] K. Azuma, K. Tamaki, and H-K. Lo. Nat.Commu. **6**, 6787 (2015).