mathematics

MDPI

Article

A Remote Quantum Error-Correcting Code Preparation Protocol on Cluster States

Qiang Zhao [1,2], Haokun Mao [1], Yucheng Qiao [3], Ahmed A. Abd El-Latif [1,4,5] and Qiong Li [1,*]

[1] Information Countermeasure Technique Institute, School of Cyberspace Science, Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China
[2] Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong 999077, China
[3] School of Information Engineering, Guilin University of Electronic Science and Technology, Guilin 541004, China
[4] EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[5] Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shibin Al Kawm 32511 , Egypt
* Correspondence: qiongli@hit.edu.cn

Abstract: The blind quantum computation (BQC) protocol allows for privacy-preserving remote quantum computations. In this paper, we introduce a remote quantum error correction code preparation protocol for BQC using a cluster state and analyze its blindness in the measurement-based quantum computation model. Our protocol requires fewer quantum resources than previous methods, as it only needs weak coherent pulses, eliminating the need for quantum memory and limited quantum computing. The results of our theoretical analysis and simulations show that our protocol requires fewer quantum resources compared to non-coding methods with the same qubit error rate.

Keywords: blind quantum computation; quantum error-correcting code; cluster state; preparation

MSC: 81P73

check for updates

Citation: Zhao, Q.; Mao, H.; Qiao, Y.; El-Latif, A.A.A.; Li, Q. A Remote Quantum Error-Correcting Code Preparation Protocol on Cluster States. *Mathematics* **2023**, *11*, 3035. https://doi.org/10.3390/math11143035

Academic Editors: Carsten Schneider and Jonathan Blackledge

Received: 20 May 2023
Revised: 27 June 2023
Accepted: 5 July 2023
Published: 8 July 2023

1. Introduction

With the rapid development of quantum technology, quantum computing has attracted increasing attention from researchers because of its theoretically super-high computing power. In the classical field, it is very hard for conventional computers to deal with the non-deterministic polynomial (NP) problems. However, these tasks have the potential to be solved by a quantum computer in the future [1–6]. At present, a practical quantum computer requires large-scale quantum resources, expensive equipment, and low-temperature environment, etc., which ordinary clients cannot afford. A blind quantum computation (BQC) protocol as an optimal potential solution can address this problem at hand. By harnessing of the power of BQC, the client (Alice) can effectively delegate intricate computing tasks to a remote quantum server (Bob) while guaranteeing the privacy of Alice's information [7–9]. The breakthrough of QBC is not only the low cost of overcoming Alice's computing limitations but also protecting sensitive data well. In recent years, many extension BQC protocols have emerged [10–16]. The universal blind quantum computation (UBQC) proposed by Broadbent, Fitzsimons, and Kashefi [9] is very popular among these protocols, in which Alice only needs to prepare the single-photon states.

In UBQC, the preparation is a very important process [9] which directly determines the number of pulses to be sent and the state of the desired qubits and is the basis of the successful execution of subsequent quantum computing. In Alice's preparation, she prepares the required single photon pulses for a desired computing and sends them to Bob through a quantum channel. However, the probability of the photon number satisfies the

Poisson distribution, which results in a lower generated probability of single photons. It is also inevitable that two or multiple photon pulses are sent in the preparation, which will destroy the privacy of quantum states in Alice's preparation. Hence, a remote blind qubit state preparation (RBSP) protocol is proposed by Dunjko et al. [10] to delegate Bob to prepare qubits, which only requires Alice to send weak coherent pulses to Bob. To prepare a desired qubit, the number of pulses is of the order $O(1/T^4)$, where $T(T < 1)$ represents the transmittance of the quantum channel. Xu and Lo then presented the one decoy state-based RBSP protocol to improve the preparation efficiency [11]. The number of pulses to prepare a desired qubit can be reduced from $O(1/T^4)$ to almost $O(1/T)$. Obviously, the decoy state technique can be used to prepare more qubits in unit time. On this basis, the multi-decoy states technique in quantum key distribution [17] can also be applied to the UBQC protocol. Subsequently, Zhao and Li proposed a blind quantum state preparation protocol with two decoy states [12–14], which further improves the preparation efficiency. Their simulation experiments also show that the preparation protocol with two decoy states is more suitable for long-distance communication.

However, in the preparation of UBQC, the qubits disturbed by noise are prone to errors [16,18]. To avoid the accumulation and propagation of these errors in the subsequent computations, quantum error-correcting code [19] offers a viable solution to correct error qubits in the preparation process. Tan Xiaoqing et al. [20] proposed a fault-tolerant framework for blind quantum computing, which used 7-qubit CSS code to encode the logical GHZ states to overcome the collective-dephasing noise and the collective-rotating noise. However, the client was required to have the ability of single-qubit measurement on the third qubit of the logical GHZ state and share the remaining Bell state with the server. Morimae and Koshiba [21] have shown that it is impossible for the classical client to implement perfectly secure one-round delegated quantum computing. Therefore, the client at least requires access to the quantum channel or other quantum properties in a realistic situation. In order to reduce the client's burden and dependence on quantum, we delegate quantum error-correcting code preparation to Bob for implementation. Since the delegated preparation is implemented in the measurement-based quantum computation (MBQC) framework [22,23], the encoding circuit is required to be converted into graph states to prepare the quantum error-correcting codes in the MBQC manner.

Combined with two-decoy-state RBSP, a remote quantum error-correcting code preparation protocol on cluster state is presented to correct errors in blind quantum computation. In our protocol, the cluster states are used as graph states to prepare quantum error-correcting codes that are unknown to Bob. Then, these codes can be considered as encoded logical qubits for subsequent fault-tolerant blind quantum computation. The security of the proposed protocol is proven theoretically to be ϵ-blind. Finally, the lower bound of quantum resource consumption is estimated, i.e., the number of required pulses. When the prepared quantum error-correcting codes have the same qubit error rate, our protocol can reduce the number of pulses, which will contribute to the practical application of UBQC in the future.

The remainder of the paper is structured as follows: In Section 2, we introduce the basic knowledge. In Section 3, we present a quantum error-correcting code preparation protocol on cluster state to correct qubit errors. Furthermore, we demonstrate that the protocol is ϵ-blind and estimate the quantum resource consumption. In Section 4, simulation results show the quantum resource consumption of coding and non-coding protocols in the case of the same qubit error rate. In Section 5, the necessary conclusions are drawn.

2. Technical Preliminaries

2.1. Qubit Error

Due to environmental noise, it is inevitable that errors occur in quantum computations. Therefore, we need to build a general error model to correct qubit errors. In quantum Hilbert space, a quantum state $|\psi\rangle$ can be described as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where $|0\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix}^T, |1\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix}^T$ are the basis vectors in the Hilbert space, and $|\alpha|^2 + |\beta|^2 = 1$.

After the noise has occurred, the evolution of the quantum state $|\psi\rangle$ contains four cases: (1) no error, (2) the bit error $|0\rangle \leftrightarrow |1\rangle$, (3) the phase error $\alpha|0\rangle + \beta|1\rangle \leftrightarrow \alpha|0\rangle - \beta|1\rangle$, and (4) both bit and phase errors. Hence, an error operator E_i can be considered a linear combination of identity operator I, bit flip operator X, phase flip operator Z, and bit-phase flip operator Y [24]. These Pauli operators are

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2}$$

To simplify the analysis, suppose the noise occurs on a single qubit, so the quantum state $E_i|\psi\rangle$ can be described as a superposition state of the four possible states $I|\psi\rangle$, $X|\psi\rangle$, $Z|\psi\rangle$, and $Y|\psi\rangle$ [25]. If one measures the error quantum state $E_i|\psi\rangle$, it collapses into one of four states. In order to correct the qubit error, we need to perform a diagnostic process to determine which error occurred in four possible cases and then utilize Pauli operators to act on the error qubit to correct it.

2.2. Quantum Error-Correcting Codes

In the error-correcting process, the error syndrome measurement is used to diagnose which qubit is in error. With the increasing number of qubits in code, it is more difficult to determine where the error occurred. As a result, we use seven qubits to encode one qubit, which can correct a qubit error in an encoded block, which is called the 7-qubit Steane code,$[[7,1,3]]$. The encoded logical qubit base $\{|0\rangle_L, |1\rangle_L\}$ is shown as follows:

$$\begin{aligned} |0\rangle_L = {} & \frac{1}{2\sqrt{2}}(|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle \\ & + |1010101\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle) \\ |1\rangle_L = {} & \frac{1}{2\sqrt{2}}(|1111111\rangle + |1110000\rangle + |1001100\rangle + |1000011\rangle \\ & + |0101010\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle) \end{aligned} \tag{3}$$

Based on the encoding principle of Steane code [24], we can design the encoding circuit of quantum error-correcting code, as shown in Figure 1a. The unknown data qubit and six ancilla qubits can be used to encode an encoded logical qubit. According to the error syndrome measurement circuit in Figure 1b, one uses two Steane ancilla states to diagnose the bit and phase error syndromes, respectively. Finally, the Pauli gates are used to act on the error qubits to correct them in each encoded block.

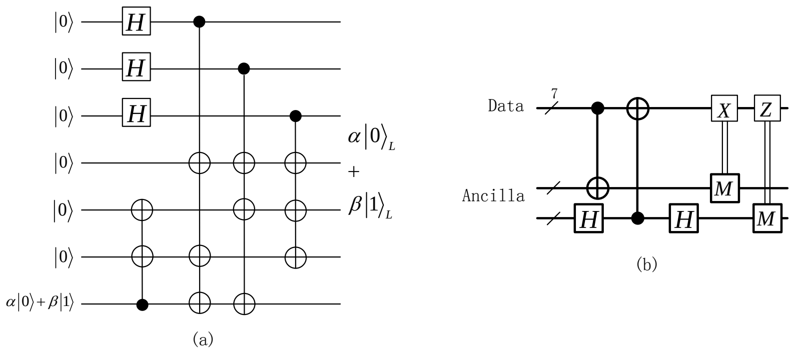

Figure 1. The quantum encoded and syndrome measurement circuits of the Steane code [[7,1,3]]. (**a**) A 7-qubit encoded logical qubit is prepared by a data qubit and six ancilla qubits. (**b**) The bit and phase errors occurring in the encoded block can be diagnosed with two Steane ancilla states and recovered by Pauli gates.

2.3. Realization of Quantum Gates on Cluster State

For a quantum circuit, we can use the ordered quantum gates to describe the computational process. Any quantum gate can be transformed into a combination of quantum gates in the universal gate group, such as $\{CNOT, H, \pi/8\}$. Hence, only if we can realize every quantum gate in the universal logic gate group can we implement arbitrary quantum computing.

In the framework of MBQC [26], we know that quantum gates can be realized by multi-particle entangled graph states, such as cluster state and brickwork state [9,22]. Note that the $[[7,1,3]]$ encoded circuit consists of Hadamard gates and CNOT gates in Figure 1. Hence, we only need to realize these two types of quantum gates on graph states. Since quantum gates in brickwork state only act on the neighboring qubit, the CNOT gate acting on non-neighboring qubits needs many SWAP gates to be realized, which is very inefficient. Hence, we use the cluster state to realize these Hadamard and CNOT gates in the encoding circuit, as shown in Figure 2.

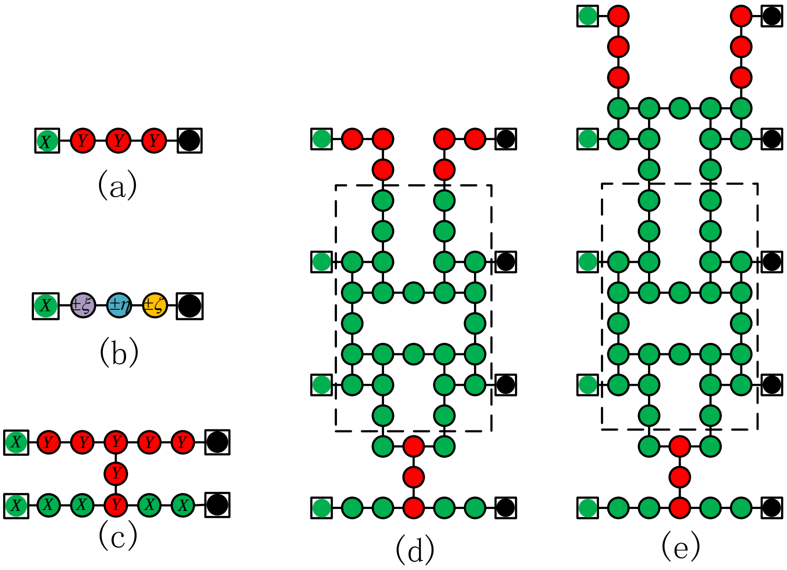

Figure 2. Implementation of basic quantum gates on cluster state. Each circle represents a qubit, and the left-most squares represent the input qubits, the right-most squares denote the output qubits. Each green circle represents a cluster qubit measured in the eigenbasis of Pauli gate X, the red denotes I. The ξ, η, and ζ represent the measurement angles δ of the measurement basis $M(\delta)$. (**a**) The Hadamard gate. (**b**) A general rotation gate. (**c**) The CNOT gate applied between adjacent logical qubits. (**d**) The CNOT gate applied between two logical qubits separated by an even number. (**e**) The CNOT gate applied between two logical qubits separated by an odd number.

In Figure 2, these diagrams are used to illustrate the realization of quantum gates on cluster states. (a) represents the pattern to realize the Hadamard gate. Each circle symbolizes a qubit, and the lines indicate entangling operators. Controlled-Z (CZ) gates are employed to interact between neighboring qubits, preparing the entangled state. The qubits are measured in a specifically selected basis, with the green (red) circle representing a measurement in the eigenstates of the X (Y) Pauli gate. The measurement basis $M(\delta)$ is determined by the measurement angle δ. The eigenbasis of X (Y) corresponds to $\delta = 0(\pi/2)$. The computational basis $\{|0\rangle, |1\rangle\}$ is the eigenbasis of Z. (b) illustrates a general one-qubit rotating quantum gate through one-qubit measurement in a cluster state, where the measurement basic angles $\pm\xi, \pm\eta, \pm\zeta$ depend on the measurement results of other qubits. (c), (d), and (e) show the CNOT gate applied between different distance logical qubits. One can repeat the rectangle parts enclosed by the black dashed line in (d) and (e) to deal with any separation. In quantum computing in a cluster state, the $\{|0\rangle, |1\rangle\}$ basis is used to eliminate the redundant qubits, and the adaptive basis $M(\theta)$ is used to measure the remaining qubits to implement any quantum gate.

3. Quantum Error-Correcting Code Preparation on Cluster State

In the field of quantum computation, it is widely recognized that cluster states can be used to realize arbitrary quantum gates. Indeed, the essence of a quantum circuit resides in its meticulously ordered sequence of quantum gates, forming the fundamental backbone of quantum computing. Consequently, each quantum circuit can be efficiently performed in a cluster state [22]. By harnessing the power of cluster states, the quantum encoding circuit can also be feasible, enabling the generation of quantum error-correcting codes. These encoded qubits can then be utilized to construct novel brickwork states to facilitate the realization of fault-tolerant quantum computing.

According to the implementation of quantum gates on cluster state in the preliminaries, the encoding circuit of [[7,1,3]] code needs to be transformed into MBQC on cluster state, then the quantum error-correcting code preparation can be realized through measuring each qubit on cluster state, as shown in Figure 3. In the preparation process, Bob initiates the construction of the initial cluster state, followed by the judicious utilization of the computational basis $\{|0\rangle, |1\rangle\}$ to eliminate the redundant qubits based on the precise positional information provided by Alice. In accordance with Alice's designated measurement bases $M(\delta)$, the remaining qubits of the cluster state serve as a platform for preparing quantum error-correcting codes. These bases are meticulously designed to be orthogonally projected onto the states $|\pm_\delta\rangle = (|0\rangle \pm e^{i\delta}|1\rangle)/\sqrt{2}$, where $\delta \in [0, 2\pi]$ designates the measurement angle. Note that the specific values of δ such as $\delta = 0$ or $\pi/2$ corresponds to the X or Y Pauli measurement, respectively. It is important to emphasize that these measurements are inherently destructive. Obviously, the measurement is understood as a destructive measurement. The measurement outcome of qubit i is denoted by $s_i \in \mathbb{Z}_2$. Our convention dictates that $s_i = 0$ when the state collapses to $|+_\delta\rangle$ as a result of the measurement, and $s_i = 1$ when it collapses to $|-_\delta\rangle$.

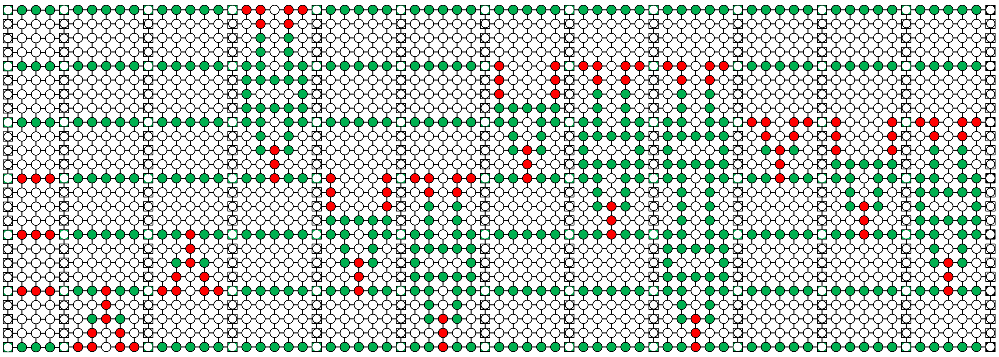

Figure 3. The implementation of the [[7,1,3]] encoding circuit on cluster state. The measured cluster qubits are denoted by the green, red, and white circles, representing the measurements in the eigenbases of X, Y, and Z, respectively.

During the process of removing redundant qubits, an inherent challenge arises concerning the potential leakage of quantum gates used, which could inadvertently disclose the underlying structural information of the cluster state to Bob. However, Alice's primary concern lies in ensuring the security of the encoded logical qubit $|+_{\theta_i}\rangle_L$ during the preparation, while the quantum gates employed in the encoded circuit can be made public to Bob. To accomplish preparation, three distinct measurement bases are employed, including $\{|0\rangle, |1\rangle\}$, $M(0)$ and $M(\pi/2)$ corresponding to the eigenbases of the Pauli gates Z, X, Y, respectively. These measurement bases exhibit a notable characteristic: their independence from the polarization angle θ_i. As a result, the information pertaining to θ_i remains entirely secure and undisclosed to Bob throughout the process. These findings shed light on the potential of cluster states for secure and efficient quantum information processing in quantum error-correcting code preparation.

In UBQC, the delegated preparation process contains Alice's preparation, Bob's preparation, and the interaction measurement. In Alice's preparation, Alice sends N data pulses to Bob, which comprise signal states and two decoy states, and their polarization is ρ^{σ}, where σ is chosen randomly from $\left\{\frac{k\pi}{4} : 0 \leq k \leq 7\right\}$. In addition, Alice needs to send a series of ancilla pulses to Bob, and their polarization is $|+\rangle$, which is allowed to be public. In Bob's preparation, the required qubit $|+_{\theta_i}\rangle$ can be generated based on non-coding RBSP [13]. Among the generated qubit $|+_{\theta_i}\rangle$ and a series of ancilla qubits, Bob utilizes CZ gates to entangle them to build an initial cluster state. During the interaction measurement, Bob follows Alice's instructions and eliminates the redundant qubits from the initial cluster state in the computational basis, as shown in the white circles in Figure 3. According to Alice's measurement basis $M(\delta_{ij}), \delta_{ij} \in \{0, \pi/2\}$, the remaining qubits on cluster state are measured sequentially until the final outcome is obtained. Finally, Bob can achieve the required quantum error-correcting codes. As depicted in Algorithm 1, we propose an innovative protocol for remote quantum error-correcting code preparation on cluster state, which lays the groundwork for subsequent fault-tolerant blind quantum computing.

Algorithm 1: A remote quantum error-correcting code preparation on cluster state

```
Input: data pulses with polarization $\rho^{\sigma}$, $\sigma \in_R \{k\pi/4 :\ 0 \leq k \leq 7\}$ including
       signal and two decoy states; ancilla pulses with polarization $|+\rangle$.
Output: the encoding logical qubits: $\{|+_{\theta_i}\rangle_L\}_1^S$.
Alice uses the laser to send the required data and ancilla pulses to Bob.
for $i = 1$ to $S$; do
    Bob utilizes non-coding RBSP to prepare qubit $|+_{\theta_i}\rangle$, then uses it and a series
      of ancilla qubits $\{|+\rangle\}$ to build the cluster state.
    for $x = 1$ to $m$, $y = 1$ to $n$; do
        Based on Figure 3, Bob performs the [[7,1,3]] encoding circuit on cluster
          state
        if $q_{xy}$ is white then Bob performs measurement in $\{|0\rangle, |1\rangle\}$ ;
        if $q_{xy}$ is green then Bob performs measurement in $M(0)$;
        if $q_{xy}$ is red then Bob performs measurement in $M(\pi/2)$;
    end
    Bob generates quantum error-correcting code $\{|+_{\theta_i}\rangle_L\}$.
end
return $\{|+_{\theta_i}\rangle_L\}_1^S$.
```

The [[7,1,3]] encoding circuit is designed based on the generator matrix, and its correctness had been proven by Preskill [24]. Since the preparation on cluster state is equivalent to the encoding circuit model, our protocol can generate the correct quantum error-correcting codes. In order to ensure Alice's information privacy, the encoding logical qubits (quantum error-correcting codes) are required to be unknown to Bob in UBQC. In other words, the polarization angle θ is always unknown to Bob in the preparation process of the encoding logical qubits $|+_{\theta}\rangle_L$.

In UBQC, the client and server share a joint state that describes the evolution of the entire system. The ideal state is symbolized as π_{AB}^{ideal} that effectively guarantees the client's information against potential malicious attacks. During the preparation, the ideal state π_{AB}^{ideal} evolves into a set of states, which can be conveniently represented by $\mathcal{F}(\pi_{AB}^{ideal})$. To ensure robust security against any server actions, it is imperative that all states with this set remain equally blind. To assess the security level achievable in practical implementation, we explore scenarios where the client transmits a realistic state ρ^{θ_i} to replace a perfect state $|+_{\theta_i}\rangle$. In the following, we introduce the concept of almost blindness by quantifying the proximity between the realistic joint state and the ideal joint state, i.e., ϵ-blind [10].

Definition 1. *A UBQC protocol with imperfect preparation is ϵ-blind if the trace distance between the ideal joint state $\pi_{AB}^{\theta_i}$ and realistic joint state $\pi_{AB}^{\rho^{\theta_i}}$ is less than $\epsilon > 0$. Finally, we have:*

$$\min_{\pi_{AB}^{\theta_i}\in\mathcal{F}} \frac{1}{2}\left\|\pi_{AB}^{\{\rho^{\theta_i}\}} - \pi_{AB}^{\{\theta_i\}}\right\| \leq \varepsilon. \tag{4}$$

Theorem 1. *Our preparation Algorithm 1 is ϵ-blind to Bob.*

Proof. In our protocol, the measurement-based quantum computation is used to realize quantum error-correcting code preparation on cluster state. The prepared data qubit $|+_\theta\rangle$ and a series of ancilla qubits $|+\rangle$ can be considered as quantum resources to build the cluster state. Based on the RBSP protocol [10,13], the generated data qubit $|+_\theta\rangle$ is ϵ-blind. In order to demonstrate the ϵ-blindness of the encoded logical qubit $|+_\theta\rangle_L$, we only need to prove that the encoding circuit on cluster state is ϵ-blind. In other words, the angle of polarization θ of $|+_\theta\rangle_L$ in the preparation process is unknown to Bob.

To be more precise, it is necessary to illustrate that the measurements on cluster state do not reveal any information about polarization angle θ. The cluster state is built by multiple entanglement qubits. For the purpose of simplicity, it suffices to prove that the polarization angle θ is ϵ-blind to Bob during the measurements on the minimum cluster state. Further, we analyze three kinds of measurements on cluster state according to the [[7,1,3]] encoding circuit. The eigenstates of X, Y, Z are used to measure the qubits on the minimum cluster state, respectively. We explore whether there is information leakage of the polarization angle θ during the measurements.

$$\begin{aligned}
|+_\theta\rangle_1 \otimes |+\rangle_2 &= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{i\theta}|1\rangle\Big)_1 \otimes |+\rangle_2 \\
&\xrightarrow{CZ} \frac{1}{\sqrt{2}}|0\rangle_1 \otimes |+\rangle_2 + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle_1 \otimes |-\rangle_2 \\
&\overset{M(X)}{=\!=\!=} \frac{|+\rangle_1 \otimes (H|+_\theta\rangle_2) + |-\rangle_1 \otimes (X\cdot H|+_\theta\rangle_2)}{\sqrt{2}} \\
&\overset{M(Y)}{=\!=\!=} \frac{|+_{\pi/2}\rangle_1 \otimes (XHS|+_\theta\rangle_2) + |-_{\pi/2}\rangle_1 \otimes (HS|+_\theta\rangle_2)}{\sqrt{2}}
\end{aligned} \tag{5}$$

The first qubit $|+_\theta\rangle$ and the second qubit $|+\rangle$ are used to build the minimum cluster state using CZ gate, as shown in Figure 4. If the first qubit is measured in the eigenstates of X gate, as shown in Figure 4a, the quantum state is $|+\rangle$ or $|-\rangle$ with an equal probability. The second qubit is evolved into $(X)^k \cdot H|+_\theta\rangle_2, k \in \{0,1\}$, where k represents the measurement result of the first qubit, as shown in Equation (5). If the eigenstates of Y gate are used to measure the first qubit, as shown in Figure 4b, the polarization state of the second qubit is evolved into $(X)^k \cdot H \cdot S|+_\theta\rangle_2, k \in \{0,1\}$, k is also determined by measurement result of the first qubit, as shown in Equation (5). It can be seen that the information of the first qubit is transmitted to the second qubit through MBQC without loss of information. If the first qubit $|+\rangle$ and the second qubit $|+_\theta\rangle$ are entangled into the minimum using CZ gate, as shown in Figure 4c, and the eigenstates of Z gate are used to measure the first qubit, the second qubit is still $|+_\theta\rangle$, as shown in Equation (6). Obviously, the remaining qubits are unchanged when the redundant qubits are eliminated by Z.

$$\begin{aligned}
|+\rangle_1 \otimes |+_\theta\rangle_2 &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_1 \otimes |+_\theta\rangle_2 \\
&\xrightarrow{CZ} \frac{1}{\sqrt{2}}|0\rangle_1 \otimes |+_\theta\rangle_2 + \frac{1}{\sqrt{2}}|1\rangle_1 \otimes |-_\theta\rangle_2 \\
&\overset{M(Z)}{=\!=\!=} \frac{|0\rangle_1 \otimes |+_\theta\rangle_2 + |1\rangle_1 \otimes (Z|+_\theta\rangle_2)}{\sqrt{2}}
\end{aligned} \tag{6}$$

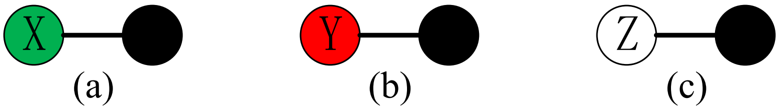

Figure 4. The cluster state with two qubits. The green, red, and white represent the measurements of X, Y, and Z gates. (**a**) The first qubit of the cluster state is measured in the eigenbasis of X. (**b**) The first qubit is measured in Y. (**c**) The first qubit is measured in Z.

Thus, the polarization angle θ is irrelevant to the eigenstates of X, Y, and Z. During the measurements on cluster state, Bob can not obtain any information about the angle of polarization θ. Hence, the generated encoded logical qubit $|+_\theta\rangle_L$ is ϵ-blind in our Algorithm 1 if the input data qubit $|+_\theta\rangle$ is ϵ-blind. □

In our protocol, these pulses sent by Alice consist of two parts, data and ancilla. Based on non-coding RBSP, note that data pulses are employed to generate the required data qubits $\{|+_{\theta_i}\rangle\}_1^S$. Each data qubit is then transformed into its corresponding logical qubit as required. Consequently, the number of data pulses used aligns with that of the non-coding RBSP, denoted as N^d [14]. The number of ancilla pulses depends on the cluster state used to prepare encoded states, as shown in Figure 3. It is important to highlight that the number of ancilla qubits is a constant if one encoded qubit is prepared, denoted as C. The transmittance of the quantum channel between client and server directly affects the probability of the pulses being received, denoted as T, and the scale of quantum computation is denoted as S, the number of required ancilla pulses $N^a = CS/T$. Hence, we can derive the lower bound of the total number of pulses in Algorithm 1.

$$\begin{aligned} N &= N^d + N^a \\ &\geq N^{L,v_1,v_2} + \frac{CS}{T} \\ &= \frac{S}{T}\left[\frac{\ln(\epsilon/S)}{p_\mu \mu \ln\left(1 - p_1^{L,v_1,v_2}\right)} + \mathrm{C}\right] \end{aligned} \tag{7}$$

where ϵ represents the secure parameter. μ,v_1, v_2 are the average photon number of signal states and two decoy states, respectively. p_1 represents the proportion of single-photon states in the signal states, and the lower bound is denoted as p_1^{L,v_1,v_2} [13]. The probabilities of signal pulses chosen by the client are defined as p_μ. S is the computational scale, and T represents the transmittance of the quantum channel.

We assume that the qubit errors are independent. We can repeatedly use ancilla qubits in the correction, so we do not consider the ancilla qubit consumption in the correction process, as shown in Figure 1b. In the $[[7,1,3]]$ code, we note that each encoded block can correct one error. Therefore, before encoding, the error probability of each qubit is e ($e < 1$), and after encoding, it changes to e^2. In a quantum computation with computation scale S, the error rate of each generated qubit based on non-coding RBSP [13] is e. If an error qubit occurs in all generated qubits, the preparation process fails. Since the error rate of each encoded qubit is e^2 in the preparation of Algorithm 1, the successful probability of encoded preparation is derived as $(1-e^2)^S$. We consider the non-coding RBSP protocol as a repeated Bernoulli experiment, then the success probability of preparation is $(1-e)^S$. By repeating the process k times, the success probability can be calculated as $1-[1-(1-e)^S]^k$. In the scenario where the success probabilities are equal for both coded and non-coded cases, specifically indicated by $1-[1-(1-e)^S]^k = (1-e^2)^S$, the number of repetitions, denoted as k, can be determined using the following derivation:

$$k = \ln[1-(1-e^2)^S] / \ln[1-(1-e)^S]. \tag{8}$$

Hence, when the generated qubit error rate in the coding case is e^2, the non-coding RBSP needs to repeatedly send kN^d pulses to achieve the same generated qubit error rate.

In UBQC, we assume that Alice has a laser transmitter with frequency f, and Bob has a full-fledged quantum computer. By deriving the preparation efficiency of UBQC, which represents the rate at which qubits are generated per second, we can gain valuable insights into the system's performance. According to Equation (7), the upper bound of the efficiency for the concatenation code can be estimated as

$$\begin{aligned} E &= S \cdot f / N \\ &\leq S \cdot f / \left(N^{L,v_1,v_2} + N^{a} \right). \end{aligned} \tag{9}$$

In summary, our Algorithm 1 can prepare ϵ-blind quantum error-correcting codes to correct qubit errors. Under the condition of the same generated qubit error rate, our approach can reduce the number of weak coherent pulses and improve preparation efficiency compared with the non-coding RBSP protocol.

4. Simulation Results

An Intel(R) Core(TM) i7-6700HQ CPU, 12.0GB RAM, and Win 10 pro OS were utilized to implement the simulations through MATLAB software. The transmittance T contains the outside fiber, the inside fiber, and the detection efficiency between Alice and Bob, which can be calculated as follows:

$$T = t_s \cdot \eta_s \cdot 10^{-\alpha L/10} \tag{10}$$

where α represents the loss coefficient in decibels per kilometer (dB/km), L represents the length of the fiber optic cable in kilometers (km), t_s stands for the internal transmittance of Bob's optical components, and η_s represents the detector efficiency. The average photon number of signal states is denoted as μ, and two decoy states are represented as v_1, v_2. The signal state is chosen with probability p_μ, and two decoy states are chosen with p_{v_1}, p_{v_2}. The scale of quantum computation is S. The secure parameter is symbolized as ϵ. The error rate per qubit is denoted as e. According to Figures 1 and 3, the required number of ancilla qubits can be determined, i.e., $C = 1774$. The repetition frequency of the laser transmitter is $f = 1$ MHZ. The relative parameters setting in our simulation are shown in Table 1 (refer to the data in [11,17]).

Table 1. The simulation parameters for our protocol.

α	t_S	η_S	μ	v_1	v_2	p_μ	p_{v_1}	p_{v_2}	S	ϵ	e
0.2	0.45	0.1	0.6	0.125	0	0.9	0.05	0.05	1000	10^{-10}	0.01

In Figure 5, note that the number of pulses in the coding case is comparatively lower than that in the non-coding RBSP [13] with the same qubit error rate and is closer to the asymptotic scenario (with infinite data-size and no qubit error [13,17]). The error rate of the generated qubits using Algorithm 1 is significantly lower than that of the non-coding RBSP. In order to obtain the same error rate, the non-coding case is required to repeat k times. Under the encoding condition of the same qubit error rate, the number of pulses required in our Algorithm 1 is lower than that of the previous coding case [14]. On the one hand, since our approach uses the cluster state instead of the brickwork state to realize remote delegated preparation, it can reduce many SWAP gates when utilizing CONT gates between non-adjacent qubits. On the other hand, our approach requires the CNOT gates with a high execution probability to avoid using too many ancilla qubits in the preparation to realize the operations of the fault-tolerant CNOT gates. Both aspects can greatly reduce the consumption of ancilla qubits; thereby, our proposed Algorithm 1 can reduce the number of pulses required.

In Figure 6, the preparation efficiency E in the coding case is less than the non-coding RBSP with the same qubit error rate and is closer to the asymptotic case. Especially, the efficiency of our proposed Algorithm 1 is better than the previous protocols [13,14] with the same qubit error rate. This reason is that our approach can reduce the consumption of

SWAP gates and ancilla qubits. With the increasing distance, the value of efficiency E grows rapidly, implying the significant impact of channel loss and corresponding qubit error rate. For long-distance communication, our protocol surpasses the non-coding case, primarily due to the fact that the value of E is closer to the asymptotic scenario (with an infinitely large data size and no qubit error [13,17]). These advantages underscore the enhanced performance and efficacy of our protocol, making it a favorable choice for long-distance blind quantum computing.

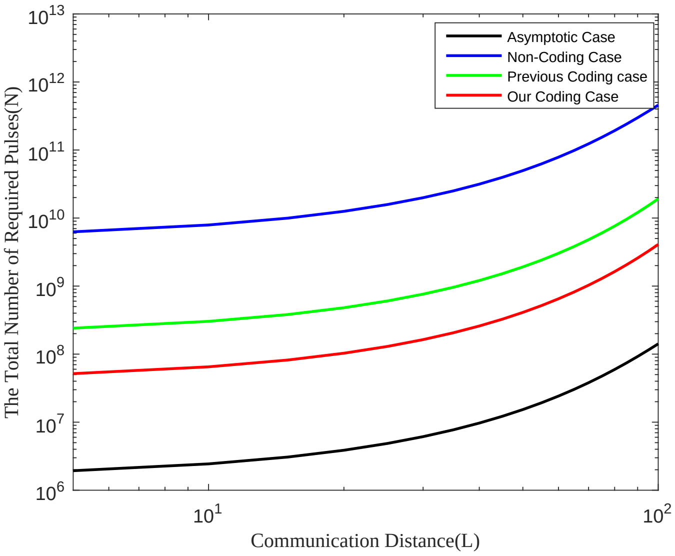

Figure 5. The relationship between the total number of pulses N case and the communication distance L with the same qubit error rate. The red line represents the quantum resource consumption of Algorithm 1 with coding, the green line represents the simulation results of the previous coding case [14], and the blue line depicts the results in the non-coding case [13]. The simulation results depicted by the black line show the outcomes in the asymptotic scenario, characterized by an infinitely large data size and near-perfect preparation of qubits.

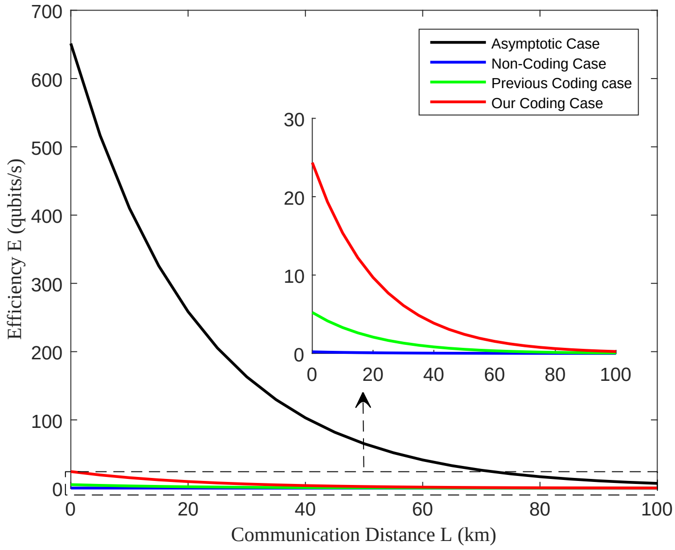

Figure 6. The relationship between preparation efficiency E and the communication distance L with the same qubit error rate. The red line represents the preparation efficiency of Algorithm 1 with coding, the green line represents the simulation results of the previous coding case [14], and the blue line depicts the results in the non-coding case [13]. The simulation results represented by the black line illustrate the outcomes in the asymptotic scenario, characterized by an infinitely large data size and near-perfect preparation of qubits.

Therefore, our protocol holds the potential to enhance not only the preparation efficiency but also the conservation of quantum resources. Furthermore, the quantum error-correcting codes can be used as logical qubits to facilitate subsequent fault-tolerant blind quantum computation. The capability of our protocol ensures an optimized utilization of quantum resources while maintaining the integrity and reliability of the preparation in UBQC.

5. Conclusions

In this study, we propose an innovative protocol for remote quantum error-correcting code preparation on cluster states, which can be used to correct error qubits in the preparation of UBQC. Based on the blindness of the original RBSP protocol, we demonstrate that Algorithm 1 is also ϵ-blind. Alice only needs to send weak coherent pulses, without quantum memory or extensive quantum computing capabilities. By incorporating quantum error-correcting codes, our protocol can reduce the number of pulses when preparing the quantum error-correcting codes with the same qubit error rate. Furthermore, these quantum error-correcting codes prepared by our protocol are unknown logical qubits to Bob, which can be used to build a new encoded brickwork state to realize the fault-tolerant blind quantum computation. Our proposed preparation protocol provides a theoretical basis for the practical application of blind quantum computation in the future. In our approach, when CNOT gates are executed, they need to run with a high probability. This will limit the generalized application of blind quantum computation. Hence, we will continue to research the surface codes and the concatenated codes with high fault tolerance to better balance the quantum resource consumption and the qubit error rate, so as to generalize the preparation protocol of quantum error-correcting codes.

Author Contributions: Writing—original draft preparation, Q.Z.; writing—review and editing, Q.Z., H.M., Y.Q., Q.L., and A.A.A.E.-L.; funding acquisition, Q.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (grant Number: 62071151). Also, Ahmed A. Abd El-Latif acknowledges the Talented Young Scientist Program (TYSP) and its support.

Institutional Review Board Statement: This research is not applicable to studies involving humans or animals.

Informed Consent Statement: This research is not applicable to studies involving humans.

Data Availability Statement: In our work, no new real data were created, and all the data were simulated data generated by the parameters in the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelpgia, PA, USA, 22–24 May 1996 ; ACM: New York, NY, USA , 1996; pp. 212–219.
2. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
3. Tanaka, S.; Tamura, R.; Chakrabarti, B.K. *Quantum Spin Glasses, Annealing and Computation*; Cambridge University Press: Cambridge, UK, 2017.
4. Albash, T.; Lidar, D.A. Adiabatic quantum computation. *Rev. Mod. Phys.* **2018**, *90*, 015002. [CrossRef]
5. Alsubai, S.; Alqahtani, A.; Binbusayyis, A.; Sha, M.; Gumaei, A.; Wang, S. Quantum Computing Meets Deep Learning: A Promising Approach for Diabetic Retinopathy Classification. *Mathematics* **2023**, *11*, 2008. [CrossRef]
6. Lee, X.; Xie, N.; Cai, D.; Saito, Y.; Asai, N. A Depth-Progressive Initialization Strategy for Quantum Approximate Optimization Algorithm. *Mathematics* **2023**, *11*, 2176. [CrossRef]
7. Childs, A.M. Secure assisted quantum computation. *Quantum Inf. Comput.* **2005**, *5*, 456–466. [CrossRef]
8. Arrighi, P.; Salvail, L. Blind quantum computation. *Int. J. Quantum Inf.* **2006**, *4*, 883–898. [CrossRef]

9. Broadbent, A.; Fitzsimons, J.; Kashefi, E. Universal blind quantum computation. In Proceedings of the Foundations of Computer Science, 2009, FOCS'09, 50th Annual IEEE Symposium, Atlanta, GA, USA, 25–27 October 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 517–526.
10. Dunjko, V.; Kashefi, E.; Leverrier, A. Blind quantum computing with weak coherent pulses. *Phys. Rev. Lett.* **2012**, *108*, 200502. [CrossRef] [PubMed]
11. Xu, K.; Lo, H.K. Blind Quantum Computing with Decoy States. *arXiv* **2015**, arXiv:1508.07910.
12. Zhao, Q.; Li, Q. *Blind Quantum Computation with Two Decoy States*; Springer International Publishing: Berlin/Heidelberg, Germany, 2017.
13. Zhao, Q.; Li, Q. Finite-data-size study on practical universal blind quantum computation. *Quantum Inf. Process.* **2018**, *17*, 171. [CrossRef]
14. Zhao, Q.; Li, Q.; Mao, H.; Wen, X.; Han, Q.; Li, M. Fault-tolerant quantum error correction code preparation in UBQC. *Quantum Inf. Process.* **2020**, *19*, 236. [CrossRef]
15. Cojocaru, A.; Colisson, L.; Kashefi, E.; Wallden, P. On the possibility of classical client blind quantum computing. *Cryptography* **2021**, *5*, 3. [CrossRef]
16. Shan, R.T.; Chen, X.; Yuan, K.G. Multi-party blind quantum computation protocol with mutual authentication in network. *Sci. China Inf. Sci.* **2021**, *64*, 1–14. [CrossRef]
17. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
18. Chien, C.H.; Van Meter, R.; Kuo, S.Y. Fault-tolerant operations for universal blind quantum computation. *ACM J. Emerg. Technol. Comput. Syst.* **2015**, *12*, 9. [CrossRef]
19. Fujii, K. *Quantum Computation with Topological Codes: From Qubit to Topological Fault-Tolerance*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 8.
20. Tan, X.; Tao, H.; Zhang, X.; Zeng, X.; Xu, Q. Fault-tolerant blind quantum computing using GHZ states over depolarization channel. *Quantum Inf. Process.* **2021**, *20*, 1–14. [CrossRef]
21. Morimae, T.; Koshiba, T. Impossibility of perfectly-secure one-round delegated quantum computing for classical client. *Quantum Inf. Comput.* **2019**, *19*, 214–221. [CrossRef]
22. Raussendorf, R.; Browne, D.E.; Briegel, H.J. Measurement-based quantum computation on cluster states. *Phys. Rev. A* **2003**, *68*, 022312. [CrossRef]
23. Broadbent, A.; Fitzsimons, J.; Kashefi, E. Measurement-based and universal blind quantum computation. In Proceedings of the International School on Formal Methods for the Design of Computer, Communication and Software Systems, Bertinoro, Italy, 21 June 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 43–86.
24. Preskill, J. Fault-tolerant quantum computation. In *Introduction to Quantum Computation and Information*; World Scientific: Singapore,1998; pp. 213–269.
25. Nielsen, M.A.; Chuang, I. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2002.
26. Raussendorf, R.; Briegel, H.J. A one-way quantum computer. *Phys. Rev. Lett.* **2001**, *86*, 5188. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.