Quantum Information Processing (2025) 24:182
https://doi.org/10.1007/s11128-025-04798-3

Universal blind quantum computing assisted by quantum teleportation

Xiaoqian Zhang[1]

Received: 25 January 2025 / Accepted: 24 May 2025 / Published online: 16 June 2025

Abstract
Blind quantum computing (BQC) allows classical clients to delegate quantum computing tasks to cloud servers while maintaining privacy throughout the computation. Although the circuit-based BQC protocol proposed by Childs laid the foundation for the field, the implementation of quantum algorithm encryption has remained a significant challenge. Here, we propose a novel BQC protocol that combines quantum teleportation with one-time-pad cryptography, effectively addressing the challenges of implementing universal BQC within the circuit model. In our protocol, the client only needs the capability to prepare single-qubit states and apply X and Z gates, while the server creates all required quantum states, performs the quantum computations and the Bell measurement. In contrast to measurement-based BQC protocols, the proposed scheme significantly reduces server-side hardware complexity and overall resource consumption by avoiding the need to prepare large-scale graph states, thereby simplifying the state preparation requirements for the server. This work introduces a novel approach for efficient BQC and contributes to the advancement of privacy protection techniques in quantum computing.

Keywords Blind quantum computation · Teleportation · One-time-pad cryptography

1 Introduction

The rapid progress in quantum computing has led to the development of various quantum computers by leading institutions, which are now being deployed for practical use. Notable examples include the Condor superconducting quantum computer [1], the Benyuan Wukong superconducting quantum computer [2], and the Jiuzhang photonic quantum computer [3]. These organizations [1, 2] have also launched cloud computing platforms, providing quantum resources to researchers and enabling individuals without quantum computers to easily obtain computational support. As a

✉ Xiaoqian Zhang
zhangxq64@jnu.edu.cn

[1] College of Information Science and Technology, Guangzhou 510632, China

result, outsourcing quantum computing tasks to cloud servers has become an increasingly attractive option. Despite the growing availability of cloud resources, high costs and unresolved privacy concerns remain significant challenges. Therefore, protecting client privacy has become a critical issue in the practical application of quantum computing.

Blind quantum computing (BQC) enables secure delegation of quantum computations, allowing clients with minimal quantum capabilities to outsource tasks while preserving input, output, and algorithm privacy [4–22]. Recent developments have significantly expanded the scope of BQC. Innovations in protocol design have decreased quantum resource demands through improved brickwork states [12], more compact schemes [13], and reductions in qubit usage [14]. Simultaneously, research has enhanced verifiability and authentication through multiparty and multi-client extensions [15, 16], strengthening resilience against malicious interference. Experimental investigations on photonic and ion-trap platforms [17, 18] have confirmed the viability of BQC in practical settings, while theoretical efforts continue to address latent security gaps and improve the generality of protocol designs [19]. These developments collectively represent a multi-pronged advance toward scalable and practical BQC. Within this evolving landscape, two principal categories of BQC have been established: measurement-based BQC [4–13] and circuit-based BQC [20–22]. The circuit-based protocol presented by Childs in 2005 [20] laid the foundation for this field. Although the protocol offers some solutions, two issues remain that require further improvement. First, T-gate encryption is constrained by technical challenges, such as errors that Pauli correction cannot fully eliminate. Second, the encryption mechanism only protects the input quantum states, leaving the quantum gate operations exposed to the servers. To address the first issue, Broadbent proposed an enhanced T-gate hiding protocol [21], which corrects errors by first applying the T-gate and then performing a hidden phase gate S. This approach reduces resource requirements compared to directly hiding the T-gate and has been validated on optical platforms [22]. However, effectively hiding quantum gates using one-time-pad encryption remains an unresolved challenge.

Recent experimental work reflects continued progress in addressing these challenges, with BQC demonstrated across a range of platforms and models. Experimental implementations fall into three major categories: measurement-based, circuit-based, and quantum fully homomorphic encryption (QFHE) protocols [23–30]. In the measurement-based model, Barz et al. [23] demonstrated the first experimental BQC by preparing a four-qubit graph state on a discrete optical setup. Later work by Barz et al. [24] and Greganti et al. [26] confirmed the correctness of the results using similar methods. In the circuit-based model, Fisher et al. [25] carried out the protocol introduced by Childs [20], providing one of the first experimental tests of this framework. Huang et al. [27] showed a blind version of Shor's algorithm on a discrete optical platform, proving the model can handle more complex computations. More recently, Li et al. [30] implemented the protocol on an integrated photonic chip, moving toward more compact and scalable systems. For QFHE, Tham et al. [28] performed a basic two-party secure computation using discrete optics. Zeuner et al. [29] extended this by demonstrating encrypted single-qubit gates and multi-qubit quantum walks on a non-birefringent integrated chip, opening up new possibilities for secure multi-qubit

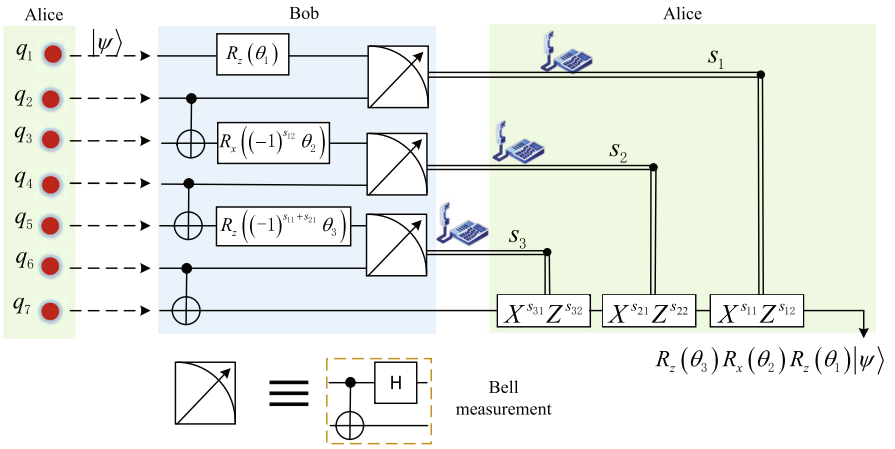

Fig. 1 (Colour online) Schematic of the single-qubit gate teleportation protocol in BQC. Alice prepares the qubits q_1 through q_7 and sends them to Bob. Bob constructs Bell states using CNOT gates, applies the rotation gates $R_z(\theta_1)$, $R_x((-1)^{s12}\theta_2)$ and $R_z((-1)^{s11+s21}\theta_3)$ in sequence followed by Bell measurements consisting of a CNOT gate and a Hadamard gate. The measurement outcomes s_1, s_2 and s_3 are sent to Alice sequentially via a classical channel. Alice applies the corrections for the by-product operators $X^{s11+s21+s31}Z^{s12+s22+s32}$, thus recovering the target quantum gate $R_z(\theta_3)R_x(\theta_2)R_z(\theta_1)$

operations. Together, these experimental efforts illustrate the feasibility and flexibility of BQC across different physical architectures.

To address the remaining issue of gate exposure in BQC protocols, we turn to the concept of quantum teleportation [31]. As a fundamental technique in quantum communication and computing, quantum teleportation has applications in remote quantum communication [32], distributed quantum networks [33], and measurement-based quantum computing [34, 35]. The key feature of quantum teleportation is that the entanglement shared between two participants enables the remote transfer of quantum states via classical communication. The quantum state undergoing Bell measurement collapses with equal probability, a feature that effectively protects the privacy of quantum operations. Therefore, quantum teleportation not only ensures the remote transfer of quantum states but also provides robust support for quantum gate hiding in blind quantum computing. Furthermore, we observe that any unitary operator can be expressed as a sequence of rotation operators, with the angles of these rotations encrypted. Using this property, we propose a new approach that combines quantum teleportation with encryption mechanisms, thereby addressing the issue of exposed quantum gates in existing protocols.

In this paper, we propose a new circuit-based blind quantum computing (CBQC) protocol assisted by quantum teleportation (UBQCQT). In this protocol, the client only needs to prepare single-qubit states and perform X and Z gates, while the server prepares all necessary quantum states, performs the quantum computations, and executes the Bell measurement. The protocol requires only two times of quantum communication between the client and server, ensuring the privacy of the process. This protocol has significant potential for applications in distributed quantum computing.

2 Theoretical framework of quantum gate teleportation

Before detailing the UBQCQT protocol, we first review its foundational principles. According to Ref. [36], for a unitary operator U acting on a single qubit, there exist real numbers δ, α, β, and γ such that

$$U = e^{i\delta} R_z(\alpha) R_x(\beta) R_z(\gamma),$$

where $R_x(\cdot)$ and $R_z(\cdot)$ are the rotation operator around the x-axis and z-axis.

Before discussing the teleportation of single-qubit gates, we define the correspondence between Bell states and classical bits: $|\phi^+\rangle \leftrightarrow 00$, $|\psi^+\rangle \leftrightarrow 01$, $|\phi^-\rangle \leftrightarrow 10$, $|\psi^-\rangle \leftrightarrow 11$. In the main text, s_j and $s'_j \in \{00, 01, 10, 11\}$ $(j = 1, 2, 3, \cdots)$ represent the Bell measurement outcomes and the classical information encoded in the initial Bell state. Figure 1 illustrates the detailed implementation of quantum gate transmission in a blind quantum computing scenario, involving a client (Alice) and a server (Bob).

(1) *Initialization*— Alice prepares the qubits q_1 through q_7. The computational qubit q_1, which will carry the computational task, is initialized as $|\psi\rangle = a|0\rangle + b|1\rangle$ $(|a|^2 + |b|^2 = 1)$. The auxiliary qubits q_2 to q_7 are initialized in non-orthogonal single-qubit states $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $|0\rangle$, or $|1\rangle$, and will assist in achieving the target quantum computation in subsequent operations. After preparing all qubits, Alice transmits them to Bob via a quantum channel, while sending the operation instructions through a classical channel. (2) *Preparation*— Upon receiving the qubits, Bob sequentially applies CNOT gates to the qubit pairs q_2 and q_3, q_4 and q_5, and q_6 and q_7, with the control qubits initialized in $|\pm\rangle$ states and the target qubits in $|0\rangle$ and $|1\rangle$, respectively. This operation generates the desired Bell states. Subsequently, Bob applies a rotation gate $R_z(\theta_1)$ to qubit q_1 in preparation for the following measurements and operations. (3) *First Classical Communication*— Bob performs a Bell measurement on qubits q_1 and q_2, then transmits the measurement outcome s_1 to Alice via a classical channel. Using s_1 and the classical information s'_1 from the initial Bell state, Alice computes the classical bits s_{11} and s_{12}, and instructs Bob to apply the rotation gate $R_x((-1)^{s_{12}}\theta_2)$ to qubit q_3. (4) *Second Classical Communication*— Bob performs a Bell measurement on qubits q_3 and q_4, and transmits the measurement outcome s_2 to Alice via a classical channel. Similarly, Alice computes the classical bits s_{21} and s_{22}, then instructs Bob to apply the rotation gate $R_z((-1)^{s_{11}+s_{21}}\theta_3)$ to qubit $q5$. (5) *Third Classical Communication and Quantum Communication*— Bob performs a Bell measurement on qubits q_5 and q_6, transmitting the measurement outcome s_3 to Alice. Finally, Bob sends qubit q_7 back to Alice via a quantum channel. (6) *Alice's Correction*— Upon receiving qubit q_7, Alice applies a correction operator $X^{s_{11}+s_{21}+s_{31}} Z^{s_{12}+s_{22}+s_{32}}$ to the quantum state, using the measurement outcomes s_1, s_2, and s_3 to cancel the unintended operators introduced during the gate transfer process (where $s_{j2}s_{j1} = s'_j \oplus s_j$). This results in the successful implementation of the target quantum gate $R_z(\theta_3)R_x(\theta_2)R_z(\theta_1)$. The detailed calculation process is as follows, based on the description provided:

$$\begin{aligned} & X^{s_{31}} Z^{s_{32}} R_z((-1)^{s_{11}+s_{21}}\theta_3) X^{s_{21}} Z^{s_{22}} R_x((-1)^{s_{12}}\theta_2) X^{s_{11}} Z^{s_{12}} R_z(\theta_1)|\psi\rangle \\ &= X^{s_{31}} Z^{s_{32}} R_z((-1)^{s_{11}+s_{21}}\theta_3) X^{s_{21}} Z^{s_{22}} X^{s_{11}} Z^{s_{12}} R_x(\theta_2) R_z(\theta_1)|\psi\rangle \\ &= X^{s_{31}} Z^{s_{32}} X^{s_{21}} Z^{s_{22}} X^{s_{11}} Z^{s_{12}} R_z(\theta_3) R_x(\theta_2) R_z(\theta_1)|\psi\rangle \\ &= X^{s_{31}+s_{21}+s_{11}} Z^{s_{32}+s_{22}+s_{12}} R_z(\theta_3) R_x(\theta_2) R_z(\theta_1)|\psi\rangle, \end{aligned} \tag{1}$$

where $\theta_j \in \{0, \frac{\pi}{4}, \cdots, \frac{7\pi}{4}\}$. During the correction process, the propagation relation of the rotation operators is given by:

$$\begin{aligned} & R_x(\beta)X = XR_x(\beta), \quad R_x(\beta)Z = ZR_x(-\beta), \\ & R_y(\beta)X = XR_y(-\beta), \ R_y(\beta)Z = ZR_y(-\beta), \\ & R_z(\beta)X = XR_z(-\beta), \ R_z(\beta)Z = ZR_z(\beta). \end{aligned} \tag{2}$$

The commutation relation $XZ = -ZX$ ensures that any global phase factor introduced during the commutation of adjacent operators can be disregarded. As shown in Eq.(1), an adaptive selection of the rotation angles is necessary. Ultimately, the cumulative effects of the ancillary operators X and Z are fully eliminated. To illustrate the computational process of the above formula, we provide the following example. In Fig. 1, suppose $|Bell\rangle_{23} = |\phi^+\rangle_{23}$ and $|\psi\rangle_1 = a|0\rangle + b|1\rangle$, where $|a|^2 + |b|^2 = 1$, the process of teleportation is as follows:

$$\begin{aligned} R_z(\theta)|\psi\rangle_1 \otimes |Bell\rangle_{23} &= e^{-\frac{i\theta}{2}}(a|0\rangle + e^{i\theta}b|1\rangle)_1 \otimes |\phi^+\rangle_{23} \\ &= e^{-i\theta/2}/\sqrt{2}(a|0\rangle + e^{i\theta}b|1\rangle)_1(|00\rangle + |11\rangle)_{23} \\ &= e^{-i\theta/2}/\sqrt{2}(a|000\rangle + a|011\rangle + be^{i\theta}|100\rangle + be^{i\theta}|111\rangle) \\ &= e^{-i\theta/2}/2[|\phi^+\rangle(a|0\rangle + be^{i\theta}|1\rangle) + |\phi^-\rangle(a|0\rangle - be^{i\theta}|1\rangle) \\ &\quad + |\psi^+\rangle(a|1\rangle + be^{i\theta}|0\rangle) + |\psi^-\rangle(a|1\rangle - be^{i\theta}|0\rangle)]_{12,3} \end{aligned}$$

If Bob1's measurement outcome is $|\phi^-\rangle$, then Alice obtains the results $s_{j2}s_{j1} = s_j \oplus s'_j = 00 \oplus 10 = 10$. That is, the by-product operator is X^0Z^1. And Alice can obtain $(a|0\rangle + be^{i\theta}|1\rangle)$ from $X^0Z^1(a|0\rangle - be^{i\theta}|1\rangle)$.

In the previous section, we described the single-qubit gates teleportation. In universal blind quantum computation, realizing more complex multi-qubit operations requires the teleportation of CNOT gates. Here, we discuss how to implement the CNOT gate by teleportation controlled-rotation gates (as shown in Fig. 2).

1) *Initialization*— Alice prepares the qubits, labeled q_1 through q_6. The computational qubits q_1 and q_2, responsible for the computational task, are initialized as $|\psi_i\rangle = a_i|0\rangle \pm b_i|1\rangle (i = 1, 2$ and $|a_i|^2 + |b_i|^2 = 1)$. The auxiliary qubits are initialized in non-orthogonal single-qubit states $|\pm\rangle$, $|0\rangle$ or $|1\rangle$. Alice then transmits these qubits to Bob via a quantum channel and sends the circuit instructions through a classical channel. 2) *Preparation*— Upon receiving the quantum bits, Bob applies a CNOT gate to q_1 and q_2, preparing them as the target quantum state. Bob then entangles q_3 and q_4, as well as q_5 and q_6, using CNOT gates to generate the necessary quantum resource state. In this process, the control qubits are initialized in the $|\pm\rangle$ states, while

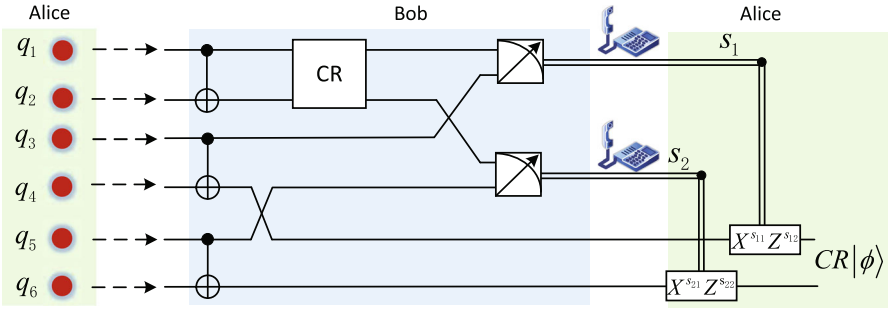

Fig. 2 (Colour online) Schematic of two-qubit gate teleportation in BQC. Alice prepares all qubits q_1 through q_6 and transmits them to Bob. Bob prepares Bell states using CNOT gates and applies the target controlled-rotation (CR) gate to q_1 and q_2. Bell measurements are then performed on q_1 and q_2, as well as q_3 and q_4, with the measurement outcomes s_1 and s_2 transmitted to Alice via a classical channel. Using the feedback results, Alice reconstructs the target state $CR|\phi\rangle$

the target qubits are set to $|0\rangle$ and $|1\rangle$, respectively. Subsequently, Bob applies the target controlled-rotation (CR) gate to q_1 and q_2. 3) *Classical Communication and Quantum Communication*— Bob performs Bell measurements on the qubit pairs q_1, q_3 and q_2, q_5, and transmits the measurement results s_1 and s_2 to Alice via a classical channel. Additionally, Bob sends the quantum states of q_4 and q_6 back to Alice via a quantum channel. 4) *Alice's Correction*— Alice uses the measurement outcomes s_1 and s_2, along with the classical information s_1' and s_2' from the initial Bell states, to compute the classical bits s_{11}, s_{12}, s_{21} and s_{22} required for the correction operations. Finally, Alice applies the correction operations $X^{s_{11}}Z^{s_{12}}$ and $X^{s_{21}}Z^{s_{22}}$ to q_4 and q_6, respectively, to eliminate the accumulated error operators in the protocol, restoring the CR gate operation. Notably, $CR_x(\pi)$ corresponds to the implementation of the CNOT gate operation.

3 UBQCQT protocol

The principles of single-qubit gate and two-qubit gate teleportation have been outlined in the second section. Based on these principles, we now present our universal blind quantum computing protocol. The steps are detailed below:

1. Alice's Preparation

Alice prepares a sufficient number of quantum states $|\psi_i\rangle = a_i|0\rangle \pm b_i|1\rangle$ $(i = 1, 2, 3, \cdots,$ and $|a_i|^2 + |b_i|^2 = 1)$ to encode computational tasks, along with auxiliary qubits $|\pm\rangle$, $|0\rangle$, $|1\rangle$. These states are sent to Bob via a quantum channel.

2. Bob's Preparation

Bob creates Bell states and prepares the target quantum states required for the computational tasks.

3. Classical Interaction, Computation, and Measurement

3.1 Alice calculates the rotation angles $\theta_j' = r_j\pi + (-1)^{s_{lk}}\theta_j$, where $\theta_j \in \{0, \frac{\pi}{4}, \cdots, \frac{7\pi}{4}\}$, the value of r_j is chosen randomly from {0,1}, and s_{lk} depends on r_j. For the first rotation gate,$s_{lk} = 0$ is assigned by Alice. Alice informs Bob whether

to execute the circuit shown in Figs. 1 or 2 based on the computational task. The relationship between the encrypted angles and the original angles is given by:

$$R_{x/y/z}(\theta'_j) = R_x(r_j\pi + (-1)^{s_{lk}}\theta_j) = R_{x/y/z}(r_j\pi)R_x((-1)^{s_{lk}}\theta_j),$$

where $R_x(\pm\pi) = \pm iX$, $R_y(\pm\pi) = \pm XZ$, $R_z(\pm\pi) = \mp iZ$, $R_{x/y/z}(0) = I$.

3.2 Bob returns the measurement results s_j to Alice immediately after each Bell measurement.

3.3 Trap particles are handled in the same manner as computational particles. We assume that trap particles are also Bell states. Entanglement swapping is performed on any two designated Bell states. When a rotation operation is applied to the Bell states at predefined positions, the Bell state remains unchanged, enabling prediction of the measurement results after entanglement swapping. For example, the rotation operations on the qubit 1 and on the qubit 2 are as follows:

$$\begin{aligned}
|\phi^+\rangle_{12} &\xrightarrow{R_z(\theta)_1R_z(\text{-}\theta)_2 \ or \ R_x(\theta)_1R_x(\text{-}\theta)_2 \ or \ R_y(\theta)_1R_y(\theta)_2} |\phi^+\rangle_{12},\\
|\phi^-\rangle_{12} &\xrightarrow{R_z(\theta)_1R_z(\text{-}\theta)_2 \ or \ R_x(\theta)_1R_x(\theta)_2 \ or \ R_y(\theta)_1R_y(\text{-}\theta)_2} |\phi^-\rangle_{12},\\
|\psi^+\rangle_{12} &\xrightarrow{R_z(\theta)_1R_z(\theta)_2 \ or \ R_x(\theta)_1R_x(\text{-}\theta)_2 \ or \ R_y(\theta)_1R_y(\text{-}\theta)_2} |\psi^+\rangle_{12},\\
|\psi^-\rangle_{12} &\xrightarrow{R_z(\theta)_1R_z(\theta)_2 \ or \ R_x(\theta)_1R_x(\theta)_2 \ or \ R_y(\theta)_1R_y(\theta)_2} |\psi^-\rangle_{12}.
\end{aligned} \tag{3}$$

While the verification scheme shares structural features with teleportation-based gates and introduces measurement ambiguity, the concealed distribution of trap qubits prevents the server and potential eavesdroppers from discerning the identity of the final entangled pairs, thereby enhancing security. The limited number of trap qubits constrains the frequency of verification, but the resulting overhead is negligible and does not impact the overall protocol efficiency.

3.4 Alice designates specific positions of quantum states for Bob to return. She then verifies the measurement results of the trap particles. If the results match expectations, it indicates that Bob is honest and the computation accuracy is acceptable. Alice then reconstructs the quantum states used for the computational tasks, completing the complex quantum computation.

4 Proof of correctness and blindness

In this section, we analyze the correctness and blindness of the proposed universal blind quantum computing protocol.

Correctness. If Alice and Bob follow the UBQCQT protocol step by step, all Bell measurement results and quantum outputs will be guaranteed to be correct.

Proof In the teleportation process for single-qubit gates, let the angles of the first rotation gates be $\theta'_1 = r_1\pi + \theta_1$, $\theta'_2 = r_2\pi + (-1)^{r_1}\theta_2$ and $\theta'_3 = r_3\pi + (-1)^{r_2}\theta_3$. When the given rotation gate angles are θ'_1, θ'_2 and θ'_3, the quantum state after teleportation is: $X^{s_{31}+s_{21}+s_{11}}Z^{s_{32}+s_{22}+s_{12}}R_z(\theta'_3)R_x(\theta'_2)R_z(\theta'_1)|\psi\rangle$. We now derive how

$R_z(\theta_3')R_x(\theta_2')R_z(\theta_1')$ is restored to $R_z(\theta_3)R_x(\theta_2)R_z(\theta_1)$.

$$\begin{aligned}
&R_z(\theta_3')R_x(\theta_2')R_z(\theta_1')|\psi\rangle \\
&= R_z(r_3\pi + (-1)^{r_2}\theta_3)R_x(r_2\pi + (-1)^{r_1}\theta_2)R_z(r_1\pi + \theta_1)|\psi\rangle \\
&= R_z(r_3\pi)R_z((-1)^{r_2}\theta_3)R_x(r_2\pi)R_x((-1)^{r_1}\theta_2)R_z(r_1\pi)R_z(\theta_1)|\psi\rangle \\
&= R_z(r_3\pi)R_z((-1)^{r_2}\theta_3)R_x(r_2\pi)R_z(r_1\pi)R_x(\theta_2)R_z(\theta_1)|\psi\rangle \\
&= R_z(r_3\pi)R_x(r_2\pi)R_z(r_1\pi)R_z((-1)^{r_2}\theta_3)R_x(\theta_2)R_z(\theta_1)|\psi\rangle \\
&= R_z((r_1+r_3)\pi)R_x(r_2\pi)R_z((-1)^{r_2}\theta_3)R_x(\theta_2)R_z(\theta_1)|\psi\rangle
\end{aligned} \tag{4}$$

Hence, the final correction operator is derived as: $X^{s_{31}+s_{21}+s_{11}+r_2}Z^{s_{32}+s_{22}+s_{12}+r_1+r_3}$.

For the teleportation process of the two-qubit controlled-rotation gate, the proof follows a similar approach, and the detailed derivation is omitted here.

Blindness (quantum inputs). The auxiliary quantum states sent by Alice to Bob are non-orthogonal single-qubit states $|\pm\rangle$, $|0\rangle$ and $|1\rangle$. Due to their non-orthogonality, Bob is unable to extract any information about the initial quantum states. From the server's perspective, these states are effectively indistinguishable, appearing as though they have undergone a depolarizing channel.

Blindness (algorithms and outputs). The blindness of quantum algorithms and outputs can be demonstrated using Bayes' theorem. First, the rotation angles θ_j' that Alice sends to Bob are encrypted, with both θ_j and θ_j' belonging to the set $S = \{\frac{k\pi}{4}|k = 0, 1, 2, \cdots, 7\}$. By Bayes' theorem, $p(\theta_j|\theta_j', s_j) = p(\theta_j)$, which guarantees the privacy of the quantum algorithm. Second, while Bob can access all measurement results s_j, these results do not directly determine the correction operator's key. The true key is derived from the classical information carried by the initial Bell states and the random numbers r_j, both of which are exclusively known to Alice. Thus, from Bob's perspective, all quantum outputs are effectively one-time-pad encrypted. Bayes' theorem further ensures that $p(s_j|\theta_j', \theta_j) = p(s_j)$, thereby preserving the privacy of the quantum outputs. □

5 Conclusion

In this paper, we propose a universal blind quantum computing protocol assisted by quantum teleportation, involving two participants: Alice (the client) and Bob (the server). In this protocol, Alice prepares the initial single-qubit states and sends them to Bob, who is responsible for generating the required quantum states, performing quantum computations and Bell measurements, and returning the measurement results, necessary quantum states, and part of the trap quantum states to Alice. By combining quantum teleportation with one-time-pad encrypted rotation angles, the protocol successfully conceals fundamental universal gates (e.g., H, T, and CNOT gates), protecting the privacy of quantum gate operations. The blindness and correctness of the protocol are rigorously established.

In Table 1, the protocol proposed in this paper is compared with several representative blind quantum computation protocols, including Childs' circuit-based protocol

Table 1 Comparison of typical BQC Protocols

Protocol	Model	Client's Capability	Sever's Capability	DEQA	Participants	Noise resistance
Childs' protocol [20]	CBQC	Single-qubit states Pauli operations	H,T,CNOT	No	A client A server	No
Broadbent's protocol [4]	MBQC	Single-qubit states Pauli operations	Brickwork states Single-qubit measurement	Yes	A client A server	No
Morimae and Fujii's protocol [37]	MBQC	Completely classical	Bell measurement Brickwork states Single-qubit measurement	Yes	A client A trusted center Two servers	Yes
Sheng and Zhou's protocol [38]	MBQC	Completely classical	Bell measurement Brickwork states Single-qubit measurement	Yes	A client A trusted center Two servers	Yes
Li's protocol [7]	MBQC	Quantum channel	Bell measurement Brickwork states Single-qubit measurement	Yes	A client A trusted center Three servers	No
Our protocol	CBQC	Single-qubit states Pauli operations	Bell states Rotation operations Bell measurement	Yes	A client A server	No

[20], Broadbent's measurement-based protocol [4], the noise-resilient double-server protocols by Morimae and Fujii [37] and by Sheng and Zhou [38], as well as the triple-server protocol by Li et al. [7]. The comparison covers several critical aspects, including the underlying protocol model, the quantum capabilities required by the client and the server, the ability to directly encrypt quantum algorithms (DEQA), the participant structure, and noise resistance. Compared to these existing protocols, the proposed scheme offers several notable advantages. First, it eliminates the need for complex graph states, thereby simplifying state preparation on the server side. Second, it requires only a small number of qubits, resulting in reduced input resource demands and improved computational efficiency. Most importantly, the protocol exhibits excellent scalability and is well suited for applications in distributed quantum computing and quantum cloud services, effectively addressing both privacy protection and the need for efficient quantum processing.

Acknowledgements This work was supported by the Natural Science Foundation of Guangdong Province of China (Grant No. 2023A1515011556), 2024 Guangzhou Basic and Applied Basic Research Project 'Sailing Project' (No. 2024A04J3268) and (826) Central University Education and Teaching Reform Project (No. 82624636).

Author Contributions X.Z. completed the methodology, conceptualization, validation and writing-original draft of manuscript.

Data Availability No datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. https://www.ibm.com/quantum
2. https://originqc.com.cn/index.html?lang=en_US
3. Deng, Y.H., et al.: Solving graph problems using Gaussian Boson sampling. Phys. Rev. Lett. **130**, 190601 (2023)
4. Broadbent, A., Fitzsimons, J., Kashefi, E.: Universal blind quantum computation. In: Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science 517-526 (2009)
5. Barz, S., et al.: Demonstration of blind quantum computing. Science **335**, 303–308 (2012)
6. Morimae, T., Fujii, K.: Secure entanglement distillation for double-server blind quantum computation. Phys. Rev. Lett. **111**, 020502 (2013)
7. Li, Q., Chan, W.H., Wu, C.H., Wen, Z.H.: Triple-server blind quantum computation using entanglement swapping. Phys. Rev. A **89**, 040302 (2014)
8. Sheng, Y.B., Zhou, L.: Deterministic entanglement distillation for secure double-server blind quantum computation. Sci. Rep. **5**, 7815 (2015)
9. Morimae, T., Fujii, K.: Blind topological measurement-based quantum computation. Nat. Commun. **3**, 1036 (2012)
10. Morimae, T., Dunjko, V., Kashefi, E.: Ground state blind quantum computation on AKLT states. Quant. Inf. Comput. **15**, 200–234 (2015)
11. Fitzsimons, J.F.: Private quantum computation: an introduction to blind quantum computing and related protocols. NPJ Quant. Inf. **3**, 1–11 (2017)
12. Ma, S.Q., Zhu, C.H., Liu, X.C., Li, H.G., Li, S.B.: Universal blind quantum computation with improved brickwork states. Phys. Rev. A **109**, 012606 (2024)

13. Yan, Y.Z., et al.: Blind quantum computation with fewer quantum and delegated cost of client. Int. J Quant. Inf. **23**, 2530001 (2025)
14. Xie, X.J., Li, Q., Tan, X.Q., Gao, L.M., Hong, Y.: Flexible blind quantum computation with unnecessarily universal quantum servers. Opt. Laser Technol. **18**, 111548 (2025)
15. Quan, J.Y., Li, Q., Li, L.Z.: Verifiable blind quantum computation with identity authentication for multi-type clients. IEEE Trans. Inf. Forensics Secur. **19**, 1687–1698 (2024)
16. Polacchi, B., et al.: Multi-client blind quantum computing over a Qline architecture. Quantum 2.0 Conference and Exhibition (2024)
17. Dam, J.V., et al.: Hardware requirements for trapped-ion-based verifiable blind quantum computing with a measurement-only client. Quant. Sci. Technol. **9**, 045031 (2024)
18. Drmota, P., et al.: Verifiable blind quantum computing with trapped ions and single photons. Phys. Rev. Lett. **132**, 150604 (2024)
19. Yang, Z., Wu, G.Y., Bai, M.Q.: Half-blind quantum computation with operation teleportation. J. Phys. A: Math. Theor. **57**, 195302 (2024)
20. Childs, A.M.: Secure assisted quantum computation. Quant. Inf. Comput. **5**, 456–466 (2005)
21. Broadbent, A.: Delegating private quantum computations. Can. J. Phys. **93**, 941–946 (2015)
22. Fisher, K., et al.: Quantum computing on encrypted data. Nat. Commun. **5**, 3074 (2014)
23. Barz, S., et al.: Demonstration of blind quantum computing. Science **335**, 303 (2012)
24. Barz, S., Fitzsimons, J.F., Kashefi, E., Walther, P.: Experimental verification of quantum computation. Nat. Phys. **9**, 727–731 (2013)
25. Fisher, K., et al.: Quantum computing on encrypted data. Nat. Commun. **5**(3074), 1–7 (2014)
26. Greganti, C., et al.: Demonstration of measurement-only blind quantum computing. New J. Phys. **18**, 013020 (2016)
27. Huang, H.L., et al.: Experimental blind quantum computing for a classical client. Phys. Rev. Lett. **119**, 050503 (2017)
28. Tham, W.K., et al.: Experimental demonstration of quantum fully homomorphic encryption with application in a two-party secure protocol. Phys. Rev. X **10**, 011038 (2020)
29. Zeuner, J., et al.: Experimental quantum homomorphic encryption. NPJ Quantum Information **7**, 25 (2021)
30. Li, Y., et al.: Experimental quantum homomorphic encryption using a quantum photonic chip. Phys. Rev. Lett. **132**, 200801 (2024)
31. Bennett, C.H., et al.: Teleporting an unknown quantum state via dual classic and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)
32. Briegel, H.J., Dur, W., Cirac, J.I., Zoller, P.: Quantum repeaters: the role of imperfect local operations in quantum communication. Phys. Rev. Lett. **81**, 5932–5935 (1998)
33. Kimble, H.J.: The quantum internet. Nature **453**, 1023–1030 (2008)
34. Gottesman, D., Chuang, I.: Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature **402**, 390–393 (1999)
35. Knill, E., Laflamme, R., Milburn, G.J.: A scheme for efficient quantum computation with linear optics. Nature **409**, 46–52 (2001)
36. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
37. Morimae, T., Fujii, K.: Secure entanglement distillation for double-server blind quantum computation. Phys. Rev. Lett. **111**, 020502 (2013)
38. Sheng, Y.B., Zhou, L.: Deterministic entanglement distillation for secure double-server blind quantum computation. Sci. Rep. **5**, 7815 (2015)