Efficient and Secure Multi-Qubit Broadcast-Based Quantum Federated Learning

Rui Zhang, Jian Wang, Nan Jiang, Md Armanuzzaman, and Ziming Zhao

***Abstract*—Quantum Federated Learning (QFL) has emerged as a promising research direction by combining the strengths of quantum computing and federated learning. However, existing QFL solutions have consistently failed to simultaneously improve client training efficiency and ensure communication security. In this paper, we present a novel Multi-qubit Broadcast-based QFL framework (MB-QFL) to address the efficiency and security challenges of existing approaches. The framework employs a novel multi-qubit broadcast protocol and a quantum average method to secure the information transmission process. The multi-qubit broadcast protocol overcomes the limitations of existing protocols by allowing the transmission of an arbitrary S-qubit state from one sender to multiple (Q) receivers, whereas earlier protocols were restricted to broadcast one or two qubit state to recipients. Additionally, we propose an averaging method for quantum states, which exploits the probabilistic cloning technique to achieve aggregation in MB-QFL. The security analysis demonstrates that MB-QFL can effectively protect against inference attacks from malicious clients, as well as eavesdropping and intercept-and-resend attacks during communication. The algorithm complexity of MB-QFL is significantly lower than existing QFLs. Besides, the experimental results indicate that MB-QFL achieves higher classification accuracy than other QFLs.**

***Index Terms*—Quantum federated learning, quantum machine learning, quantum computation.**

I. Introduction

DISTRIBUTED machine learning enables collaborative model training across multiple devices or nodes while preserving data privacy [1], [2], [3], [4]. Quantum Federated Learning (QFL) is a form of distributed quantum machine learning developed to address stringent privacy regulations and the difficulties of acquiring large amounts of real data [5], [6], [7], [8], [9], [10], [11], [12]. In this approach, multiple quantum computing nodes, each with its own local dataset, collaborate to train a shared quantum machine learning model. Each node processes its own data independently, ensuring privacy and security by not transferring raw data between nodes. QFL theoretically offers better computational power and security compared to classical federated learning [12].

In QFL, since the raw data does not need to be shared, the security of client information is partially ensured. However, similar to classical algorithms, QFL also faces risks such as Byzantine attacks [13], gradient attacks [14], and adversarial attacks [15]. In particular, eavesdropping attacks during communication and inference attacks by malicious clients are key challenges in existing QFL. This is primarily because, even after the client model is trained using quantum algorithms, the parameters between clients and the server are still transmitted using classical algorithms [9], [16].

Therefore, some schemes were proposed utilizing the quantum properties for privacy protection [17], [18], [19], [20], [21]. A QFL framework that allows distributed quantum neural network training on encrypted data was introduced using Quantum Homomorphic Encryption (QHE-QFL) [22]. In QHE-QFL, encryption and decryption operations are required, which increases computational overhead. Quantum federated learning based on Quantum Key Distribution (QKD-QFL) defends against eavesdropping attacks but requires secure key generation as a prerequisite [18].

Although the QFL algorithm mentioned above uses quantum algorithms to resist eavesdropping attacks during communication, it requires additional resources to resist eavesdropping attacks. Quantum teleportation enables the efficient transmission of quantum states by leveraging quantum entanglement and classical communication, thereby eliminating the need for complex quantum circuits. Therefore, the quantum teleportation-based QFL (QT-QFL) is proposed, which significantly reduces computational overhead [23], [24]. Although quantum teleportation avoids transmitting the physical medium carrying quantum information, it requires the prior distribution of entangled states-a process susceptible to intercept-and-resend attacks by malicious intermediaries. In addition, existing algorithms use variational quantum algorithms or classical algorithms to train client models. Each client needs to know the updated information, which provides opportunities for malicious clients to conduct inference attacks. As a result, all existing algorithms cannot guarantee the security of client information and the efficiency of training at the same time.

Received 11 November 2024; revised 16 May 2025 and 18 June 2025; accepted 18 June 2025. Date of publication 27 June 2025; date of current version 8 July 2025. This work was supported in part by Beijing Jiaotong University and Beijing University of Technology through the Fundamental Research Funds for the Central Universities under Grant 2022JBZY020 and in part by the Beijing Jiaotong University and Beijing University of Technology through the National Key Research and Development Program of China under Grant 2023YFB2703702. The associate editor coordinating the review of this article and approving it for publication was Dr. Dusit Niyato. *(Corresponding author: Nan Jiang.)*

Rui Zhang and Jian Wang are with Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China (e-mail: zhangrui121@bjtu.edu.cn; wangjian@bjtu.edu.cn).

Nan Jiang is with the College of Computer Science, Beijing University of Technology, Beijing 100124, China (e-mail: jiangnan@bjut.edu.cn).

Md Armanuzzaman and Ziming Zhao are with the CyberspACe securiTy and forensIcs lab (CactiLab), Northeastern University, Boston, MA 02115 USA (e-mail: m.armanuzzaman@northeastern.edu; z.zhao@northeastern.edu).

Digital Object Identifier 10.1109/TIFS.2025.3583901

In this paper, we present a novel Multi-qubit Broadcast-based QFL framework (MB-QFL) to enhance QFL through quantum properties and address the limitations of previous works. To improve training efficiency, we employ quantum algorithms for local model training, while communication security between clients and the server is ensured through quantum communication. The contributions of this work are as follows:

- We present a multi-qubit broadcast protocol that can transmit an arbitrary S-qubit state from one sender to Q receivers. This protocol is inherently secure due to the no-cloning theorem. Additionally, we construct a unitary operator consisting of the simplest and most commonly used computational basis for measurements. Consequently, the measurement result can be simpler, easier to decompose and transmit;
- We propose an amplitude storage-based quantum average method for aggregation, using probabilistic cloning techniques to average the Q received quantum states, which is used to store the updated parameters. Our proposed method can calculate the average value of multiple superposition states;
- We propose the MB-QFL framework, which employs only quantum algorithms for model training, communication, and aggregation. This approach simultaneously resists inference and eavesdropping attacks while enhancing training efficiency compared to existing QFL methods. Models trained using MB-QFL can achieve accuracies comparable to those achieved with centralized training. Furthermore, the algorithm presented in this paper demonstrates lower complexity than other QFL algorithms while maintaining a consistent level of accuracy.

II. Background Knowledge

In this section, we present the background knowledge on quantum computation and communications.

A. Quantum Computation

Quantum computing is technology based upon phenomena of quantum mechanics, such as superposition and entanglement. In quantum computing, the information is stored by the quantum bit (qubit), which is an analogy to the bit in the classical digital computer. The arbitrary 1-qubit state $|\rho_1\rangle$ can be described by a linear superposition of $|0\rangle$ and $|1\rangle$: $|\rho_1\rangle = a_0|0\rangle + a_1|1\rangle$, where $|\cdot\rangle$ is called the Dirac notation, a_0 and a_1 are complex number that satisfy $|a_0|^2 + |a_1|^2 = 1$. Generally, a_0 and a_1 are called amplitudes, and $|0\rangle$ and $|1\rangle$ are called basis states. Information can be stored in the basis states or in the amplitudes.

In quantum mechanics, the tensor product is used to describe composite quantum systems. For instance, the tensor product of $|v\rangle$ and $|w\rangle$ is denoted as $|v\rangle \otimes |w\rangle$, or simply $|vw\rangle$. Similarly, the n fold tensor product $|v\rangle \otimes |v\rangle \otimes \ldots \otimes |v\rangle$ of $|v\rangle$ is abbreviated as $|v\rangle^{\otimes n}$.

In the computational basis, the 2^S basis vectors are shown in Eq. (1) using the binary strings of length S.

$$|00\ldots00\rangle, |00\ldots01\rangle, \ldots, |11\ldots11\rangle \tag{1}$$

For convenience, the binary numbers in Eq. (1) are usually converted into the decimal numbers $|0\rangle, |1\rangle, \ldots, |2^S - 1\rangle$.

An arbitrary vector in Hilbert space can be written either as a weighted sum of the basis vectors in the Dirac notation, or as a single column matrix. Therefore, a S-qubits state $|\rho_S\rangle$ can be represented as follows:

$$|\rho_S\rangle = \sum_{s=0}^{2^S-1} a_s|s\rangle = \left[a_0\ a_1\ \ldots\ a_{2^S-1}\right]^{\mathrm{T}} \tag{2}$$

where $a_0, a_1, \ldots, a_{2^S-1}$ are complex numbers such that $\sum_{s=0}^{2^S-1} |a_s|^2 = 1$.

Suppose C_1 and C_2 are linear operators on $|v\rangle$ and $|w\rangle$ respectively. Then C_1 and C_2 is the linear operator on $|v\rangle \otimes |w\rangle$ defined by:

$$(C_1 \otimes C_2)(|v\rangle \otimes |w\rangle) = C_1|v\rangle \otimes C_2|w\rangle \tag{3}$$

A quantum gate is a unitary operator acting on qubits, mathematically represented by a unitary matrix. Some of the basic gates and their corresponding matrices are shown in Eq. (4) including H gate, X gate, Y gate, Z gate, and Controlled-NOT gate ($CNOT$).

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix};\ X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix};\ Y = \begin{bmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{bmatrix};$$
$$Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix};\ CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \tag{4}$$

Quantum measurement plays a very important role in quantum computation, as it allows us to obtain information about quantum states. Quantum measurements are described by a collection $\{E_e\}$ of measurement operators. Immediately before measurement if the state of the quantum system is $|\rho_S\rangle$, then the probability that result e occurs is given by $P(e) = \langle\rho_S|E_e^+E_e|\rho_S\rangle$, where E_e^+ represents the conjugate transpose of E_e. The state of the system after the measurement is $|\rho_S'\rangle = \frac{E_e|\rho_S\rangle}{\sqrt{P(e)}}$. The measurement operators satisfy the completeness equation $\sum_e E_e^+E_e = I$, where I is the identity matrix. The completeness equation expresses the fact that probabilities sum to one, in short, $\sum_e P(e) = 1$.

In some quantum circuits, measurements are performed at intermediate stages, and the results are used to conditionally control subsequent quantum gates. According to a fundamental principle, these classically conditioned operations can be replaced with quantum-conditioned operations. The principle of deferred measurement states that measurements in a quantum circuit can always be postponed to the end of the circuit. If measurement results are used at any stage to control operations, these classically controlled operations can be replaced with quantum conditional operations.

B. Quantum Communication

One of the most common forms of quantum communication is quantum teleportation [25]. To teleport the quantum state of a qubit, $|\rho_1\rangle$, to the receiver, an entanglement channel must be established between them. The four Bell states are often used as the entanglement channel for this purpose:

$$|\Phi_{0,1}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Phi_{2,3}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \quad (5)$$

If $|\Phi_0\rangle$ is used as an entanglement channel, then the initial quantum state in teleportation is:

$$|\rho_1\rangle|\Phi_0\rangle = \frac{1}{\sqrt{2}}(a_0|0\rangle(|00\rangle + |11\rangle) + a_1|1\rangle(|00\rangle + |11\rangle)) \quad (6)$$

The first two qubits belong to the sender, while the third qubit belong to the receiver. At first, the sender performs a *CNOT* gate on its qubits, obtaining:

$$\frac{1}{\sqrt{2}}(a_0|0\rangle(|00\rangle + |11\rangle) + a_1|1\rangle(|10\rangle + |01\rangle)) \quad (7)$$

Then, the sender performs an H gate on the first qubit, obtaining:

$$\frac{1}{2}(a_0(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + a_1(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)) \quad (8)$$

By regrouping terms, the state in Eq. (8) may be re-written in the following way:

$$\begin{aligned}\frac{1}{2}&(|00\rangle(a_0|0\rangle + a_1|1\rangle) + |01\rangle(a_0|1\rangle + a_1|0\rangle)\\ &+ |10\rangle(a_0|0\rangle - a_1|1\rangle) + |11\rangle(a_0|1\rangle - a_1|0\rangle))\end{aligned} \quad (9)$$

This expression can be divided into four terms. In the first term, the sender's qubits are in the state $|00\rangle$, and the receiver's qubit is in the state $a_0|0\rangle + a_1|1\rangle$, which is the original state $|\rho_1\rangle$. This means that if the sender measures and obtains the result 00, then the receiver's system will be in the state $|\rho_1\rangle$. Similarly, based on the sender's measurement results, we can describe the receiver's corresponding post-measurement states as follows:

$$\begin{aligned} 00 &\mapsto a_0|0\rangle + a_1|1\rangle \qquad 01 \mapsto a_0|1\rangle + a_1|0\rangle\\ 10 &\mapsto a_0|0\rangle - a_1|1\rangle \qquad 11 \mapsto a_0|1\rangle - a_1|0\rangle \end{aligned} \quad (10)$$

Based on the sender's measurement outcome, the receiver's qubit will collapse into one of the four possible states. If the outcome is 00, the receiver does not need to take any action. The receiver performs X gate in case of 01 and if it receives 01, the receiver performs Z gate. Lastly, if the outcome is 11, the receiver fixes up its state by applying an X gate and a Z gate respectively.

Furthermore, the generalized quantum teleportation allows the teleportation of an arbitrary S-qubit state $|\rho_S\rangle$ from the sender to the receiver using the general Bell states [26], [27]. Additionally, another form of quantum communication, known as the quantum broadcast protocol, enables the transmission of a quantum state to multiple receivers [28], [29].

III. Multi-Qubit Broadcast Protocol: Broadcasting Arbitrary S-Qubit State to Q Receivers

In MB-QFL, updated parameters are stored in a quantum state, necessitating the server to broadcast this state to all clients. In this section, we introduce a broadcast protocol that can transmit an arbitrary S-qubit state $|\phi_S\rangle$ from one sender to Q receivers. To enable the measurement operator to be composed of the simplest computational basis, we also construct the unitary operator R, which consists of the information to be broadcast.

For simplicity, we denote A as the sender, B as the collection of Q receivers, and B_q ($q = 0, 1, \ldots, Q-1$) as the qth receiver.

A. The Broadcasting Unitary Operator

To broadcast the amplitude of the quantum state $|\phi_S\rangle = \sum_{s=0}^{2^S-1} \alpha_s|s\rangle$ to Q receivers, the sender A should perform a unitary operator R to modify the measurement basis, where the coefficients $\alpha_0, \alpha_1, \ldots, \alpha_{2^S-1}$ are real numbers and satisfy the normalization condition $\sum_{s=0}^{2^S-1} |\alpha_s|^2 = 1$.

The unitary operator can be expressed as $R = M^{\otimes Q}$, where M is an arbitrary $2^S \times 2^S$ orthogonal matrix with rows composed of $\pm\alpha_0$, $\pm\alpha_1$, ..., $\pm\alpha_{2^S-1}$. The following shows that R is a unitary operator. Since the orthogonal matrix M satisfies $MM^{\mathrm{T}} = M^{\mathrm{T}}M = I$ and its elements are real numbers, it is also a unitary matrix. Consequently, since R satisfies $RR^{\mathrm{T}} = M^{\otimes Q}M^{\mathrm{T}^{\otimes Q}} = I$, R is also unitary and can therefore be used as a quantum gate [30].

Each row in matrix M is constructed by rearranging the elements of $[\alpha_0\ \alpha_1\ \ldots\ \alpha_{2^S-1}]$ and potentially changing their signs. Therefore, there exists a signed permutation matrix U_s such that $U_s M_{s,:} = [\alpha_0\ \alpha_1\ \ldots\ \alpha_{2^S-1}]$ for $s = 0, 1, \ldots, 2^S - 1$, where $M_{s,:}$ represents the sth row of M. The permutation matrix U_s satisfies $U_s U_s^{\mathrm{T}} = I$, and its elements consist of ± 1 and 0. Consequently, these permutation matrices (U_s, $s = 0, 1, \ldots, 2^S - 1$) are unitary, meaning they can be used as quantum gates [30]. For example, when $S = 2$:

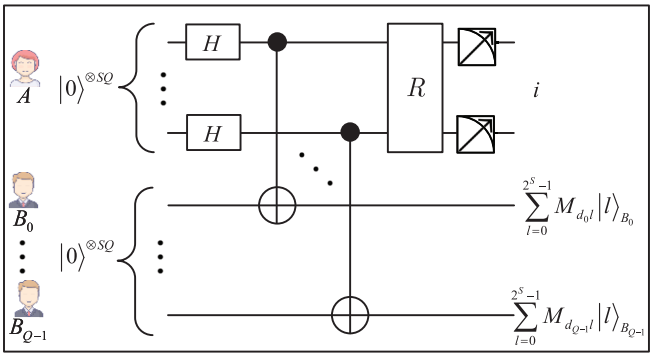
$$M = \begin{bmatrix} \alpha_0 & -\alpha_1 & \alpha_2 & -\alpha_3 \\ \alpha_1 & \alpha_0 & -\alpha_3 & -\alpha_2 \\ -\alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1 \\ \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 \end{bmatrix} \quad (11)$$

And M in Eq. (11) is used to construct $R = M^{\otimes Q}$, the corresponding permutation matrices are as follows:

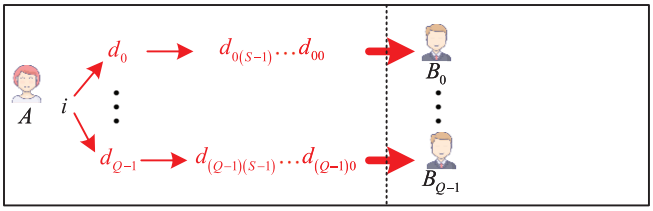
$$\begin{aligned} U_0 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, U_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix},\\ U_2 &= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, U_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{aligned} \quad (12)$$

B. The Broadcast Protocol

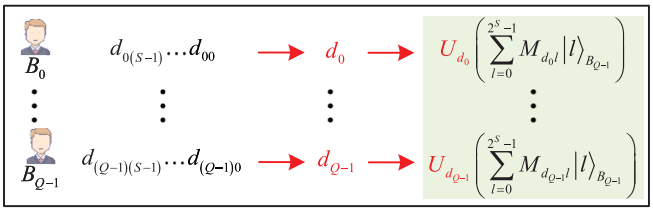
The quantum state $|\phi_S\rangle = \sum_{s=0}^{2^S-1} \alpha_s|s\rangle$ is broadcast to Q receivers $\{B_q\}_{q=0}^{Q-1}$ through the following three steps:



Step 1: A gets the result i and B_q receives the unknown quantum state



Step 2: A transmits the measurement results to B_q



Step 3: B_q reconstructs the quantum state

Fig. 1. The process of broadcasting an arbitrary S-qubit state to Q receivers.

1) B_q Receives the Unknown Quantum State: To broadcast the quantum state, as shown in Step 1 of Figure 1, an entangled quantum channel $|\Phi\rangle_1$ should be prepared first using the H gate and the *CNOT* gate:

$$|\Phi\rangle_1 = \frac{1}{\sqrt{2^{SQ}}} \sum_{j=0}^{2^{SQ}-1} |j\rangle_A |j\rangle_B \tag{13}$$

The entangled quantum state $|\Phi\rangle_1$ is then distributed to the sender and the receivers. A holds the first SQ qubits, while B holds the last SQ qubits. Therefore, we use $|j\rangle_A$ and $|j\rangle_B$ to represent the qubits held by A and B, respectively. Additionally, the (qS)th to $((q+1)S-1)$th qubits in $|j\rangle_B$ belong to B_q $(q = 0, 1, \ldots, Q-1)$.

Then, A performs the unitary operator $R = M^{\otimes Q}$ on its SQ qubits, resulting in the following state:

$$|\Phi\rangle_2 = \frac{1}{\sqrt{2^{SQ}}} \sum_{j=0}^{2^{SQ}-1} (R|j\rangle_A)|j\rangle_B \tag{14}$$

If the entry in the i th row and j th column of the matrix R is denoted as R_{ij} for $i, j = 0, 1, \ldots, 2^{SQ}-1$, then:

$$|\Phi\rangle_2 = \frac{1}{\sqrt{2^{SQ}}} \sum_{j=0}^{2^{SQ}-1} \left(\sum_{i=0}^{2^{SQ}-1} R_{ij}|i\rangle_A \right) |j\rangle_B$$

$$= \frac{1}{\sqrt{2^{SQ}}} \sum_{i=0}^{2^{SQ}-1} |i\rangle_A \left(\sum_{j=0}^{2^{SQ}-1} R_{ij}|j\rangle_B \right) \tag{15}$$

The matrix R, when acting on this set of basis states, can be viewed as an orthogonal transformation that maps one set of orthonormal bases to another. According to the properties of tensor products:

$$R \begin{bmatrix} |0\rangle \\ |1\rangle \\ \vdots \\ |2^{SQ}-1\rangle \end{bmatrix} = M^{\otimes Q} \begin{bmatrix} |0\rangle \\ |1\rangle \\ \vdots \\ |2^{S}-1\rangle \end{bmatrix}^{\otimes Q}$$

$$= \left(M \begin{bmatrix} |0\rangle \\ |1\rangle \\ \vdots \\ |2^{S}-1\rangle \end{bmatrix} \right)^{\otimes Q} \tag{16}$$

Then, $\sum_{j=0}^{2^{SQ}-1} R_{ij}|j\rangle_B$ in Eq. (15) can be written as:

$$\sum_{j=0}^{2^{SQ}-1} R_{ij}|j\rangle_B = \prod_{q=0}^{Q-1} \left(\sum_{l=0}^{2^S-1} M_{d_q l}|l\rangle_{B_q} \right) \tag{17}$$

where $d_{Q-1}d_{Q-2}\ldots d_0$ is a base-2^S number converted by the base-10 number i. Specifically, i can be expressed as $i = d_{Q-1} \times (2^S)^{Q-1} + d_{Q-2} \times (2^S)^{Q-2} + \ldots + d_0 \times (2^S)^0$ [31].

Therefore, Eq. (15) can be rewritten as:

$$|\Phi\rangle_2 = \frac{1}{\sqrt{2^{SQ}}} \sum_{i=0}^{2^{SQ}-1} |i\rangle_A \left(\prod_{q=0}^{Q-1} \left(\sum_{l=0}^{2^S-1} M_{d_q l}|l\rangle_{B_q} \right) \right) \tag{18}$$

If the sender performs a measurement, the quantum state obtained by the receiver B_q collapses to the quantum state $\sum_{l=0}^{2^S-1} M_{d_q l}|l\rangle_{B_q}$. This quantum state can be viewed as the result of applying a certain permutation matrix to the quantum state $|\phi_S\rangle$. However, since the receivers have no knowledge of the specific permutation matrix at this stage, they are unable to know the exact form of the quantum state $\sum_{l=0}^{2^S-1} M_{d_q l}|l\rangle_{B_q}$. Consequently, this state differs from the quantum state $|\phi_S\rangle$ broadcast by A.

2) A Transmits the Measurement Results to B_q: Next, A performs a measurement on its SQ qubits using the computational basis states $\{|0\rangle, |1\rangle, \ldots, |2^{SQ}-1\rangle\}$, and then transmits the measurement results to all receivers.

Suppose A's measurement outcome is $i = d_{Q-1} \times (2^S)^{Q-1} + d_{Q-2} \times (2^S)^{Q-2} + \ldots + d_0 \times (2^S)^0$. A should then transmit the binary representation $d_{q(S-1)}d_{q(S-2)}\ldots d_{q0}$ (Classical bits) of d_q to B_q via classical communication.

3) B_q Reconstructs the Quantum State: B_q converts the received binary string $d_{q(S-1)}d_{q(S-2)}\ldots d_{q0}$ of d_q into decimal value d_q. Since $U_{d_q}M_{d_q,:} = \begin{bmatrix}\alpha_0 & \alpha_1 & \ldots & \alpha_{2^S-1}\end{bmatrix}$, B_q performs the unitary operator U_{d_q} on its qubits according to $d_{q(S-1)}d_{q(S-2)}\ldots d_{q0}$. After applying U_{d_q}, B_q obtains the quantum state $|\phi_S\rangle$. Figure 1 represents the flow of broadcasting arbitrary S-qubit state to Q receivers.

The classical communication bits, the quantum state held by B_q, and the unitary operator U_{d_q} performed by B_q are given in Table I, in which the corresponding permutation matrices

TABLE I
THE MEASUREMENT RESULTS AND CORRESPONDING OPERATORS

Classical bits	d_q	The quantum satate holding by B_q	The unitary operators performed by B_q
00	0	$\sum_{l=0}^{3} M_{0l}\|l\rangle = \alpha_0\|0\rangle - \alpha_1\|1\rangle + \alpha_2\|2\rangle - \alpha_3\|3\rangle$	U_0
01	1	$\sum_{l=0}^{3} M_{1l}\|l\rangle = \alpha_1\|0\rangle + \alpha_0\|1\rangle - \alpha_3\|2\rangle - \alpha_2\|2\rangle$	U_1
10	2	$\sum_{l=0}^{3} M_{2l}\|l\rangle = -\alpha_2\|0\rangle + \alpha_3\|1\rangle + \alpha_0\|2\rangle - \alpha_1\|3\rangle$	U_2
11	3	$\sum_{l=0}^{3} M_{3l}\|l\rangle = \alpha_3\|0\rangle + \alpha_2\|1\rangle + \alpha_1\|2\rangle + \alpha_0\|3\rangle$	U_3

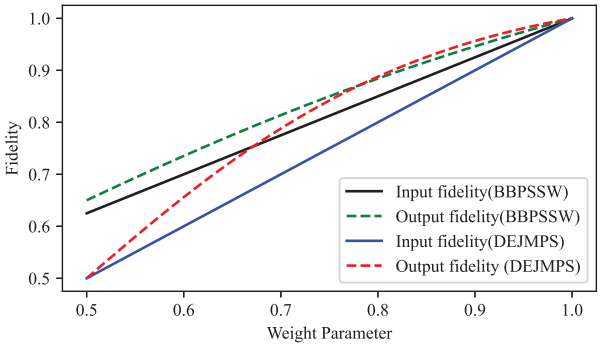


Fig. 2. Comparison of fidelity before and after purification.

are shown in Eq. (12). Such as, if $d_q = 0$, the quantum state held by B_q is $\sum_{l=0}^{3} M_{0l}|l\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle + \alpha_2|2\rangle - \alpha_3|3\rangle$, and the unitary permutation matrix performed by B_q is U_0.

It is worth noting that entanglement distribution, as a fundamental component of the broadcast protocol, is highly susceptible to noise introduced by imperfect entanglement sources and transmission channels. The technique of purification was developed to compensate for the degradation of entanglement resources caused by such noise. Figure 2 illustrates the improvement in fidelity achieved by two representative purification protocols: BBPSSW [32] and DEJMPS [33]. In Figure 2, the input fidelity curve reflects the closeness between the noisy entangled state and the ideal Bell state, whereas the output fidelity curve characterizes the fidelity between the purified state and the ideal target. The weight parameter serves to quantify the fraction of the ideal entangled component embedded in the noisy state. As shown in Figure 2, both protocols can enhance the fidelity effectively within a certain parameter range. In this study, we consider entanglement distribution under ideal conditions, i.e., in the absence of noise.

IV. MB-QFL: A Multi-Qubit Broadcast-Based Quantum Federated Learning Framework

In this section, we present MB-QFL, which follows a process similar to classical federated learning, consisting of four steps: local model training, uploading model parameters to the server, quantum aggregation, and broadcasting the parameters to all clients. We first introduce the quantum average method, which can calculate the average value of multiple superposition states. MB-QFL is then provided.

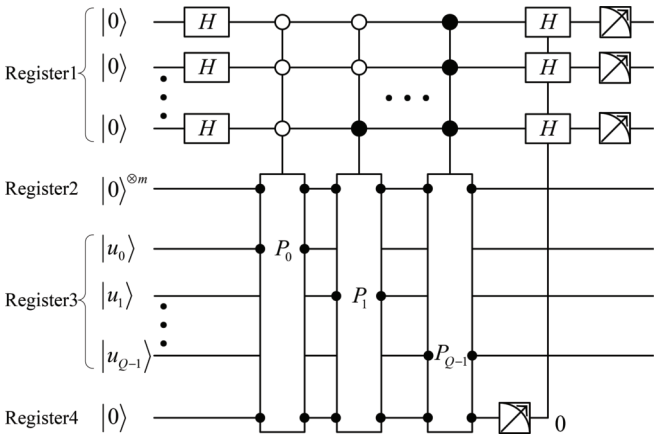


Fig. 3. Quantun circuit of the quantum average method.

A. Quantum Average

Each quantum state corresponds to a column vector. The average value of Q quantum states is actually the average value of multiple column vectors. Since the elements of those vectors are stored in the amplitude of the quantum state, the average value of Q quantum states corresponds to the sum of the amplitudes and divided by the total number of quantum states. If the existing quantum adder based on ground state storage is used, that is, the sum of the numbers stored in the ground state is calculated and then divided by the number of quantum states, the information stored in the amplitude needs to be transferred to the ground state, which will consume a lot of resources. Hence, we propose an amplitude storage-based quantum averaging algorithm, which employs probabilistic cloning [34] to compute the quantum average state

$$|u\rangle = \frac{1}{\sqrt{Q}}\left(|u_0\rangle + |u_1\rangle + \cdots + |u_{Q-1}\rangle\right) \tag{19}$$

of the input states $\{|u_0\rangle, |u_1\rangle, \ldots, |u_{Q-1}\rangle\}$. The quantum circuit of quantum average method is shown in Figure 3.

The initial quantum state $|\Psi_1\rangle$ is as follows:

$$|\Psi_1\rangle = |0\rangle^{\tilde{q}}|0\rangle^{m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle \tag{20}$$

where $\tilde{q} = \log_2 Q$, $m = \log_2(K+1)$ represents the number of qubits in the quantum states $|u_q\rangle$ for $q = 0, 1, \cdots, Q-1$, K represents the number of samples and each sample is represented by an N-dimensional feature vector, and we denote $|0\rangle^{\tilde{q}}$, $|0\rangle^{\otimes m}$, $|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle$, and $|0\rangle$ as the first, second, third, and fourth registers, respectively.

At first, the tensor product of $\tilde{q}$ H gates, denoted as $H^{\otimes\tilde{q}}$, is applied to the first register $|0\rangle^{\otimes\tilde{q}}$. As a result we get:

$$\begin{aligned}
|\Psi_2\rangle &= (H^{\otimes\tilde{q}}|0\rangle^{\otimes\tilde{q}})|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle \\
&= \frac{1}{\sqrt{Q}}(|0\rangle + |1\rangle + \ldots + |Q-1\rangle)|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle \\
&\quad \ldots|u_{Q-1}\rangle|0\rangle \\
&= \frac{1}{\sqrt{Q}}(|0\rangle|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle \\
&\quad + |1\rangle|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle \\
&\quad + \ldots + |Q-1\rangle|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle)
\end{aligned} \tag{21}$$

Let P_q ($q = 0, 1, \ldots, Q-1$) represent the operator that realize probabilistic cloning [34], that is:

$$P_q|0\rangle^{\otimes m}|u_q\rangle|0\rangle = \sqrt{\delta}|u_q\rangle|u_q\rangle|0\rangle + \sqrt{1-\delta}|\varepsilon_q\rangle|1\rangle \tag{22}$$

where δ represents the probability of successful cloning and $|\varepsilon_q\rangle$ is the quantum state obtained by failed cloning. The qubit in the forth register is the flag qubit, where the state $|0\rangle$ indicates a successful clone and $|1\rangle$ indicates a failure.

Then, we apply the operator P_q controlled by q to the second register $|0\rangle^{\otimes m}$:

$$\begin{aligned}
&|\Psi_3\rangle \\
&= \frac{1}{\sqrt{Q}}(|0\rangle P_0|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle \\
&\quad + |1\rangle P_1|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle \\
&\quad + \ldots + |Q-1\rangle P_{Q-1}|0\rangle^{\otimes m}|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle) \\
&= \frac{1}{\sqrt{Q}}(\sqrt{\delta}|0\rangle|u_0\rangle|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle + \sqrt{1-\delta}|\varepsilon_0\rangle|1\rangle \\
&\quad + \sqrt{\delta}|1\rangle|u_1\rangle|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle + \sqrt{1-\delta}|\varepsilon_1\rangle|1\rangle \\
&\quad + \ldots + \sqrt{\delta}|Q-1\rangle|u_{Q-1}\rangle|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle|0\rangle \\
&\quad + \sqrt{1-\delta}|\varepsilon_{Q-1}\rangle|1\rangle) \\
&= \frac{1}{\sqrt{Q}}(\sqrt{\delta}(|0\rangle|u_0\rangle + |1\rangle|u_1\rangle + |Q-1\rangle|u_{Q-1}\rangle)|u_0\rangle|u_1\rangle \\
&\quad \ldots|u_{Q-1}\rangle|0\rangle + \sqrt{1-\delta}(|\varepsilon_0\rangle + |\varepsilon_1\rangle + \ldots + |\varepsilon_{Q-1}\rangle)|1\rangle)
\end{aligned} \tag{23}$$

At this time, when the qubit of the fourth register is $|0\rangle$, cloning is successful. Therefore, the fourth register is measured and when the measurement result is 0, the first, second, and third registers collapse to $\frac{1}{\sqrt{Q}}(|0\rangle|u_0\rangle + |1\rangle|u_1\rangle + \ldots + |Q-1\rangle|u_{Q-1}\rangle)|u_0\rangle|u_1\rangle\ldots|u_{Q-1}\rangle$. At this time, the third register is in a non-entangled state and can be discarded directly. The quantum state of this first and second register is $\frac{1}{\sqrt{Q}}(|0\rangle|u_0\rangle + |1\rangle|u_1\rangle + |Q-1\rangle|u_{Q-1}\rangle)$.

Finally, the operator $H^{\otimes\tilde{q}}$ is applied to the first register:

$$\begin{aligned}
|\Psi_4\rangle &= \frac{1}{Q}[(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\ldots(|0\rangle + |1\rangle)|u_0\rangle \\
&\quad + (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\ldots(|0\rangle - |1\rangle)|u_1\rangle \\
&\quad + \ldots + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\ldots(|0\rangle - |1\rangle)|u_{Q-1}\rangle] \\
&= \frac{1}{Q}|00\ldots0\rangle(|u_0\rangle + |u_1\rangle + \ldots + |u_{Q-1}\rangle) \\
&\quad + \frac{1}{Q}|00\ldots1\rangle(|u_0\rangle - |u_1\rangle + \ldots - |u_{Q-1}\rangle) + \ldots
\end{aligned} \tag{24}$$

The first term of the second equal sign of Eq. (24) consists of two parts: $|00\ldots0\rangle$ and $\frac{1}{Q}(|u_0\rangle + |u_1\rangle + \ldots + |u_{Q-1}\rangle)$, where later is exactly the average value $|u\rangle$. Therefore, it is necessary to measure the qubits in the first register. When the measurement results are $00\ldots0$, the quantum state of the second register is the average $|u\rangle$.

As shown in Figure 3, the complexity of the Q-controlled gate is $O(\log Q)$, and the complexity of operator P_q is $O(\log K)$. Besides, the cloning success probability is δ. Thus, the total complexity of the quantum aggregation is $O\left(\frac{Q\log(QK)}{\delta}\right)$.

B. The MB-QFL Framework

MB-QFL consists of four steps.

1) Step 1: Each client independently trains a local model using quantum algorithms, such as variational quantum neural networks and quantum support vector machine, on their respective datasets. After completing the model training, each client obtains the optimal model parameters $|u_q\rangle$, where $q = 0, 1, \ldots, Q-1$.

2) Step 2: The model parameters from all clients are sent to the server for aggregation. The m-qubit state $|u_q\rangle = \sum_{k=0}^{K} u_{qk}|k\rangle$ is transmitted to the server using the generalized quantum teleportation [25], [26], [27].

3) Step 3: The amplitude storage-based quantum average method is used to calculate the average $|u\rangle = \frac{1}{Q}(|u_0\rangle + |u_1\rangle + \ldots + |u_{Q-1}\rangle)$ of $|u_0\rangle, |u_1\rangle, \ldots, |u_{Q-1}\rangle$.

4) Step 4: The server shares the aggregation result $|u\rangle$ with all clients using multi-qubit broadcast protocol in Section III. At first, the mQ-qubit entangled state:

$$\frac{1}{\sqrt{2^{mQ}}}\sum_{j=0}^{2^{mQ}-1}|j\rangle_A|j\rangle_B$$

is prepared and shared by the server and all clients. The operator R_{mQ} and the measurement are performed by the server. At this stage, the amplitude of the quantum state obtained by the q th client corresponds to a rearrangement, potentially with a signed change of the amplitude of $|u\rangle$. The measurement result i should then be converted to a base-2^m number, i.e., $d_{Q-1}d_{Q-2}\ldots d_0$. Next, the binary number $d_{q(m-1)}d_{q(m-2)}\ldots d_{q0}$ of d_q is transmitted to B_q for $q = 0, 1, \ldots, Q-1$. Finally, based on the classical bits $d_{q(m-1)}d_{q(m-2)}\ldots d_{q0}$ from the server, the q th client reconstructs the state by performing unitary operator.

Note that the amplitude of $|u\rangle$ should be known when broadcasting an arbitrary S-qubit state to Q receivers. Therefore, we use quantum state tomography to obtain the amplitude of $|u\rangle$ [35], [36]. The complexity of quantum state tomography based on compressed sensing can be reduced to $\mathcal{O}(rK\log^2 K)$, where r denotes the rank of the quantum state's density matrix [37], [38]. In this work, we consider the ideal case where the quantum state is pure and hence $r = 1$. Therefore, this complexity scales polynomially with the system dimension generally [35], [36], [39]. In the subsequent analysis, the complexity of quantum state tomography is denoted as $\mathcal{O}(\text{poly}(K))$.

V. Security and Complexity Analysis of MB-QFL

In this section, we present a comprehensive security and complexity analysis of MB-QFL and conduct a comparative analysis with existing QFLs.

A. Security Analysis

Assuming that all clients are honest but curious in this paper. Specifically, while all clients strictly adhere to the prescribed protocol by correctly computing and honestly uploading local model updates, they may attempt to infer sensitive information from intermediate updates such as model parameters. Crucially, we maintain the fundamental assumption that clients do not deviate from the protocol through the submission of

malicious updates, including model poisoning or backdoor attacks. Furthermore, we assume that the server is honest, meaning that it is responsible solely for coordinating and aggregating the model updates from clients, without accessing or tampering with the clients' private data. The server adheres strictly to the protocol, ensuring that the aggregation process is carried out accurately and that the global model is distributed to the clients as intended.

This section presents a focused security analysis of MB-QFL, examining its resilience against three critical threats: (1) inference attack, where adversaries attempt to deduce sensitive information from shared model updates; (2) eavesdropping attack, where adversaries channels in an attempt to extract confidential information without disturbing the quantum states; and (3) intercept-and-resend attack, in which malicious entities intercept and retransmit qubits to compromise the learning process.

We analyze the effectiveness of MB-QFL's defense mechanisms against these attacks.

1) Inference Attack Resilience: A malicious client cannot conduct inference attacks by obtaining model parameters for two reasons. Firstly, clients do not need to know the updated parameters and can directly use them as input for the next iteration. In MB-QFL, the generalized quantum teleportation and multi-qubit broadcast protocol are used to transmit the parameters. As the generalized quantum teleportation transmits an unknown quantum state, there is no need to reveal any information when uploading model parameters. Thus, neither the clients nor the server need to know the specifics of $|u_0\rangle, |u_1\rangle, \cdots, |u_{Q-1}\rangle$. Additionally, in multi-qubit broadcast protocol, the quantum state is known to the sender but unknown to the receivers, preventing a malicious client from inferring other clients' privacy.

On the other hand, if a malicious client tries to disrupt MB-QFL by measuring the state to gain information, they would need multiple measurements to obtain probabilistic information, as the information is stored in the amplitude. Measurements inherently disrupt the quantum state, alerting the server about the attacker's presence and correspondingly the server would cease transmitting further messages. However, a single measurement cannot capture the amplitude information of the quantum state in probabilistic form. Therefore, even if a malicious client conducts measurements regardless of the consequences, no specific information can be obtained.

2) Eavesdropping Attack Resilience: In MB-QFL, both the generalized quantum teleportation and multi-qubit broadcast protocol require quantum channels and classical channels to complete the communication between the clients and the server. In scenarios where an attacker wants to perform eavesdropping attacks on the communication channel, several barriers prevent them from obtaining the parameter information. If an attacker intercepts the quantum channel and acquires the qubits carrying the parameters, they lack the classical communication bits necessary to decipher the information. Consequently, even with access to the qubits, an attacker cannot retrieve the parameter details without the corresponding classical information. Similarly, by only intercepting the classical bits without the qubits, they cannot obtain the parameter information.

Furthermore, even if attackers manage to capture both the qubits and the classical bits, they still cannot determine the parameter information. This is because the recipient of the information must perform specific unitary operators based on the received classical bits to restore the quantum state. Since attackers do not know which unitary operators correspond to the classical bits, they are unable to reconstruct the transmitted quantum state.

3) Intercept-and-Resend Attacks Resilience: In MB-QFL, the generalized quantum teleportation and multi-qubit broadcast protocol are used to transmit information between clients and server. Both communication methods require the distribution of entangled quantum states and the transmission of classical information. During the distribution process, it may suffer from intercept-and-resend attacks [40], [41]. When using the generalized quantum teleportation to upload model parameters to the server, the client (taking client 0 as an example) prepares entangled quantum states and distributes part of them to the server. The attacker Eve attempts to intercept the distributed qubits and resends fake qubits. However, even if Eve intercepts the qubits, she cannot obtain the transmitted parameters. This is mainly because after client 0's entanglement and measurement operator, the information stored in the qubits intercepted by Eve. This quantum state needs to undergo a unitary matrix to recover $|u_q\rangle$. However, Eve cannot obtain the classical information and the corresponding unitary matrix, so even if she intercepts the qubits, she cannot obtain the relevant information.

Moreover, since the server does not measure the received qubits, it will not detect the presence of the attacker and will still use the fake qubits transmitted by Eve for subsequent operators, which may lead to performance degradation or even failure of the model. To promptly detect the existence of intercept-and-resend attacks, auxiliary qubits can be added. Taking client 0 transmitting a single-qubit state $|\rho_1\rangle$ to the server as an example, as shown in Figure 4, the blue area in Figure 4 represents the part owned by client 0 before transmission, and the yellow area represents the part owned by the server after transmission. Client 0 first prepares the initial state $|\rho_1\rangle|\Phi_{00}\rangle|0\rangle$. The transmission of $|\rho_1\rangle$ to the server is divided into two parts. The first part is to detect whether there is an intercept-and-resend attack. First, an H gate is applied to register 4, and then a *CNOT* gate is performed on register 3 under the control of register 4, evolving the initial state into:

$$\frac{1}{2}|\rho_1\rangle(|00\rangle|0\rangle + |01\rangle|1\rangle + |11\rangle|0\rangle + |10\rangle|1\rangle) \tag{5-19}$$

Then, the qubits in registers 3 and 4 are transmitted to the server. If there is no intercept-and-resend attack during the transmission, after the server receives the qubits, it performs the inverse operators of the *CNOT* gate and H gate, which are also the *CNOT* gate and H gate. The quantum state in register 4 is $|0\rangle$, and the measurement result is also 0. If there is an intercept-and-resend during the distribution, once the attacker measures register 3, the quantum state in register 4 will collapse to $|0\rangle$ or $|1\rangle$. After the server performs the *CNOT*

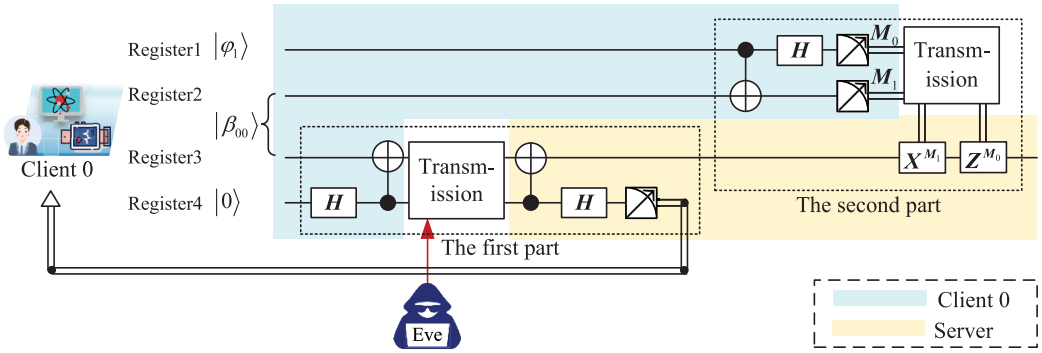


Fig. 4. The generalized quantum teleportation with the ability to detect intercept-and-resend attack.

gate and H gate, the quantum state in register 4 will become a superposition state, and the measurement will yield 0 with a probability of $\frac{1}{2}$ and 1 with a probability of $\frac{1}{2}$. In other words, there is a $\frac{1}{2}$ probability of detecting the presence of an intercept-and-resend attack. After the qubits in the register are safely delivered to the server, client 0 and the server execute the second part, which is the entanglement and measurement in the generalized quantum teleportation and the recovery of the quantum state, to complete the transmission task.

When the auxiliary qubits used to detect intercept-and-resend attacks are $|0\rangle^{\otimes n}$, if there is no intercept-and-resend attack during the distribution, after the first part, the server measures the auxiliary qubits and obtains $00\cdots0$. If there is an intercept-and-resend during the distribution, after the first part, the server's measurement of the auxiliary qubits may yield one of the states in the set $[00\cdots0, 00\cdots1, \cdots, 11\cdots1]$. Therefore, the probability of detecting an intercept-and-resend attack is $\frac{2^n-1}{2^n}$. The same applies when using the multi-qubit broadcast protocol, where the existence of intercept-and-resend attacks can be detected by increasing the number of auxiliary qubits.

4) Comparison With Other Algorithms: In the following, we analyze the security of DP-QFL [14], QKD-FL [17], QHE-QFL [22], and QT-QFL [24] while comparing with the security of MB-QFL. As discussed above, MB-QFL is capable of effectively defending against inference attacks on clients, as well as eavesdropping and intercept-and-resend attacks that may occur during communication. Below we analyze the security of the other QFLs from three aspects: client side, communication process, and server side.

For the client side, in DP-QFL, clients receive noise-added updated information, thus ensuring security. In contrast, QKD-FL, QHE-QFL, and QT-QFL require clients to access updated parameters, which allows semi-honest clients to perform inference attacks. For the communication process, DP-QFL transmits noise-added information, ensuring security; QKD-QFL and QHE-QFL employ quantum key distribution and quantum homomorphic encryption respectively to guarantee security; while QT-QFL may suffer interception-resend attacks during quantum state distribution. For the server side, DP-QFL's server receives noise-added information, ensuring security; QKD-QFL and QT-QFL's server needs updated parameters, causing privacy leakage; while QHE-QFL's servers don't need parameter information, thus ensuring security.

TABLE II
MB-QFL COMPARED WITH DP-QFL, QKD-FL, QHE-QFL, AND QT-QFL IN TERMS OF SECURITY

	DP-QFL [14]	QKD-FL [17]	QHE-QFL [22]	QT-QFL [24]	MB-QFL
Client	○	×	×	×	√
Communication	○	√	√	×	√
Server	○	×	√	×	×

Notably, DP-QFL combines blind quantum computation with differential privacy, enabling clients to delegate training tasks to quantum computers while ensuring security at all three levels (client, communication, and server). However, its effectiveness is closely related to noise intensity when using differential privacy: stronger noise better masks sensitive information and reduces privacy risks, but affects model accuracy by causing deviations in gradients/parameter updates; weaker noise maintains model performance but makes it easier for attackers to infer sensitive data, reducing privacy protection effectiveness. Therefore, noise intensity requires careful balancing between privacy protection and model performance.

The security of these QFLs across the three aspects is summarized in Table II, where "√" denotes secure protection, "×" indicates vulnerability to attacks that may lead to privacy leakage, and "○" reflects conditional security in Table II. The results show that, compared with existing approaches, the proposed MB-QFL provides robust protection for both client-side and the communication process.

B. Complexity Analysis

In MB-QFL, each client uses the quantum support vector machine to complete the training task, with a complexity of $\mathcal{O}\left(\frac{\log(KN)}{\varepsilon}\right)$ [42], [43], where ε is the accuracy. The generalized quantum teleportation is used to send the $K+1$ parameters to the server, with a complexity of $\mathcal{O}(\log K)$. Therefore, when Q clients send information to the server, the complexity is $\mathcal{O}(Q\log K)$. When the server uses the quantum averaging algorithm to complete the aggregation task, the complexity of the quantum averaging algorithm is $\mathcal{O}\left(Q\frac{\log(KN)}{\delta}\right)$. Prior to executing multi-qubit broadcast protocol, quantum state

tomography is required to obtain the quantum state information, with a complexity of $\mathcal{O}(\text{poly}(K))$ [35], [36], [39]. In the quantum circuit implementation of multi-qubit broadcast protocol, the server must decompose the unitary matrix M into elementary quantum gates, incurring a complexity of $\mathcal{O}(\text{poly}(K))$ [44], [45]. Therefore, the overall complexity of multi-qubit broadcast protocol is:

$$\begin{aligned}&\mathcal{O}(\text{poly}(K)) + \mathcal{O}(\text{poly}(K)) + \mathcal{O}(Q\log K)\\&= \mathcal{O}(\text{poly}(K)) + \mathcal{O}(Q\log K)\end{aligned} \tag{25}$$

Therefore, the total complexity of MB-QFL is:

$$\begin{aligned}&\mathcal{O}\left(Q\frac{\log(KN)}{\varepsilon}\right) + \mathcal{O}(Q\log K) + \mathcal{O}\left(Q\frac{\log(KN)}{\delta}\right)\\&\quad + \mathcal{O}(\text{poly}(K)) + \mathcal{O}(Q\log K)\\&= \mathcal{O}\left(\left(\frac{1}{\varepsilon}+\frac{1}{\delta}\right)Q\log(KN) + \text{poly}(K)\right)\end{aligned} \tag{26}$$

Next, we analyze the complexity of other QFLs from the perspectives of the client, communication, and server. In terms of client model training, DP-QFL, QHE-QFL, and QT-QFL all use variational quantum algorithms. The total complexity for Q clients training KN-dimensional samples is $\mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''^2}\right)$ [46], [47], [48], where ε'' is the precision. In the case of QKD-QFL, where classical algorithms are used for client model training, the total complexity for Q clients training KN-dimensional samples is at least $\mathcal{O}\left(\frac{Q\text{poly}(K)N}{\varepsilon'}\right)$, where ε' is the error rate. For communication, in DP-QFL, QHE-QFL, and QT-QFL, each client first prepares $\mathcal{O}(\log N)$ parameters into a quantum state and then propagates them, resulting in a total complexity of $\mathcal{O}(Q\log N)$ for all clients. In QKD-QFL, the total complexity for all clients is $\mathcal{O}(QN)$. In aggregation, the complexity for DP-QFL, QHE-QFL, and QT-QFL is $\mathcal{O}(Q\log N)$, while for QKD-QFL, the complexity is $\mathcal{O}(QN)$. Based on the analysis above, the complexity of DP-QFL is:

$$\begin{aligned}&\mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''^2}\right) + \mathcal{O}(Q\log N) + \mathcal{O}(Q\log N)\\&\quad + \mathcal{O}(Q\log N) = \mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''^2}\right)\end{aligned} \tag{27}$$

QKD-QFL uses quantum algorithms only during the communication process, with a total complexity of:

$$\begin{aligned}&\mathcal{O}\left(\frac{Q\text{poly}(K)D}{\varepsilon'}\right) + \mathcal{O}(QN) + \mathcal{O}(QN)\\&\quad + \mathcal{O}(QN) = \mathcal{O}\left(\frac{Q\text{poly}(K)D}{\varepsilon'}\right) + \mathcal{O}(QN)\end{aligned} \tag{28}$$

QHE-QFL uses quantum algorithms in both client model training and communication, with a total complexity of:

$$\begin{aligned}&\mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''}\right) + \mathcal{O}(Q\log N) + \mathcal{O}(Q\log N)\\&\quad + \mathcal{O}(Q\log N) = \mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''}\right)\end{aligned} \tag{29}$$

QT-QFL uses quantum algorithms in client model training, communication, and aggregation, with a total complexity of:

$$\begin{aligned}&\mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''}\right) + \mathcal{O}(Q\log N) + \mathcal{O}(Q\log N)\\&\quad + \mathcal{O}(Q\log N) = \mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''}\right)\end{aligned} \tag{30}$$

In MB-QFL, the overall complexity is $\mathcal{O}\left(\left(\frac{1}{\varepsilon}+\frac{1}{\delta}\right)Q\log(KN) + \text{poly}(K)\right)$, which offers a clear advantage over other QFLs' complexity of $\mathcal{O}\left(\frac{Q\text{poly}(K)\log N}{\varepsilon''}\right)$. This bound is lower because the logarithmic dependence on the dataset size and feature dimension, $\log(KN)$, grows much more slowly than the polynomial dependence on K in $\text{poly}(K)$, especially when K is large.

TABLE III
SOFTWARE AND HARDWARE SPECIFICATION FOR IBM QISKIT QUANTUM SIMULATION

Qiskit	v0.12.2
Qiskit Element	Qiskit Aer
Simulator	QASM
Python	v3.7.11
Local OS	Windows 10
Local Hardware	Processor: R7 3700X; RAM: 16GB

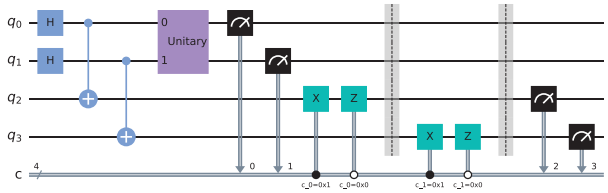


Fig. 5. The quantum circuit of broadcasting $|\alpha_1\rangle$.

VI. SIMULATION AND EVALUATION

We implemented MB-QFL on a quantum simulator running locally on a classical computer. Each sequence of quantum gates is designed using the IBM Qiskit Python library. [1] The hardware and software specifications are detailed in Table III.

A. Simulating Multi-Qubit Broadcast Protocol and Comparison

We simulated multi-qubit broadcast protocol by conducting experiments with an example where $S = 1$ and $Q = 2$. This scenario involves a three-party quantum broadcast with one sender (A) and two receivers (B_0 and B_1).

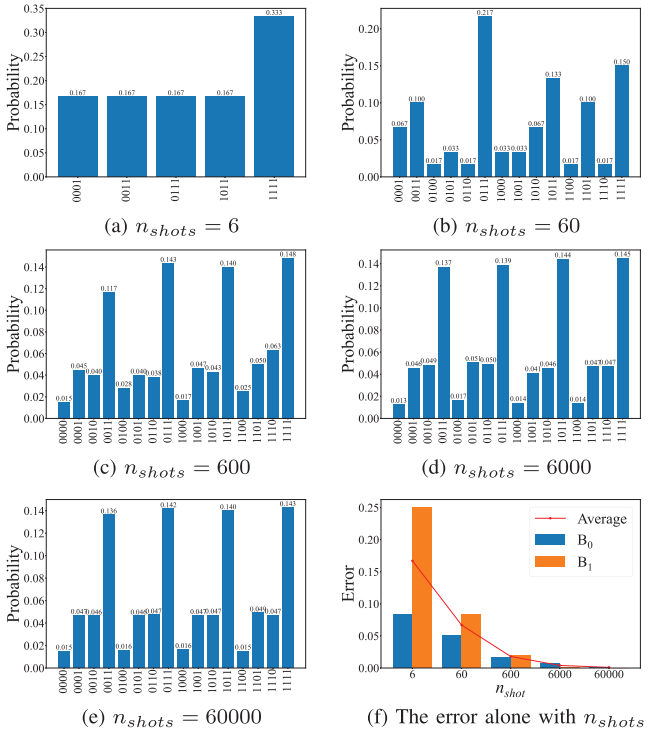
To broadcast $|\alpha_1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ to two receivers, four qubits are required. As shown in Figure 5, the following is a three-step introduction.

Step 1: An entangled state is prepared, with qubit q_2 belongs to B_0, qubit q_3 belongs to B_1, and qubits q_0 and q_1 belong to A. Then, Alice applies a unitary operation, denoted as the "Unitary" gate in Figure 5, which is as follows:

$$\begin{bmatrix} \frac{1}{4} & \frac{-\sqrt{3}}{4} & \frac{-\sqrt{3}}{4} & \frac{3}{4} \\ \frac{\sqrt{3}}{4} & \frac{1}{4} & \frac{-3}{4} & \frac{-\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{-3}{4} & \frac{1}{4} & \frac{-\sqrt{3}}{4} \\ \frac{3}{4} & \frac{\sqrt{3}}{4} & \frac{\sqrt{3}}{4} & \frac{1}{4} \end{bmatrix} \tag{31}$$

Finally, a measurement is performed, and the resulting classical information is stored in the register located at the bottom of Figure 5.

[1] https://qiskit.org/



(a) $n_{shots} = 6$ (b) $n_{shots} = 60$ (c) $n_{shots} = 600$ (d) $n_{shots} = 6000$ (e) $n_{shots} = 60000$ (f) The error alone with n_{shots}

Fig. 6. The simulation results of broadcasting $|\alpha_1\rangle$.

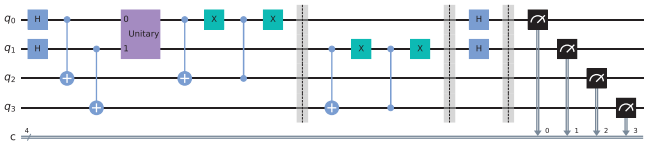


Fig. 7. The equivalent circuit of broadcasting $|\alpha_1\rangle$.

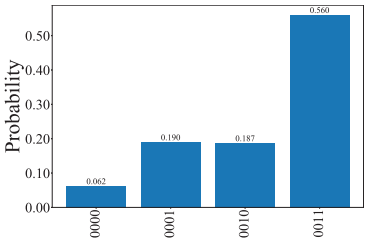
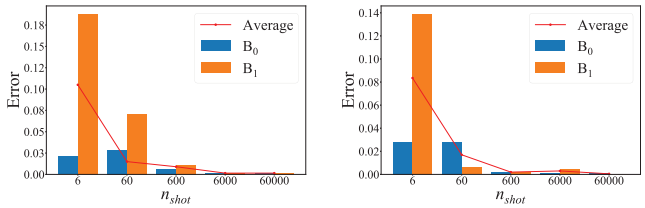


Fig. 8. The simulation result of the equivalent circuit.



(a) $|\alpha_2\rangle$ (b) $|\alpha_3\rangle$

Fig. 9. The simulation results of broadcasting $|\alpha_2\rangle$ and $|\alpha_3\rangle$.

Step 2: The measurement outcomes are sent to B_0 and B_1. Since this is a simulated experiment, no actual transmission is performed; the classical information remains stored in the register at the bottom of Figure 5.

Step 3: B_0 and B_1 apply appropriate unitary operations to their respective qubits based on the received classical information. According to the matrix form of the "Unitary" gate, an X gate is applied when the classical bit is 1, and a Z gate is applied when the bit is 0.

We used probability to verify the effectiveness of multi-qubit broadcast protocol. Theoretically, both B_0 and B_1 should receive the state $|\alpha_1\rangle$. Thus, the probabilities of measuring 0 and 1 are $C(0) = 0.25$ and $C(1) = 0.75$, respectively. We ran the protocol for $n_{shots} = 6, 60, 600, 6000$, and 60000 times, and the results are shown in Figure 6(a)-(e).

In Figure 6 (a)-(e), the x-axis represents the measurement results of the quantum circuit in Figure 5, with the outcomes corresponding to q_0, q_1, q_2, and q_3 from bottom to top. The y-axis represents the probability of obtaining these results. For instance, when $n_{shots} = 6000$, the probability of q_2 being 0 is calculated as $P_2(0) = 0.013 + 0.046 + 0.017 + 0.051 + 0.014 + 0.041 + 0.014 + 0.047 = 0.243$ and the probability of q_3 being 0 is $P_3(0) = 0.013 + 0.049 + 0.017 + 0.050 + 0.014 + 0.046 + 0.014 + 0.047 = 0.250$. Since the sum of the probability of getting 0 and the probability of getting 1 is 1, the errors of obtaining 0 for B_0 and B_1, as well as the average error, are displayed in Figure 6 (f). From the Figure, we can observe that as n_{shots} increases, the error gradually decreases. When $n_{shots} \geq 6000$, the error is less than 0.01.

The final states of q_0 and q_1 are both $|\alpha_1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. Since the circuit involves classical bits, it cannot be packaged into a pure quantum circuit for subsequent experiments. Therefore, we provide the equivalent circuit of Figure 5. Based on the principle of deferred measurement, we can change the operation controlled by the classical bit in Figure 5 to be controlled by qubits. The equivalent circuit of Figure 5 is shown in Figure 7. The simulation result of Figure 7 is shown in Figure 8 for $n_{shots} = 6000$. We can see that the probability of q_2 being 0 is $P_2(0) = 0.062 + 0.190 = 0.252$, and the probability of it being 1 is $P_2(1) = 0.187 + 0.560 = 0.747$. Similarly, the probability of q_3 being 0 is $P_3(0) = 0.062 + 0.187 = 0.249$, and the probability of it being 1 is $P_3(1) = 0.190 + 0.560 = 0.750$. The error in these probabilities is less than 0.01.

Next, we respectively broadcast the 2-qubit state $|\alpha_2\rangle = \frac{1}{4}(\sqrt{3}|00\rangle + 2\sqrt{2}|01\rangle + 2|10\rangle + |11\rangle)$ and the 3-qubit state $|\alpha_3\rangle = \frac{1}{6}(|000\rangle + \sqrt{2}|001\rangle + \ldots + \sqrt{7}|111\rangle + \sqrt{8}|111\rangle)$ to two receivers. The errors of broadcasting $|\alpha_2\rangle$ and $|\alpha_3\rangle$ are shown in Figures 9 (a) and (b), respectively. It can be seen that as n_{shots} increases, the error gradually decreases. When $n_{shots} \geq 6000$, the error is less than 0.01.

The following is a comparison of the qubit consumption between multi-qubit broadcast protocol and existing quantum broadcast protocols (M-QBP [49], P-QBP [50], L-QBP [29]). Since existing quantum broadcast protocols can only transmit a single qubit, Figure 10 illustrates the number of qubits consumed for transmitting a single qubit. It is evident that the number of qubits consumed by our protocol and L-QBP remains consistent as the number of receivers increases, whereas the qubit consumption of other algorithms

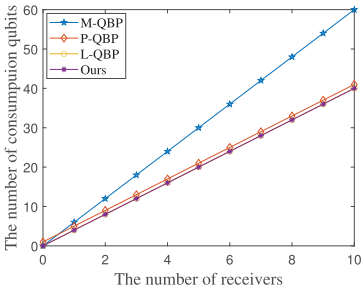


Fig. 10. The comparison between multi-qubit broadcast protocol and other quantum broadcast protocols.

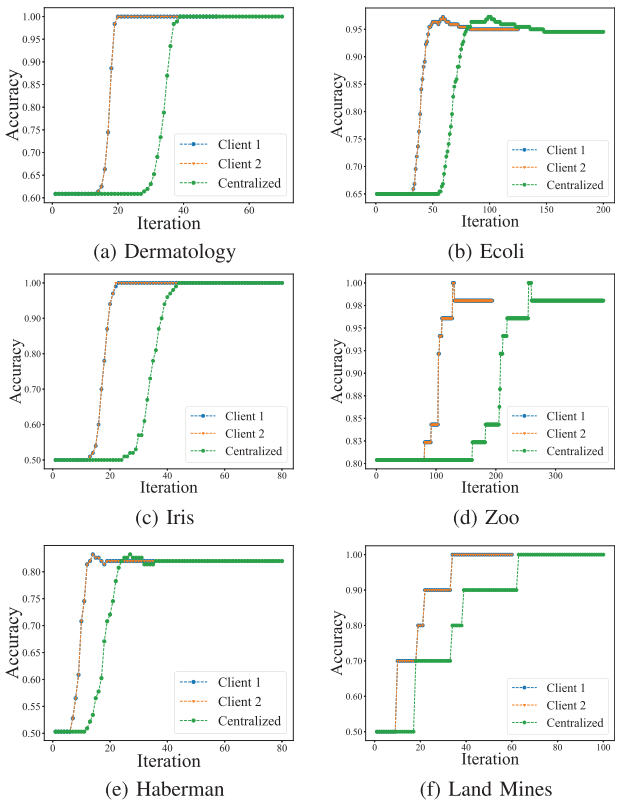
is higher. However, the proposed protocol can transmit any S-qubit quantum state, making it a more versatile and efficient broadcast protocol.

B. Comparing MB-QFL and Centralized Learning

To evaluate the performance of MB-QFL compared to centralized learning, we conduct simulations for a classification task using six datasets: Dermatology, Ecoli, Iris, Zoo, Haberman, and Land Mines [51]. The simulations consider two scenarios: one where each client has similar data and another where each client has entirely dissimilar data, achieved by shuffling the dataset using "random.shuffle" operations. The similar data setting serves as a baseline to isolate the effects of the proposed algorithm without the confounding influence of data heterogeneity, allowing for a clearer comparison of learning performance. In contrast, the heterogeneous data setting reflects practical federated learning environments, where client data is typically non-IID. Evaluating both scenarios ensures a comprehensive assessment of the proposed method under both idealized and realistic conditions. Experiments are conducted separately for two clients and four clients.

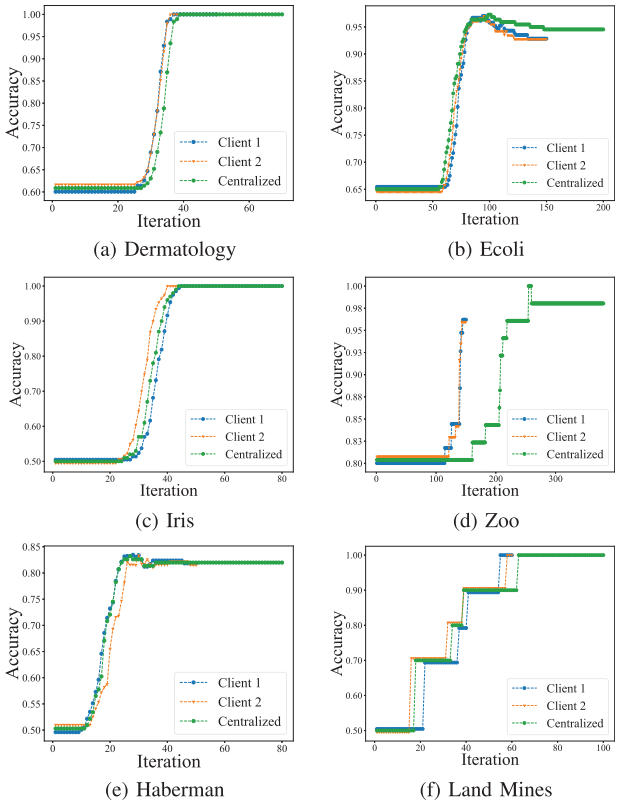
Prior to the experiment, all datasets are preprocessed. For datasets with more than two class labels, only two classes are selected for binary classification. Since the number of samples is relatively small, each dataset is duplicated and then distributed among the clients.

Initially, we assume two clients in MB-QFL, splitting the complete dataset into two parts. Federated Learning allows clients to train the model without sharing their raw data, achieving similar results to training on combined data. We use classification accuracy to compare the performance of MB-QFL against a centralized model. Experiments are conducted on the six datasets mentioned above. Figures 11 and 12 illustrate how accuracy changes with the number of iterations. Figures 11 illustrates the scenario where both clients use identical datasets. As the data is similar, the accuracy curves of the two clients remain identical throughout the training iterations. In contrast, Figures 12 shows the case where the two clients use dissimilar data. Due to the data heterogeneity, the accuracy curves vary between the two clients during training. Nevertheless, it can be observed that regardless of whether the clients use the similar or dissimilar data, the results indicate that the accuracy achieved by MB-QFL is nearly identical to that of the centralized model.



(a) Dermatology (b) Ecoli (c) Iris (d) Zoo (e) Haberman (f) Land Mines

Fig. 11. The comparison between MB-QFL for two clients and the centralized model when the datasets are similar.



(a) Dermatology (b) Ecoli (c) Iris (d) Zoo (e) Haberman (f) Land Mines

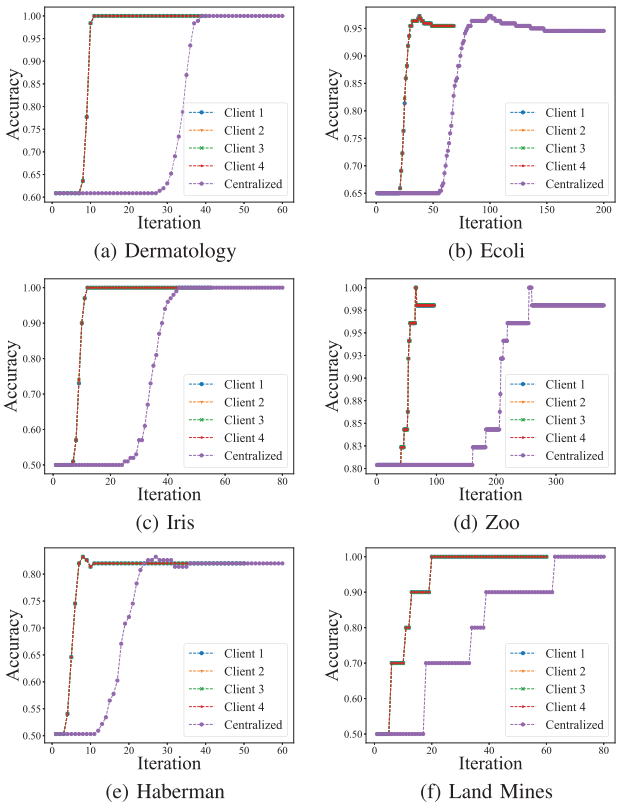
Fig. 12. The comparison between MB-QFL for two clients and the centralized model when the datasets are dissimilar.

To quantify this, we calculate the error between the accuracy of the final iteration of the centralized model and MB-QFL.

TABLE IV

THE ERRORS BETWEEN MB-QFL FOR TWO CLIENTS AND THE CENTRALIZED MODEL WHEN THE DATASETS ARE SIMILAR

Dataset \ Models	Centralized Model	MB-QFL Client 1	MB-QFL Client 2	Error
Dermatology	1	1	1	0
Ecoli	0.945	0.950	0.950	0.005
Iris	1	1	1	0
Zoo	0.980	0.980	0.980	0
Haberman	0.820	0.820	0.820	0
Land Mines	1	1	1	0

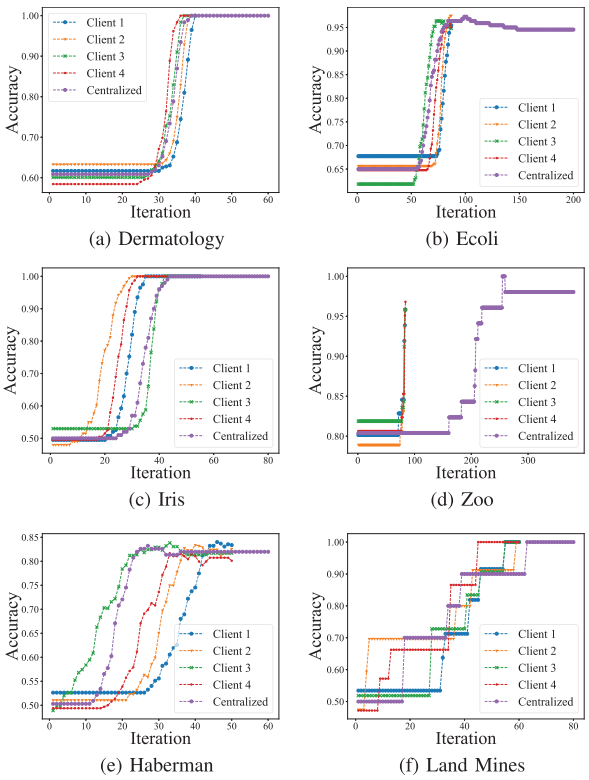


(a) Dermatology (b) Ecoli (c) Iris (d) Zoo (e) Haberman (f) Land Mines

Fig. 13. The comparison between MB-QFL for four clients and the centralized model when the datasets are similar.

Tables IV and V show the errors for similar and dissimilar data scenarios, respectively. The errors ($\frac{1}{2}\sum_{i=1}^{2}|A_c - A_{f_i}|$) between MB-QFL and the centralized model are less than 0.02, where A_c represents the classification accuracy of the centralized model, and A_{f_i} represents the classification accuracy of the i th client. Thus, MB-QFL proves to be an effective model.

Next, we assume four clients in MB-QFL, conducting experiments on the same six datasets. Figures 13 and 14 illustrate the schematic diagram of the change in accuracy with the number of iterations. Figure 13 illustrates the scenario where both clients use similar datasets. As the data is the same, the accuracy curves of the two clients remain identical throughout the training iterations. In contrast, Figure 14 shows the case where the two clients use dissimilar datasets. Due to the data heterogeneity, the accuracy curves vary between the two clients during training. Nevertheless, it can be observed that regardless of whether the clients use the similar or dissimilar datasets, the results demonstrate that the accuracy gap between MB-QFL and the centralized model remains small.



(a) Dermatology (b) Ecoli (c) Iris (d) Zoo (e) Haberman (f) Land Mines

Fig. 14. The comparison between MB-QFL for four clients and the centralized model when the datasets are dissimilar.

TABLE V

THE ERRORS BETWEEN MB-QFL FOR TWO CLIENTS AND THE CENTRALIZED MODEL WHEN THE DATASETS ARE DISSIMILAR

Dataset \ Models	Centralized Model	MB-QFL Client 1	MB-QFL Client 2	Error
Dermatology	1	1	1	0
Ecoli	0.945	0.928	0.927	0.018
Iris	1	1	1	0
Zoo	0.980	0.962	0.960	0.019
Haberman	0.820	0.818	0.815	0.004
Land Mines	1	1	1	0

TABLE VI

THE ERRORS BETWEEN MB-QFL FOR FOUR CLIENT AND THE CENTRALIZED MODEL WHEN THE DATASETS ARE SIMILAR

Dataset \ Models	Centralized Model	MB-QFL Client 1	Client 2	Client 3	Client 4	Error
Dermatology	1	1	1	1	1	0
Ecoli	0.945	0.954	0.954	0.954	0.954	0.009
Iris	1	1	1	1	1	0
Zoo	0.980	0.980	0.980	0.980	0.980	0
Haberman	0.820	0.820	0.820	0.820	0.820	0
Land Mines	1	1	1	1	1	0

For four clients, we also calculate the error between the accuracy of the last iteration of the centralized model and MB-QFL. The two scenarios, having similar data and dissimilar data, are shown in Tables VI and VII, It can be seen from these tables that the errors ($\frac{1}{4}\sum_{i=1}^{4}|A_c - A_{f_i}|$) between MB-QFL and the central model are less than 0.04. Therefore, MB-QFL remains an effective model.

Additionally, it is evident from Figures 11 and 13 that MB-QFL requires fewer iterations compared to the centralized model when each client possesses the same dataset.

TABLE VII

THE ERRORS BETWEEN MB-QFL FOR FOUR CLIENTS AND THE CENTRALIZED MODEL WHEN THE DATASETS ARE DISSIMILAR

Models / Dataset	Centralized Model	MB-QFL Client 1	MB-QFL Client 2	MB-QFL Client 3	MB-QFL Client 4	Error
Dermatology	1	1	1	1	1	0
Ecoli	0.945	0.955	0.975	0.948	0.950	0.012
Iris	1	1	1	1	1	0
Zoo	0.980	0.958	0.958	0.958	0.960	0.022
Haberman	0.820	0.834	0.826	0.817	0.801	0.036
Land Mines	1	1	1	1	1	0

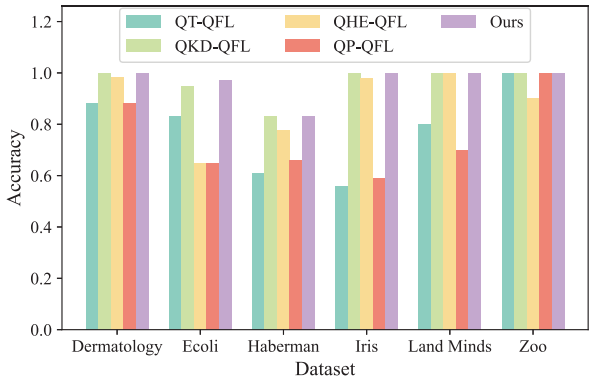


Fig. 15. The comparison between MB-QFL and other quantum federated learning methods when the datasets are similar.

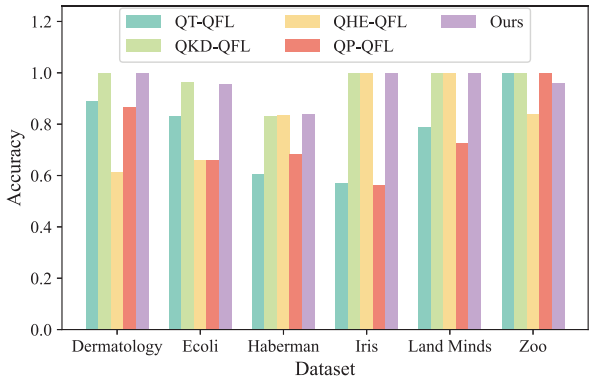


Fig. 16. The comparison between MB-QFL and other quantum federated learning methods when the datasets are dissimilar.

C. Comparing MB-QFL and Other QFL Algorithms

This subsection compares the accuracy of the proposed MB-QFL with other QFLs, including DP-QFL [14], QKD-FL [17], QHE-QFL [22], and QT-QFL [24]. In all experiments, the number of clients is fixed at four. For QKD-QFL, the client models are trained using classical convolutional neural networks, while for DP-QFL, QHE-QFL, and QT-QFL, variational quantum algorithms are adopted for client-side model training. The depth of the parameterized quantum circuits used in all clients is set to five layers.

Figure 15 and Figure 16 present the maximum accuracy achieved by each QFL under two scenarios: similar across clients and dissimilar among clients, respectively. As shown in Figure 15, when client datasets are similar, the proposed method MB-QFL consistently outperforms other QFLs across all datasets. Similarly, as illustrated in Figure 16, when client datasets are dissimilar, the proposed method MB-QFL demonstrates superior performance on all datasets except for the Zoo dataset.

TABLE VIII

SUMMARY OF QUANTUM BROADCAST PROTOCOLS IN TERMS OF THE NUMBER OF QUBITS AND RECEIVERS

The number of qubits	The number of receivers	Reference
1/2	2	Y-QBP [28], [54]
1	$2n$	M-QBP [49]
1	n	L-QBP [29]/P-QBP [50]

VII. RELATED WORKS

In this section, we present related works on quantum broadcast protocol and quantum adder.

A. Quantum Broadcast Protocol

Existing quantum broadcast protocols (QBPs) can be categorized into two distinct types: those that broadcast known quantum states, where the amplitude is known [28], [29], and those that broadcast unknown quantum states [52], [53]. Our work focuses on the former—broadcasting known quantum states.

Yu et al. proposed the Y-QBP protocol, which enables the broadcasting of 1-qubit and 2-qubit states to two receivers [28], [54]. In this protocol, the broadcasted information consists of real numbers. Luo et al. presented two QBP algorithms (L-QBP) designed for broadcasting real numbers and complex numbers separately, enabling the broadcast of a 1-qubit state to n receivers [29]. In 2022, Peng et al. proposed a protocol P-QBP, for broadcasting complex numbers [50]. Mafi et al. introduced M-QBP, a control QBP for $2n$ receivers which can improve the security [49].

Table VIII summarizes the number of qubits and receivers in existing QBP protocols. None of these protocols can broadcast an arbitrary S-qubit state to Q receivers. Therefore, we present a protocol for broadcasting an arbitrary S-qubit state to Q receivers.

B. Quantum Adders

In quantum computing, averaging, like in classical computing, involves both addition and division. However, existing research has primarily focused on quantum adders, leaving a gap in the development of quantum averaging algorithms. The first quantum adder was introduced by Vedral et al, which implements the transformation $|a, b\rangle \rightarrow |a, a + b\rangle$, where $|a\rangle$ and $|b\rangle$ are quantum registers with n qubits [55]. Since then, various quantum adders have been designed and classified into three main types: quantum half adders, which operate on two-digit inputs; quantum full adders, which include an additional carry-in input; and quantum carry propagate adders, capable of summing two N-qubit numbers [56], [57], [58], [59], [60], [61].

In existing approaches, addends are stored in separate registers, typically limited to two addends, as seen in traditional quantum adder (TA-QA) models. Sracic's quantum row adder algorithm improves efficiency by storing data in the basis state, making it suitable for intermediate computations [62].

However, it does not leverage superposition and parallelism, failing to reflect the superiority of quantum algorithms. Despite improvements, TA-QA remains inefficient when summing values stored in superposition states due to the mixing of these values.

To address this, a quantum adder for superposition states (SS-QA) has been proposed, where addends are stored in basis states. However, this method faces challenges when dealing with information stored in amplitudes, which are crucial in applications like quantum support vector machines and quantum federated learning [5], [63]. Converting information between amplitude and ground states is resource-intensive. To our knowledge, there has been no literature addressing the summation of information stored directly in quantum state amplitudes. This paper proposes a quantum averaging algorithm based on amplitude storage to enable efficient quantum aggregation.

VIII. Limitation and Future Work

Although MB-QFL offers significant security advantages, it has several limitations. The algorithm is designed and simulated under ideal conditions, while the existing quantum environments are largely noisy. It is mainly due to the formation of mixed states in multipartite entanglement, resulting from decoherence and interactions with the environment. In such realistic settings, quantum fidelity and entanglement purification become critical factors affecting system performance [64], [65]. Although our simulations assume ideal channels, future implementations must consider the degradation of fidelity and the cost of purification, both of which could impact the convergence and accuracy of the algorithm. Additionally, the algorithm relies on a linear support vector machine for client training, whereas real-world classification tasks are often nonlinear. Finally, as discussed in Section V-A4 and illustrated in Table II, MB-QFL is vulnerable to privacy leakage on the server side, primarily due to the use of the quantum broadcast protocol.

To overcome the limitations, a prospective direction would be to consider scenarios under non-ideal conditions, recognizing the challenges associated with preparing or maintaining multipartite entangled states. MB-QFL could be enhanced or adapted to leverage the full potential of support vector machines by incorporating nonlinear classifiers based on kernel functions [66]. Additionally, the proposed quantum broadcast protocol, utilizing high-dimensional entangled quantum channels, could be integrated into existing QFL algorithms to boost their efficiency. Besides, the current framework MB-QFL assumes semi-honest clients, extending the model to defend against fully malicious clients (e.g., poisoning attacks) remains an open challenge. We will explore robust aggregation methods to defend against other attacks.

IX. Conclusion

Existing approaches have not fully leveraged quantum mechanics to enhance both training efficiency and security simultaneously. In this paper, we introduce MB-QFL, which utilizes the generalized quantum teleportation and multi-qubit broadcast protocol for information transmission, along with a quantum averaging method for aggregation. Security analysis and simulation results show that MB-QFL improves algorithm efficiency while effectively resisting eavesdropping and inference attacks. Its classification accuracy is comparable to that of a centralized model, and it achieves the lowest complexity among current QFL algorithms.

References

[1] R. Zhang et al., "Generative AI agents with large language model for satellite networks via a mixture of experts transmission," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 12, pp. 3581–3596, 2024.

[2] R. Zhang et al., "Generative AI for space-air-ground integrated networks," *IEEE Wireless Commun.*, vol. 31, no. 6, pp. 10–20, Dec. 2024.

[3] J. Verbraeken, M. Wolting, J. Katzy, J. Kloppenburg, T. Verbelen, and J. S. Rellermeyer, "A survey on distributed machine learning," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–33, 2020.

[4] M. Cho, M. Chikkam, W. Xu, and L. Lai, "Tree network design for faster distributed machine learning process with distributed dual coordinate ascent," in *Proc. IEEE Int. Conf. Acoust.*, Mar. 2024, pp. 6080–6084.

[5] S. Y.-C. Chen and S. Yoo, "Federated quantum machine learning," *Entropy*, vol. 23, no. 4, p. 460, Apr. 2021.

[6] J. Qi, X.-L. Zhang, and J. Tejedor, "Optimizing quantum federated learning based on federated quantum natural gradient descent," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Jun. 2023, pp. 1–5.

[7] Z. Qu, Y. Li, B. Liu, D. Gupta, and P. Tiwari, "DTQFL: A digital twin-assisted quantum federated learning algorithm for intelligent diagnosis in 5G mobile network," *IEEE J. Biomed. Health Informat.*, vol. 29, no. 6, pp. 1–10, Jun. 2024.

[8] S. Kais, A. S. Bhatia, and M. S. Alam, "Quantum federated learning in healthcare: The shift from development to deployment and from models to data," *Res. Square*, pp. 1–15, May 2023. [Online]. Available: https://assets-eu.researchsquare.com/files/rs-2723753/v1_covered_d97e51f5-98b7-460c-9c62-94be5cf26e2d.pdf?c=1684124669

[9] M. Chehimi, S. Y.-C. Chen, W. Saad, D. Towsley, and M. Debbah, "Foundations of quantum federated learning over classical and quantum networks," *IEEE Netw.*, vol. 38, no. 1, pp. 1–7, Jan. 2024.

[10] T. Wang, H.-H. Tseng, and S. Yoo, "Quantum federated learning with quantum networks," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2024, pp. 13401–13405.

[11] R. Rofougaran, S. Yoo, H. E. Tseng, and S. Y.-C. Chen, "Federated quantum machine learning with differential privacy," in *Proc. IEEE Int. Conf. Acoust.*, Mar. 2024, pp. 9811–9815.

[12] Z. Qu, Z. Chen, S. Dehdashti, and P. Tiwari, "QFSM: A novel quantum federated learning algorithm for speech emotion recognition with minimal gated unit in 5G IoV," *IEEE Trans. Intell. Vehicles*, vol. 9, no. 10, pp. 6512–6523, Oct. 2024.

[13] Q. Xia, Z. Tao, and Q. Li, "Defending against Byzantine attacks in quantum federated learning," in *Proc. 17th Int. Conf. Mobility, Sens. Netw. (MSN)*, Dec. 2021, pp. 145–152.

[14] W. Li, S. Lu, and D.-L. Deng, "Quantum federated learning through blind quantum computing," *Sci. China Phys., Mech. Astron.*, vol. 64, no. 10, Oct. 2021, Art. no. 100312.

[15] W. Yamany, N. Moustafa, and B. Turnbull, "OQFL: An optimized quantum-based federated learning framework for defending against adversarial attacks in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 893–903, Jan. 2023.

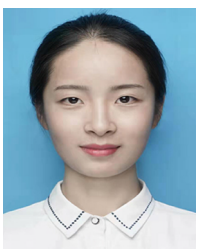
[16] C. Qiao, M. Li, Y. Liu, and Z. Tian, "Transitioning from federated learning to quantum federated learning in Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 3, p. 1, Jan. 2024.

[17] Q. Xu, L. Zhao, Z. Su, D. Fang, and R. Li, "Secure federated learning in quantum autonomous vehicular networks," *IEEE Netw.*, vol. 37, no. 6, pp. 240–247, Nov. 2023.

[18] M. Xu et al., "Stochastic resource allocation in quantum key distribution for secure federated learning," in *Proc. IEEE Global Commun. Conf.*, Dec. 2022, pp. 4377–4382.

[19] H. Zhao, "Non-IID quantum federated learning with one-shot communication complexity," *Quantum Mach. Intell.*, vol. 5, no. 1, p. 3, Jun. 2023.

[20] R. Kaewpuang, M. Xu, D. Niyato, H. Yu, Z. Xiong, and X. S. Shen, "Adaptive resource allocation in quantum key distribution (QKD) for federated learning," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2023, pp. 71–76.
[21] Y. Zhang, C. Zhang, C. Zhang, L. Fan, B. Zeng, and Q. Yang, "Federated learning with quantum secure aggregation," 2022, *arXiv:2207.07444*.
[22] C. Chu, L. Jiang, and F. Chen, "CryptoQFL: Quantum federated learning on encrypted data," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Sep. 2023, pp. 1231–1237.
[23] B. Narottama and S. Y. Shin, "Federated quantum neural network with quantum teleportation for resource optimization in future wireless communication," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14717–14733, Nov. 2023.
[24] T. Wang, P. Li, Y. Wu, L. Qian, Z. Su, and R. Lu, "Quantum-empowered federated learning in Space-Air-Ground integrated networks," *IEEE Netw.*, vol. 38, no. 1, pp. 96–103, Oct. 2023.
[25] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993.
[26] P.-X. Chen, S.-Y. Zhu, and G.-C. Guo, "General form of genuine multipartite entanglement quantum channels for teleportation," *Phys. Rev. A, Gen. Phys.*, vol. 74, no. 3, Sep. 2006, Art. no. 032324.
[27] C. Min, Z. Shi-Qun, and F. Jian-Xing, "Teleportation of n -Particle state via n pairs of EPR channels," *Commun. Theor. Phys.*, vol. 41, no. 5, pp. 689–692, May 2004.
[28] Y. Yu, X. W. Zha, and W. Li, "Quantum broadcast scheme and multi-output quantum teleportation via four-qubit cluster state," *Quantum Inf. Process.*, vol. 16, no. 2, p. 41, Dec. 2016.
[29] M. Luo, Y. Deng, X. Chen, Y. Yang, and H. Li, "Faithful quantum broadcast beyond the no-go theorem," *Quantum Inf. Process.*, vol. 12, no. 5, pp. 1969–1979, Nov. 2012.
[30] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[31] C. Heuberger, H. Prodinger, and S. G. Wagner, "Positional number systems with digits forming an arithmetic progression," *Monatshefte für Math.*, vol. 155, nos. 3–4, pp. 349–375, Dec. 2008.
[32] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, no. 5, pp. 722–725, Jan. 1996.
[33] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett.*, vol. 77, no. 13, p. 2818, 1996.
[34] H. Chen et al., "Experimental demonstration of probabilistic quantum cloning," *Phys. Rev. Lett.*, vol. 106, no. 18, May 2011, Art. no. 180404.
[35] J. Xiao, J. Wen, S. Wei, and G. Long, "Reconstructing unknown quantum states using variational layerwise method," *Frontiers Phys.*, vol. 17, no. 5, p. 51501, Apr. 2022.
[36] S. Xue, Y. Liu, Y. Wang, P. Zhu, C. Guo, and J. Wu, "Variational quantum process tomography of unitaries," *Phys. Rev. A, Gen. Phys.*, vol. 105, no. 3, Mar. 2022, Art. no. 032427.
[37] Y. I. Bogdanov, G. Brida, M. Genovese, S. P. Kulik, E. V. Moreva, and A. P. Shurupov, "Statistical estimation of the efficiency of quantum state tomography protocols," *Phys. Rev. Lett.*, vol. 105, no. 1, Jul. 2010, Art. no. 010404.
[38] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing," *Phys. Rev. Lett.*, vol. 105, no. 15, Oct. 2010, Art. no. 150401.
[39] S. Chen, J. Li, and A. Liu, "An optimal tradeoff between entanglement and copy complexity for state tomography," in *Proc. 56th Annu. ACM Symp. Theory Comput.*, vol. 2596, Jun. 2024, pp. 1331–1342.
[40] M. Sisodia, "A theoretical study of controlled quantum teleportation scheme for n-qubit quantum state," *Int. J. Theor. Phys.*, vol. 61, no. 12, p. 270, Dec. 2022.
[41] J. Chen, D. Li, M. Liu, Y. Yang, and Q. Zhou, "Quantum controlled teleportation of bell state using seven-qubit entangled state," *Int. J. Theor. Phys.*, vol. 59, no. 5, pp. 1402–1412, May 2020.
[42] R. Zhang, J. Wang, N. Jiang, H. Li, and Z. Wang, "Quantum support vector machine based on regularized Newton method," *Neural Netw.*, vol. 151, pp. 376–384, Jul. 2022.
[43] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum support vector machine for big data classification," *Phys. Rev. Lett.*, vol. 113, no. 13, Sep. 2014, Art. no. 130503.
[44] D. Fedoriaka, "Decomposition of unitary matrix into quantum gates," 2025, *arXiv:2501.07786*.
[45] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, "Efficient decomposition of quantum gates," *Phys. Rev. Lett.*, vol. 92, no. 17, Apr. 2004, Art. no. 177902.
[46] D. T. Hoang, F. Metz, A. Thomasen, T. D. Anh-Tai, T. Busch, and T. Fogarty, "Variational quantum algorithm for ergotropy estimation in quantum many-body batteries," *Phys. Rev. Res.*, vol. 6, no. 1, Jan. 2024, Art. no. 013038.
[47] Y. Y. Liu et al., "Application of a variational hybrid quantum-classical algorithm to heat conduction equation and analysis of time complexity," *Phys. Fluids*, vol. 34, no. 11, Nov. 2022, Art. no. 117121.
[48] J. Tilly et al., "The variational quantum Eigensolver: A review of methods and best practices," *Phys. Rep.*, vol. 986, pp. 1–128, Nov. 2022.
[49] Y. Mafi, P. Kazemikhah, A. Ahmadkhaniha, H. Aghababa, and M. Kolahdouz, "Efficient controlled quantum broadcast protocol using 6n-qubit cluster state in noisy channels," *Opt. Quantum Electron.*, vol. 55, no. 7, p. 653, May 2023.
[50] P. Jia-yin, Z. Yang, L. Tang, and J.-s. Peng, "Controlled quantum broadcast and multi-cast communications of complex coefficient single-qubit states," *Quantum Inf. Process.*, vol. 21, no. 8, p. 287, Aug. 2022.
[51] M. Kelly, R. Longjohn, and K. Nottingham. (2023). *The UCI Machine Learning Repository*. [Online]. Available: https://archive.ics.uci.edu
[52] H. Sukeno, T.-C. Wei, M. Hillery, J. A. Bergou, D. Fields, and V. S. Malinovsky, "Broadcasting single-qubit and multiqubit entangled states: Authentication, cryptography, and distributed quantum computation," *Phys. Rev. A, Gen. Phys.*, vol. 107, no. 6, Jun. 2023, Art. no. 062605.
[53] M. Hillery, J. A. Bergou, T.-C. Wei, S. Santra, and V. Malinovsky, "Broadcast of a restricted set of qubit and qutrit states," *Phys. Rev. A, Gen. Phys.*, vol. 105, no. 4, Apr. 2022, Art. no. 042611.
[54] Y. Yu, N. Zhao, and C. Pei, "Multicast-based multiparty remote state preparation schemes of two-qubit states," *Quantum Inf. Process.*, vol. 18, no. 10, p. 319, Aug. 2019.
[55] V. Vedral, A. Barenco, and A. Ekert, "Quantum networks for elementary arithmetic operations," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 1, pp. 147–153, Jul. 1996.
[56] F. Orts, G. Ortega, E. F. Combarro, and E. M. Garzón, "A review on reversible quantum adders," *J. Netw. Comput. Appl.*, vol. 170, Aug. 2020, Art. no. 102810.
[57] H. A. Bhat, F. A. Khanday, and B. K. Kaushik, "Optimized quantum implementation of novel controlled adders/subtractors," *Quantum Inf. Process.*, vol. 22, no. 4, p. 174, Apr. 2023.
[58] R. Sarma and R. Jain, "Quantum gate implementation of a novel reversible half adder and subtractor circuit," in *Proc. Int. Conf. Intell. Circuits Syst. (ICICS)*, Apr. 2018, pp. 72–76.
[59] M. Mohammadi and M. Eshghi, "On figures of merit in reversible and quantum logic designs," *Quant. Inf. Process.*, vol. 8, no. 4, pp. 297–318, 2009.
[60] M. Valinataj, M. Mirshekar, and H. Jazayeri, "Novel low-cost and fault-tolerant reversible logic adders," *Comput. Elect. Eng.*, vol. 53, pp. 56–72, Jul. 2016.
[61] C. Gidney, "Halving the cost of quantum addition," *Quantum*, vol. 2, p. 74, Jun. 2018.
[62] M. Sracic. (2011). *Quantum Circuits for Matrix Multiplication*. [Online]. Available: http://www.math.ksu.edu/reu/sumar/Quantum Algorithms.pdf
[63] R. Zhang, J. Wang, N. Jiang, and Z. Wang, "Quantum support vector machine without iteration," *Inf. Sci.*, vol. 635, pp. 25–41, Jan. 2023.
[64] X. Hu et al., "Long-distance entanglement purification for quantum communication," *Phys. Rev. Lett.*, vol. 126, no. 1, Jan. 2021, Art. no. 010503.
[65] M. Victora, S. Tserkis, S. Krastanov, A. S. de la Cerda, S. Willis, and P. Narang, "Entanglement purification on quantum networks," *Phys. Rev. Res.*, vol. 5, no. 3, Sep. 2023, Art. no. 033171.
[66] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, Sep. 1995.



Rui Zhang received the M.S. degree from the School of Mathematics and Statistics, Henan University, China, in 2020. She is currently pursuing the Ph.D. degree with Beijing Jiaotong University, China. Her research interests include quantum computing, quantum signal processing, and quantum machine learning.

Jian Wang received the Ph.D. degree in cryptography from Beijing University of Posts and Telecommunications, Beijing, in 2008. He is currently an Associate Professor with Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, China. His research interests include quantum computing and data privacy.

Nan Jiang received the Ph.D. degree in cryptography from Beijing University of Posts and Telecommunications, Beijing, China, in 2006. She is currently a Professor with the College of Computer Science, Beijing University of Technology, China. Her research interests include quantum computing, quantum machine learning, and data privacy.

Md Armanuzzaman received the bachelor's degree from Khulna University of Engineering and Technology in 2017, and the Ph.D. degree in computer science and engineering from the University at Buffalo, NY, in 2023. He is a Post-Doctoral Research Associate at the Khoury College of Computer Sciences, Northeastern University, Boston, USA. His work has been published in venues, such as ACM ASIACCS, IEEE SEED, and ACM SAC. His research interests include embedded systems security, software security, and cyber-physical systems security.

Ziming Zhao received the bachelor's and master's degrees from Beijing University of Posts and Telecommunications in 2006 and 2009, respectively, and the Ph.D. degree in computer science from Arizona State University, Tempe, AZ, in 2014. He is an Associate Professor at the Khoury College of Computer Sciences and the Director of the CyberspACe securiTy and forensIcs lab (CactiLab), Northeastern University, Boston, USA. His current research interests include systems and software security, network and web security, and human-centric security. His research has been supported by U.S. National Science Foundation (NSF), U.S. Department of Defense, U.S. Air Force Office of Scientific Research, and U.S. National Centers of Academic Excellence in Cybersecurity (part of the National Security Agency). He was a recipient of the NSF CAREER Award and the NSF CRII Award. His research outcomes have appeared in IEEE S&P, USENIX Security, ACM CCS, NDSS, ACM MobiSys, ACM/IEEE DAC, IEEE RTAS, ACM TISSEC/TOPS, IEEE TDSC, and IEEE TIFS. He was a recipient of the Test-of-Time Paper Award at ACM SACMAT 2024 and the Best/Distinguished Paper Awards from several prestigious conferences, including USENIX Security 2019, ACM AsiaCCS 2022, ACM CODASPY 2014, and ITU Kaleidoscope 2016.