

杨俊鸿, 王帮海, 钟志. 云量子机器学习研究进展[J]. 广东工业大学学报, 2025, 42(3): 1-11. doi: 10.12052/gdutxb.240118.
Yang Junhong, Wang Banghai, Zhong Zhi. Progress in cloud-based quantum machine learning[J]. Journal of Guangdong University of Technology, 2025, 42(3): 1-11.
doi: 10.12052/gdutxb.240118.

云量子机器学习研究进展

杨俊鸿¹, 王帮海¹, 钟志²

(1. 广东工业大学 计算机学院, 广东 广州 510006; 2. 广东工业大学 继续教育学院, 广东 广州 510006)

摘要: 随着量子计算和信息技术的飞速进步, 云量子机器学习作为一种新兴解决方案, 为资源受限的用户通过远程量子服务器处理量子机器学习任务提供可能, 同时确保了数据与模型的隐私保护。本文较全面地展示了该领域的最新研究动态, 从量子内积和变分量子算法的基本理论出发, 分析了基于量子内积的多种云量子机器学习和云变分量子算法的实施细节与应用实例。文章还讨论了当前技术面临的挑战, 并对未来的研究方向提供了展望。

关键词: 云量子机器学习; 隐私保护; 量子内积; 变分量子算法

中图分类号: TP305; TP399

文献标志码: A

文章编号: 1007-7162(2025)03-0001-11

Progress in Cloud-based Quantum Machine Learning

Yang Junhong¹, Wang Banghai¹, Zhong Zhi²

(1. School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China; 2. School of Continuing Education, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: With the rapid advancement of quantum computing and information technology, cloud-based quantum machine learning has emerged as a promising solution, enabling resource-constrained users to perform quantum machine learning tasks via remote quantum servers while ensuring privacy protection for both data and models. A relatively comprehensive overview of the latest developments in this field is provided, starting from the fundamental theories of quantum inner products and variational quantum algorithms. An analysis is conducted on the implementation details and application examples of various cloud-based quantum machine learning methods based on quantum inner products and cloud-based variational quantum algorithms. Additionally, the challenges faced by current technologies are discussed and insights into future research directions are offered.

Key words: cloud-based quantum machine learning; privacy protection; quantum inner product; variational quantum algorithms

量子计算^[1] (Quantum Computation) 是一种依托于量子力学原理进行信息处理的新型计算模式, 在复杂计算任务方面展现出了显著优势。利用量子比特(Qubit) 的叠加和纠缠现象, 量子计算能够实现传统计算机所无法达到的并行处理能力。自从量子计算被提出以来, 它一直被视为推动未来信息技术发展的核心力量。特别是2012年“Quantum Supremacy (量子优势或量子霸权)”概念的引出^[2], 标志着量子计算进入了新的发展阶段。我国在此领域也取得了丰硕成果, 如2023年量子计算机“九章”系列的显著

进展, 成功将光子操控数量从76个提升至255个^[3]。

与此同时, 机器学习作为现代人工智能的核心技术, 在处理复杂问题和优化决策过程中扮演着关键角色。量子机器学习^[4] (Quantum Machine Learning, QML) 是结合了量子计算的并行处理能力和机器学习的模型优化的前沿技术, 正在开拓数据处理和解决优化问题的新境界。量子算法与机器学习的结合, 已经催生出如量子支持向量机^[5]、量子强化学习^[6]、量子联邦学习^[7]等传统机器学习算法的量子版本, 推动了整个领域的进步。

收稿日期: 2024-10-17 录用日期: 2024-12-04

基金项目: 国家自然科学基金资助项目(62072119)

作者简介: 杨俊鸿(1999-), 男, 硕士研究生, 主要研究方向为量子计算与量子信息, E-mail: junhong.yang@foxmail.com

通信作者: 王帮海(1974-), 男, 教授, 博士, 主要研究方向为量子计算与量子信息, E-mail: bhwang@gdut.edu.cn

然而,量子资源目前主要集中在少数大型企业和科研机构中,这限制了一般用户直接访问和利用这些先进量子计算能力进行机器学习任务的可能。这种资源集中趋势明显增加了量子计算的普及难度,成为量子机器学习广泛应用的一大障碍。应对这一挑战,量子云计算平台^[8]的出现提供了一种解决方案。这些平台通过远程访问服务,允许缺乏量子资源的用户运用量子算法来处理复杂的机器学习任务,显著扩展了量子计算的可用性和实际应用范围。量子云计算的核心优势在于其能为资源受限的用户提供安全的远程量子计算服务,降低了对高昂设备和运维成本的依赖。随着量子加密技术和量子安全通信技术的持续发展^[9],这种模式的安全性和实用性已得到显著增强,尤其是在确保数据隐私方面。利用云基础设施,用户可以借助量子算法高效处理高维数据集,并执行那些在传统计算模型中难以有效处理的任务。随着技术的进步和算法的优化,如何确保数据隐私的同时高效利用量子技术的策略,已成为研究的重点。

本文旨在回顾云量子机器学习的发展历程,重点探讨基于量子内积的量子机器学习和云变分量子算法的最新研究进展。通过分析这些技术在实际应用中的适用场景与面临的挑战,在总结现有的研究成果上,提出了未来的研究方向,以推动云量子机器学习领域的进一步发展。

1 预备知识

量子机器学习可以通过多种策略实现,例如直接的策略是内积的精确计算,以及针对中等规模且含噪声的量子^[10](Noisy Intermediate-scale Quantum, NISQ)时代下的变分量子算法(Variational Quantum Algorithms, VQAs)。

1.1 量子内积

在量子机器学习中,内积是完成多项任务的核心策略之一。经典机器学习中,内积用于评估向量之间的相似度,广泛应用于相似度测量和核方法的构建^[11]。在量子计算中,内积用于评估量子态之间的相似性,拓宽了其应用领域。量子内积,又称态矢量的重叠,可表示为 $\langle \mathbf{u} | \mathbf{v} \rangle$,其中 $|\mathbf{u}\rangle$ 和 $|\mathbf{v}\rangle$ 分别代表2个不同的量子纯态。此外,量子内积不仅可以用来估计量子比特间的距离,而且适用于多种度量方式,包括但不限于欧几里得度量(欧氏距离)、汉明距离,以及保真度。以欧氏距离为例,描述2个量子态 $|\mathbf{u}\rangle$ 和 $|\mathbf{v}\rangle$ 的几何距离,其表达式为

$$D = \sqrt{\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\| \|\mathbf{v}\| \langle \mathbf{u} | \mathbf{v} \rangle} \quad (1)$$

量子K近邻算法(Quantum K-nearest Neighbors Algorithm, QKNN)^[12]通过测量量子态之间的距离进行分类。在二分类问题中,算法评估数据点与2个类别中心的距离,根据距离(例如式(1)中定义的欧几里得距离)将数据点归类至距离较小的类别。此外,量子内积作为关键技术,也应用于量子支持向量机(Quantum Support Vector Machine, QSVM)^[5],通过量子内积构建核函数,实现量子核方法。在量子计算中,内积的计算可以在高维希尔伯特空间中执行,捕捉比经典内积更复杂的数据关系。

1.2 变分量子算法

变分量子算法^[13]是适应中等规模噪声环境的一类量子机器学习算法。它本质上是一种经典-量子混合算法,其中梯度计算由经典中央处理单元(Central Processing Unit, CPU)完成。常见的变分量子算法包括变分量子特征值求解算法^[14]和量子近似优化算法^[15]等,该类算法的优化依赖于含可调参数的变分量子线路以及经典优化器。

在处理经典数据时,数据首先通过编码线路被转化为量子态。常见的量子编码方式^[16]包括振幅编码、角度编码以及混合编码等。变分量子算法的优化过程涉及对含参量子门(如Pauli旋转门以及Ising门)的参数进行调整,以实现模型的训练。Pauli旋转门包括沿布洛赫球(Bloch Sphere) x , y 和 z 方向的旋转门,其数学形式分别为

$$R_X(\gamma) = e^{-i\frac{\gamma}{2}X} = \begin{bmatrix} \cos \frac{\gamma}{2} & -i \sin \frac{\gamma}{2} \\ -i \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix} \quad (2)$$

$$R_Y(\gamma) = e^{-i\frac{\gamma}{2}Y} = \begin{bmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix} \quad (3)$$

$$R_Z(\gamma) = e^{-i\frac{\gamma}{2}Z} = \begin{bmatrix} e^{-i\frac{\gamma}{2}} & 0 \\ 0 & e^{i\frac{\gamma}{2}} \end{bmatrix} \quad (4)$$

式(2)~(4)中: γ 为指定的旋转角度, X , Y , Z 为固定的Pauli矩阵。

训练过程中,参数的更新通常遵循参数位移规则^[17],其中梯度更新公式为

$$\frac{\partial C(\theta)}{\partial \theta_j} = \frac{\partial f(E(\theta))}{\partial E(\theta)} \times \frac{\partial E(\theta)}{\partial \theta_j} = \frac{1}{2} \left(\frac{\partial f(E(\theta))}{\partial E(\theta)} \right) \times [E(\theta_{j+}) - E(\theta_{j-})] \quad (5)$$

式(5)中: $\theta_{j\pm} = \{\theta_0, \dots, \theta_j \pm \frac{\pi}{2}, \dots, \theta_p\}$, ∂ 表示对相应变

量的偏导。假设 $|\psi(\theta)\rangle$ 为变分量子线路的输出态, $E(\theta)$ 为给定参数 θ 时输出态 $|\psi(\theta)\rangle$ 的期望值, $\mathbf{O}$ 是测量的可观测量,函数 f 是目标函数,例如均方误差或交叉熵。目标函数 $C(\theta)$ 可表示为

$$C(\theta) = f(E(\theta)) = f(\langle\psi(\theta)|\mathbf{O}|\psi(\theta)\rangle) \quad (6)$$

2 基于内积的云量子机器学习

在云量子机器学习领域中,量子内积的估计常通过远程服务器代理执行相应的量子线路来实现。近年来,相关计算协议逐步得到了发展。

2.1 基于光学线路模型

利用远程服务器进行基于量子内积计算的云量子机器学习的概念,最早由Sheng等^[18]在2017年提出,所设计的光学线路如图1所示。其中(Polarizing Beam Splitter, PBS)偏振分束器用于分离和反射偏振态的光子,而半波片(Halfwave Plate, HWP)用于将 $|0\rangle$ 和 $|1\rangle$ 转换为 $|+\rangle$ 和 $|-\rangle$ 。 R_1, R_2 用于对偏振光子的任意旋转。Fredkin门(受控交换门)则通过光学Kerr非线性效应和(Beam Splitter, BS)分束器共同构建, S_1, S_2, S_3 分别为量子纠缠源,生成用于计算的纠缠光子对,客户端的光子路径为 a_1, a_2, a_3, a_4 ,分别对应客户端发送到服务器的光子信号;而服务器的光子路径 b_1, b_2, b_3 则用于在服务器端处理这些信号,最终通过路径 b_4 输出计算结果。该协议的具体实施步骤阐述如下:

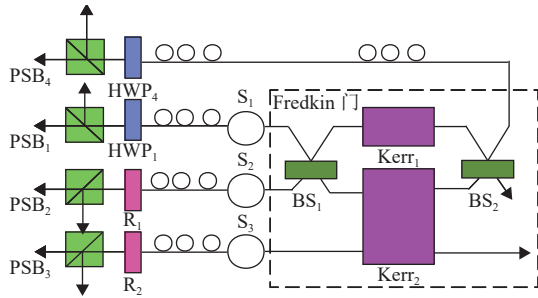


图1 隐私保护量子内积计算的光学线路实现^[18]

Fig.1 Optical circuit implementation of privacy-preserving quantum inner product calculation^[18]

检查阶段:(1) 服务器利用3个纠缠源 S_1, S_2 和 S_3 分别制备 $2N$ 对Bell态

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (7)$$

式(7)中一半设为检查组,另一半设置为信息组。

(2) 在检查组中, N 个光子随机分配给服务器进行测量,测量基在 $\mathbf{X}$ 和 $\mathbf{Z}$ 中随机取得。服务器将选取的测量基和测量结果发送给客户端,客户端使用相

同的基对另一半光子进行测量。如果两者的测量结果不一致,则表明存在中间人攻击,协议终止。

(3) 服务器将另外 $3N$ 对光子发送给客户端。客户端在接收到光子后,随机选择部分光子进行与(2)相同的检查,以确保没有窃听行为。客户端对其光子进行随机测量,并将测量结果传递给服务器。

计算阶段:(1) 客户端通过 R_1, R_2 操作对光子进行旋转变换,最终可以得到2个参与计算量子内积的量子态。

$$|u\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \quad (8)$$

$$|v\rangle = \alpha_2|0\rangle + \beta_2|1\rangle \quad (9)$$

(2) 服务器执行Fredkin三量子比特操作,包含1个控制位和2个目标位。控制位可能是 $|0\rangle, |1\rangle, |+\rangle, |-\rangle$,服务器将其返回给客户端。经过Fredkin操作后,控制位为 $|0\rangle$ 所对应的量子态为 $|0uv\rangle$; $|1\rangle$ 所对应的量子态为 $|1vu\rangle$; $|\pm\rangle$ 所对应的量子态为

$$\frac{1}{2} [|+\rangle(|uv\rangle + |vu\rangle) \pm |-\rangle(|uv\rangle - |vu\rangle)] \quad (10)$$

(3) 客户端依据对控制位 $|\pm\rangle$ 进行测量所获得的概率信息来推导出内积。采用 $\mathbf{X}$ 基进行测量,若 $P|+\rangle$ 与 $P|-\rangle$ 分别代表测量结果为 $|+\rangle$ 与 $|-\rangle$ 的概率,可得出内积的表达式为

$$\langle u|v\rangle = \sqrt{2P(|+\rangle) - 1} = \sqrt{1 - 2P(|-\rangle)} \quad (11)$$

此过程严格保障了内积计算的安全性。客户端的光子偏振态信息以及测量结果对服务器来说都是保密的,且客户端在整个过程中并未传输任何具体的数值信息,从而有效防范了潜在窃听者的干扰。该协议基于用户-服务器模型构建,并具有进一步扩展至用户-服务器-数据库模型的潜力,以支持第三方机构提供数据并确保安全计算的实施。

2.2 基于线路模型的盲量子计算

Zhou等^[19]提出了2种基于线路模型的盲量子计算(Blind Quantum Computation Based on Circuit Model, BQCCM)协议,使用了量子一次性密码本(Quantum One-time Pad, QOTP)技术^[20]用于安全计算量子内积。服务器使用通用门序列

$$\{\text{Fredkin}, \text{CNOT}, \mathbf{H}\} \quad (12)$$

以及交换测试线路(如图2所示)来安全计算量子内积,式(12)中:CNOT为受控非门(Controlled-NOT Gate), $\mathbf{H}$ 为哈德玛门(Hadamard Gate)。客户端仅提供 $\mathbf{X}$ 门和 $\mathbf{Z}$ 门用于加解密操作,交换线路中的所有量子

门则由服务器代理完成。

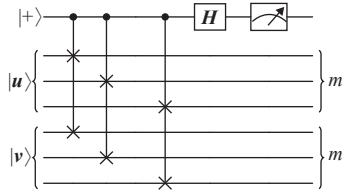


图2 交换测试线路^[19]

Fig.2 Swap test circuit^[19]

交换测试线路的输入包含1个辅助量子比特 $|+\rangle$ 和参与计算内积的2个 m 维量子态 $|u\rangle$ 和 $|v\rangle$ 。该线路包含 m 个Fredkin门(其中控制位为辅助量子比特,2个目标位对应于各自量子态上位置相同的每一位量子比特),1个作用在辅助量子比特上的 H 门和1个辅助量子比特上的 Z 基测量共同完成该计算。

基于这一结构,Zhou等^[19]提出了2种量子内积计算协议:(1)半盲协议:该协议仅使用QOTP技术实现。客户端首先利用随机计算的私钥对输入量子态进行加密,量子门作用于量子态后,客户端利用QOTP计算私钥,并利用该私钥对量子态进行解密,需要代理的交换测试线路暴露给服务器。(2)全盲协议:该协议结合QOTP和线路隐藏技术。与半盲协议类似,客户端首先利用随机计算的私钥对输入量子态进行加密,量子门作用于量子态后,客户端再利用QOTP计算私钥,并利用私钥对量子态进行解密。然而,客户端还需要根据关系

$$\text{Fredkin}_{123} = (I_1 \otimes \text{CNOT}_{23}) (\text{Toffoli}_{123}) (I_1 \otimes \text{CNOT}_{23}) \quad (13)$$

提前将线路中的Fredkin门替换为1个Toffoli门和2个CNOT门,且额外引入3个辅助量子比特 $|0\rangle$,并通过循环委托服务器执行固定的量子门操作组合

$$\{H, \text{CNOT}, \text{Toffoli}\} \quad (14)$$

以隐藏协议真正代理的交换测试线路,从而达到全盲性,两类协议的具体比较如表1所示。

表1 基于线路模型的2类盲量子计算协议比较

Table 1 Comparison of two types of BQCCM

协议	实现方式	隐私保护
半盲协议	QOTP	除交换测试线路暴露给服务器外的信息均保密
全盲协议	QOTP+线路隐藏	所有信息均保密

2种协议都需要进行类似于2.1的验证步骤,以便检测中间人攻击。客户端使用量子随机存储器(QRAM)将经典数据编码为量子态,并随机生成用

于量子比特加密的私钥 $\{(a_i, b_i)\}_{i=1}^N \in \{0, 1\}^{2N}$ 。对于经典输入 $x = \{x_i\}_{i=1}^N$, QRAM将其编码为 $\{|\psi(x_i)\rangle\}_{i=1}^N$,并通过私钥 $\{(a_i, b_i)\}_{i=1}^N$ 进行加密。加密后的量子态形式为

$$|\psi_{\text{encrypted}}\rangle = \bigotimes_{i=1}^N (X^{a_i} Z^{b_i} |\psi(x_i)\rangle) \quad (15)$$

式(15)中: N 为变分子线路的宽度(输入量子比特数),根据式(15),输入量子态的密度矩阵为

$$\rho = \frac{1}{2^{N+1}} \sum_{i=1}^N (Z^{b_i} X^{a_i} |\psi(x_i)\rangle \langle \psi(x_i)| X^{a_i} Z^{b_i}) \quad (16)$$

由式(16)可知,输入量子态变为最大混合态,因此服务器无法猜测客户端输入的量子态。加密的输入量子态经过量子门后,客户端利用QOTP更新用于解密输出量子态的私钥,与输入量子态相同,输出量子态在解密前也可证明为最大混合态,从而确保了整个过程的安全性。

以单量子比特 H 门为例,具体阐释使用QOTP对量子态加解密的具体过程。客户端首先随机生成用于量子比特加密的私钥 $(a_1, b_1) \in \{0, 1\}^2$,根据关系

$$X^{a_1} Z^{b_1} H = H Z^{a_1} X^{b_1} \quad (17)$$

客户端的私钥会被更新为 (b_1, a_1) 。客户端并对服务器的输出量子态作用 $X^{b_1} Z^{a_1}$ 门。Fredkin、CNOT、CZ(Controlled-Z Gate,受控Z门)和SWAP门(交换门)的过程同理,但Fredkin门的输出量子态在利用QOTP进行解密时,涉及到客户端无法独立执行的CNOT、CZ和SWAP门,这些门的实现需要客户端重新利用QOTP对量子态进行加解密。

在完成对交换测试线路中所有量子门的代理操作后,客户端对辅助量子比特执行 Z 基测量,若 $P|0\rangle$, $P|1\rangle$ 分别代表测量结果为 $|0\rangle$ 与 $|1\rangle$ 的概率,则根据式(11)可以同理推导出量子内积为

$$\langle u|v\rangle = \sqrt{2P(|0\rangle) - 1} = \sqrt{1 - 2P(|1\rangle)} \quad (18)$$

2.3 基于量子双边关联算法

除了使用简单的光学线路和基于线路模型的盲量子计算协议外,Li等^[21]提出了一种基于量子双边关联算法的安全内积计算协议。此方法为基于内积的量子机器学习提供了新的实现思路。具体来说,服务器和客户端分别持有数据向量 x 和 y ,客户端需要对其数据向量 y 进行额外编码,并使用相位门加入隐藏的相位信息 $g = \{g_1, g_2, \dots, g_N\}$,以加密数据及内积计算结果。

首先,服务器对所有输入寄存器的量子比特 $|0\rangle$ 均施加 H 门以得到叠加态 $|+\rangle$,其中 t 为输入量子比特数。接着,服务器对每一个寄存器量子比特施加Grover算符^[22]。在此过程中,服务器通过局部Oracle算符^[23]处理与向量 $\mathbf{x}$ 有关的量子态,并将其发送给客户端。客户端使用自身的局部Oracle操作制备量子态

$$\frac{1}{\sqrt{N}} \sum_{i=1}^N (-1)^{x_i y_i} |i x_i y_i g_i\rangle_{i o_1 o_2 o_3} \quad (19)$$

式中: o_1 为服务器局部Oracle的辅助量子比特, o_2 和 o_3 为客户端局部Oracle的辅助量子比特。随后客户端作用受控 Z 门于 o_1 和 o_2 上,并在 o_3 上施加 Z 门,完成纠缠操作以提取数据向量 $\mathbf{x}$ 和 $\mathbf{y}$ 之间的关联信息。通过多次迭代,对所有寄存器量子比特施加Oracle算符,从而逐步逼近 $\mathbf{x}$ 和 $\mathbf{y}$ 之间的内积信息 $\overline{\mathbf{x}\mathbf{y}}$ 。

最后,服务器执行量子逆傅里叶变换,并对输出量子比特进行投影测量。此过程等效于将输出量子比特投影到具有相位 $2^{1-t} j\pi$ 的量子态 $|j\rangle$,其中 $j=0$ 或 1 ,从而得到测量结果为

$$\sigma_j = \begin{cases} 2 \arcsin(\sqrt{\overline{\mathbf{x}\mathbf{y}}}), & j=0 \\ 2\pi - 2 \arcsin(\sqrt{\overline{\mathbf{x}\mathbf{y}}}), & j=1 \end{cases} \quad (20)$$

服务器由式(20)估计内积值 $\overline{\mathbf{x}\mathbf{y}}$,并通过经典通信将它传递给客户端,客户端利用式(21)以及隐藏的相位信息 $\mathbf{g}$ 对 $\overline{\mathbf{x}\mathbf{y}}$ 进行调整,最终准确估算量子内积 $\mathbf{x}\mathbf{y}$ 。

$$\overline{\mathbf{x}\mathbf{y}} = \frac{1}{N} \sum_{i=1}^N (x_i y_i + g_i) \quad (21)$$

3 云变分量子算法

云变分量子算法是量子机器学习的核心工具之一,其重点在于确保在加密数据状态下进行准确的计算。目前,研究主要集中在盲量子计算、量子同态加密等技术的创新和探索。

3.1 基于测量模型的盲量子计算

Li等^[24]基于Broadbent等^[25]提出的通用盲量子计算(Universal Blind Quantum Computation, UBQC)协议设计了云变分量子算法,并将其用于量子联邦学习。此外,他们使用了依赖于资源态(如砖墙态)的假设(Ansatz)以减少线路深度,见图3中的蓝色区域。量子线路通过多个重复的Ansatz,然后经过多个CNOT门进行量子纠缠处理,最后对辅助量子比特进行测量,以完成变分量子算法的后处理,算法的安全

性和正确性由UBQC保证。

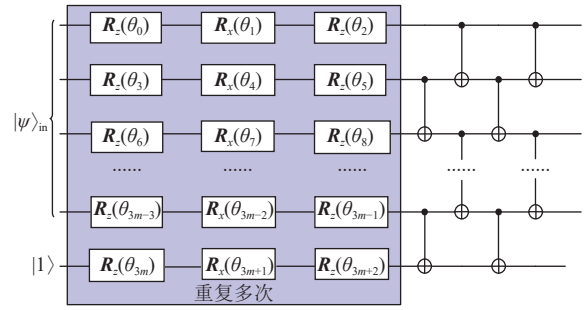


图3 适用于通用盲量子协议的变分量子线路^[25]

Fig.3 Variational quantum circuit designed for UBQC^[25]

协议的流程图如图4所示,绿色区域代表编码线路,蓝色区域代表Ansatz线路,黄色区域则对应输出层的量子比特。假设客户端需要代理的变分量子线路为

$$U(\theta) = \prod_{\mathcal{R}} U_{\mathcal{R}}(\theta_{\mathcal{R}}) \quad (22)$$

准备阶段:(1)客户端在初始参数下计算用于梯度计算的所有量子线路,包括编码线路和Ansatz线路。根据式(5),假设需要代理的变分量子线路的参数个数为 $\mathcal{R}$,则客户端需要代理 $2\mathcal{R}+1$ 个量子线路。客户端接着把这些量子线路转换为适用于测量模型的线路,并计算测量模型中位于资源态各个位置 ξ, ζ 的量子比特的实际测量角度 $\phi_{\xi, \zeta}$ 。(2)对每一个量子线路,客户端将量子比特初始化为

$$|\gamma_{\xi, \zeta}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\gamma_{\xi, \zeta}} |1\rangle), \quad \gamma_{\xi, \zeta} \in \left\{ \frac{k\pi}{4} \mid k \in \{0, 1, \dots, 7\} \right\} \quad (23)$$

式中: $\gamma_{\xi, \zeta}$ 是从给定集合中均匀随机选取的参数。服务器随后将这些量子比特纠缠为砖墙态,如图4所示,其中砖墙态由 m 行 n 列、旋转角度随机的量子比特构成。

计算阶段:(1)客户端依次将加密的测量角度 $\delta_{x, y}$ 发送给服务器,其中

$$\delta_{\xi, \zeta} = \phi'_{\xi, \zeta} + \gamma_{\xi, \zeta} + r\pi \quad (24)$$

$$\phi'_{\xi, \zeta} = (-1)^{x_{\xi, \zeta}} \gamma_{\xi, \zeta} + s_{\xi, \zeta}^Z \pi + \phi_{\xi, \zeta} \quad (25)$$

$$s_{x, y}^X = \bigotimes_{(\xi, \zeta) \in \mathcal{D}_{\xi, \zeta}} s_{\xi, \zeta}^X \in \{0, 1\} \quad (26)$$

$$s_{\xi, \zeta}^Z = \bigotimes_{(\xi, \zeta) \in \mathcal{D}_{\xi, \zeta}} s_{\xi, \zeta}^Z \in \{0, 1\} \quad (27)$$

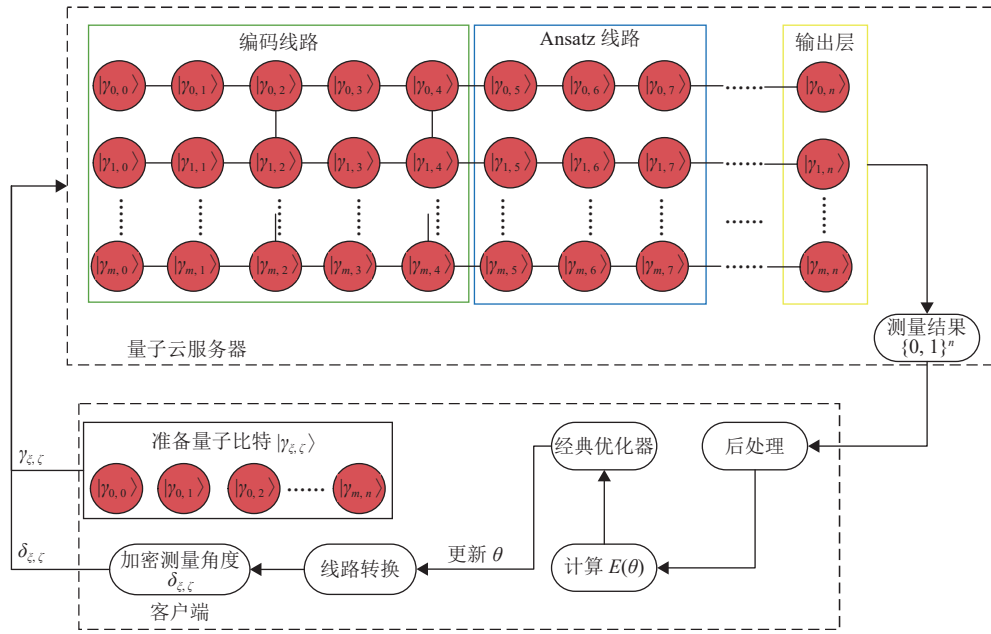


图4 基于通用盲量子计算的云变分子算法流程图

Fig.4 Flowchart of cloud-based VQAs using UBQC

$s_{\xi,\zeta}^X, s_{\xi,\zeta}^Z$ 分别为测量模型^[26]中的 X 基、 Z 基依赖； $D_{\xi,\zeta}$ 和 $D'_{\xi,\zeta}$ 为与测量模型中流结构^[26]相关的依赖集； r 在0和1随机取值；变量 $s_{\xi,\zeta}$ 表示服务器对在位置 ξ, ζ 上的量子比特的测量结果。

(2) 服务器在布洛赫球的 xoy 平面上以角度 $\delta_{x,y}$ 进行测量，并把结果发送给客户端，若 $r=1$ ，客户端对接收到的结果进行翻转以得到正确的测量值。服务器在最后一层量子比特中进行可观测量为 $\{O_k\}_{k=1}^N$ 的加密测量，随后将测量结果传输给客户端。客户端结合 X 基依赖和随机变量 r 对测量结果相异或对测量结果进行解密，以获得正确的输出结果，并重复代理计算梯度所需要的 $2R+1$ 个量子线路。

(3) 客户端重复执行上述步骤，利用式(5)计算期望值，利用式(6)计算目标函数 $C(\theta)$ 并更新参数 θ 以最小化 $C(\theta)$ 。

(4) 客户端根据参数 θ 重新计算需要代理的 $2R+1$ 个量子线路，并重新执行上述过程直到参数 θ 收敛。

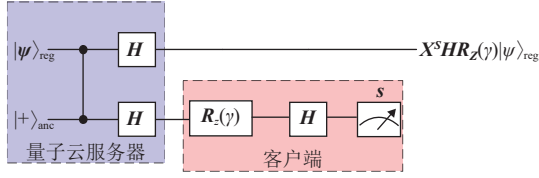
(5) 客户端输出训练好的变分子量子电路参数序列 $\{\theta_1, \dots, \theta_R\}$ 。

上述方案同样适用于客户端仅执行测量的盲量子协议模型^[27]，唯一不同之处在于协议中资源态由服务器准备，服务器将资源态发送至客户端，客户端对每个量子比特进行加密测量，具体步骤与之前一致，此方案在光学环境下对用户量子能力的要求较低^[27]。Wang等^[28]基于此，通过资源态循环策略，进一

步减少了服务器中需要纠缠的量子比特数^[29]，用于QAOA中变分子量子线路的构建。近年来，随着对盲量子计算研究的深入^[30]，在盲量子计算的各个方面取得了显著进展。例如，在减少量子线路深度方面，可以采用改进的砖墙态等资源态来实现^[31]；在减少客户端量子能力方面，也可以采用基于UBQC扩展的单服务器^[32]、双服务器^[33]或三服务器^[34]等协议，使客户端能够完全得以经典方式参与计算；此外，量子噪声问题也有了有效的应对策略^[35]。在基于测量模型的盲量子计算中，不同的实现方案赋予客户端不同的量子计算能力，且所有方案中均可加入验证机制^[36-37]。

3.2 基于辅助驱动的盲量子计算

云变分子量子算法也可以利用线路模型实现，但需要借助基于测量模型的量子计算间接实现任意角度的旋转门的安全代理，以上可以通过辅助驱动的通用量子计算(Ancilla-driven Universal Quantum Computation, ADUQC)^[38]来实现。辅助驱动的量子计算在本质上类似于量子隐形传态，通过固定量子线路装置使辅助量子比特和寄存器量子比特纠缠，对辅助量子比特进行指定测量基测量，从而完成对目标寄存器量子比特的指定酉演化。Shingu等^[39]基于ADUQC提出了一种方案，将辅助量子比特在量子云服务器与寄存器量子比特进行纠缠操作后发送给客户端进行测量，从而在服务器实现寄存器量子比特的目标旋转角度，进而得到旋转算符 $J(\gamma)$ ，如图5所示。

图5 旋转算符线路^[38]Fig.5 Rotation operator circuit^[38]

其中旋转算符 $J(\gamma)$ 为

$$J(\gamma) = H R_z(\gamma) \quad (28)$$

通过欧拉角分解,任意单量子比特门 U 可以表示为

$$U = H [R_z(\gamma_1) R_x(\gamma_2) R_z(\gamma_3)] = J(\gamma_1) J(\gamma_2) J(\gamma_3) \quad (29)$$

式中: γ_1 、 γ_2 、 γ_3 为控制参数。根据式(29),客户端只需分别以 γ_1 、 γ_2 、 γ_3 作为目标旋转角度执行3次图5中的操作,即可实现任意单量子比特门 U 。

对于双量子比特控制门 CU ,可以利用以下分解形式

$$CU = \left[R_z(\phi_1) \otimes R_x(\phi_2) R_y\left(\frac{\phi_3}{2}\right) \right] CZ \times \left[I \otimes R_y\left(-\frac{\phi_3}{2}\right) R_x\left(-\frac{\phi_4 + \phi_2}{2}\right) \right] CZ \times \left[I \otimes R_x\left(\frac{\phi_4 - \phi_2}{2}\right) \right] \quad (30)$$

式(30)中: ϕ_1 、 ϕ_2 、 ϕ_3 、 ϕ_4 为控制参数。通过式(30)~(33),控制双比特门 CU 可以被分解为由 $J(\gamma)$ 算符、 CZ 门、 H 门以及相位门 S 和 $S^\dagger$ 组成的电路,其中 $J(\gamma)$ 算符通过图5所示线路实现,而 CZ 门、 H 门、相位门 S 和 $S^\dagger$ 由服务器提供。该方案的步骤与3.1基于测量模型的盲量子计算类似,不同之处在于它通过ADUQC把对资源态上基于测量模型等效为线路模型实现。

$$R_x(\gamma) = J(\gamma) H \quad (31)$$

$$R_y(\gamma) = S J(\gamma) H S^\dagger \quad (32)$$

$$R_z(\gamma) = H J(\gamma) \quad (33)$$

相较于基于通用盲量子计算的方案,辅助驱动计算的方式显著减少了服务器所需的量子资源,服务器仅需 $N+1$ 个量子比特。然而,该方案的缺点也较为明显,线路的深度远多于使用通用盲量子计算的方式。此外,这种方式的验证难度较大,若考虑信道丢失的情况,协议中需要重新执行变分量子线路的

概率随线路的深度指数增长。

3.3 基于量子同态加密

线路模型的云变分量子算法还可以间接通过量子同态加密技术实现,这一想法由Li等^[40]实现。客户端首先要把经典的数据编码为量子态,再生成随机私钥对其进行加密。对通用量子门集合

$$G = \{X, Z, H, CNOT, T\} \quad (34)$$

前4个门为Clifford门,可以利用QOTP更新私钥对输出量子态进行解密。但对于非Clifford门 T ,由于其不能与Pauli门对易,导致简单的QOTP技术无法直接用于加解密。导致该问题的关键在于式(35)。

$$T X^a Z^b = S^a X^a Z^b T, \{a, b\} \in \{0, 1\}^2 \quad (35)$$

由式(35)可以看出, T 门作用于加密的量子态后,会引入一个额外的相位误差 S^a ,由于这一相位误差无法被简单的Pauli门加密所抵消,因此客户端需要自行设计额外的 T 装置来完成加密量子态的解密。

T 门装置主要使用经典客户端远程态制备技术,具体步骤如下。

(1) 客户端首先随机选择一个属于式(36)的量子比特,接着客户端再随机选择一个属于 $\{|+\rangle, |-\rangle\}$ 的量子比特。选择完成后,这些量子比特被上传至服务器。

$$\left\{ |+\rangle, |-\rangle, \left| \frac{\pi}{2} \right\rangle, \left| \frac{3\pi}{2} \right\rangle \right\} \quad (36)$$

(2) 服务器对客户端上传的2个量子比特使用固定的耦合操作式(37)进行Bell态 $|\Phi^+\rangle$ 的制取,2个量子比特最终根据测量结果演化为表2中所示的8个量子态的一种。可以看出,这些量子态等价于使用随机生成的私钥 $\{a, b\}$ 对Bell态 $|\Phi^+\rangle$ 进行加密,并且可能附带相位信息 $S^\dagger$,可以根据式(38)对它进行消除。

$$(I \otimes H) CZ \quad (37)$$

$$S^\dagger S = I \quad (38)$$

(3) 服务器对 $|\Phi^+\rangle$ 执行Bell联合测量,客户端根据测量结果和QOTP更新的私钥进行解密。客户端需代理的变分量子线路与式(22)一致,基于量子同态加密的云变分量子算法协议的步骤如下。

准备阶段:

(1) 客户端生成密钥:客户端首先使用Solovay-Kitae算法^[41]将每个变分量子门 $U_R(\theta_R)$ 分解为离散的通用量子门集 G 。例如,对于一个 $R_y(2.40)$ 门,可以分

表2 纠缠态制取
Table 2 Entangled state preparation

量子态	$ +\rangle$	$ -\rangle$	$ \frac{\pi}{2}\rangle$	$ \frac{3\pi}{2}\rangle$
$ +\rangle$	$(X^0 Z^0 \otimes I) \Phi^+\rangle$	$(X^0 Z^1 \otimes I) \Phi^+\rangle$	$(S^\dagger X^0 Z^1 \otimes I) \Phi^+\rangle$	$(S^\dagger X^0 Z^0 \otimes I) \Phi^+\rangle$
$ -\rangle$	$(X^1 Z^0 \otimes I) \Phi^+\rangle$	$(X^1 Z^1 \otimes I) \Phi^+\rangle$	$(S^\dagger X^1 Z^1 \otimes I) \Phi^+\rangle$	$S^\dagger X^1 Z^0 \Phi^+\rangle$

解为

$$R_Y(2.40) = HZTHZTHZTHZ \quad (39)$$

分解后,客户端记录每个量子门中 T 门的数量 L 。

(2) 客户端根据系统的安全参数 κ (决定密钥的长度和加密的强度)和 T 门的数量 L ,通过量子同态加密算法的密钥生成步骤来生成:① 私钥(sk):由客户端保留,用于解密量子比特和生成量子评估密钥;② 公钥(pk):发送给服务器,并用于生成量子评估密钥;③ 量子评估密钥(evk):用于在加密态上执行 T 门装置,需要公钥和私钥共同参与,并在客户端上完成制备。

计算阶段:

(1) 客户端对数据集中的每个经典输入 x_i 准备对应的量子态 $|\psi(x_i)\rangle$,并使用QOTP随机生成私钥,同2.2。

(2) 服务器接收 $|\psi_{\text{encrypted}}(x)\rangle$,使用Solovay-Kitaev算法将需要执行的量子门分解为通用门集 G 。针对非 T 门,客户端可以通过QOTP直接更新私钥对输出量子态进行解密。而对于 T 门,客户端则需等待服务器使用客户端提供的量子评估密钥,在执行 T 门装置后,进行私钥的更新,客户端再利用私钥对输出量子态进行解密。

(3) 服务器使用双方可行的可观测量 $\{O_k\}_{k=1}^N$ 对线路的输出量子态进行测量,随后将测量结果传输给客户端。客户端使用解密密钥对量子态进行解密。

(4) 客户端重复执行上述步骤,向服务器代理 $2R+1$ 个量子线路以利用式(5)计算期望值。通过式(6),客户端计算目标函数 $C(\theta)$ 并更新参数 θ ,以最小化 $C(\theta)$ 。

(5) 客户端根据参数 θ 重新计算需要代理 $2R+1$ 个量子线路,并重新执行上述过程直到参数 θ 收敛。

(6) 客户端输出训练好的变分量子电路参数序列 $\{\theta_1, \dots, \theta_R\}$ 。

3.4 其他云变分量子算法研究

在上述所有方案中,探讨的均属于分布式梯度计算框架。在这一框架下,客户端负责梯度计算任

务,利用服务器中的量子测量结果进行模型参数的更新。然而,这种策略不可避免地增加了通信成本。为了解决这一问题,可以借鉴Sun等^[42]提出的方法,该方法将数据加密与预训练相结合。在该方法中,数据集的每个元素在训练前经过加密处理,并与原始数据一同用于模型的预训练。这一策略不仅有效保护了数据隐私,还提升了模型对新加密数据的分类能力,从而增强了模型的泛化能力。尽管如此,模型仍然容易被第三方窃取。

针对这一问题,Wang等^[43]则提出了量子模型安全架构,它将量子机器学习模型分割并分布于量子云提供商上,即使部分提供商被攻击,攻击者也无法因此重构出完整的量子模型。此外,该架构还采用了强化学习作为安全引擎,以优化分布式模型设计并保证性能与安全性。与此同时Gupta等^[44]则提出了基于量子机器学习的恶意用户预测模型。该模型结合了用户行为建模单元和量子神经网络,并采用差分进化优化算法。该模型能够分析用户请求并预测恶意行为,从而在数据分配前增强云通信系统的安全性。尽管这些方法提高了模型的安全性,但相比前面的方案,降低了数据的隐私性保护。

4 讨论

在基于内积的云量子机器学习中,客户端依赖于远程云服务器来计算量子内积,从而间接执行如QKNN和QSVM等量子机器学习任务。此过程通常涉及使用交换测试或Grover算法等特定线路来代理内积计算。然而,随着数据维度的增加,相应的线路结构变得更加复杂。基于光学线路模型的方法对光学器件的精度要求极高,基于线路模型的盲量子计算需要加解密的门序列,且这些门序列随数据规模呈指数增长,而基于量子双边关联算法则需要设计更加复杂的Oracle算符。这些挑战在量子深度学习模型扩展^[45]时尤为突出,仅依赖于内积计算已无法满足大型模型的需求。相较之下,变分量子算法提供了一种更通用且灵活的量子机器学习实现方式。

在云变分量子算法的实施中,传统的线路模型加密方法是一种基础且直接的方案。该方法要求户

端具备制备和存储基本量子比特的能力,并能执行量子态加密和解密操作,如X门和Z门。此外,为了实现量子旋转门,通常还需要使用Solovay-Kitaev算法进行精确分解,然后在基于线路的盲量子协议中,通过添加辅助线路来掩盖实际的量子门操作^[19],或者采用量子同态加密技术^[40]以增强安全性。尽管这种分解方式提升了算法的安全性,却带来了较高的通信成本和更长的训练时间。此外,由于量子编码过程完全由客户端负责,客户端通常只能采用如角度编码等简单的量子编码方式。对于更复杂的量子编码,虽然可以考虑委托云服务器处理,但这种选择可能因资源态深度过大而导致量子噪声增加和通信复杂性加剧。

与此相比,基于测量模型的盲量子计算提供了一种更为合理的选择。在这种方法中,服务器负责构建资源态,而客户端仅需具备量子比特制备或测量的能力。然而,该方法主要适用于简单的编码线路,

并依赖于资源态结构的Ansatz。当资源态过深时,服务器同样需要面临噪声问题。此外,该方法在服务器或客户端执行测量前需要服务器进行复杂的纠缠操作,这要求服务器拥有大量量子寄存器,尽管服务器可以通过资源循环^[28]策略来避免这个问题,但服务器的执行计算的总时间仍然是限制因素。并且在引入纠错和验证机制时,服务器所需的量子资源和通信成本也会显著增加。虽然基于辅助驱动的盲量子计算能够减少服务器所需的量子资源,但这通常会导致更深的量子线路,超过通用盲量子计算所需的线路深度。本文在云变分量子算法中所讨论的其他模型或架构则注重通过在服务器端安全地执行梯度计算以降低通信开销,但这可能牺牲一定的安全性,如模型的保护强度或数据的加密强度。因此,用户需根据具体的应用场景和需求选择适合的实现策略。为方便理解,表3对不同云量子机器学习方法进行了比较,展示了各类别方法的应用场景及其缺点。

表 3 不同类别云量子机器学习方法的比较
Table 3 Comparison of different categories of cloud-based quantum machine learning methods

类别	方法	应用场景	缺点
基于内积的量子机器学习	基于光学线路模型 ^[18]	数据维度小的可由光学系统直接实现的基于内积的分类任务	不适合大型量子模型、对光学器件的精度要求高
	基于线路模型的盲量子计算 ^[19]	数据维度适中的基于内积的分类任务	不适合大型量子模型、通信成本高
	基于量子双边关联算法 ^[21]	数据维度适中的基于内积的分类任务	不适合大型量子模型、算法线路设计复杂
云变分量子算法	基于测量模型的盲量子计算 ^[25,28]	客户端量子能力有限的变分量子算法分类任务	量子资源消耗大,量子线路深度过深带来噪声问题和通信开销
	基于辅助驱动的盲量子计算 ^[38]	客户端量子能力有限且服务器量子资源受限的变分量子算法分类任务	量子线路深度过深带来噪声问题和通信开销
	基于量子同态加密 ^[40]	客户端具备一定量子能力且服务器量子资源受限的变分量子算法分类任务	客户端需具备一定量子能力,量子线路深度增加带来噪声问题和通信开销
	基于非分布式梯度计算 ^[42-44]	在控制通信开销的同时牺牲部分安全性的变分量子算法分类任务	牺牲部分数据或模型的安全性

5 结论与展望

作为量子计算与量子通信融合的产物,云量子机器学习依托量子云计算平台上实现高效及安全的量子任务,已取得显著进展。尽管现有技术在降低通信成本方面已有所成就,但在确保数据隐私的同时,量子线路深度和通信复杂度仍影响着性能。展望未来,云量子机器学习仍需在隐私安全与通信效率之间找到更佳平衡,特别是在量子算法创新与系统架构优化方面。例如,基于测量模型的量子机器学习^[46]方法不直接把线路模型转换为测量模型,而是把测量模型中的测量角度作为变量进行优化,这种策略可能为云量子机器学习中的量子线路和资源利用的优化提供全新的路径。此外,通过多学科交叉合作,结合经典机器学习与量子计算的优势,本领域

有望迎来突破性发展。同时,量子网络^[47]和量子分布式计算^[48]等新兴技术的理论创新,将为云量子机器学习的大规模应用奠定基础。期待这些领域将取得更深入的研究成果,进一步推动云量子机器学习的实际应用。

参考文献:

[1] DIVINCENZO D P. Quantum computation[J]. *Science*, 1995, 270(5234): 255-261.

[2] ARUTE, F, ARYA, K., BABBUSH, R, *et al.* Quantum supremacy using a programmable superconducting processor [J]. *Nature*, 2019, 574(7779): 505-510.

[3] DENG Y H, GU Y C LIU H L, *et al.* Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage[J]. *Physical Review Letters*, 2023, 131(15): 150601.

- [4] BIAMONTE J, WITTEK P, PANCOTTI N, *et al.* Quantum machine learning[J]. *Nature*, 2017, 549(7671): 195-202.
- [5] REBENTROST P, MOHSENI M, LLOYD S. Quantum support vector machine for big data classification[J]. *Physical Review Letters*, 2014, 113(13): 130503.
- [6] 韦云凯, 王志宏, 冷甦鹏. 量子强化学习技术及研究进展[J]. *广州大学学报*, 2021, 20(1): 56-68.
WEI Y K, WANG Z H, LENG S P. Review of quantum reinforcement learning[J]. *Journal of Guangzhou University*, 2021, 20(1): 56-68.
- [7] 赵翔. 基于量子计算的联邦学习模型: 202210115079[P]. 2024-10-10.
- [8] SOEPARNO H, PERBANGSA A S. Cloud quantum computing concept and development: a systematic literature review[J]. *Procedia Computer Science*, 2021, 179: 944-954.
- [9] 张雪, 高飞, 秦素娟, 等. 量子密码协议研究现状与未来发展[J]. *中国工程科学*, 2022(004): 024.
ZHANG X, GAO F, QIN S J, *et al.* Current status and future development of quantum cryptographic protocols[J]. *Strategic Study of CAE*, 2022(004): 024.
- [10] LAU J W Z, CAI Z, THOMAS N, *et al.* NISQ computing: where are we and where do we go?[J]. *AAPPS Bulletin*, 2022, 32(1): 27.
- [11] MOUSAVI M H, MADDAH-ALI M A, MIRMOHSENI M. Private inner product retrieval for distributed machine learning[C]//*Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT)*. Paris: IEEE, 2019: 778-782.
- [12] LI J Y, ZHANG J, ZHANG J L, *et al.* Quantum KNN classification with K value selection and neighbor selection[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2024, 43(5): 1332-1345.
- [13] CEREZO M, ARRASMITH A, BABBUSH R, *et al.* Variational quantum algorithms[J]. *Nature Reviews Physics*, 2021, 3(9): 625-644.
- [14] TILLY J, CHEN H, CAO S X, *et al.* The variational quantum eigensolver: a review of methods and best practices[J]. *Physics Reports*, 2022, 986: 1-128.
- [15] ZHOU L, WANG S T, CHOI S W, *et al.* Quantum approximate optimization algorithm: performance, mechanism, and implementation on near-term devices[J]. *Physical Review X*, 2020, 10(2): 021067.
- [16] SCHULD M, SWEKE R, MEYER J J. Effect of data encoding on the expressive power of variational quantum-machine-learning models[J]. *Physical Review A*, 2021, 103(3): 032430.
- [17] WIERICH S D, IZAAC J, WANG C, *et al.* General parameter-shift rules for quantum gradients[J]. *Quantum*, 2022, 6: 677.
- [18] SHENG Y B, ZHOU L. Distributed secure quantum machine learning[J]. *Science Bulletin*, 2017, 62(14): 1025-1029.
- [19] ZHOU X, QIU D. Blind quantum machine learning based on quantum circuit model[J]. *Quantum Information Processing*, 2021, 20: 363.
- [20] AMBAINIS A, MOSCA M, TAPP A, *et al.* Private quantum channels[C]//*Proceedings of the 41st Annual Symposium on Foundations of Computer Science*. Washington: IEEE, 2000: 547-553.
- [21] LI C H, LI B N, AMER O, *et al.* Blind quantum machine learning with quantum bipartite correlator[J]. *Physical Review Letters*, 2024, 133(12): 120602.
- [22] GRASSL M, LANGENBERG B, ROETTELER M, *et al.* Applying Grover's algorithm to AES: quantum resource estimates[C]//*Proceedings of the International Workshop on Post-Quantum Cryptography*. Fukuoka: Springer International Publishing, 2016: 29-43.
- [23] BERTHIAUME A, BRASSARD G. Oracle quantum computing[J]. *Journal of Modern Optics*, 1994, 41(12): 2521-2535.
- [24] LI W K, LU S R, DENG D L. Quantum federated learning through blind quantum computing[J]. *Science China Physics, Mechanics & Astronomy*, 2021, 64: 100312.
- [25] BROADBENT A, FITZSIMONS J, KASHEFI E. Universal blind quantum computation[C]//*Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)*. Atlanta: IEEE, 2009: 517-526.
- [26] BRIEGEL H J, BROWNE D E, DÜR W, *et al.* Measurement-based quantum computation[J]. *Nature Physics*, 2009, 5(1): 19-26.
- [27] MORIMAE T, FUJII K. Blind quantum computation protocol in which Alice only makes measurements[J]. *Physical Review A*, 2013, 87(5): 050301.
- [28] HOUSHMAND M, HOUSHMAND M, FITZSIMONS J F. Minimal qubit resources for the realization of measurement-based quantum computation[J]. *Physical Review A*, 2018, 98(1): 012318.
- [29] WANG Y X, QUAN J Y, LI Q. A delegated quantum approximate optimization algorithm[C]//*Proceedings of the 2022 14th International Conference on Wireless Communications and Signal Processing (WCSP)*. Nanjing: IEEE, 2022: 804-808.
- [30] 王帮海, 徐海茹. 盲量子计算研究进展[J]. *广东工业大学学报*, 2015, 32(3): 51-55.
WANG B H, XU H R. Progress in blind quantum computation[J]. *Journal of Guangdong University of Technology*, 2015, 32(3): 51-55.
- [31] MA S Q, ZHU C H, LIU X C, *et al.* Universal blind quantum computation with improved brickwork states[J]. *Physical Review A*, 2024, 109(1): 012606.
- [32] XU H R, WANG B H. Universal single-server blind quantum computation for classical clients[J]. *Laser Physics*

- Letters, 2021, 19(1): 015202.
- [33] MORIMAE T, FUJII K. Secure entanglement distillation for double-server blind quantum computation[J]. *Physical Review Letters*, 2013, 111(2): 020502.
- [34] LI Q, CHAN W H, ZHANG C, *et al.* Triple-server blind quantum computation using entanglement swapping[J]. *Physical Review A*, 2014, 89(4): 040302.
- [35] ZHAO Q, LI C, LIU Y, *et al.* Fault-tolerant quantum error correction code preparation in UBQC[J]. *Quantum Information Processing*, 2020, 19(8): 236.
- [36] FITZSIMONS J F, KASHEFI E. Unconditionally verifiable blind quantum computation[J]. *Physical Review A*, 2017, 96(1): 012303.
- [37] MORIMAE T. Verification for measurement-only blind quantum computing[J]. *Physical Review A*, 2014, 89(6): 060302.
- [38] ANDERS J, OI D K L, KASHEFI E, *et al.* Ancilla-driven universal quantum computation[J]. *Physical Review A*, 2010, 82(2): 020301.
- [39] SHINGU Y, TAKEUCHI Y, ENDO S, *et al.* Variational secure cloud quantum computing[J]. *Physical Review A*, 2022, 105(2): 022603.
- [40] LI Q, QUAN J Y, SHI J J, *et al.* Secure delegated variational quantum algorithms[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2024, 43(10): 3129-3142.
- [41] DAWSON C M, NIELSEN M A. The Solovay-kitaev algorithm[J]. *Quantum Information and Computation*, 2006, 6(1): 81-95.
- [42] SUN W L, CHANG Y, WANG D C, *et al.* Delegated quantum neural networks for encrypted data[J]. *Physica Scripta*, 2024, 99(5): 055102.
- [43] WANG Z P, LI J Y, HU Z R, *et al.* Qumos: a framework for preserving security of quantum machine learning model[C]// Proceedings of the 2023 IEEE International Conference on Quantum Computing and Engineering (QCE). Bellevue: IEEE, 2023: 1089-1097.
- [44] GUPTA R, SAXENA D, GUPTA I, *et al.* Quantum machine learning driven malicious user prediction for cloud network communications[J]. *IEEE Networking Letters*, 2022, 4(4): 174-178.
- [45] WIEBE N, KAPOOR A, SVORE K M. Quantum deep learning[J]. *Quantum Information & Computation*, 2016, 16(7-8): 541-587.
- [46] MANTILLA CALDERÓN L C. Measurement-based quantum machine learning[D]. Vancouver: University of British Columbia, 2023.
- [47] 李静, 刘强, 王丽, 等. 量子网络系统研究进展与关键技术分析[J]. *中国工程科学*, 2024, 25(6): 80-95.
LI J, LIU Q, WANG L, *et al.* Research progress and key technology analysis of quantum network systems[J]. *Strategic Study of CAE*, 2024, 25(6): 80-95.
- [48] 王升斌, 张伟, 刘晨, 等. 分布式量子计算研究进展[J]. *中国量子电子学报*, 2024, 41(1): 1-25.
WANG S B, ZHANG W, LIU C, *et al.* Research progress of distributed quantum computing[J]. *Chinese Journal of Quantum Electronics*, 2024, 41(1): 1-25.
- (责任编辑: 张玮欣 英文审核: 熊荣斌)