doi:10.3969/j.issn.1673-9833.2025.02.012

基于测量的盲量子计算研究进展

李建设[1]，柳闻鹃[2]

（1. 湖南工业大学 计算机学院，湖南 株洲 412007；2. 湖南工业大学 理学院，湖南 株洲 412007）

摘 要：量子计算机具有广阔的前景和发展潜力，但其物理实现目前面临巨大挑战。基于测量的盲量子计算，由于其允许量子能力有限甚至没有量子能力的普通用户，可通过借助远程量子服务器，使用基于测量的量子计算模型完成计算任务，并保证其数据、算法和结果的私密性。因此，这种委托量子计算的方式将成为未来普通用户共享量子计算资源的一种重要应用模式。基于此，阐述了基于测量的量子计算模型包括的两种常用资源态—簇态和图态，以及测量模式的定义和形式化描述；分析了基于测量的盲量子计算的基本原理，包括通用资源态—Brickwork 态的构造、盲量子计算测量模式和通用盲量子计算协议；梳理了解决基于测量的盲量子计算根本问题的不同技术路线和实验成果；探讨了其未来的发展方向。

关键词：盲量子计算；测量模式；经典客户端；量子成本

中图分类号：O413；TP385 **文献标志码**：A **文章编号**：1673-9833(2025)02-0087-10

引文格式：李建设，柳闻鹃 . 基于测量的盲量子计算研究进展 [J]. 湖南工业大学学报，2025，39(2)：87-96.

Research Progress of Measurement-Based Blind Quantum Computation

LI Jianshe[1]，LIU Wenjuan[2]

（1. College of Computer Science，Hunan University of Technology，Zhuzhou Hunan 412007，China；
2. College of Science，Hunan University of Technology，Zhuzhou Hunan 412007，China）

Abstract：With broad prospects and development potential, quantum computers currently faces enormous challenges in their physical implementation. Measurement-based blind quantum computing allows ordinary users with limited or no quantum capabilities to complete computing tasks using measurement based quantum computing models through remote quantum servers, while ensuring the privacy of their data, algorithms, and results. Therefore, this proposed method of entrusting quantum computing becomes an important application model for ordinary users to share quantum computing resources in the future. On basis of this, the measurement based quantum computing model includes two universal resource states - cluster state and graph state, as well as the definition and formal description of measurement modes, followed by an analysis of the basic principles of measurement-based blind quantum computing, including the construction of a universal resource state Brickwork state, blind quantum computing measurement mode, and universal blind quantum computing protocol, with a summary of different technical approaches and experimental results for the solution of the fundamental problem of measurement based blind quantum computing, as well as an inquiry into its future development direction.

Keywords：blind quantum computation；measurement mode；classical client；quantum cost

收稿日期：2024-06-20

基金项目：湖南省教育厅科学研究基金资助项目（22C0307）；湖南省教育厅教学研究基金资助项目（HNJG-2021-0130）

作者简介：李建设，男，湖南工业大学副教授，主要研究方向为网络空间安全，量子计算与量子信息，E-mail：lijianshe@hut.edu.cn

通信作者：柳闻鹃，女，湖南工业大学教授，主要研究方向为量子力学，量子计算与量子信息，E-mail：liuwenjuan@hut.edu.cn

0 引言

基于量子力学基本原理的量子计算，以量子态为信息载体，以量子态的酉演化为逻辑运算，凭借量子态相干叠加和纠缠的固有属性，使其具有内禀的并行处理能力，计算能力远超经典图灵计算模型。盲量子计算（blind quantum computation，BQC）是一种为普及量子计算而提出的类似于“云”计算模式，其目的是让量子能力有限的用户（一般称为Alice）可将计算任务委托给具通用量子能力的远程服务器（一般称为Bob），并保证用户的数据、算法和结果的隐私性[1−3]。BQC可以使用两种通用量子计算方法：基于电路的量子计算模型（circuit-based quantum computation，CBQC）[4−5]和基于测量的量子计算模型（measurement-based quantum computation，MBQC）[6−8]。BQC是量子密码学和量子计算的结合，它实现了量子计算中心（或量子服务器）计算能力的共享，为只有弱量子能力甚至没有量子能力的用户提供了一种通用量子计算的安全访问模式。

量子计算机，实现了在2^n维状态空间中通过酉变换U对n-qubit进行操作。量子计算的自然框架是标准电路模型。CBQC模型从纯量子态开始，使用一系列量子门转换量子态，最终的输出状态携带处理后的计算结果信息[9]。1-qubit酉算符和受控非门（CNOT）一起构成量子计算的一个通用门集，可实现n-qubit上的任意酉操作[10]。MBQC取决于纠缠态的制备和对qubit的测量操作。MBQC模型在理论上与量子门电路模型等价，都可实现普适的量子计算[10]。在基于电路的BQC中，通过量子电路实现盲性，客户端需要具备一些操作量子门和量子储存的能力。在基于测量的BQC中，对客户端量子能力的要求可更弱，更便于量子计算的普及。

本文拟从量子力学和计算机科学角度，阐述MBQC模型的相关理论和基于测量的BQC的基本原理。并总结不同技术路线下基于测量的BQC研究及其实验进展，探讨其未来的研究方向，希望能对目前带噪声中等规模量子（noisy intermediate-scalequantum，NISQ）时代背景[11]下的研究有所启示。

1 基于测量的量子计算模型

1.1 资源态

MBQC一般是指R. Raussendorf等[6]首次提出的单向量子计算（one-way quantum computation，1WQC）模型。该模型通过对高度纠缠的资源态进行一系列测量来完成计算任务。1WQC常用的普适资源态为量子簇态（cluster states）和量子图态（graph states）[12−14]，簇态是一种由多个qubit构成的特殊纠缠态。簇C的量子态$|\psi\rangle_C$按特定哈密顿量进行演化，可得：

$$|\psi\rangle_C=\bigotimes_{c\in C}\left(|0\rangle_c\bigotimes_{t\in T}\boldsymbol{\sigma}_Z^{c+t}+|1\rangle_c\right)。\tag{1}$$

式中：$\boldsymbol{\sigma}_Z$为泡利矩阵。

当$c+t\neq 1$时，$\boldsymbol{\sigma}_Z^{c+t}=1$，对于一维、二维和三维量子态，$T$分别为{1}、{(1, 0), (0, 1)}和{(1, 0, 0), (0, 1,0), (0, 0, 1)}，式（1）形式的量子态被称为簇态。簇态有最大关联性（maximum connectedness）和纠缠相关性（persistency of entanglement）。量子簇态的定义可推广到与图相联系的量子图态。

图态与一个无向图$G=(V, E)$相关联，其中，V为顶点，且$V=\{1, 2, \cdots, N\}$，代表qubit；E为边，且$E\subset[V]^2$，代表纠缠关系。图G的每个顶点$i\in V$对应的1-qubit，有一个与之相关的厄米算符$K_{N_G(i)}$。

$$K_{N_G(i)}\coloneqq X_i\left(\prod\nolimits_{j\in N_G(i)}Z_j\right),\ (i,j)\in E。\tag{2}$$

式中：X和Z为泡利算符；$N_G(i)$为i在G中的邻居集合；$K_{N_G(i)}$为与顶点i及其所有邻居$j\in N_G(i)$相关的qubit的可观测量。

对于任意$i\in V$，$\left\{K_{N_G(i)}\right\}_{i\in V}$定义了与顶点集$V$相关的qubit系统的可观测量的完整集合。因此它们具有一组共同特征向量集，将$K_{N_G(i)}$所有特征值等于1的公共特征向量称为与图G相关联的图态$|G\rangle$，即

$$K_{N_G(i)}|G\rangle=|G\rangle,\ i\in V。\tag{3}$$

在量子信息论中，由集合$\left\{K_{N_G(i)}\right\}_{i\in V}$生成的有限阿贝尔群$S_G=\left\langle\left\{K_{N_G(i)}\right\}_{i\in V}\right\rangle$，也称为图态$|G\rangle$的稳定子[14]。

在MBQC框架中，给定图G的资源态，执行计算的标准过程是先识别G上的两个qubit集合$\{I, O\}$。该过程中，定义了一个开放图态（open graph state）(G, I, O)，它由一个无向图$G=(V, E)$、输入I和输出O两个非空子集组成。I、$O\subseteq V$，I^c和O^c分别为V中I和O的补集。$E_G\coloneqq\prod_{(i,j)\in G}E_{ij}$为与$G$关联的全局纠缠操作。

1.2 测量模式

在MBQC模型中，计算可以分为如下3个阶段：1）qubit的制备和纠缠，构造计算所需要的资源态；2）1-qubit测量，利用纠缠的特性以测量引起量子态的塌缩，使后面qubit状态发生变化，测量将引起

非确定性；3）为获得确定性结果，对测量引起的非确定性进行相关修正。MBQC 模型中，计算涉及的命令有[1,15−16]：1-qubit 制备 N_i^{α}、2-qubit 纠缠操作 $E_{ij}=C_Z(i,j)$、1-qubit 测量 M_i^{θ} 和 1-qubit 泡利修正 X_i、Z_i，其中 i、j 表示操作使用的 qubit，参数 α、$\theta\in[0,2\pi]$。具体地说，制备 N_i^{α} 定义为制备状态为 $|+_{\alpha}\rangle_i$ 的 qubit i，且 $|\pm_{\alpha}\rangle=\left(|0\rangle\pm \mathrm{e}^{\mathrm{i}\alpha}|1\rangle\right)/\sqrt{2}$。测量 M_i^{θ} 定义为应用于 qubit i 的正交投影 $|\pm_{\theta}\rangle\langle\pm_{\theta}|_i$，投影测量结果记为 S_i，$|+_{\theta}\rangle\langle+_{\theta}|_i$ 测量结果为 0，$|-_{\theta}\rangle\langle-_{\theta}|_i$ 测量结果为 1，测量结果求和 $s=\sum_{i\in I}s_i$。泡利算符 X_i^s 和 Z_i^s 控制不确定性相关修正。

定义 1　测量模式（measurement pattern）MBQC 模型中的测量模式，由与其相关联的开放图态（G, I, O）、流 $(f,\succ)$（符号$\succ$为部分序 partial order，$j\succ i$ 表示 qubit i 的测量优先于 qubit j）以及 Bloch 球的 X−Y 平面上的测量角度集 $\{\theta_i\}_{i\in O^c}$ 给出。

开放图态（G, I, O）给出了所包含的 qubit 集合 V 及它们的纠缠方式 E_G、输入 qubit 集合 I 和输出 qubit 集合 O。要完成模式定义，还需要确定 I^c 中 qubit 制备的角度（一般在制备时取 0 或随机选取）和 O^c 中 qubit 的测量角度，以及获得确定性结果所需要的相关修正。为此引入流（flow）的概念[16−20]。

定义 2　流　给定开放图态（G, I, O），如果存在函数 $f:O^c\to I^c$ 以及在 V 上的部分序$\succ$，使得对于任意 $i\in O^c$，以下条件都成立，则该图态存在流 $(f,\succ)$：1）$(i,f(i))\in G$；2）$f(i)\succ i$；3）对于 $f(i)$，除 i 以外的所有邻域 $\left(k\in N_G\left(f(i)\right)\backslash\{i\}\right)$，总有 $k\succ i$。

可见，流由两个结构组成：顶点上的函数 f 和与顶点相关的部分序$\succ$。具有流的图态的测量模式中确定性所需的相关修正由函数 f 来定义，命令的执行顺序由流引起的部分序$\succ$给出。测量模式的执行需要函数 f 和部分序$\succ$之间的相互配合。

对于有效经典算法$\mathcal{A}$，以开放图态（G, I, O）描述实现算法$\mathcal{A}$的某一量子电路 U，$(f,\succ)$ 是对应的流。M_i^{θ} 为非输出 qubit $i\in O^c$ 上的投影测量基，测量角度 θ_i 与图态结构及量子电路 U 有关。将实现图态的量子电路 U 分解为 $U=U_nU_{n-1}\cdots U_1$，其中 $U_i\in\mathbb{U}$，$\mathbb{U}$为任意通用门集，则可以输出关于图态上的全部测量角度 $\{\theta_i\}_{i\in O^c}$。对于能够实现任何量子电路的通用图态（universal graph state）[1, 21−22]，$\{\theta_i\}_{i\in O^c}$ 可以被看作是仅与量子电路 U 相关，即仅由 $\mathcal{A}_G\left(U_nU_{n-1}\cdots U_1\right)$ 便可推算出 $\{\theta_i\}_{i\in O^c}$。定理 1 给出了图态测量模式的形式化描述。

定理 1　设开放图态（G, I, O）存在流 $(f,\succ)$，则测量模式

$$\mathcal{M}_{f,G,\succ,\theta}:=\prod_{i\in O^c}^{\succ}\left(X_{f(i)}^{s_i}\prod_{k\in N_G(f(i))\backslash\{i\}}Z_k^{s_i}M_i^{\theta_i}\right)E_GN_{I^c}^0 \quad (4)$$

是可运行的，并且是一致和强确定性的[16]，其酉嵌入为

$$U_{G,I,O,\theta}:=\left(\prod_{i\in O^c}\langle+_{\theta_i}|_i\right)E_GN_{I^c}^0。$$

式（4）中：$s_i\in\{0,1\}$ 为 qubit i 测量的经典结果；$X_{f(i)}^{s_i}\prod_{k\in N_G(f(i))\backslash\{i\}}Z_k^{s_i}$ 为 qubit i 测量后需要执行的修正操作；$N_{I^c}^0=\left(\prod_{i\in I^c}|+_0\rangle_i\right)$；$E_G=\left(\prod_{(i,j)\in E}CZ_{i,j}\right)$。

下面给出简单的证明，由顶点 i 的图稳定子定义式（3），有以下关系：

$$K_{N_G(i)}E_GN_{I^c}^0=E_GN_{I^c}^0,$$

利用 $\langle+_{\theta}|_i=M_i^{\theta}Z_i^{s_i}$ 得

$$\mathcal{M}_{f,G,\succ,\theta}:=\prod_{i\in O^c}^{\succ}\left(M_i^{\theta_i}Z_k^{s_i}K_{N_G(f(i))}^{s_i}\right)E_GN_{I^c}^0,$$

再由式（2），得式（4）。

对于测量角度 $\{\theta_i\}_{i\in O^c}$，根据测量的等价性得修正的测量角为

$$\theta_i'=(-1)^{s_{f^{-1}(i)}}\theta_i+\sum_{\substack{j:f(j)\in N_G(i)\\(j\neq i)}}s_j\pi。\quad (5)$$

式中：$f^{-1}(i)$ 是 $f(i)$ 的逆，即如果 $f(i)=j$，则 $f^{-1}(j)=i$，对于 $i\in I$，$s_{f^{-1}(i)}=0$。

2　基于测量的 BQC 基本原理

将要执行的计算任务委托给具有通用量子计算能力的服务器，这种委托要求服务器执行盲计算。也就是说，除了图 $G=(V,E)$、输出集 O 和流 $(f,\succ)$ 确定测量顺序外，服务器不应知道有关计算的任何其他信息。为此，A. Broadbent 等[1]在 MBQC 框架基础上提出了第一个通用的盲量子计算（universal blind quantum computation，UBQC）协议，也称 BFK 协议。协议中 Alice 将量子计算委托给一个远程服务器 Bob，服务器制备多 qubit 高度纠缠的通用图态 Brickwork 态为资源态，通过执行一系列测量和修正实现 BQC，且保证了 Alice 的输入、输出及算法隐私，同时客户端还可检测服务器是否诚实地执行了所请求的计算任务。

2.1　Brickwork 态构造

Brickwork 态是一种将 qubit 按照一定规则进行纠缠的特殊图态（见图 1）。具体的构造方法由定

义 3 给出。

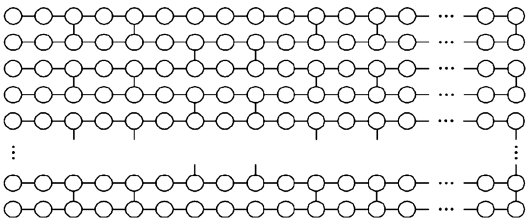

图 1 Brickwork 态 $\mathcal{G}_{n\times m}$

Fig. 1 Brickwork state $\mathcal{G}_{n\times m}$

定义 3 Brickwork 态 一个 Brickwork 态 $\mathcal{G}_{n\times m}$ 是按如下方式由 $n\times m$ 个 qubit 构造的多粒子纠缠态，其中 $m\equiv 5\ (\mathrm{mod}\ 8)$。

1）制备量子态为 $|+\rangle$ 的所有 qubit，给每一个 qubit 分配一个索引（i,j），其中 i 为行（$i\in[n]$），j 为列（$j\in[m]$）。

2）对于每一行，在 qubit（i,j）和（i,j+1）之间应用受控 Z 门操作，其中 $1\leqslant j\leqslant m-1$。

3）对于每一列 $j\equiv 3\ (\mathrm{mod}\ 8)$ 和每一个奇数行 i，在 qubit（i, j）和（i+1, j）之间以及（i, j+2）和（i+1, j+2）之间应用受控 Z 门操作。

4）对于每一列 $j\equiv 7\ (\mathrm{mod}\ 8)$ 和每一个偶数行 i，在 qubit（i, j）和（i+1, j）之间以及（i, j+2）和（i+1, j+2）之间应用受控 Z 门操作。

在图 1 所示的 Brickwork 态 $\mathcal{G}_{n\times m}$ 中，qubit $|\psi\rangle_{x,y}$ $(x=1,2,\cdots,n,\ y=1,2,\cdots,m)$ 按照 x 行和 y 列排列，与图中顶点对应，最初处于 $|+\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)$ 状态。再由边连接的 qubit 之间执行受控 Z 门操作。Brickwork 态对 BQC 是通用的。量子计算中任意希尔伯特空间的酉变换可通过通用逻辑门集为 {*CNOT*, *H*, π/8} 的操作组合实现 [10]。图 2 中的测量模式和基础图态隐含了为保证确定性的流给出的修正，测量可逐列进行。通用逻辑门集中任意量子门的测量模式具有相同的基础图态（underlying graph state），都包含了 10 个 qubit，具相同位置纠缠连接，称为 brick，如图 2a~e 所示 [23−26]。实现通用门集中每个 brick 的前 3 个 qubit 按照图 2a 所示旋转操作进行测量。由于受控 Z 门和相位旋转门 $R_Z(\alpha)$ 是对易的，且量子门是自可逆的，因此图 2b~d 中给出的每个门的测量模式与相应的量子电路都是等价的。通过分配具体测量角度，可得单位门、π/8 门和 Hadamard 门 [27−28]。图 2e 给出了 2-qubit 的 *CNOT* 门量子电路与测量模式的等价关系，根据图中量子电路，等价性验证过程如下：

$$CZR_X(0)HR_Z\left(\frac{\pi}{4}\right)H\otimes R_X\left(-\frac{\pi}{4}\right)HR_Z(0)HCZR_X(0)HR_Z(0)H\otimes R_X\left(\frac{\pi}{4}\right)HR_Z(0)H=$$

$$CZHR_Z\left(\frac{\pi}{4}\right)H\otimes HR_Z\left(-\frac{\pi}{4}\right)HCZHH\otimes HR_Z\left(\frac{\pi}{4}\right)H=CZI\otimes R_X\left(-\frac{\pi}{4}\right)CZR_Z\left(\frac{\pi}{4}\right)\otimes R_X\left(\frac{\pi}{4}\right)=CNOT。$$

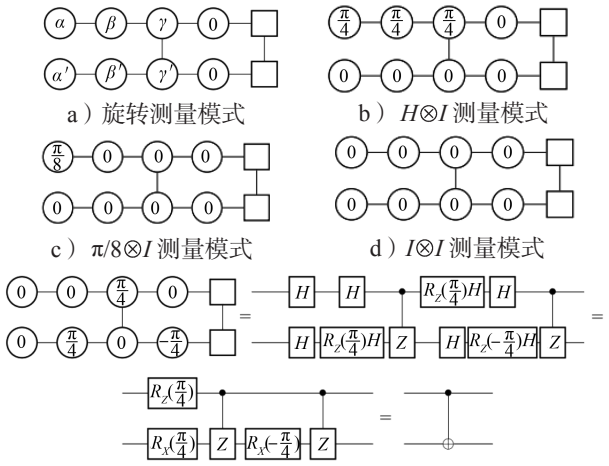

图 2 通用逻辑门集测量模式

Fig. 2 Measurement pattern for universal logic gate set

通用逻辑门集中的量子门测量模式的拼接可实现任意的量子电路。图 3 给出了如何在 Brickwork 态 $\mathcal{G}_{9,4}$ 上实现含有 3 个量子门 U_1、U_2 和 U_3 的 4-qubit 电路。量子电路中的逻辑线用单位门的测量模式实现。通过推广该技术，可得图 1 定义的 Brickwork 态族。由此可知，任何量子门都可用一系列通用逻辑门集 $\mathbb{U}$ 中量子门构造，任意量子电路都可由 brick 拼接方式实现。因此，Brickwork 态可作为基于测量的 BQC 中通用资源态。另外，实现不同逻辑门的 brick 具相同的 qubit 数和纠缠结构，所以服务器无法区分它们，这样用户想实现的电路对服务器来说是隐藏的 [28−29]。

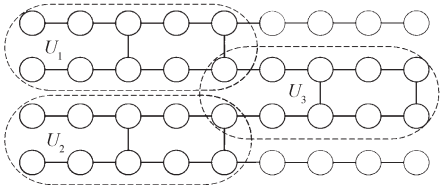

图 3 3 个门的 4-qubit 电路的平铺法

Fig. 3 Tiling method for a 4-qubit circuit with three gates

2.2 测量模式

在基于测量的 BQC 中，测量模式是指服务器端在资源态上的测量模式，根据 MBQC 模型可知，其测量模式为 $\langle(G,I,O),(f\succ),\{\theta_i\}_{i\in O^c}\rangle$，由客户端给

出。客户端将图的描述 G、I、O 和流 $(f, \succ)$ 确定的测量顺序发送给服务器，然后制备并发送构造资源态所需的 qubit 给服务器，服务器利用收到的 G、I、O 和测量顺序及 qubit，构造计算所需的 Brickwork 态。

在 Brickwork 态中，最左侧的一列表示输入 qubit 集合 I，最右侧的一列表示输出 qubit 集合 O，而中间部分表示非输入非输出 qubit 集合 $I^c \cap O^c$。测量顺序由左至右逐列进行，且可对每列 n 个 qubit 同时进行测量。测量顺序的流可定义为

$f:\{1,2,\cdots,n\}\times\{1,2,\cdots,m-1\}\to\{1,2,\cdots,n\}\times\{2,3,\cdots,m\}$。

具体地，对于 Brickwork 上每个在 X-Y 平面的任意一个非输出 qubit (x, y)，有 $f(x, y)=(x, y+1)$，其中 $x\in\{1, 2, \cdots, n\}$，$y\in\{1, 2, \cdots, m-1\}$，而 $f^{-1}(x, y)=(x, y-1)$。每个非输出 qubit $(x, y)\in O^c$ 上都有一测量角度为 $\theta_{x,y}$、一泡利算符 X 依赖的集合 $D^X_{x,y}$（$D^X_{x,y}=f^{-1}(x, y)$）和一 Z 依赖的集合 $D^Z_{x,y}$（$D^Z_{x,y}=\{(u,v):(x,y)\in N_G(f(u,v))\}$，且 $(u, v)\neq(x, y)$。每个 qubit 的实际测量角度 $\theta'_{x,y}$ 是 $\theta_{x,y}$ 的修正结果，取决于先前 qubit 的测量结果。令 $s^X_{x,y}=\oplus_{(x,y)\in D^X_{x,y}} s_{x,y}$、$s^Z_{x,y}=\oplus_{(x,y)\in D^Z_{x,y}} s_{x,y}$ 分别为 $D^X_{x,y}$、$D^Z_{x,y}$ 中所有 qubit 测量结果模 2 加，则由式（5）知，实际测量角度 $\theta'_{x,y}=(-1)^{s^X_{x,y}}\theta_{x,y}+s^Z_{x,y}\pi$。服务器由此可从 $\theta'_{x,y}$ 和相关测量结果推算出 $\theta_{x,y}$。为保证委托计算对服务器是盲的，客户端需将所有修正测量角度及测量结果 $\{\theta'_{x,y},\ s_{x,y}\}_{(x,y)\in O^C}$ 进行加密。

为加密修正测量角度，构造 Brickwork 态时，客户端制备的每个 qubit 的状态 $|+_\alpha\rangle$ 是随机的，其中 $\alpha\in\Theta$，$\Theta=\{k\pi/4\}_{k\in\{0,1,\cdots,7\}}$。由于 $|+_\alpha\rangle\equiv R_Z(\alpha)|+\rangle$ 且 $R_Z(\alpha)$ 与受控 Z 门对易，$|+_\alpha\rangle$ 的制备也可由客户端先制备状态 $|+\rangle$，并发送给服务器，服务器按照定义 3 构造 Brickwork 态，再对每个 qubit 执行随机的 Z 旋转算符。另外，引入了随机比特 $r_{x,y}\in\{0, 1\}$ 加密测量结果 $b_{x,y}$，即 $s_{x,y}=b_{x,y}\otimes r_{x,y}$，服务器每个非输出 qubit $(x, y)\in O^c$ 上的测量角度调整为

$$\delta_{x,y}=\theta'_{x,y}+\alpha_{x,y}+r_{x,y}\pi=(-1)^{s^X_{x,y}}\theta_{x,y}+\alpha_{x,y}+(s^Z_{x,y}+r_{x,y})\pi,\quad(6)$$

这样，服务器从所得到测量角度 $\delta_{x,y}$ 就无法推算出测量模式中的真实测量角度和测量结果了。

2.3　UBQC 协议

使用量子输入和量子输出的 UBQC 协议，输入 qubit 存放在寄存器中。为使资源态中所有 qubit 的测量角度都加密，Alice 将输入 qubit 先加密然后发送给 Bob。计算结束时，Bob 将最后一列的 qubit 发送给 Alice，Alice 执行泡利修正，从而完成量子输出。

客户端输入：一个 $\langle((G,I,O),(f,\succ),\{\theta_i\}_{i\in O^c}\rangle$ 测量模式和一个包含输入 qubit $i\in I$ 的量子寄存器。

1）Alice 发送图的描述 G、I、O 和测量顺序给 Bob；

2）Alice 制备并且发送所有在 $O^c\cup I$ 中的 qubit 给 Bob：

①对于 $i\in I$，它选择一个随机比特 $a_i\in\{0, 1\}$ 和一个随机的 $\alpha_i\in\Theta$，将 $R_Z(\alpha_i)X^{a_i}$ 应用到 qubit i 上并发送给 Bob；

②对于 $i\in I^c$，它随机选择一个 $\alpha_i\in\Theta$，制备 $|+_{\alpha_i}\rangle$ 并发送给 Bob；

3）如果（I, j）是 G 的边，则 Bob 在 qubit（I, j）之间应用受控 Z 门；

4）对于所有 $i\in O^c$，Alice 按照流 $(f, \succ)$ 指定的顺序，计算出测量角度 δ_i，并发送给 Bob，Bob 使用测量基 $|\pm\delta_i\rangle$ 测量 qubit i 并将测量结果 $b_i\in\{0, 1\}$ 发给 Alice。

$$s_i=b_i\oplus r_i,\quad s'^X_i=\bigoplus_{j\in D^X_i}s_j\oplus a_i,\quad s'^Z_i=\bigoplus_{j\in D^Z_i}s_j\oplus a_{f^{-1}(i)}。$$

式中，D^X_i（或 D^Z_i）是 qubit i 的 X（或 Z）依赖集合，且 $D^X_i=f^{-1}(i)$，$D^Z_i=\{j:i\in N_G(f(j))\}$。

由此可得实际的测量角度为

$$\theta'_i=(-1)^{s'^X_i}\theta_i+s^Z_i\pi,$$

$$\delta_i=\theta'_i+\alpha_i+r_i\pi=(-1)^{s'^X_i}\theta_i+\alpha_i+(s^Z_i+r)\pi,$$

式中，r_i 由 Alice 随机选取，且 $r_i\in\{0, 1\}$；

5）Bob 返回输出 qubit $i\in O$；

6）Alice 对接收到的 qubit $i\in O$，应用 $Z^{s'^Z_i}X^{s'^X_i}$。

协议主要分为 2 个阶段：准备阶段和交互测量阶段。1）准备阶段。Alice 需要将存储在量子寄存器中的输入 qubit $i\in I$ 应用泡利算符 X 和旋转算符 $R_Z(\alpha)$ 进行量子一次一密加密[1, 30-32]并发给 Bob；同时，Alice 还需要制备 I^c 中的所有 1-qubit 发给服务器，Bob 根据图 G 构造一个 Brickwork 态，后续测量在 Brickwork 态上进行。2）交互测量阶段。Alice 驱使 Bob 依据测量模式对 Brickwork 态中 qubit $(x, y)\in O^c$ 进行测量，并将最后一列的 qubit 发给 Alice，由 Alice 对接收到的 qubit 进行泡利修正以完成量子计算。

量子输入输出 UBQC 协议要求客户端必须至少具有制备 qubit、执行泡利算符 X 和 Z 及访问双向量子信道的量子能力。这个协议还可改为使用经典输入

和输出，此时客户端仅需具制备 qubit 及访问客户到服务器的单向量子信道的量子能力。在使用经典输入时，如果协议要实现酉算符 U 的 BQC，Alice 可将计算的输入 qubit $i\in I$ 内置在 U 中。由于服务器端构造资源态时会将其放在第一列，这样，客户端可通过输入与 U 的第一列相关的经典测量角度实现量子输入。使用经典输出时，服务器会对最后一列 qubit 进行测量，并将得到的经典结果返回给客户端，客户端不需对最后一列执行泡利修正，仅需解密就可得到结果。

3 基于测量的 BQC 研究进展

使用基于测量的 BQC 的目的是为普通用户提供高性能量子计算服务，解决经典计算机难以处理的某些 NP 问题 [33−36]。近年来，量子计算技术发展迅速，基于测量的 BQC 从理论研究到实验进行了多方面研究。特别是对于 BQC 协议中的两个根本问题，即如何降低对普通用户量子能力的要求及减少计算所需量子资源、降低量子成本，展开了深入研究。

3.1 降低对客户端量子能力要求

3.1.1 单服务器的 UBQC

为降低对客户端量子能力的要求，从客户端的角度，基于测量的 UBQC 先后出现了 3 种模式：一是由 A. Broadbent 等 [1] 提出的最早的 UBQC 协议，协议中客户端需要具有制备单 qubit 和访问单向量子信道的能力。二是 T. Morimae 等 [37−39] 提出的客户端仅需要执行特定 1-qubit 测量的仅测量的 BQC 模式（the measurement-only BQC model，MOBQC）。在量子光学系统中，Alice 通过使用阈值检测器，对单光子状态进行偏振测量来实现计算。相比单光子 qubit 的产生，测量其状态要容易得多，这使 Alice 的设备能够更加经典。协议首先让 Bob 准备一个基于测量的量子计算的资源态；然后 Bob 通过量子信道向 Alice 发送一个资源态的 qubit；最后，Alice 以某一角度测量 qubit，该角度由计算任务确定的算法决定。重复后面两步直到计算完成。三是 Li Q. 等 [40] 提出的一种客户端只需具备执行 1-qubit 门的 UBQC 协议。协议中 Bob 先向 Alice 发送 m+k+l 个处于计算基矢态 $|0\rangle$的 qubit，Alice 选择其中 m 个用于计算，其余 k+l 个 qubit 分别用于诱饵和陷阱以实现协议的安全和验证。Alice 再对用于计算的 m 个 qubit 执行 H 门操作，然后作用 n 次 $\sigma_z^{1/4}$ 门（其中 n 随机地从 {0, 1, ⋯, 7} 中选择，使 qubit 的状态为 $\left(|0\rangle\pm \mathrm{e}^{in\pi/4}|1\rangle\right)/\sqrt{2}$），并发回给 Bob，Bob 收到这些 qubit 后，执行与 BFK 协议相同的步骤构造计算所需 Brickwork 态，并完成后面操作。与前两种模式相比，由于单 qubit 门是这些模式中最精确的操作，因此它更适合在一些实验装置中实施，例如离子阱和超导系统中。

3.1.2 多服务器的 UBQC

从降低客户端所需要的量子能力这一研究思路出发，出现了一些多服务器协议。例如 T. Morimae 等 [41−42] 提出了双服务器 UBQC 协议，该协议引入可信中心制备并且分发 Bell 态，可信中心制备 m 个 Bell 态 $\otimes_{i=1}^{m}\left|\psi_{z_i,x_i}\right\rangle$（其中，$\left|\psi_{z_i,x_i}\right\rangle\equiv\left(I\otimes X^{x_i}Z^{z_i}\right)\left(|0\rangle|0\rangle+|1\rangle|1\rangle\right)/\sqrt{2}$，$\{z_i,x_i\}\in\{0,1\}^2$），并将每个 Bell 态的两个 qubit 分发给 Bob1 和 Bob2。Alice 发送经典信息 $\left\{\theta'\equiv(-1)^{x_i}\theta_i+z_i\pi\right\}_{i=1}^{m}$ 给 Bob1（其中 $\theta_i\in\Theta$ 是随机产生的）。Bob1 使用基 $\left\{\left|\pm\theta_i'\right\rangle\right\}_{i=1}^{m}$ 测量它的第 i 个 Bell 态，并将结果 $\{b_i\}_{i=1}^{m}\in\{0,1\}$ 发送给 Alice。此时 Bob2 所拥有的对应部分量子态将变为 $\otimes_{i=1}^{m}\left|\theta_i+b_i\pi\right\rangle$，形成计算所需要的资源态。Alice 用 $\{\theta_i+b_i\pi\}_{i=1}^{m}\in\{0,1\}$ 代替 $\{\theta_i\}_{i=1}^{m}\in\{0,1\}$，与 Bob2 执行 BFK 协议后的操作。协议使客户端可以完全经典，但要求两个服务器间不能通信，降低了协议的可用性。

Li Q. 等 [43−44] 基于纠缠交换思想，设计出三服务器 UBQC 协议，可信中心制备 2n 个 Bell 态 $\left|\psi_{0,0}\left(B1_k,A_k\right)\right\rangle$ $(k=1,2,\cdots,n)$ 和 $\left|\psi_{0,0}\left(B2_l,A_l'\right)\right\rangle(l=1,2,\cdots,n)$，并将其中 n 个 Bell 态的第一个 qubit 发送给 Bob1，将另外 n 个 Bell 态的第一个 qubit 发送给 Bob2，将这 2n 个 Bell 态的第二个 qubit 都发给 Alice，Alice 随机地转发其中 2m 个 qubit 给 Bob3。Alice 请求 Bob3 在 2m 个 qubit $\left\{A_{s_i}\right\}_{i=1}^{m}$ 和 $\left\{A_{t_i}'\right\}_{i=1}^{m}$ 中指定 qubit 对 A_{s_i} 和 A_{t_i}'（其中 $i\in\{1,2,\cdots,m\}$）进行 Bell 测量，并将结果 $\left(z_{s_i}',x_{s_i}'\right)\in\{0,1\}$ 发送给 Alice，依据纠缠交换原理，此时与 A_{s_i} 和 A_{t_i}' 对应的 $B1_{s_i}$ 和 $B2_{t_i}$ 的联合状态为 $\left|\psi_{z_{s_i},x_{s_i}}\left(B1_{s_i},B2_{t_i}\right)\right\rangle$。Alice 以收到的测量结果计算测量角度 $\left\{\theta'=(-1)^{x_k}\theta_k+Z_k\pi\right\}_{k=1}^{n}$（其中 $k\in\{1,2,\cdots,n\}-\{s_1,s_2,\cdots,s_m\}$，$\theta_k\in\Theta$，$\left(z_{s_i},x_{s_i}\right)\in\{0,1\}$）并发给 Bob1，Bob1 使用基 $\left|\pm\theta_i'\right\rangle$ 对其 qubit 进行测量，并将测量结果 $\{b_k\}_{k=1}^{n}$ 发给 Alice。Bob1 测量结束后，Bob2 的 qubit 状态为 $\otimes_{i=1}^{m}\left|\theta_i+b_i\pi\right\rangle$，构造出计算所需的 Brickwork 态。之后，Alice 用 θ_i+$b_i\pi$ 代替 θ_i，与 Bob2 执行 BKF 协议的交互测量阶段，协议中客户端

只需要具备访问量子信道的能力。显然 3 个服务器之间能够相互通信，但该协议存在安全漏洞 [45]。

为此，Xu H. R. 等 [46] 优化了三服务器协议，提出了单服务器经典客户端 UBQC 协议。可信中心制备 $2n$ 个 Bell 态 $\left|\psi_{0,0}\left(B_k, A_k\right)\right\rangle (k=1,2,\cdots,2n)$，并将每个 Bell 态的第一个 qubit B_k 发送给 Bob，第二个 qubit A_k 发送给 Alice。Alice 从中随机选出 $2m$ 个传给 Bob，Bob 对接收到的 $2m$ 个 qubit 按 Alice 指定的 qubit 对 A_{s_i} 和 A_{t_j}（$i, j \in \{1, 2, \cdots, m\}$）逐一进行 Bell 测量，并将测量结果 $\left(z'_{s_i}, x'_{t_j}\right) \in \{0,1\}^2$ 发送给 Alice。测量后 Bob 原本分别与 A_{s_i} 和 A_{t_j} 纠缠的 qubit 形成联合态 $\left|\psi_{z_{s_i},\, x_{t_j}}\left(B_{s_i}, B_{t_j}\right)\right\rangle$。Alice 依据收到的测量结果计算测量角度 $\left\{\theta'_k=(-1)^{x_k}\theta_{s_i}+z_k\pi\right\}_{k=1}^{n}$ 并发给 Bob，其中 $k \in \{1, 2, \cdots, n\}-\{s_1, s_2, \cdots, s_m\}$，$\theta_{s_i} \in \Theta$，$\left(z_k, x_k\right) \in \{0,1\}$，$\left(z_k, x_k\right)$ 是依据上一步 $\left(z_{s_i}, x_{s_j}\right)$ 的值。Bob 使用基 $\left|\pm\theta'_i\right\rangle$ 测量从可信中心收到的 n 个 qubit B_k，并将结果 $\{b_k\}_{k=1}^{n}$ 发给 Alice。至此 Bob 拥有的 qubit 的状态为 $\otimes_{i=1}^{m}\left|\theta_i+b_i\pi\right\rangle$，构造出计算所需的 Brickwork 态。之后，Alice 用 $\theta_i+b_i\pi$ 代替 θ_i，与 Bob 执行 BFK 协议。

上述这些协议或者需要多个服务器，或者需要第三方可信中心，这就增加了 UBQC 的量子成本和安全风险，降低了协议的可用性。

3.2　减少量子成本

基于测量的 UBQC 使用多 qubit 纠缠态完成计算任务。随着计算规模增大，纠缠态数量成倍增长，量子成本大幅增加。BFK 协议是解决盲量子计算问题的技术要求最低的方案之一 [1, 21]，该协议在量子光学环境中已得到了实验验证 [47]。然而，问题在于该协议是否最优，即是否有可能利用更少的资源完成计算任务。为此，A. Mantri 等 [48] 给出了确定执行 BQC 所需资源范围的通用方法，并证明当客户端仅具有制备 1-qubit 能力时，BFK 协议在最优值的 8/3 倍以内。

Zhang X. Q. 等 [49] 提出了一种基于小资源的 UBQC 协议，通过优化实现通用门集的簇态，将 10 qubit 的标准 brick 减少为 6~8 qubit，从而降低了构建 brickwork 态的 qubit 数量。Yang Z. 等 [50] 提出利用服务器的量子能力来降低客户端量子成本的方案，计算过程中，通过增加服务器执行量子门 T 或 H 操作，减少了实现量子门中 qubit 的个数，进而使客户端制备的 qubit 数目比标准 brick 所需的 10 个 qubit 降低近 40%，同时也减少了构造资源态所需量子资源。严玉瞻等 [51] 提出了实系数输入和复系数输入的 1-qubit BQC 协议，协议中利用纠缠态由 8-qubit 簇态构造实现了通用 1-qubit 门集 H 和 T。与已有的 MOBQC 协议相比，大幅降低了客户端的量子成本和委托成本。由图 2 可知，在 Brickwork 态中实现单 qubit 基本门平均需消耗 4 个辅助 qubit，另外，由于 Brickwork 态的具体结构是固定的，实际需要的辅助 qubit 数要远大于此。Ma S. Q. 等 [52] 利用断裂（break）和桥接（bridge）量子操作等技术，使 Brickwork 态的结构不再固定，有效减少了辅助 qubit 的消耗。具体地，构建了 3 种改进的 Brickwork 状态，可以不同程度地减少 qubit 开销。第一种改进的 Brickwork 态，即方形 Brickwork 态（square brickwork state），它比原始 Brickwork 态减少约一半的辅助 qubit 消耗。第二种改进是方形 Brickwork 态的一种变体，即超 Brickwork 态（hyper brickwork state），它使得在实现不相邻的 2-qubit 门时辅助 qubit 的消耗可以大幅减少。最后一种改进是方形 Brickwork 态的进一步变体，即环形 Brickwork 态（circular brickwork state），它利用三维空间特性，有效降低了 Brickwork 态的构造难度，同时进一步减少了辅助 qubit 开销。

3.3　实验进展

除了基于测量的 BQC 的理论研究外，在实验室环境下的演示性实验也取得了突破性进展 [53−57]。利用光子和热态（thermal state）等已实现了 MBQC 的实验验证和演示 [58−62]。在此基础上，S. Barz 等 [53] 利用 MBQC 模型，首次验证了客户端将计算委托给量子服务器的可行性，演示了在客户端只需要制备并传输单个光子 qubit 的情况下，通过生成的 4-qubit 簇态族，实现 1-qubit 和 2-qubit 量子逻辑门的通用门集以及 Deutsch 与 Grover 算法，这对 UBQC 协议的发展具有里程碑意义。S. Barz 等 [54] 还进行了可验证 UBQC 的首次实验验证，实验中客户端仅具有生成单个 qubit 并传输到量子计算机的能力。通过 4 个光子 qubit 簇态演示了客户端测试服务器执行 MBQC 的能力以及验证计算的过程。C. Greganti 等 [55] 通过实验验证了 MOBQC 的原理，利用光子生成 4-qubit 线型和星型簇态进行计算并验证。客户端可行的技术要求和与设备无关的盲性使得该方案非常适用于未来的安全量子网络，协议向更现实的安全量子计算模型又迈进了一步。Huang H. L. 等 [56] 为完全经典的客户端实施了 BQC 原理实验验证。通过实验证明了通过两个量子服务器之间共享 3 个 EPR（Einstein Podolsky Rosen）态，利用可验证 BQC 框架，采用量子隐形传态计算模型实现了求解 N=15 的 Shor 算法，结合

CHSH（Clauser-Horne Shimony-Holt）[63-64] 和稳定子测试 [65-66] 进行验证，提供了一种经典客户端委托量子服务器执行可验证 BQC 的方法，这对安全的云量子计算具有重要意义。P. Drmota 等 [57] 首次使用混合物－光子实现了基于测量的可验证 BQC，实验在以 $^{43}Ca^{+}$ 作为资源态 qubit 实现的离子阱量子服务器中，通过基于 $^{88}Sr^{+}$ 单光子接口，与仅具单光子偏振测量的光子探测系统的客户端，建立光纤量子链路。在该光子接口离子阱量子信息平台上，由于服务器中量子逻辑操作的确定性，且与客户端交互是预先的，消除了对后选择（post-selection）[67] 的需要，这不仅提高了工作效率，还实现了服务器对计算规模的可扩展性。为将量子计算从具有最小量子资源的客户端，安全委托给完全有能力但是不可信的量子服务器铺平了道路。

4 基于测量的 BQC 研究展望

目前，对于无第三方的单服务器协议，从客户端量子能力来看，总需要具有制备、测量或者执行逻辑门 3 种量子能力之一才能实现 UBQC，而多服务器或需要可信中心的协议，这会使协议由于过于复杂而存在安全或者可用性等问题，同时也增加了量子成本。因此，构建无第三方参与的经典客户端单服务器 UBQC 协议的方案成为重要的探究目标。A. Mantri 等 [68] 证明了利用 MBQC 模型中流模糊性可以构建一个无第三方、客户端完全经典的单一量子服务器的 BQC 协议。这里流模糊性的含义是指对于一个固定的图态，存在输入和输出顶点集的多种选择，这些选择会导致与相同的固定顶点排序一致的确定性测量模式。这样，仅具有计算测量角度能力的经典用户，就可以驱动远程量子服务器来执行基于测量的量子计算，同时隐藏计算的关键环节，从而实现盲性。但是利用流模糊效应能否隐藏一组通用计算以实现 UBQC，并且完成对服务器的验证，还有待进一步研究。同时，通过对 MBQC 模型计算过程的深入研究，挖掘其他的构造无第三方经典客户端的单服务器 UBQC 方案也是一个值得探讨的问题。总之，我们期待将来的研究能够消除客户端和服务器之间的量子信道，使客户端完全经典，并且在不需要可信中心的情况下实现 UBQC。

另外，探究将服务器强大的通用量子计算能力与 Brickwork 态的结构特征相结合，通过改造优化 Brickwork 态结构，以进一步减少用户 qubit 的资源开销，使得 BQC 所需要量子成本更低，也是一个值得研究的方向。

参考文献：

[1] BROADBENT A，FITZSIMONS J，KASHEFI E. Universal Blind Quantum Computation[C]//2009 50th Annual IEEE Symposium on Foundations of Computer Science. Atlanta：IEEE，2009：517-526.

[2] ARRIGHI P，SALVAIL L. Blind Quantum Computation[J]. International Journal of Quantum Information，2006，4(5)：883-898.

[3] AHARONOV D，BEN-OR M，EBAN E. Interactive Proofs for Quantum Computations[J/OL]. Quantum Physics. (2017-04-14)［2024-07-28］. https://doi.org/10.48550/arXiv. 1704.04487.

[4] BARENCO A，BENNETT C H，CLEVE R，et al. Elementary Gates for Quantum Computation[J]. Physical Review A，1995，52(5)：3457-3467.

[5] CHILDS A M. Secure Assisted Quantum Computation[J]. Quantum Information and Computation，2005，5(6)：456-466.

[6] RAUSSENDORF R，BRIEGEL H J. A One-Way Quantum Computer[J]. Physical Review Letters，2001，86(22)：5188-5191.

[7] BROADBENT A，FITZSIMONS J，KASHEFI E. Measurement-Based and Universal Blind Quantum Computation [EB/OL].（2010-06-21）[2024-06-20]. https:// DOI:10.1007/978-3-642-13678-8_2, 2010.

[8] MORIMAE T，FUJII K. Blind Topological Measurement-Based Quantum Computation[J]. Nature Communications，2012，3：1036.

[9] WEI T C. Measurement-Based Quantum Computation[J/OL]. Oxford Research Encyclopedia of Physics. (2021-09-21) [2024-07- 28]. https://doi.org/10. 1093/acrefore/9780190871994. 013.31.

[10] NIELSEN M A，CHUANG I L. Quantum Computation and Quantum Information[M]. Cambridge：Cambridge University Press，2012：56-62.

[11] PRESKILL J. Quantum Computing in the NISQ Era and Beyond[J]. Quantum，2018，2：79.

[12] HEIN M，DÜR W，EISERT J，et al. Entanglement in Graph States and Its Applications[J/OL]. Quantum Physics. (2006-02-11) [2024-07-28]. https://doi.org/10.48550/arXiv. quant-ph/0602096.

[13] RAUSSENDORF R，BROWNE D E，BRIEGEL H J. Measurement-Based Quantum Computation on Cluster States[J]. Physical Review A，2003，68(2)：022312.

[14] HEIN M，EISERT J，BRIEGEL H J. Multiparty Entanglement in Graph States[J]. Physical Review A，2004，69(6)：062311.

[15] DANOS V，KASHEFI E，PANANGADEN P. The

Measurement Calculus[J]. Journal of the ACM，2007，54(2)：8.

[16] DANOS V，KASHEFI E. Determinism in the One-Way Model[J]. Physical Review A，2006，74(5)：052310.

[17] BOOTH R I，KISSINGER A，MARKHAM D, et al. Outcome Determinism in Measurement-Based Quantum Computation with Qubits[J]. Journal of Physics A-Mathematical and Theoretical，2023，56(9)：115303.

[18] KAPOURNIOTIS T，KASHEF I E，LEICHTLE D，et al. A Framework for Verifiable Blind Quantum Computation[J/OL]. Quantum Physics. (2022-06-01) [2024-07-28]. https://doi.org/10.48550/arXiv.2206.00631.

[19] BEAUDRAP N D，DANOS V，KASHEFI E. Phase Map Decomposition for Unitarizes[J/OL]. Quantum Physics. (2006-03-29) [2024-08-22]. https://doi.org/10.48550/arXiv. quant-ph/ 0603266.

[20] BROWNE D E，KASHEFI E，MHALLA M，et al. Generalized Flow and Determinism in Measurement-Based Quantum Computation[J]. New Journal of Physics，2007，9(8)：250-266.

[21] FITZSIMONS J F，KASHEFI E. Unconditionally Verifiable Blind Quantum Computation[J]. Physical Review A，2017，96(1)：012303.

[22] JOZSA R. An Introduction to Measurement Based Quantum Computation[J/OL]. Quantum Physics. (2005-08-17) [2024-08-22]. https://doi.org/10.48550/arXiv.quant-ph/ 0508124.

[23] SUEKI T，KOSHIBA T，MORIMAE T. Ancilla-Driven Universal Blind Quantum Computation[J]. Physical Review A，2013，87(6)：060301.

[24] QU Z G，WANG K Y，ZHENG M. Secure Quantum Fog Computing Model Based on Blind Quantum Computation[J]. Journal of Ambient Intelligence and Humanized Computing，2022，13(8)：3807-3817.

[25] ZHANG X Q. Gate Teleportation-Based Universal Blind Quantum Computation[J/OL]. Quantum Physics. (2022-01-11) [2024-08-22]. https://doi.org/10.48550/arXiv.1809.00185.

[26] SONG C，XU K，LIU W X，et al. 10-Qubit Entanglement and Parallel Logic Operations with a Superconducting Circuit[J]. Physical Review Letters，2017，119(18)：180511.

[27] ZHANG X Q，LUO W Q，ZENG G Q，et al. A Hybrid Universal Blind Quantum Computation[J]. Information Sciences，2019，498：135-143.

[28] CAO S X. Multi-Agent Blind Quantum Computation Without Universal Cluster States[J]. New Journal of Physics，2023，25(10)：103028.

[29] FITZSIMONS J F. Private Quantum Computation：An Introduction to Blind Quantum Computing and Related Protocols[J/OL]. Quantum Physics. (2016-11-30) [2024-08-22]. https://doi.org/10.48550/arXiv.1611.10107.

[30] BOYKIN P O，ROYCHOWDHURY V. Optimal Encryption of Quantum Bits-Art. No. 042317[J]. Physical Review A，2003，67(4)：2317.

[31] DENG F G，LONG G L. Secure Direct Communication with a Quantum One-Time Pad[J]. Physical Review A，2004，69(5)：052319.

[32] AMBAINIS A，MOSCA M，TAPP A，et al. Private Quantum Channels[C]//Proceedings 41st Annual Symposium on Foundations of Computer Science. Redondo Beach：IEEE Comput. Soc.，2000：547-553.

[33] FEYNMAN R P. Simulating Physics with Computers[J]. International Journal of Theoretical Physics，1982，21(6)：467-488.

[34] DEUTSCH D, JOZSA R. Rapid Solution of Problems by Quantum Computation[J]. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences，1992，439(1907)：553-558.

[35] GROVER L K. A Fast Quantum Mechanical Algorithm for Database Search[C]//Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York：Association for Computing Machinery，1996：212-219.

[36] SHOR P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. SIAM Review，1999，41(2)：303-332.

[37] MORIMAE T，FUJII K. Blind Quantum Computation Protocol in Which Alice Only Makes Measurements[J]. Physical Review A，2013，87(5)：050301.

[38] GREGANTI C，ROEHSNER M C，BARZ S，et al. Demonstration of Measurement-Only Blind Quantum Computing[J]. New Journal of Physics，2016，18(1)：013020.

[39] VAN DAM J，AVIS G，PROPP T B，et al. Hardware Requirements for Trapped-Ion-Based Verifiable Blind Quantum Computing with a Measurement-Only Client[J]. Quantum Science and Technology，2024，9(4)：045031.

[40] LI Q，LIU C D，PENG Y，et al. Blind Quantum Computation Where a User Only Performs Single-Qubit Gates[J]. Optics & Laser Technology，2021，142：107190.

[41] MORIMAE T，FUJII K. Secure Entanglement Distillation for Double-Server Blind Quantum Computation[J]. Physical Review Letters，2013，111(2)：020502.

[42] SHENG Y B，ZHOU L. Deterministic Entanglement Distillation for Secure Double-Server Blind Quantum Computation[J]. Scientific Reports，2015，5：7815.

[43] LI Q，CHAN W H，WU C H，et al. Triple-Server Blind

Quantum Computation Using Entanglement Swapping[J]. Physical Review A，2014，89(4)：040302.

[44] PAN J W，BOUWMEESTER D，WEINFURTER H，et al. Experimental Entanglement Swapping：Entangling Photons That Never Interacted[J]. Physical Review Letters，1998，80(18)：3891−3894.

[45] HUNG S M，HWANG T. On the Security of Two Blind Quantum Computations[J/OL]. Quantum Physics. (2015−08−29)[2024−08−22]. https://doi.org/10.48550/arXiv.1508. 07478.

[46] XU H R，WANG B H. Universal Single-Server Blind Quantum Computation for Classical Clients[J]. Laser Physics Letters，2022，19(1)：015202.

[47] BARZ S，KASHEFI E，BROADBENT A，et al. Demonstration of Blind Quantum Computing[J]. Science，2012，335(6066)：303−308.

[48] MANTRI A，PÉREZ-DELGADO C A，FITZSIMONS J F. Optimal Blind Quantum Computation[J]. Physical Review Letters，2013，111(23)：230502.

[49] ZHANG X Q. Measurement-Based Universal Blind Quantum Computation with Minor Resources[J]. Quantum Information Processing，2021，21(1)：14.

[50] YANG Z，BAI M Q，MO Z W. The Brickwork State with Fewer Qubits in Blind Quantum Computation[J]. Quantum Information Processing，2022，21(4)：125.

[51] 严玉瞻，杨 振，罗元茂，等 . 基于测量的改进盲量子计算协议 [J]. 激光与光电子学进展，2024，61(9)：3788/LOP231217.
YAN Yuzhan，YANG Zhen，LUO Yuanmao，et al. Improved Measurement-Based Blind Quantum Computation Protocol[J]. Laser & Optoelectronics Progress，2024，61(9)：3788/LOP231217.

[52] MA S Q，ZHU C H，LIU X H，et al. Universal Blind Quantum Computation with Improved Brickwork States[J]. Physical Review A，2024，109(1)：012606

[53] BARZ S，KASHEFI E，BROADBENT A，et al. Demonstration of Blind Quantum Computing[J]. Science，2012，335(6066)：303−308.

[54] BARZ S，FITZSIMONS J F，KASHEFI E，et al. Experimental Verification of Quantum Computation[J]. Nature Physics，2013，9(11)：727−731.

[55] GREGANTI C，ROEHSNER M，BARZ S，et al. Demonstration of Measurement-Only Blind Quantum Computing[J]. New Journal of Physics，2016，18(1)：013020.

[56] HUANG H L，ZHAO Q，MA X F，et al. Experimental Blind Quantum Computing for a Classical Client[J]. Physical Review Letters，2017，119(5)：050503.

[57] DRMOTA P，NADLINGER D，MAIN D，et al. Verifiable Blind Quantum Computing with Trapped Ions and Single Photons[J]. Physical Review Letters，2024，132(15)：150604.

[58] WALTHER P，RESCH K J，RUDOLPH T，et al. Experimental One-Way Quantum Computing[J]. Nature，2005，434：169−176.

[59] CHEN K，LI C M，ZHANG Q，et al. Experimental Realization of One-Way Quantum Computing with Two-Photon Four-Qubit Cluster States[J]. Physical Review Letters，2007，99(12)：120503.

[60] LI Y，BROWNE D E，KWEK L C，et al. Thermal States as Universal Resources for Quantum Computation with Always-on Interactions[J]. Physical Review Letters，2011，107(6)：060501.

[61] FUJII K，MORIMAE T. Topologically Protected Measurement-Based Quantum Computation on the Thermal State of a Nearest-Neighbor Two-Body Hamiltonian with Spin-3/2 Particles[J]. Physical Review A，2012，85(1)：010304.

[62] SU X L，HAO S H，DENG X W，et al. Gate Sequence for Continuous Variable One-Way Quantum Computation[J]. Nature Communications，2013，4：2828.

[63] REICHARDT B W，UNGER F，VAZIRANI U. Classical Command of Quantum Systems[J]. Nature，2013，496：456−460.

[64] REICHARDT B W，UNGER F，VAZIRANI U. Classical Command of Quantum Systems Via Rigidity of CHSH Games[J/OL]. Quantum Physics. (2012−09−03)[2024−08−22]. https://doi.org/10.48550/arXiv.1209.0449.

[65] LI Z H，ZHU H J，HAYASHI M. Robust and Efficient Verification of Graph States in Blind Measurement-Based Quantum Computation[J]. NPJ Quantum Information，2023，9：115.

[66] HAYASHI M，MORIMAE T. Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing[J]. Physical Review Letters，2015，115(22)：220502.

[67] LI Y，HUMPHREYS P C，MENDOZA G J，et al. Resource Costs for Fault-Tolerant Linear Optical Quantum Computing[J]. Physical Review X，2015，5(4)：041007.

[68] MANTRI A，DEMARIE T F，MENICUCCI N C，et al. Flow Ambiguity：A Path Towards Classically Driven Blind Quantum Computation[J]. Physical Review X，2017，7(6)：031004.

（责任编辑：廖友媛）