激光与光电子学进展

基于测量的改进盲量子计算协议

严玉瞻[1,2]，杨振[1,2]，罗元茂[1,2]，吴光阳[1,2]，柏明强[1,2*]，莫智文[1,2**]

[1]四川师范大学数学科学学院，四川 成都 610066；

[2]四川师范大学智能信息和量子信息研究所，四川 成都 610066

摘要 盲量子计算是指有限量子能力或完全经典的客户端将复杂的计算任务委托给充足量子能力的服务器完成，以解放客户端的计算压力。为减轻客户端的经济压力和提高盲量子计算协议的执行效率，利用单粒子测量，提出了两个基于测量的改进通用盲量子计算协议，分别针对实系数输入的量子计算和复系数输入的量子计算。在协议中有两个参与方，客户端负责测量量子态，接收和发送经典或量子信息，服务器负责制备量子态但无需执行测量操作。与已有的客户端仅测量的盲量子计算协议相比，该协议在保持正确性、通用性和盲性的情况下，大大降低了客户端的量子成本和委托成本。

关键词 量子计算；盲量子计算；量子成本；委托成本

中图分类号 O413 **文献标志码** A **DOI**：10.3788/LOP231217

Improved Measurement-Based Blind Quantum Computation Protocol

Yan Yuzhan[1,2], Yang Zhen[1,2], Luo Yuanmao[1,2], Wu Guangyang[1,2], Bai Mingqiang[1,2*], Mo Zhiwen[1,2**]

[1]*School of Mathematical Sciences, Sichuan Normal University, Chengdu* 610066, *Sichuan, China*;

[2]*Institute of Intelligent Information and Quantum Information, Sichuan Normal University, Chengdu* 610066, *Sichuan, China*

Abstract Blind quantum computation refers to the delegation of complex computation from a client with limited quantum capabilities or complete classical abilities to a server possessing ample quantum power. This reduces computational demands from the client. To reduce the economic pressure of the client and improve the execution effectiveness of blind quantum computation protocols, this paper introduces two enhanced measurement-based universal blind quantum computation protocols utilizing single-particle measurements. These protocols cater to quantum inputs featuring either real or complex coefficients. Each protocol involves two participants: the client, responsible for quantum state measurements and the exchange of classical or quantum information, and the server, tasked with preparing quantum states without measurement requirements. These protocols stand in contrast to the existing blind quantum computation approaches wherein the client solely undertakes measurements. The proposed protocols considerably reduce both the client's quantum and delegated costs while maintaining correctness, universality, and the concept of blindness.

Key words quantum computation; blind quantum computation; quantum cost; delegated cost

1 引 言

近几年，随着量子[1-3]计算技术突飞猛进，越来越多人希望将来能利用量子计算机来完成计算任务。然而，大多数的研究者们认为在将来很长一段时间内，当普通的经典计算机与具有少量量子能力的客户想要利用量子计算机完成计算任务时，只能将计算任务委托给远程量子计算机。但在这个委托过程中，经典计算机客户的数据安全将会面临巨大的威胁。盲量子计算协议（BQC）的提出顺利地解决了这个安全问题，在不影响客户端Alice的输入、输出和算法的情况下，将复杂的计算委托给拥有成熟量子服务器Bob完成。

多年以来，学者们大多研究基于测量[4-5]的量子

收稿日期：2023-05-04；**修回日期**：2023-06-01；**录用日期**：2023-06-20；**网络首发日期**：2023-07-12

基金项目：四川省自然科学基金（2022NSFSC0534）、四川省科技厅中央引导地方自由探索项目（22ZYZYTS0064）、成都市科技局重大科技应用示范项目（2021-YF09-0016-GX）、四川师范大学重点项目（XKZX-02）

通信作者：*baimq@sicnu.edu.cn；**mozhiwen@263.net

计算和基于线路[6]的量子计算这两种模型的盲量子计算协议[7-17]。Childs[8]在2005年提出了基于线路模型的盲量子计算协议，但是该方案需要客户端具有量子储存能力。2009年，Broadbent等[7]提出基于测量的通用盲量子计算(UBQC)协议，客户端只需要拥有制备和发送单量子比特的能力。随后Barz等[18]在实验上验证了UBQC协议的可行性，其中客户端仅制备和传输单个光子量子比特。

不仅如此，基于UBQC协议，大量的盲量子计算协议也相继被提出[9-10, 12-14, 19-22]。其中，不少人致力于研究如何使盲量子计算协议更容易实现[9-10, 12, 14, 20-21]。从实用的角度来看，生成长距离传输的单量子比特不可能完美实现，因此文献[20]提出了一种远程盲量子单比特制备协议，客户端以委托的方式制备任意接近完美的单量子比特态。2013年，Morimae等[10]提出在一些实验设置(例如光学系统)中测量单量子比特状态比制备它更容易，因此他们提出了客户端仅测量的盲量子计算(MABQC)协议，从而减轻了客户端的负担。另外，在现实生活中，若让不同量子能力的客户端用同一个盲量子计算协议完成委托计算，势必会花费相同的成本，这对量子能力较强的客户端是不公平的。因此，优化客户端的成本是有必要的。于是Tan等[21]降低盲性的要求，从而使客户端发送更少的量子比特个数进而降低客户端的量子成本。

同时，对于量子计算机来说，制备应用于量子计算的纠缠态也至关重要[5]。在离子阱系统中，可纠缠的量子比特数目为20个[23]，在超导系统和光学系统中只有10个[24-25]。而目前已提出的基于测量的盲量子计算中，构造的纠缠态所需的量子比特数目太多[7, 10, 19]。因此，关于“实验上难以制备大规模纠缠态”这一难点，Zhang[12]在2021年提出利用更少量子比特数量的图态来实现通用的盲量子计算。次年，Yang等[9]提出了在保持客户端量子能力不变的条件下减少客户端制备和发送的粒子数量的方案。以上节约客户端成本并降低实验上实现大规模量子纠缠态的难度的协议大多采用的UBQC协议模式，为使这一议题得到更深入的探究，本文根据MABQC协议模式提出两个低成本盲量子计算协议。

在MABQC协议中，当实现任意一个通用单量子比特门时，客户端需在7 bit的cluster态上执行测量，服务器制备量子态以及执行测量。而本文所提出的协议，减少了客户端的测量次数，降低了客户端的量子成本以及服务器制备态的个数，并且不再要求其执行测量操作，大大降低了客户端的委托成本。最后，通过验证其正确性、通用性和盲性说明了所提协议是可行的。

2　理论基础

本节简要回顾MABQC协议[10]，具体来说，包括协议中的the unit cell纠缠态，以及如何利用该纠缠态来创建通用二维cluster态，使得Alice想要实现的量子计算对Bob保密。此外，由于MABQC协议中的cluster态与UBQC协议中的brickwork态类似，因此在下文中称为类brickwork态。

2.1　类brickwork态的定义和结构

The unit cell纠缠态是由两个7 bit的cluster态组成，其中每一个都可以实现任意的单量子比特门，而每一个the unit cell纠缠态代表通用门集合$\{I\otimes I, SH\otimes I, STH\otimes I, ST^{\dagger}H\otimes I, H\otimes I, (\mathrm{CZ})(\mathrm{CNOT})\}$中的元素，其等效关系如图1所示。

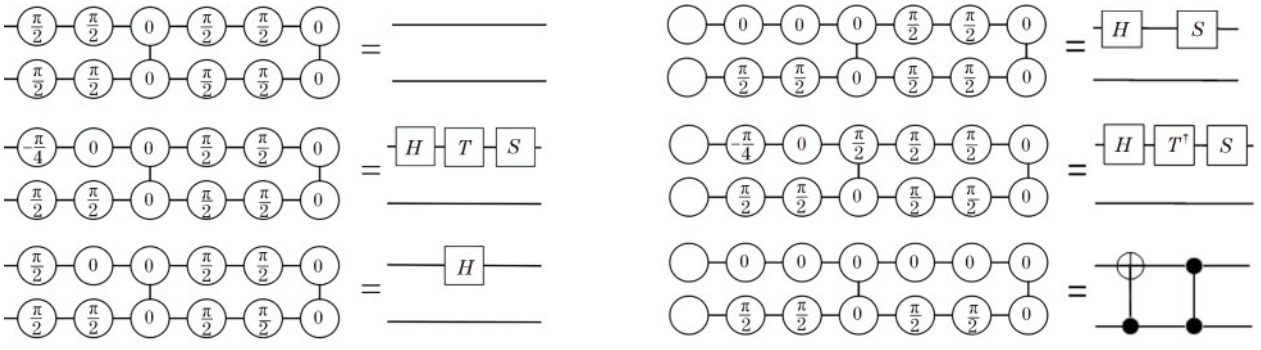

图1　The unit cell纠缠态的结构示意图

Fig. 1　Structure diagram of the unit cell entangled state

定义：一个$m\times n$维的纠缠态类brickwork态(图2)是由多个the unit cell纠缠态组成的，其中的每一个量子比特态为Bell态的一半。假设m表示水平的行，n表示垂直的列，物理量子比特被标记为索引(a,b)，其中a表示第a行，b表示第b列。

1)每一行相邻的两个量子比特存在CZ纠缠。即量子比特(a,b)和$(a,b+1)$之间存在CZ纠缠，其中$1\leqslant a\leqslant m$，$1\leqslant b\leqslant n$。

2)对于奇数行a和列$b\equiv 4(\mathrm{mod}12)$，量子比特$(a,b)$和$(a+1,b)$、$(a,b+3)$和$(a+1,b+3)$之间存在CZ纠缠。

3)对于偶数行a和列$b\equiv 10(\mathrm{mod}12)$，量子比特

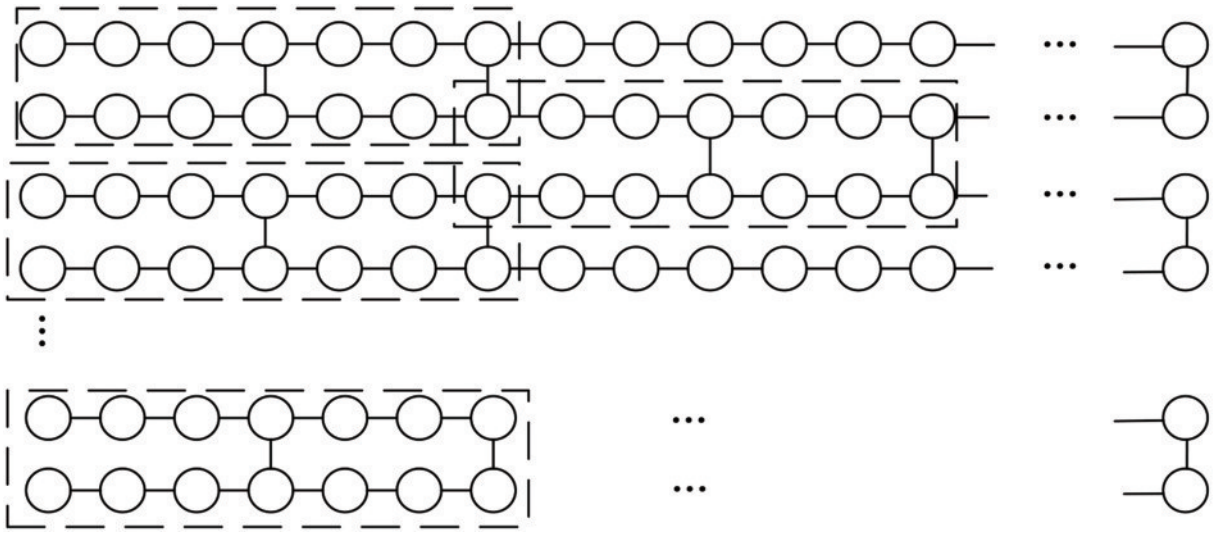

图 2　类 brickwork 态的结构图

Fig. 2　Structure diagram of the like-brickwork state

(a,b)和$(a+1,b)$、$(a,b+3)$和$(a+1,b+3)$之间存在CZ纠缠，其中CZ门表示为$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}$。

2.2　MABQC协议

2013年，Morimae和Fujii提出的客户端仅测量可抗信道丢失的盲量子计算协议步骤如下：

1）Bob准备了一对Bell态，并将其中一半通过量子信道传输给Alice，如果传输失败，则Bob需要再尝试一次；

2）在成功接收Bell态的一半后，Alice根据自己想要实现的算法确定角度θ，然后以$\{1/\sqrt{2}(|0\rangle\pm e^{i\theta}|1\rangle)\}$为基进行测量；

3）Bob对手中的一半Bell态和他寄存的单量子比特之间执行CZ纠缠，然后Bob对单量子比特以$\{|+\rangle,|-\rangle\}$为基执行测量；

4）Alice和Bob重复执行步骤1~3直到计算任务完成。

由此可知，每构造一个the unit cell纠缠态需要Alice和Bob协作实现，其中Alice和Bob执行12次分别以$\{1/\sqrt{2}(|0\rangle\pm e^{i\theta}|1\rangle)\}$为基和以$\{|+\rangle,|-\rangle\}$为基的测量，以及Bob还需制备Bell态和单量子比特。

3　低成本的盲量子计算协议

本节将分别介绍实现实系数和复系数输入单量子比特的盲量子计算协议以及可行性证明，以及如何与MABQC协议结合以实现任意算法的盲量子计算协议。

3.1　实系数输入的单量子比特盲量子计算协议

实系数单量子比特的盲量子计算协议的具体步骤如图3所示。

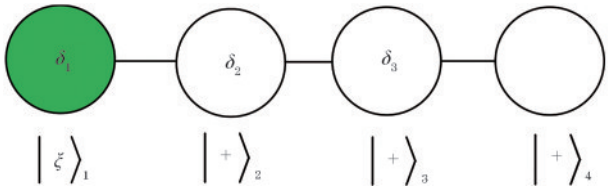

图 3　实系数输入的单量子比特盲量子计算协议过程示意图

Fig. 3　Schematic diagram of the protocol process for single-qubit blind quantum computation with real coefficient input

1）Bob制备一对Bell态，将其中的一半发送给Alice，若发送失败，则重新尝试。

2）Alice对成功接收的Bell态的一半执行实数旋转测量，其测量算符为

$$M_0=U|0\rangle\langle 0|U^{\dagger},M_1=U|1\rangle\langle 1|U^{\dagger},$$
$$U=\frac{1}{\sqrt{2}}\begin{pmatrix}x+y&x-y\\x-y&-x-y\end{pmatrix},\tag{1}$$

式中：$x,y\in\mathbf{R}$，并满足$x^2+y^2=1$。记测量结果为$a_1\in\{0,1\}$，测量后Bob手中的态为$|\xi\rangle_1$。

3）Bob制备一个新的单量子比特$|+\rangle_2$，CZ纠缠$|\xi\rangle_1$和$|+\rangle_2$，纠缠好后将$|\xi\rangle_1$发送给Alice，Alice收到后对$|\xi\rangle_1$粒子执行以$\{1/\sqrt{2}(|0\rangle\pm e^{i\delta_1}|1\rangle)\}$为基的测量，记测量结果为$a_2\in\{0,1\}$。

4）重复执行步骤3直到计算任务完成。

5）Bob将输出粒子发送给Alice。

可行性证明如下：

[正确性]在执行完步骤2的实数旋转测量后，Bob手中的粒子塌缩为$X^{a_1}Z^{a_1}H|\phi\rangle$，其中$|\phi\rangle=x|0\rangle+y|1\rangle$。在步骤3中，Bob创建的纠缠态为$CZ_{1,2}(|\xi\rangle_1\otimes|+\rangle_2)$，之后Alice执行以$\{1/\sqrt{2}(|0\rangle\pm e^{i\delta_1}|1\rangle)\}$为基的测量，Bob得到态

$$X^{a_2}HR_z(\delta_1)X^{a_1}Z^{a_1}H\left|\phi\right\rangle。\tag{2}$$

因此，最后可得到态

$$X^{a_4}HR_z(\delta_3)X^{a_3}HR_z(\delta_2)X^{a_2}HR_z(\delta_1)X^{a_1}Z^{a_1}H\left|\phi\right\rangle。\tag{3}$$

由于 $R_z(\delta)X^a=X^aR_z\left[(-1)^a\delta\right]$，$HX=ZH$，以及 $HR_z(\delta)H=R_x(\delta)$，最后可化简得到

$$X^{a_1+a_2+a_4}Z^{a_1+a_3}R_x\left[(-1)^{a_1+a_3}\delta_3\right]R_z\left[(-1)^{a_1+a_2}\delta_2\right]R_x\left[(-1)^{a_1}\delta_1\right]\left|\phi\right\rangle。\tag{4}$$

因此，当 Alice 想实现 H 门时，只需执行如下角度的 $M(\delta)$ 测量，同时 Bob 按照 Alice 的要求制备相应的量子比特

$$\delta_1=(-1)^{a_1}\frac{\pi}{2},\delta_2=(-1)^{a_1+a_2}\frac{\pi}{2},\delta_3=(-1)^{a_1+a_3}\frac{\pi}{2}。\tag{5}$$

同理，当 Alice 需要执行 T 门时，执行的测量角度分别为

$$\delta_1=0,\delta_2=(-1)^{a_1+a_2}\frac{\pi}{4},\delta_3=0。\tag{6}$$

[通用性] 由于单量子比特门集 H、T 是通用的，因此根据正确性的分析，Alice 可以委托 Bob 实现协议中的 H 门和 T 门。显然，Alice 为实现任意的单量子比特操作，可以反复委托 Bob 做 H 门和 T 门的组合。

[盲性] 首先，量子输入是盲的，即 Bob 得不到量子输入的信息，因为第一次测量是由 Alice 独自操作的，测量算子中的 x、y 只有 Alice 知道。其次，量子算法是盲的，即 Bob 不知道 Alice 具体在执行什么操作，因为 $\delta_i(i=1,2,3)$ 对 Bob 是保密的。最后，由于量子输入和量子算法对 Bob 保密，自然量子输出也是盲的。综上所述，该部分提出的盲量子计算协议满足盲性。

3.2　复系数输入的单量子比特盲量子计算协议

然而，有许多量子算法都是基于复系数，因此本部分给出一个复系数量子比特的盲量子计算协议，具体步骤如图 4 所示。

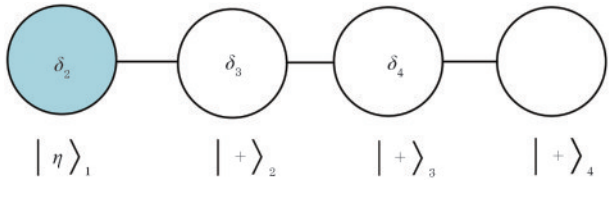

图 4　复系数输入的单量子比特盲量子计算协议过程示意图

Fig. 4　Schematic diagram of the single-qubit blind quantum computation protocol process for complex coefficient input

1) Bob 制备一对 Bell 态，将其中的一半发送给 Alice，若发送失败，则重新尝试。

2) Alice 对成功接收的 Bell 态的一半执行复数旋转测量，其测量算符为

$$M_0=U\left|0\right\rangle\left\langle0\right|U^{\dagger},M_1=U\left|1\right\rangle\left\langle1\right|U^{\dagger},$$
$$U=\begin{pmatrix}x & -y\mathrm{e}^{\mathrm{i}\delta_1}\\ y\mathrm{e}^{-\mathrm{i}\delta_1} & x\end{pmatrix},\tag{7}$$

式中：$x,y\in\mathbf{R}$，并满足 $x^2+y^2=1$。记测量结果为 $s_1\in\{0,1\}$，以及测量后 Bob 手中的态为 $\left\langle\eta\right|_1$。

3) Bob 制备一个新的单量子比特 $\left|+\right\rangle_2$，CZ 纠缠 $\left\langle\eta\right|_1$ 和 $\left\langle+\right|_2$，纠缠好后将 $\left|\eta\right\rangle_1$ 发送给 Alice，Alice 收到后对 $\left|\eta\right\rangle_1$ 粒子执行以 $\{1/\sqrt{2}\,(\left|0\right\rangle\pm\mathrm{e}^{\mathrm{i}\delta_2}\left|1\right\rangle)\}$ 为基的测量，记测量结果为 $s_2\in\{0,1\}$。

4) 重复执行两次步骤 3。

5) Bob 执行 H 门操作。

6) Alice 和 Bob 重复执行步骤 3～5 直到计算任务完成。

7) Bob 将输出粒子发送给 Alice。

可行性证明如下：

[正确性] 在执行完步骤 2 的复数旋转测量后，Bob 手中的粒子塌缩为

$$\begin{aligned}\left|\eta\right\rangle_1&=X^{s_1}Z^{s_1}R_z\left[(-1)^{s_1}\delta_1\right]\left|\phi\right\rangle=X^{s_1}Z^{s_1}(x\left|0\right\rangle+y\mathrm{e}^{(-1)^{s_1}\mathrm{i}\delta_1}\left|1\right\rangle)\doteq\\&X^{s_1}Z^{s_1}(x\left|0\right\rangle+y\mathrm{e}^{(-1)^{s_1}\mathrm{i}\delta_1}\left|1\right\rangle)=\\&X^{s_1}Z^{s_1}(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)=X^{s_1}Z^{s_1}\left|\psi\right\rangle,\end{aligned}\tag{7}$$

式中："≒"表示忽略全局相位后的相等，并记 $\left|\psi\right\rangle=\alpha\left|0\right\rangle+\beta\left|1\right\rangle$，其中 $\alpha=x,\beta=y\mathrm{e}^{(-1)^{s_1}\mathrm{i}\delta_1}$，$\delta_1\in[0,2\pi)$，因此满足 $\left|\alpha\right|^2+\left|\beta\right|^2=1$，当 CZ 纠缠 $\left|\eta\right\rangle_1$ 和 $\left|+\right\rangle_2$ 后，量子比特的状态为

$$\begin{aligned}&CZ_{1,2}(\left|\eta\right\rangle_1\left|+\right\rangle_2)=CZ_{1,2}(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)_1\\&(\left|0\right\rangle+\left|1\right\rangle)_2=\alpha\left|00\right\rangle+\alpha\left|01\right\rangle+\beta\left|10\right\rangle-\beta\left|11\right\rangle,\end{aligned}\tag{8}$$

式中：$CZ_{(i,j)}$ 表示控制 Z 门且 i 为控制比特；j 为目标比特。当对 $\left|\eta\right\rangle_1$ 执行测量后，得到的结果为

$$X^{s_2}HR_z(\delta_2)X^{s_1}Z^{s_1}\left|\psi\right\rangle。\tag{9}$$

因此最后的结果为

$$HX^{s_4}HR_z(\delta_4)X^{s_3}HR_z(\delta_3)X^{s_2}HR_z(\delta_2)X^{s_1}Z^{s_1}\left|\psi\right\rangle。\tag{10}$$

由于 $XZ=-ZX$，$HX=ZH$ 以及 $XR_z(\delta)=R_z(-\delta)X$，在忽略全局相位后最后的结果可化简为

$$X^{s_1+s_3}Z^{s_1+s_2+s_4}R_z\left[(-1)^{s_1+s_3}\delta_4\right]R_x\left[(-1)^{s_1+s_2}\delta_3\right]R_z\left[(-1)^{s_1}\delta_2\right]\left|\psi\right\rangle。\tag{11}$$

因此，当 Alice 想实现 H 门时，只需执行角度分别为 $\delta_2=(-1)^{s_1}\frac{\pi}{2},\delta_3=(-1)^{s_1+s_2}\frac{\pi}{2},\delta_4=(-1)^{s_1+s_3}\frac{\pi}{2}$ 的 $M(\delta)$ 测量，同时 Bob 按照 Alice 的要求制备相应的量子比特。同理，当 Alice 需要执行 T 门时，执行的测量角度分别为 $\delta_2=(-1)^{s_1}\frac{\pi}{4},\delta_3=0,\delta_4=0$。

[通用性] 由于单量子比特门集 H、T 是通用的，因此根据正确性的分析，Alice 可以委托 Bob 实现协

议中的H门和T门。显然，Alice为实现任意的单量子比特操作，可以反复委托Bob做H门和T门的组合。

[盲性]首先，量子输入是盲的，即Bob得不到量子输入的信息，因为第一次测量是由Alice独自操作的，测量算子中的x,y和δ_1并未泄露给其他人或实验室。其次，量子算法是盲的，即Bob不知道Alice具体在执行什么操作，因为$\delta_i(i=2,3,4)$对Bob是保密的。最后，由于量子输入和量子算法对Bob保密，自然量子输出也是盲的。综上所述，该部分提出的盲量子计算协议满足盲性。

3.3　实现任意算法的盲量子计算协议

本节将结合MABQC协议中的the unit cell纠缠态与3.1与3.2节所提的纠缠态，以减少为实现任意量子算法时Alice的量子成本和委托成本。首先，MABQC协议中的每一个the unit cell纠缠态都具有相同的结构和粒子数量并可以借此实现任意的幺正运算，因此Bob无法得知Alice委托的量子计算。同样地，本文提出的方案也具有相同的维数和结构，并且保持对Bob的盲目性。因此，上述模型可以替换the unit cell纠缠态中的H、T操作。

其次，在替换过程中，即使上下两层的粒子数不同，也不会影响替换的结果，因为被替换的单量子比特门的实现是相互独立的。对于工作在两个量子位上的CX门与上述模型的连接，只需在the unit cell纠缠态上确定相应的控制量子位、目标量子位、输入和输出量子位即可。因此，利用上述模型替换MABQC中的模型的操作是可实现的。

最后，需要考虑一种情况，如果用上述模型替换MABQC协议中模型的所有单量子比特门，根据每个纠缠态的维数，Bob能判断出受控非门的位置。事实上，只要至少保证一个单量子比特门不被上述模型替换就能避免这种情况的发生，以保证受控非门位置的盲性。换句话说，Bob只能知道受控非门的可能位置，而不知道它的明确位置，甚至不知道受控非门是否存在。因此，受控非门的位置对Bob保密。另一方面，由上述模型替换的其余单量子比特操作的位置也保持了对Bob的盲性，因为这些操作具有相同的维数和结构。

具体替换过程如图5所示。

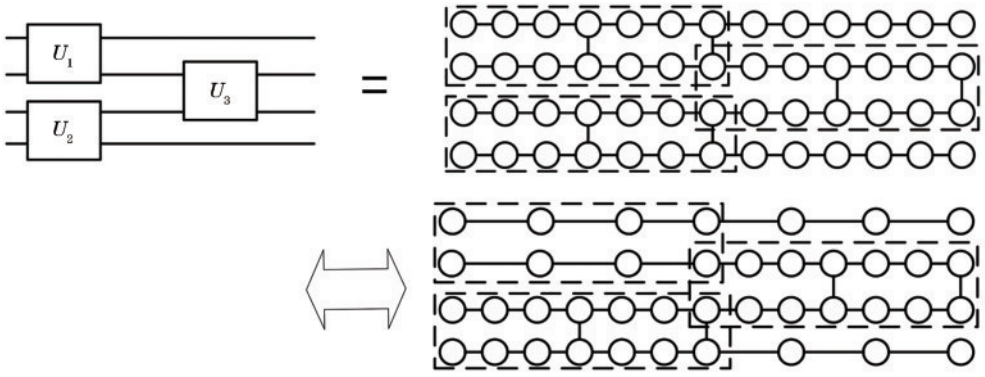

图5　类brickwork态的替换图

Fig. 5　Substitution graph for like-brickwork states

4　协议的应用:盲量子傅里叶变换

多量子比特的量子傅里叶变换是单量子比特门和双量子比特门依次组成的，接下来研究量子傅里叶变换以及相应的盲量子计算协议。

实现盲量子傅里叶变换的具体实施步骤如下：1) Alice首先设计两比特量子傅里叶变换的线路图，如图6所示。其次，将图6中的量子门按照图7中的等价线路转换为H门、T门和CX门的组合。最后划分量子线路使其适应类brickwork态中的the unit cell纠缠态，如图8所示。2)Bob制备一对Bell态，将其中的一半发送给Alice，若发送失败，则重新尝试。3)Alice根据任务计算x、y，之后对成功接收到的Bell态的一半执行实数旋转测量。4)Bob制备一个新的单量子比特$|+\rangle$，CZ纠缠量子比特$|\xi\rangle$和$|+\rangle$，然后将$|\xi\rangle$发送给Alice。5)Alice根据具体量子算法任务与前馈测量结果计算测量角度δ，对收到的量子比特$|\xi\rangle$执行以$\{1/\sqrt{2}(|0\rangle\pm e^{i\delta}|1\rangle)\}$为基的测量。6)重复步骤4、5直到获得最后结果。

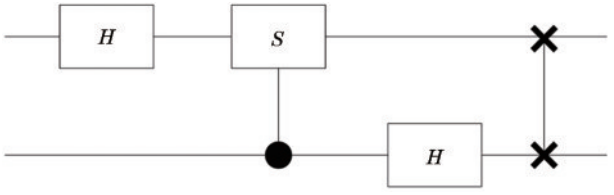

图6　两比特量子傅里叶变换示意图

Fig. 6　Illustration of the two-bit quantum Fourier transform

本协议可以帮助没有足够量子能力的客户端委托拥有强大量子计算机的服务器实现量子傅里叶变换，并且不会泄露量子输入、输出和算法。

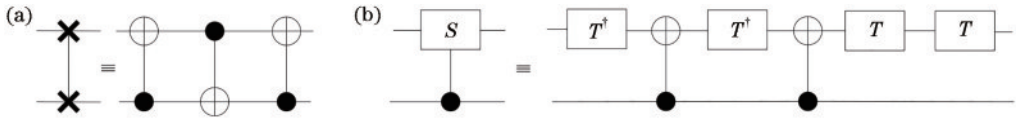

图 7　量子门分解图。(a)交换门;(b) 受控-S门

Fig. 7　Decomposition diagrams of quantum gate. (a) Swap gate; (b) controlled-S gate

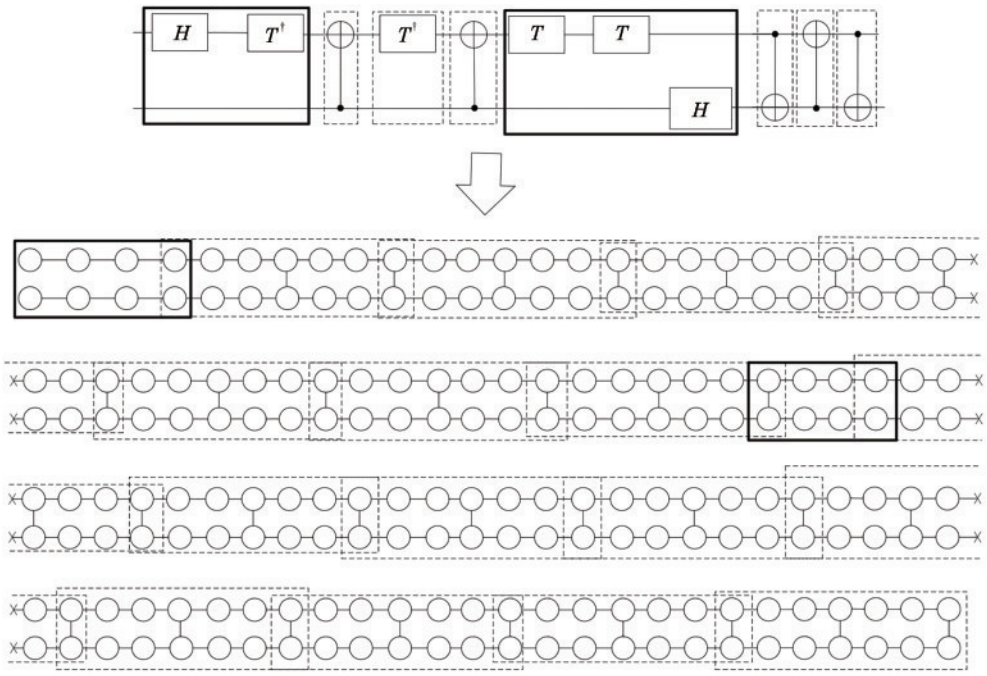

图 8　盲量子傅里叶变换示意图

Fig. 8　Schematic of the blind quantum Fourier transform

5　成本分析

与 MABQC 协议中的类 brickwork 态的 the unit cell 纠缠态相比，本文的两个方案中构造的单元 cluster 纠缠态需要的量子比特数量是 8，在实验上实现量子计算，进一步节约量子成本和委托成本，提高计算速度和整体效率。从 Alice 执行的测量次数，即量子成本来说，每当实现 m 个 H 门或 T 门时，在 MABQC 协议中，Alice 需要执行 $6m$ 次测量。而在本文协议中，Alice 仅需要执行 $3m+1$ 次测量，即当 m 趋近于无穷时，Alice 可以节约 33.3%(精确到一位小数)的量子成本。同理，在 Bob 执行的制备和测量粒子操作，即 Alice 的委托成本中，制备成本降低了 57.1%(精确到一位小数)，测量成本降低了 100%。具体如表 1 所示。

表 1　客户端成本对比表

Table 1　Comparison of client cost

Protocol	Quantum cost			Delegated cost			
	Rotation measurement	$M(\theta)$ measurements	All measurements	Preparing single-qubit	Preparing Bell state	All prepared state	Measurements
Ref. [7]	0	$6m$	$6m+1$	1	$6m$	$6m+1$	$6m$
Our protocol	1	$3m$	$3m+1$	$3m$	1	$3m+1$	0

6　结　　论

在实际情况中，有必要对本文协议进一步探讨身份认证[26-27]。事实上，虽然在第 3 节中有些量子比特是通过旋转测量得到的，但是构造的 cluster 态仍然是图态。也就是说，本文协议的身份认证可以采用 MABQC 协议身份认证的方法[27]，或者 Alice 可以使用视频监控[28]来检测 Bob 是否按照命令执行操作。

本文提出了两个基于测量的改进通用盲量子计算协议，分别实现了实系数输入的单量子比特盲量子计算协议和复系数输入的单量子比特盲量子计算协议，其中，纠缠态是由八粒子 cluster 态构造，主要实

现了单量子比特门H、T。与已有的客户端仅测量的盲量子计算协议相比，本文方案大幅降低客户端的量子成本和委托成本，在实际的应用中有一定的价值。

除此之外，若能将本文协议推广到双服务器模式的盲量子计算协议中，可以使得客户端更经典。也就是说，在两个服务器不能通信的情况下，让Bob1执行以$\{1/\sqrt{2}(|0\rangle\pm e^{i\theta}|1\rangle)\}$为基的测量、Bob2执行以$\{|+\rangle,|-\rangle\}$为基的测量。然而，阻止两个强大的量子服务器通信是不现实的，而且能否消除这样一个苛刻的要求一直是一个悬而未决的问题。因此，探究双服务器模式可实现的方式是一个有意义的问题。

参 考 文 献

[1] 何业锋, 李智, 杨梦玫. 基于四粒子团簇态的量子密钥协商协议[J]. 激光与光电子学进展, 2023, 60(21): 2127001.
He Y F, Li Z, Yang M M. Quantum key agreement protocol based on four-particle cluster states[J]. Laser & Optoelectronics Progress, 2023, 60(21): 2127001.

[2] 彭永刚. 量子Toffoli门的核磁共振物理实现[J]. 激光与光电子学进展, 2023, 60(7): 0727002.
Peng Y G. Nuclear-magnetic-resonance-based physical realization of quantum toffoli gate[J]. Laser & Optoelectronics Progress, 2023, 60(7): 0727002.

[3] 王俊辉, 李云霞, 郭瀚, 等. 免疫集体噪声的半量子盲签名协议[J]. 激光与光电子学进展, 2022, 59(19): 1927001.
Wang J H, Li Y X, Guo H, et al. Semi-quantum blind signature protocol immune to collective noise[J]. Laser & Optoelectronics Progress, 2022, 59(19): 1927001.

[4] Danos V, Kashefi E, Panangaden P. The measurement calculus[J]. Journal of the ACM, 2007, 54(2): 8-es.

[5] Raussendorf R, Briegel H J. A one-way quantum computer[J]. Physical Review Letters, 2001, 86(22): 5188-5191.

[6] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2007.

[7] Broadbent A, Fitzsimons J, Kashefi E. Universal blind quantum computation[C]//Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science, October 25-27, 2009, Atlanta, GA, USA. New York: ACM Press, 2009: 517-526.

[8] Childs A M. Secure assisted quantum computation[J]. Quantum Information & Computation, 2005, 5(6): 456-466.

[9] 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.

[10] Morimae T, Fujii K. Blind quantum computation protocol in which Alice only makes measurements[J]. Physical Review A, 2013, 87(5): 050301.

[11] Zhang X Q, Luo W Q, Zeng G Q, et al. A hybrid universal blind quantum computation[J]. Information Sciences, 2019, 498: 135-143.

[12] Zhang X Q. Measurement-based universal blind quantum computation with minor resources[J]. Quantum Information Processing, 2021, 21(1): 1-18.

[13] Morimae T, Fujii K. Secure entanglement distillation for double-server blind quantum computation[J]. Physical Review Letters, 2013, 111(2): 020502.

[14] 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.

[15] Walther P, Resch K J, Rudolph T, et al. Experimental one-way quantum computing[J]. Nature, 2005, 434(7030): 169-176.

[16] Broadbent A. Delegating private quantum computations[J]. Canadian Journal of Physics, 2015, 93(9): 941-946.

[17] Zhang X Q, Weng J, Li X C, et al. Single-server blind quantum computation with quantum circuit model[J]. Quantum Information Processing, 2018, 17(6): 134.

[18] Barz S, Kashefi E, Broadbent A, et al. Demonstration of blind quantum computing[J]. Science, 2012, 335(6066): 303-308.

[19] Morimae T, Dunjko V, Kashefi E. Ground state blind quantum computation on AKLT state[J]. Quantum Information & Computation, 2015, 15(3/4): 200-234.

[20] Dunjko V, Kashefi E, Leverrier A. Blind quantum computing with weak coherent pulses[J]. Physical Review Letters, 2012, 108(20): 200502.

[21] Tan X Q, Zhou X. Universal half-blind quantum computation[J]. Annals of Telecommunications, 2017, 72(9): 589-595.

[22] Morimae T, Fujii K. Blind topological measurement-based quantum computation[J]. Nature Communications, 2012, 3: 1036.

[23] Friis N, Marty O, Maier C, et al. Observation of entangled states of a fully controlled 20-qubit system[J]. Physical Review X, 2018, 8(2): 021012.

[24] Wang X L, Chen L K, Li W, et al. Experimental ten-photon entanglement[J]. Physical Review Letters, 2016, 117(21): 210502.

[25] 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.

[26] Gheorghiu A, Kashefi E, Wallden P. Robustness and device independence of verifiable blind quantum computing[J]. New Journal of Physics, 2015, 17(8): 083040.

[27] Morimae T. Verification for measurement-only blind quantum computing[J]. Physical Review A, 2014, 89(6): 060302.

[28] Sun Z Z, Zhang Q X, Li Y Z, et al. DPPDL: a dynamic partial-parallel data layout for green video surveillance storage[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 28(1): 193-205.