DOI: 10.3969/j.issn.1007-5461.2023.05.012

基于四粒子GHZ态的半量子私有比较协议

黄 灌*， 娄小平

(湖南师范大学信息科学与工程学院， 湖南 长沙 410081)

摘 要: 半量子通信协议允许只具有有限量子能力的参与者进行量子通信, 与全量子通信协议相比, 减少了量子资源损耗, 节约了量子硬件成本。基于半量子模型, 以四粒子Greenberger-Horne-Zeilinger (GHZ) 态作为量子资源态, 提出了一种新型半量子私有比较协议。该协议可以在半诚实第三方的帮助下比较两个经典用户Alice和Bob的信息是否相等, 且不泄露他们的秘密信息。安全性分析表明该协议可以抵御内部攻击和外部攻击, 与现有的半量子私有比较协议相比, 经典用户所需的量子能力更少, 只需执行Z基测量和反射接收的粒子, 且具有较高的量子比特效率。此外, 通过IBM量子云平台进行了仿真实验, 验证了所提协议的正确性。

关 键 词: 量子信息; 量子密码学; 半量子私有比较; 四粒子GHZ态; IBM量子云平台; 半诚实第三方

中图分类号: O431.2 **文献标识码**: A **文章编号:** 1007-5461(2023)05-00726-12

Semi-quantum private comparison protocol based on four-particle GHZ state

*HUANG Guan**, LOU Xiaoping*

(College of Information Science and Engineering, Hunan Normal University, Changsha 410081, China)

Abstract: The semi-quantum communication protocol allows participants with only limited quantum capabilities to carry out quantum communication. Compared with the full quantum communication protocol, it reduces the loss of quantum resources and saves the costs of quantum hardware. Based on a semi-quantum model, a novel semi-quantum private comparison protocol is proposed with the four-particle Greenberger-Horne-Zeilinger (GHZ) state as the quantum resource state. The protocol can compare the information of two classical users, Alice and Bob, with the help of a semi-honest third party without disclosing their secret information. Security analysis shows that this protocol can resist both internal and external attacks. Compared with the existing semi-quantum private comparison protocol, the

基金项目: 湖南省自然科学基金面上项目 (2021JJ30454)

作者简介: 黄 灌 (1997 -), 湖南郴州人, 研究生, 主要从事软件工程、量子信息等方面的研究。E-mail:1875596816@qq.com

导师简介: 娄小平 (1982 -), 女, 湖南长沙人, 教授, 硕士生导师, 主要从事信息安全技术、经典密码学、量子信息、安全通信协议等方面的研究。E-mail: louxiaoping@hunnu.edu.cn

收稿日期: 2021-10-20; **修改日期:** 2021-11-29

*通信作者。

classical user in the proposed protocol requires less quantum capability, only needs to perform Z-based measurement and reflect the received particles, and has high quantum bit efficiency. In addition, the proposed protocol is verified by simulation experiments on IBM quantum cloud platform.

Key words: quantum information; quantum cryptography; semi-quantum private comparison; four-particle GHZ state; IBM quantum cloud platform; semi-honest third party

0　引　言

量子安全多方计算 (QSMC) 是量子信息研究的重要方向之一, 量子私有比较 (QPC) 是QSMC的一个研究分支, 它解决的主要问题是: 对于两个互不信任的用户, 在第三方的帮助下比较他们的秘密信息是否相等, 且不泄露他们的秘密信息。2009年, Yang等[1]提出了第一个QPC协议, 其通过Bell态与诱骗态光子相结合, 在半诚实第三方TP的帮助下比较双方的秘密信息是否相等。此后, 研究人员根据不同的量子态提出了许多QPC协议, 比如单光子[2]、两粒子乘积态[3]、Bell态[4−6]、GHZ态[7−9]、W态[10]、簇态[11, 12]、五粒子纠缠态[13]、χ型纠缠态[14, 15]、六粒子纠缠态[16]。以上协议要求参与者和第三方TP具备全量子能力, 即参与者需要使用各种量子设备 (如量子存储器、纠缠态发生器、量子寄存器), 但这些设备价格昂贵, 并不是所有参与者都能承担这样高的资源消耗和硬件成本。因此, QPC协议需要考虑节省量子资源, 降低参与者的量子能力, 节约量子硬件成本, 从而使协议更高效实用。

Boyer等[17]在2007年提出了第一个半量子密钥分发协议并定义了半量子模型。半量子模型是指发送方Alice (量子方) 具有全量子能力而接收方Bob (半量子方) 只有有限的量子能力, 基于半量子模型的理论实现了量子方和半量子方的密钥共享。半量子方具有有限的量子能力是指只能执行以下操作: 一是使用Z基测量量子比特; 二是对量子比特进行重排序; 三是使用Z基制备量子比特;四是无干扰的情况下将粒子直接反射给量子方。自Boyer等提出半量子模型后, 量子通信领域开始应用该模型, 例如半量子秘密共享 (SQSS)[18−20]、半量子密钥分发 (SQKD)[21−23]、半量子安全直接通信 (SQSDC) 协议[24−26]、半量子私有比较 (SQPC)协议[27−30]。第一个SQPC协议是Chou等[31]在2016年提出的, 其基于Bell态, 允许两个参与者在完全不诚实第三方TP的帮助下比较他们的秘密信息是否相等。此后研究人员提出了许多SQPC协议, 如2019年Lin等[27]提出了基于单光子的SQPC协议, 该协议没有使用预密钥, 因此协议安全性不高, 有秘密信息泄露的风险。2021年, Zhou等[29]提出一个基于 d 维Bell态的SQPC协议, 该协议可以在半诚实第三方TP的帮助下比较参与者双方秘密信息的大小。然而, 这些SQPC协议仅停留在理论方面, 并没有进行实验验证。

在文献[32]的启发下, 本文提出了一个基于四粒子GHZ态的SQPC协议, 通过IBM量子云平台进行了仿真实验, 与其他没有进行仿真实验的SQPC协议相比实用性更强;此外, 经典用户对量子能力的要求更低, 只要执行Z基测量和无干扰的反射粒子, 具有更优的量子位效率。

1　四粒子GHZ态

四粒子GHZ态存在16类配置, 取其中4类如下:

$$\begin{cases} \left|\varphi_1\right\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0000\right\rangle+\left|1111\right\rangle\right)_{1234} \\ \left|\varphi_2\right\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0001\right\rangle-\left|1110\right\rangle\right)_{1234} \\ \left|\varphi_3\right\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0101\right\rangle+\left|1010\right\rangle\right)_{1234} \\ \left|\varphi_4\right\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0100\right\rangle-\left|1011\right\rangle\right)_{1234} \end{cases}. \tag{1}$$

对四粒子GHZ态执行两次CNOT操作, 第二个粒子作为控制粒子, 第三、四个粒子作为目标粒子。如果控制粒子为0, 则目标粒子不变; 如果控制粒子为1, 则目标粒子反相。经过两次CNOT操作后, 上述四粒子GHZ态可以分别转化为

$$\begin{cases} \left|G_1\right\rangle_{1234}=U_{\mathrm{CNOT}}^{23}U_{\mathrm{CNOT}}^{24}\left|\varphi_1\right\rangle_{1234}=\left|\phi^+\right\rangle_{12}\left|00\right\rangle_{34} \\ \left|G_2\right\rangle_{1234}=U_{\mathrm{CNOT}}^{23}U_{\mathrm{CNOT}}^{24}\left|\varphi_2\right\rangle_{1234}=\left|\phi^-\right\rangle_{12}\left|01\right\rangle_{34} \\ \left|G_3\right\rangle_{1234}=U_{\mathrm{CNOT}}^{23}U_{\mathrm{CNOT}}^{24}\left|\varphi_3\right\rangle_{1234}=\left|\Psi^+\right\rangle_{12}\left|10\right\rangle_{34} \\ \left|G_4\right\rangle_{1234}=U_{\mathrm{CNOT}}^{23}U_{\mathrm{CNOT}}^{24}\left|\varphi_4\right\rangle_{1234}=\left|\Psi^-\right\rangle_{12}\left|11\right\rangle_{34} \end{cases}, \tag{2}$$

其中, 4个Bell态为

$$\begin{cases} \left|\phi^+\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right) \\ \left|\phi^-\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right) \\ \left|\Psi^+\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right) \\ \left|\Psi^-\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right) \end{cases}. \tag{3}$$

2 协议描述

经典用户Alice和Bob想在半诚实第三方TP的帮助下比较他们的秘密信息X和Y是否相同。TP是半诚实的意味着它可以执行任意的攻击, 但不能与其他参与者共谋窃取秘密信息。Alice和Bob仅有有限的量子能力, 只能执行测量 (M) 操作 (使用Z基$\{\left|0\right\rangle,\left|1\right\rangle\}$测量量子比特) 和反射 (R) 操作 (在无干扰的条件下直接返回接收到的量子比特)。而TP具有全量子能力, 可以制备四粒子GHZ态并使用Bell基和Z基测量量子态。X和Y的二进制信息可表示为

$$\begin{cases} X=\{x_0,x_1,\ldots,x_{N-1}\} \\ Y=\{y_0,y_1,\ldots,y_{N-1}\} \end{cases}, \tag{4}$$

式中: $X=\sum_{i=0}^{N-1}(x_i2^i)$, $Y=\sum_{i=0}^{N-1}(y_i2^i)$, $i=0,1,\ldots,N-1$。

在本协议中, TP和Alice (Bob) 需要提前使用一个安全的SQKD协议[22]共享预密钥K_{AT}(K_{BT}), Alice和Bob也需要共享预密钥K_{AB}, 这里$K_{\mathrm{AB}}^j,K_{\mathrm{AT}}^j,K_{\mathrm{BT}}^j\in\{0,1\}$, $j=0,1,\cdots,N-1$, K_{AB}^j、K_{AT}^j、K_{BT}^j分别表示K_{AB}、K_{AT}、K_{BT}中的第j个比特。

如图1所示, 协议可分步描述如下:

步骤一: Alice和Bob划分二进制秘密信息X和Y为$\lceil N/2\rceil$组, 分别表示为$\{G_{\mathrm{A}}^{1}, G_{\mathrm{A}}^{2}, \cdots, G_{\mathrm{A}}^{\lceil N/2\rceil}\}$、$\{G_{\mathrm{B}}^{1}, G_{\mathrm{B}}^{2}, \cdots, G_{\mathrm{B}}^{\lceil N/2\rceil}\}$。如果$N \bmod 2 \neq 0$, 则添加1个0到最后一组, 且每一组包括两个二进制信息位。

步骤二: TP从(1)式中随机选择$\lceil N/2\rceil$个四粒子GHZ态进行制备, 然后TP对四粒子GHZ态执行两次CNOT操作, 转化为(2)式所示的四粒子GHZ态。随后, TP选择四粒子GHZ态的1、3粒子组成序列S_{A}, 选择2、4粒子组成序列S_{B}, 即

$$\begin{cases} S_{\mathrm{A}}=\{P_1^1, P_1^3, P_2^1, P_2^3, P_3^1, P_3^3, \cdots, P_{\lceil N/2\rceil}^1, P_{\lceil N/2\rceil}^3\} \\ S_{\mathrm{B}}=\{P_1^2, P_1^4, P_2^2, P_2^4, P_3^2, P_3^4, \cdots, P_{\lceil N/2\rceil}^2, P_{\lceil N/2\rceil}^4\} \end{cases}, \tag{5}$$

上标1、2、3、4表示四粒子GHZ态中4个不同粒子, 下标1、2、3、…、$\lceil N/2\rceil$代表四粒子GHZ态的顺序。S_{A}中1、3粒子的相对位置和S_{B}中2、4粒子的相对位置必须相同。TP发送S_{A}给Alice, 发送S_{B}给Bob。

步骤三: 在Alice和Bob收到序列后, 对S_{A}和S_{B}中相同位置的粒子P_j^1和P_j^2执行反射操作, 对粒子P_j^3和P_j^4执行测量操作。如果执行R操作, 在无干扰的环境下直接反射粒子给TP;如果执行M操作, Z基测量相应的量子比特。

步骤四: 在TP存储Alice和Bob返回的量子比特后, Alice和Bob公开宣布对哪些位置的粒子执行测量操作, 对哪些位置的粒子执行反射操作。然后, TP根据表1执行不同的操作。

案例1: Alice和Bob都执行R操作, TP对Alice和Bob反射的粒子P_j^1和P_j^2执行Bell基联合测量。粒子P_j^1和P_j^2所处的量子态是Bell纠缠态, TP根据Bell态测量结果与初始态进行比较, 如果测量结果与初始态不一致, 协议终止;否则TP公布Bell态测量结果, 进入案例2。

案例2: Alice和Bob都执行M操作, 则Alice (Bob)使用Z基测量序列$S_{\mathrm{A}}(S_{\mathrm{B}})$中第$j$个量子对$P_j^3(P_j^4)$, 测量结果记为$M_{\mathrm{A}}^j(M_{\mathrm{B}}^j)$, M_{A}^j, $M_{\mathrm{B}}^j \in \{0, 1\}$。Alice测量结果的二进制序列记为$M_{\mathrm{A}}=\{M_{\mathrm{A}}^1, M_{\mathrm{A}}^2, \cdots, M_{\mathrm{A}}^{\lceil N/2\rceil}\}$, Bob测量结果的二进制序列记为$M_{\mathrm{B}}=\{M_{\mathrm{B}}^1, M_{\mathrm{B}}^2, \cdots, M_{\mathrm{B}}^{\lceil N/2\rceil}\}$, M_{A}^j、M_{B}^j分别表示序列M_{A}、M_{B}中的第j个比特。根据表2的规则, Alice和Bob根据TP公布的Bell态测量结果和自身Z基测量结果, 将测量结果编码为C^j, C^j即他们共同知道的测量结果的编码值。然后Alice和Bob分别通过

$$\begin{cases} R_{\mathrm{A}}^j = C^j \oplus G_{\mathrm{A}}^j \oplus K_{\mathrm{AB}}^j \oplus K_{\mathrm{AT}}^j \\ R_{\mathrm{B}}^j = C^j \oplus G_{\mathrm{B}}^j \oplus K_{\mathrm{AB}}^j \oplus K_{\mathrm{BT}}^j \end{cases} \tag{6}$$

计算R_{A}^j和R_{B}^j的值, 其中$\oplus$表示模2加。最后将R_{A}和R_{B}发送给TP, $R_{\mathrm{A}}=\{R_{\mathrm{A}}^1, R_{\mathrm{A}}^2, \cdots, R_{\mathrm{A}}^{\lceil N/2\rceil}\}$, $R_{\mathrm{B}}=\{R_{\mathrm{B}}^1, R_{\mathrm{B}}^2, \cdots, R_{\mathrm{B}}^{\lceil N/2\rceil}\}$, $j=1, 2, 3, \ldots, \lceil N/2\rceil$。

步骤五: 当TP接收到R_{A}和R_{B}后, 通过

$$R^i = R_{\mathrm{A}}^j \oplus R_{\mathrm{B}}^j \oplus K_{\mathrm{AT}}^j \oplus K_{\mathrm{BT}}^j \tag{7}$$

计算R^i的值, 比较Alice和Bob的秘密信息。由(7)式, 如果$R^i = 00$, 则他们的秘密信息相同, $X = Y$; 否则不相同, 即$X \neq Y$。最后, TP公布比较结果。

表 1 三个参与者执行的操作

Table 1 Actions performed by three participants

案例	Alice 的操作	Bob 的操作	TP 的操作
1	R	R	对反射的粒子执行 Bell 联合测量, 检测窃听者的存在
2	M	M	接收 R_{A} 和 R_{B}, 计算 R^{i}, 比较双方秘密信息是否相等

表 2 $M_{\mathrm{A}}^{j}(M_{\mathrm{B}}^{j})$ 和 C^{j} 的对应关系

Table 2 The corresponding relationship between $M_{\mathrm{A}}^{j}(M_{\mathrm{B}}^{j})$ and C^{j}

M_{A}^{j}	M_{B}^{j}	C^{j}
$\|0\rangle$	$\|0\rangle$	00
$\|0\rangle$	$\|1\rangle$	01
$\|1\rangle$	$\|0\rangle$	10
$\|1\rangle$	$\|1\rangle$	11

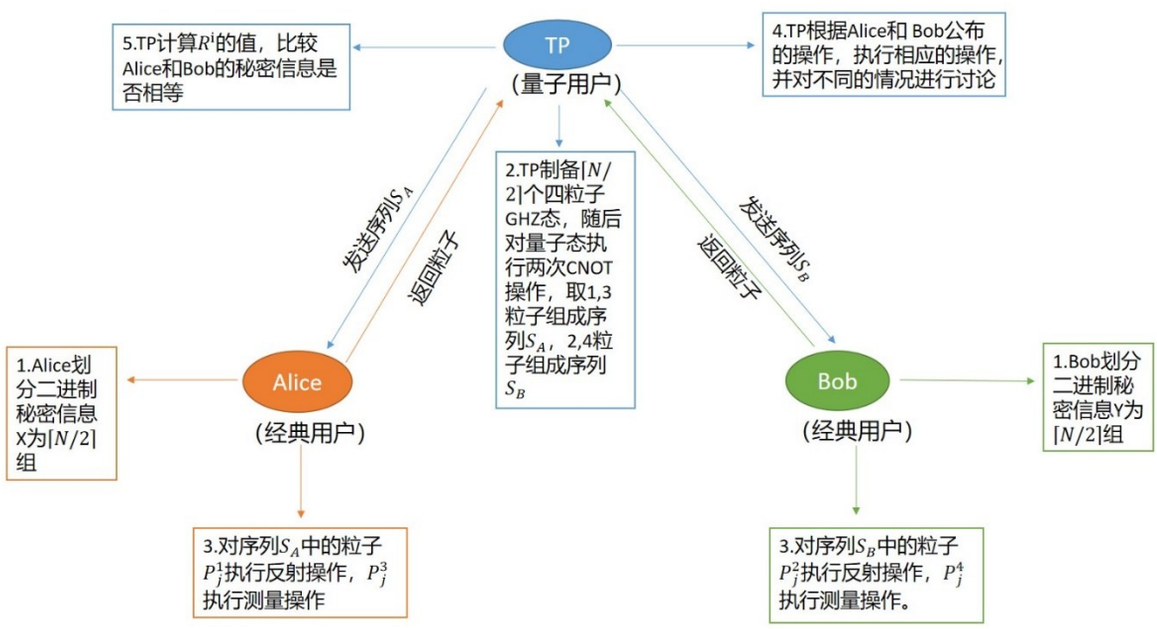

图 1 所提出协议流程图

Fig. 1 Flow chart of the proposed protocol

3 正确性分析

3.1 协议的正确性

Alice 和 Bob 是两个经典用户, 分别携带秘密信息 X 和 Y, 在半诚实 TP 的帮助下比较 X 和 Y 是否相等, 因此

$$R^{i}=R_{\mathrm{A}}^{j}\oplus R_{\mathrm{B}}^{j}\oplus K_{\mathrm{AT}}^{j}\oplus K_{\mathrm{BT}}^{j}=(C^{j}\oplus G_{\mathrm{A}}^{j}\oplus K_{\mathrm{AB}}^{j}\oplus K_{\mathrm{AT}}^{j})\oplus(C^{j}\oplus G_{\mathrm{B}}^{\mathrm{i}}\oplus K_{\mathrm{AB}}^{j}\oplus K_{\mathrm{BT}}^{j})\oplus K_{\mathrm{AT}}^{j}\oplus K_{\mathrm{BT}}^{j}=G_{\mathrm{A}}^{j}\oplus G_{\mathrm{B}}^{j}\,. \tag{8}$$

如果 $R^{i}=00$, 可以推导出 $G_{\mathrm{A}}^{j}=G_{\mathrm{B}}^{j}$, 即秘密信息 $X=Y$; 否则 $G_{\mathrm{A}}^{j}\neq G_{\mathrm{B}}^{j}$, 即秘密信息不相等 $X\neq Y$。

3.2　实例验证

为了说明协议的可行性, 用一个例子进行验证。

假设Alice和Bob共享二进制秘密信息$X=Y=1001101101$, 即$N=10$, 为了比较Alice和Bob的秘密信息X和Y是否相等, 将严格按照协议的规范进行比较。

在准备阶段, Alice和Bob共享密钥$K_{AB}=1101110101$, Alice和TP共享密钥$K_{AT}=1010001101$, Bob和TP共享密钥$K_{BT}=0110110110$。接下来按协议步骤执行, 具体描述如下。

步骤一: Alice和Bob将X和Y分成5组, $X=\{G_A^1,G_A^2,\cdots,G_A^5\}=\{10,01,10,11,01\}$, $Y=\{G_B^1,G_B^2,\cdots,G_B^5\}=\{10,01,10,11,01\}$。

步骤二: TP随机制备5个(2)式的量子态: $|G_1\rangle_{1234},|G_2\rangle_{1234},|G_3\rangle_{1234},|G_4\rangle_{1234},|G_1\rangle_{1234}$。划分为两个序列$S_A=\{P_1^1,|0\rangle,P_2^1,|0\rangle,P_3^1,|1\rangle,P_4^1,|1\rangle,P_5^1,|0\rangle\}$, $S_B=\{P_1^2,|0\rangle,P_2^2,|1\rangle,P_3^2,|0\rangle,P_4^2,|1\rangle,P_5^2,|0\rangle\}$。最后, TP将$S_A$和$S_B$分别发送给Alice和Bob。

步骤三: Alice和Bob对S_A和S_B中相同位置的粒子P_j^1和P_j^2执行R操作, 对粒子P_j^3和P_j^4执行M操作。

步骤四:

案例1: Alice和Bob分别对粒子$P_1^1,P_2^1,P_3^1,P_4^1,P_5^1(P_1^2,P_2^2,P_3^2,P_4^2,P_5^2)$执行R操作。TP收到反射的量子比特后执行Bell基联合测量。例如对P_j^1和P_j^2粒子执行Bell基联合测量, 由于理论初始态是$|\phi^+\rangle$, 如果Bell基测量结果不是$|\phi^+\rangle$, 说明通信过程存在窃听者, 协议终止, 否则TP公布测量结果$|\phi^+\rangle$, 进入下一步。假设方案中不存在窃听者, TP公布测量结果$|\phi^+\rangle,|\phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle,|\phi^+\rangle$。

案例2: Alice和Bob分别对S_A和S_B中的3、4粒子执行测量, 测量结果分别为$M_A=\{|0\rangle,|0\rangle,|1\rangle,|1\rangle,|0\rangle\}$、$M_B=\{|0\rangle,|1\rangle,|0\rangle,|1\rangle,|0\rangle\}$。根据表2, Alice和Bob根据TP公布的Bell态测量结果和自身Z基测量结果将测量结果编码为$C^j=\{00,01,10,11,00\}$。然后, Alice根据(6)式计算得到$R_A^1=00\oplus10\oplus11\oplus10=11$, $R_A^2=11$, $R_A^3=11$, $R_A^4=10$, $R_A^5=01$, 同样Bob计算得到$R_B^1=00\oplus10\oplus11\oplus01=00$, $R_B^2=11$, $R_B^3=00$, $R_B^4=00$, $R_B^5=10$。最后, Alice和Bob分别发送$R_A=\{11,11,11,10,01\}$、$R_B=\{00,11,00,00,10\}$给TP。

步骤五: TP接收到R_A、R_B后, 根据(7)式计算R^i的值, $R^1=11\oplus00\oplus10\oplus01=00$, $R^2=11\oplus11\oplus10\oplus10=00$, $R^3=00$, $R^4=00$, $R^5=00$, 即$R^1=R^2=R^3=R^4=R^5=00$, 说明Alice和Bob的秘密信息相等, 即$X=Y$, TP公布比较结果。

3.3　IBM量子云平台仿真实验验证

IBM量子云平台是一个在线平台, 用户可以通过网络访问IBM提供的原型量子处理器。接下来, 将通过IBM量子云平台仿真实验验证例子3.2的正确性。本实验假设协议中不存在窃听者, 即不执行步骤四的窃听检查过程。制备了4个不同的四粒子GHZ态, 对于不同的四粒子GHZ态, 设计了相应的量子模拟电路图, 如图2～5所示。针对所设计的电路图, 本次实验选择两个不同的后端(ibmq_qasm_simulator和ibmq_manila)并设置发射次数为8192, 其中ibmq_qasm_simulator是理想环境, ibmq_manila是真实量子环境。

本实验量子电路图的流程如下: 首先TP制备四粒子GHZ态, 分别发送序列S_A和S_B给Alice和Bob, Alice和Bob分别对S_A和S_B中的P_j^3和P_j^4粒子执行Z基测量, 实验结果如表3所示。

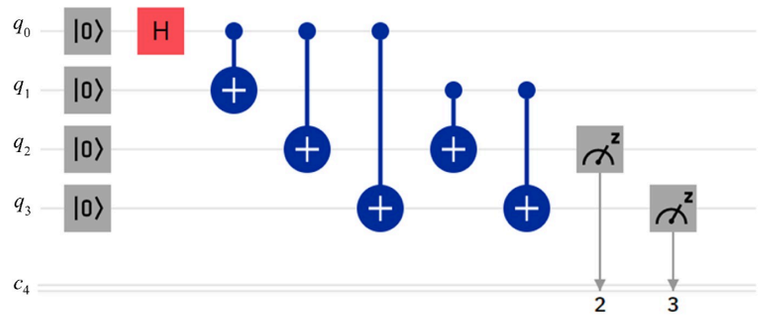

图2 量子态为$|G_1\rangle_{1234}$的量子电路图

Fig. 2 Quantum circuit diagram of quantum state for $|G_1\rangle_{1234}$

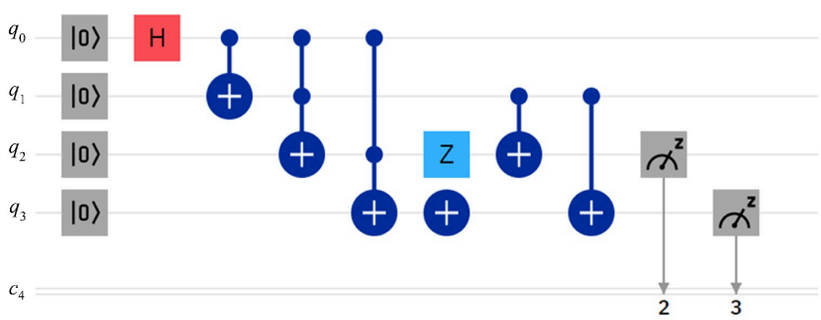

图3 量子态为$|G_2\rangle_{1234}$的量子电路图

Fig. 3 Quantum circuit diagram of quantum state for $|G_2\rangle_{1234}$

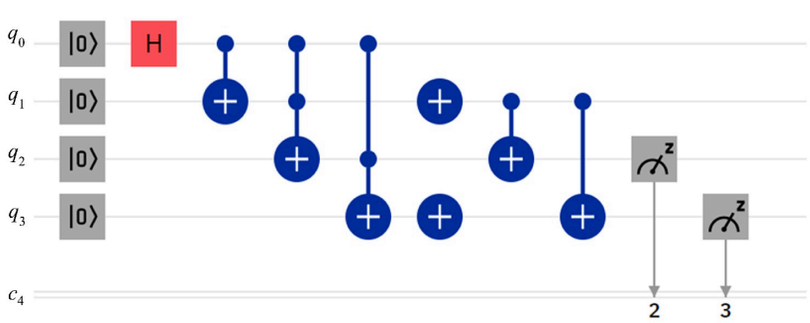

图4 量子态为$|G_3\rangle_{1234}$的量子电路图

Fig. 4 Quantum circuit diagram of quantum state for $|G_3\rangle_{1234}$

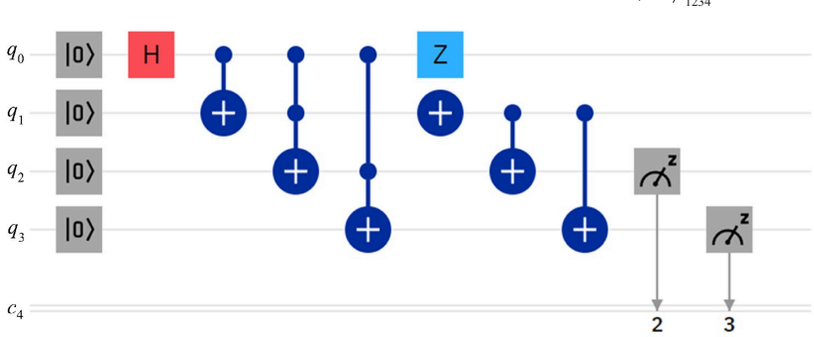

图5 量子态为$|G_4\rangle_{1234}$的量子电路图

Fig. 5 Quantum circuit diagram of quantum state for $|G_4\rangle_{1234}$

若运行环境为理想环境 (ibmq_qasm_simulator), 即不存在噪声干扰。根据表3的实验结果, 当TP制备的初始态为$\left|\varphi_1\right\rangle_{1234}$时, Alice和Bob对$P_j^3$和$P_j^4$粒子执行Z基测量, 测量结果为$|0000\rangle$的概率是100%, 其中粒子3和4的测量结果与理论预测的00态相符合。同样地, 当初始态为$\left|\varphi_2\right\rangle_{1234}$、$\left|\varphi_3\right\rangle_{1234}$、$\left|\varphi_4\right\rangle_{1234}$时, 对$P_j^3$和$P_j^4$粒子执行Z基测量, 测量结果分别为$|0001\rangle$、$|0010\rangle$、$|0011\rangle$, 概率都是100%, 其中3、4粒子分别对应01、10、11, 与理论测量结果一致。

若运行环境为真实量子环境 (ibmq_manila), 与理想环境相比, 由于存在噪声干扰, 对P_j^3和P_j^4粒子分别执行Z基测量时, 测量结果存在误差, 但3、4粒子的Z基测量结果概率整体超过了50%。

综上所述, IBM量子云平台仿真实验证明了例子3.2是正确可行的。

表3 不同量子态在不同后端的实验结果比较

Table 3 Comparison of experimental results of different quantum states at different back ends

运行环境	$\left\|\varphi_1\right\rangle_{1234}$	$\left\|\varphi_2\right\rangle_{1234}$	$\left\|\varphi_3\right\rangle_{1234}$	$\left\|\varphi_4\right\rangle_{1234}$
后端: ibmq_qasm_simulator 发射次数: 8192	$\|0000\rangle$: 100%	$\|0001\rangle$: 100%	$\|0010\rangle$: 100%	$\|0011\rangle$: 100%
后端: ibmq_manila 发射次数: 8192	$\|0000\rangle$: 86.18%	$\|0001\rangle$: 52.87%	$\|0010\rangle$: 65.04%	$\|0011\rangle$: 62.39%

4 安全性分析

4.1 外部攻击

假设存在一个窃听者Eve, 他想要窃取参与者Alice和Bob的秘密信息X和Y, 则需要得到M_A和M_B的值。接下来按照协议的步骤进行外部攻击的分析。在第2节的步骤一和步骤五中没有粒子的传输, 因此Eve不会发动任何攻击; 在第2节的步骤二中, TP将序列S_A和S_B分别发送给Alice和Bob, Eve可以发动测量重发攻击、拦截重发攻击、纠缠测量攻击等常见的攻击以窃取Alice和Bob的秘密信息。假设窃听者Eve发动拦截重发攻击获取Alice和Bob的秘密信息, Eve拦截TP发送给Alice和Bob的序列S_A和S_B, 使用量子存储器存储, 然后发送使用Z基制备的假光子序列给Alice和Bob, 并返回S_A和S_B给TP。但Eve无论如何都不能窃取到Alice和 Bob的任何信息, 因为在案例一中Alice和Bob对粒子P_j^1和P_j^2执行R操作, TP对反射的粒子执行窃听检查, 若Bell测量结果与初始态不一致, 将会发现协议中存在窃听者; 在第2节的步骤三中, Alice和Bob对粒子P_j^1和P_j^2执行R操作, 将粒子返回给TP, Eve可以发动常见的外部攻击窃取秘密信息, 但Eve同样会被TP的窃听检查检测出来; 在第2节的步骤四中, Alice和Bob将R_A和R_B发送给TP, Eve可以窃取R_A和R_B的值, 但Eve并不知道参与者之间的预密钥信息K_{AB}、K_{AT}、K_{BT}, 因此Eve无法获取参与者的任何秘密信息。

总之, Eve无法通过发动外部攻击获取参与者的秘密信息。

4.2 内部攻击

在量子通信协议中, 内部攻击比外部攻击的威胁更大, 这是因为参与者窃取秘密信息的机会更多。参与者攻击主要有两种: 第一种不诚实的参与者Alice和Bob相互窃取对方信息, 第二种半诚实TP窃取参与者Alice和Bob的秘密信息。

4.2.1 参与者Alice或Bob的攻击

假设不诚实参与者Alice想要窃取Bob的秘密信息, 为了获取Bob的秘密信息, Alice必须拦截和存储TP发送给Bob的序列以及Bob返回给TP的序列。Alice是一个外部窃听者, 由4.1外部攻击的阐述可知窃听者将会被检测出来。

此外, Alice可以通过 (2) 式以及四粒子GHZ态的纠缠特性和它自身的测量结果M_{A}^{j}推导出Bob的测量结果M_{B}^{j}, 但Alice不知道Bob和TP的密钥K_{BT}, 因此Alice无法窃取Bob的秘密信息。同样, 假设不诚实参与者Bob想要窃取Alice的秘密信息, Bob需要截取和存储TP发送给Alice的序列以及Alice返回给TP的序列, 但Bob是外部窃听者, 会被检测出来。Bob不能获取Alice和TP的密钥K_{AT}, 因此也无法获取Alice的秘密信息。

4.2.2 半诚实第三方TP的攻击

半诚实第三方TP可以实施各种攻击, 但在本协议中不允许他与任何参与者密谋。TP最有机会获取秘密信息X和Y, 因为他能获取Alice和Bob的测量结果M_{A}^{j}和M_{B}^{j}、R_{A}^{j}和R_{B}^{j}、以及Alice和Bob比较信息的结果, 但TP不知道Alice和Bob的共享密钥K_{AB}, 因此TP无法获取秘密信息X和Y, 半诚实TP的攻击是无效的。

4.3 特洛伊木马攻击

该协议不是单向传输的, 因此需要考虑延迟光子特洛伊木马攻击和不可见光子 (IPE) 窃听攻击, 为了抵御这两种攻击, Alice和Bob需要安装光子数分裂器 (PNS) 以及长波量子滤波器[33−35]。

5 比较分析

5.1 与半量子私有协议的比较

本协议参与者之间需要共享预密钥, 虽然不可避免地增加了资源消耗, 但这是可以接受的, 与文献 [27, 31] 的协议相比, 所提出协议的安全性更高。量子比特效率可以表示为[15]

$$\eta=\frac{r_{\mathrm{c}}}{r_{\mathrm{q}}}, \tag{9}$$

式中: r_{c}是比较经典位的个数, r_{q}是消耗量子的个数。文献 [31]提出的协议中比较了N个粒子的秘密信息 ($r_{\mathrm{c}}=N$), TP需要制备$2N$个Bell态, 也就是消耗$4N$个粒子, $r_{\mathrm{q}}=4N$, 因此该协议效率为25%; 文献 [3] 提出的协议中, TP需制备$8N(1+\theta)$个两粒子乘积态, 其中θ是个固定系数, 大约消耗$16N$个粒子, $r_{\mathrm{q}}=16N$, 因此该协议效率为6.25%; 文献 [27] 提出的协议中, TP需要制备$32N$个单光子态, 也就是消耗$32N$个粒子, $r_{\mathrm{q}}=32N$, 该协议效率为3.125%; 文献 [28] 中, 经计算两个协议的效率都是25%;本研究所提出协议比较了N个粒子的秘密信息, 需要TP制备$\lceil N/2\rceil$个四粒子GHZ态 (即$2N$个粒子), 效率为50%。在相同条件下, 比较其他4个SQPC协议可知本协议量子比特效率最高。此外, 本协议的经典参与者无需使用Z基制备新的量子态, 降低了经典用户对量子能力的要求, 节约了量子资源。与各协议的比较详见表4。

5.2 与全量子私有协议的比较

所提出SQPC协议中, 用户的量子操作仅需Z基测量和无干扰反射粒子, 而文献 [32] 提出的QPC协议中用户需要执行复杂的量子操作, 相比之下本协议消耗的量子资源更少。对于用户所需的量子设备, 本协议只

需要量子存储器, 而文献 [32] 的协议需要量子寄存器、纠缠态发生器、量子存储器, 量子设备价格昂贵、维护相对困难, 因此本协议量子硬件成本更低, 能更好地应对量子设备存在的硬件故障问题。总之, 与全量子QPC协议相比, 本协议节约了量子硬件成本, 量子资源消耗更少, 如表5所示。

表4 相似半量子私有比较协议的比较

Table 4 Comparison of similar semi−quantum private comparison protocols

	文献 [31] 协议	文献 [3] 协议	文献 [27] 协议	文献 [28] 协议		本研究提出的协议
				协议1	协议2	
初始量子态	Bell态	两粒子乘积态	单光子	Bell态	Bell态	四粒子GHZ态
TP的测量操作	单光子测量和Bell基测量	单光子测量	单光子测量和Bell基测量	单光子测量和Bell基测量	Bell基测量	Bell基测量
经典参与者执行的操作	使用Z基制备新的量子态; Z基测量; 无干扰的反射粒子	使用Z基制备新的量子态; Z基测量; 无干扰的反射粒子	使用Z基制备新的量子态; Z基测量; 无干扰的反射粒子	使用Z基制备新的量子态; 无干扰的反射粒子;	使用Z基制备新的量子态; Z基测量; 无干扰的反射粒子	Z基测量; 无干扰的反射粒子;
量子效率	25%	6.25%	3.125%	25%	25%	50%

表5 与全量子能力量子私有协议的比较

Table 5 Comparison with quantum private protocol of full quantum capability

	文献 [32] 协议	本研究提出的协议
用户的量子操作	产生诱骗态; 执行Bell测量和Z基测量; 将量子比特存储在量子存储器中	Z基测量; 无干扰的反射量子位
用户所需量子设备	量子寄存器, 纠缠态发生器, 量子存储器	量子存储器

注: 此处用户不包括第三方TP

6 结　论

提出了一种基于四粒子GHZ态的半量子私有比较协议, 两个经典参与者比较双方的秘密信息是否相等, 并通过分析该协议的安全性和可行性, 证明此协议是安全可靠的, 能够抵御内部和外部攻击。与其他SQPC协议相比, 经典参与者对量子能力的要求更低, 仅需Z基测量和无干扰反射粒子, 且具有更优的量子比特效率。所提出协议应用了半量子模型, 经典参与者不再需要使用价格昂贵的量子设备, 节约了硬件成本, 降低了用户对量子资源的要求, 在实验中更容易实现。此外, 通过IBM量子云平台对此协议进行了仿真实验, 保证了其可行性和正确性。

参考文献:

[1] Yang Y G, Wen Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement [J]. *Journal of Physics A: Mathematical and Theoretical*, 2009, 42(5): 055305.

[2] Yang Y G, Cao W F, Wen Q Y. Secure quantum private comparison [J]. *Physica Scripta*, 2009, 80(6): 065002.

[3] Ye T Y, Ye C Q. Measure-resend semi-quantum private comparison without entanglement [J]. *International Journal of Theoretical Physics*, 2018, 57(12): 3819-3834.

[4] Liu W, Wang Y B, Cui W. Quantum private comparison protocol based on bell entangled states [J]. *Communications in Theoretical Physics*, 2012, 57(4): 583-588.

[5] Ji Z X, Ye T Y. Multi-party quantum private comparison based on the entanglement swapping of *d*-level cat states and *d*-level Bell states [J]. *Quantum Information Processing*, 2017, 16(7): 177.

[6] Wu W Q, Zhao Y X. Quantum private comparison of size using *d*-level Bell states with a semi-honest third party [J]. *Quantum Information Processing*, 2021, 20(4): 155.

[7] Liu W, Wang Y B. Quantum private comparison based on GHZ entangled states[J]. *International Journal of Theoretical Physics*, 2012, 51(11): 3596-3604.

[8] Huang S L, Hwang T, Gope P. Multi-party quantum private comparison protocol with an almost-dishonest third party using GHZ states [J]. *International Journal of Theoretical Physics*, 2016, 55(6): 2969-2976.

[9] Ji Z X, Fan P R, Zhang H G, *et al*. Greenberger-Horne-Zeilinger-based quantum private comparison protocol with bit-flipping [J]. *Physica Scripta*, 2021, 96(1): 015103.

[10] Zhang W W, Li D, Li Y B. Quantum private comparison protocol with W states [J]. *International Journal of Theoretical Physics*, 2014, 53(5): 1723-1729.

[11] Sun Z W, Long D Y. Quantum private comparison protocol based on cluster states [J]. *International Journal of Theoretical Physics*, 2013, 52(1): 212-218.

[12] Zhou M K. Improvements of quantum private comparison protocol based on cluster states [J]. *International Journal of Theoretical Physics*, 2018, 57(1): 42-47.

[13] Ye T Y, Ji Z X. Two-party quantum private comparison with five-qubit entangled states [J]. *International Journal of Theoretical Physics*, 2017, 56(5): 1517-1529.

[14] Liu W, Wang Y B, Jiang Z T, *et al*. New quantum private comparison protocol using χ-type state [J]. *International Journal of Theoretical Physics*, 2012, 51(6): 1953-1960.

[15] Pan H M. Quantum private comparison based on χ-type entangled states [J]. *International Journal of Theoretical Physics*, 2017, 56(10): 3340-3347.

[16] Ji Z X, Ye T Y. Quantum private comparison of equal information based on highly entangled six-qubit genuine state [J]. *Communications in Theoretical Physics*, 2016, 65(6): 711-715.

[17] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical bob [J]. *Physical Review Letters*, 2007, 99(14): 140501.

[18] Yin A H, Chen T. Authenticated semi-quantum secret sharing based on GHZ-type states [J]. *International Journal of Theoretical Physics*, 2021, 60(1): 265-273.

[19] Tian Y, Li J, Chen X B, *et al*. An efficient semi-quantum secret sharing protocol of specific bits [J]. *Quantum Information Processing*, 2021, 20(6): 1-11.

[20] Tsai C W, Yang C W, Lee N Y. Semi-quantum secret sharing protocol using W-state [J]. *Modern Physics Letters A*, 2019, 34 (27): 1950213.

[21] Tsai C W, Yang C W, Lee N Y. Lightweight mediated semi-quantum key distribution protocol [J]. *Modern Physics Letters A*, 2019, 34(34): 1950281.

[22] Lin P H, Tsai C W, Hwang T. Mediated semi-quantum key distribution using single photons [J]. *Annalen Der Physik*, 2019, 531 (8): 1800347.

[23] Hajji H, El Baz M. Qutrit-based semi-quantum key distribution protocol [J]. *Quantum Information Processing*, 2021, 20(1): 1-25.

[24] Rong Z B, Qiu D W, Mateus P, *et al*. Mediated semi-quantum secure direct communication [J]. *Quantum Information Processing*, 2021, 20(2): 1-13.

[25] Sun Y H, Yan L L, Chang Y, *et al*. Two semi-quantum secure direct communication protocols based on Bell states [J]. *Modern Physics Letters A*, 2019, 34(1): 1950004.

[26] Rong Z B, Qiu D W, Zou X F. Semi-quantum secure direct communication using entanglement [J]. *International Journal of Theoretical Physics*, 2020, 59(6): 1807-1819.

[27] Lin P H, Hwang T, Tsai C W. Efficient semi-quantum private comparison using single photons [J]. *Quantum Information Processing*, 2019, 18(7): 207.

[28] Jiang L Z. Semi-quantum private comparison based on Bell states [J]. *Quantum Information Processing*, 2020, 19(6): 1-21.

[29] Zhou N R, Xu Q D, Du N S, *et al*. Semi-quantum private comparison protocol of size relation with *d*-dimensional Bell states [J]. *Quantum Information Processing*, 2021, 20(3): 1-15.

[30] Yan L L, Zhang S B, Chang Y, *et al*. Semi-quantum private comparison protocol with three-particle G-like states [J]. *Quantum Information Processing*, 2021, 20(1): 17.

[31] Chou W, Hwang T, Gu J. Semi-quantum private comparison protocol under an almost-dishonest third party [OL]. 2016, arXiv: 1607.07961, https://arxiv.org/abs/1607.07961.

[32] Xu Q D, Chen H Y, Gong L H, *et al*. Quantum private comparison protocol based on four-particle GHZ states [J]. *International Journal of Theoretical Physics*, 2020, 59(6): 1798-1806.

[33] Deng F G, Li X H, Zhou H Y, *et al*. Improving the security of multiparty quantum secret sharing against Trojan horse attack [J]. *Physical Review A*, 2005, 72(4): 044302.

[34] Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons [J]. *Physics Letters A*, 2006, 351(1-2): 23-25.

[35] Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles [J]. *Physical Review A*, 2006, 74(5): 054302.