基于 d 级单粒子态的能实现大小比较的半量子隐私比较

耿茂洁, 徐天婕, 陈颖, 叶天语*

浙江工商大学信息与电子工程学院, 杭州 310018

*联系人, E-mail: happyty@aliyun.com

收稿日期: 2022-01-15; 接受日期: 2022-03-04; 网络出版日期: 2022-08-02

国家自然科学基金(编号: 62071430, 61871347)和浙江省属高校基本科研业务费专项(编号: JRK21002)资助

摘要 本文提出一个新颖的基于 d 级单粒子态的能实现大小关系比较的半量子隐私比较(Semiquantum Private Comparison, SQPC)协议. 该协议假定存在一个被允许按照他自己的意愿错误行事但不能与其他任何人共谋的半忠诚第三方(Third Party, TP). 在TP的帮助下, 该协议能比较出两个经典用户秘密信息的大小关系. 正确性分析表明, 该协议能得到正确的比较结果; 安全性分析表明, 该协议能抵抗一些著名的外部攻击和参与者攻击. 该协议仅采用 d 级单粒子态作为初始量子资源, 只需要TP进行 d 级单粒子测量, 并且能确保TP无法知道准确的比较结果. 与目前唯一能实现大小关系比较的SQPC协议[Quantum Inf. Process. **20**, 124 (2021)]相比, 该协议在初始量子资源的实验制备、TP的实验测量以及TP是否知道比较结果这几个方面具有一定的优势.

关键词 半量子隐私比较, 大小关系, d 级单粒子态, 半忠诚第三方

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

1 引言

1982年, Yao^[1]提出了首个经典隐私比较协议; 该协议后来被生动地称为“百万富翁问题”. 该协议的目的是在不暴露百万富翁真实财产的前提下比较出谁更富有. 随后, 经典隐私比较在无记名投票、电子拍卖、数据挖掘等场景中发挥了核心作用. 经典隐私比较协议的安全性高度依赖于计算复杂性. 然而, 随着量子并行计算的发展, 经典隐私比较变得越来越脆弱.

在1984年, Bennett和Brassard^[2]提出了首个量子密

码协议, 即BB84量子密钥分配(Quantum Key Distribution, QKD)协议. 从那以后, 量子密码学得到了迅速发展. 2009年, Yang和Wen^[3]将经典隐私比较引入到量子领域从而提出了首个量子隐私比较(Quantum Private Comparison, QPC)协议. 随后, 学者们提出了一系列QPC协议^[4-15]. 已有的QPC协议可以划分为两类: 一类只实现秘密信息相等性的比较; 另一类能实现秘密信息大小关系的比较. 例如, 文献[3-9]的QPC协议属于第一类, 而文献[10-15]的QPC协议属于第二类.

在2007和2009年, Boyer等人^[16,17]提出了两个具有

引用格式: 耿茂洁, 徐天婕, 陈颖, 等. 基于 d 级单粒子态的能实现大小比较的半量子隐私比较. 中国科学: 物理学 力学 天文学, 2022, 52: 290311
Geng M J, Xu T J, Chen Y, et al. Semiquantum private comparison of size relationship based on d -level single-particle states (in Chinese). Sci Sin-Phys Mech Astron, 2022, 52: 290311, doi: 10.1360/SSPMA-2022-0025

代表性的半量子密钥分配(Semiquantum Key Distribution, SQKD)协议, 这意味着半量子密码学的诞生. 2016年, Chou等人^[18]利用Bell纠缠态和量子纠缠交换提出了首个半量子隐私比较(Semiquantum Private Comparison, SQPC)协议. 后来, 学者们相继提出了许多SQPC协议^[19-23]. 例如, 文献[19]利用两粒子乘积态提出了一个具有测量-重发特征的SQPC协议, 实现了两个经典用户秘密信息相等性的比较; 文献[20-22]利用单光子提出了不同的SQPC协议, 也实现了两个经典用户秘密信息相等性的比较; 文献[23]基于 d 维Bell纠缠态设计了一个SQPC协议, 实现了两个经典用户秘密信息大小关系的比较. 值得指出的是, 文献[23]的协议是目前唯一能实现两个经典用户秘密信息大小关系比较的SQPC协议.

基于以上分析, 为了实现两个经典用户秘密信息的大小关系比较, 本文提出了一种新颖的基于 d 级单粒子态的能实现大小关系比较的SQPC协议. 该协议假定存在一个被允许按照她自己意愿错误行事但不能与其他任何人共谋的半忠诚第三方(Third Party, TP)^[24]. 该协议仅采用 d 级单粒子态作为初始量子资源, 只需要TP进行 d 级单粒子测量, 并确保TP无法知道具体的比较结果. 与目前唯一能实现秘密信息大小关系比较的SQPC协议^[23]相比, 该协议降低了初始量子资源的实验制备难度, 降低了TP的实验测量难度以及增强了比较结果对于TP的隐秘性.

本文剩余部分安排如下: 第2节描述所提出的基于 d 级单粒子态的能实现秘密信息大小关系比较的SQPC协议; 第3节进行正确性分析; 第4节详细验证安全性; 最后, 第5节给出讨论和结论.

2 协议描述

在 d 级希尔伯特空间, 可以定义一个常用的正交基为 $MB_Z = \{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$. 在对 MB_Z 基内的量子态进行 d 级离散量子傅里叶变换后, 可以得到一组新的正交基 $MB_F = \{F|0\rangle, F|1\rangle, \dots, F|d-1\rangle\}$, 其中

$$F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i j k}{d}} |k\rangle, \quad (1)$$

且 $j=0, 1, \dots, d-1$. 这里, MB_Z 和 MB_F 是两组共轭基.

假设两个经典用户, Alice和Bob, 分别拥有秘密信息 $X = (x_1, x_2, \dots, x_n)$ 和 $Y = (y_1, y_2, \dots, y_n)$, 其中 $x_i, y_i \in \{0, 1, \dots, h\}$, $i = 1, 2, \dots, n$ 和 $d = 2h + 1$. Alice和Bob事先通过一个安全的带第三方的SQKD协议^[25]共享一个密钥序列 $K_{AB} = \{K_{AB}^1, K_{AB}^2, \dots, K_{AB}^n\}$, 其中 $K_{AB}^i \in \{0, 1, \dots, d-1\}$. 所提出的基于 d 级单粒子态的能实现大小比较的SQPC协议的具体步骤说明如下. 为清晰起见, 图1给出了它的流程图. 需要说明的是, 协议中涉及的量子信道被假设为理想量子信道.

步骤1: TP制备一个长度为 $N=8n(1+\delta)$ 的单粒子态序列 $S_A = \{|S_A^1\rangle, |S_A^2\rangle, \dots, |S_A^N\rangle\}$ ($S_B = \{|S_B^1\rangle, |S_B^2\rangle, \dots, |S_B^N\rangle\}$), 其中, n 是秘密信息的长度, δ 是大于0的参数, N 是大于0的整数, $|S_A^i\rangle$ ($|S_B^i\rangle$)是以相等概率从 MB_Z 或 MB_F 随机选出. 然后, TP将 S_A (S_B)的粒子一个个地发送给Alice (Bob). 在TP传送第一个粒子给Alice (Bob)后, 她只在接收到前一个粒子后才发送下一个粒子.

步骤2: 在从TP接收到每个粒子后, Alice (Bob)从以下两个操作中随机选择一个: 利用 MB_Z 基测量接收到的粒子并重新发送一个新的与测量所得态相同的量子态给TP (这种操作称为MEASURE模式); 直接返回接收到的粒子给TP (这种操作称为REFLECT模式). 当她(他)选择MEASURE时, Alice (Bob)记录下相应的测量结果.

步骤3: 在接收到Alice (Bob)发送的所有粒子后, TP给她(他)发送一个确认信号. 然后, TP利用初始制备基测量每个粒子. 之后, TP宣布哪些粒子被制备处于 MB_Z 基, 而Alice (Bob)宣布她(他)选择REFLECT的位置. 这里, 定义4种类型的粒子, 即 B_{Z-M} 粒子、 B_{Z-R} 粒子、 B_{F-R} 粒子以及 B_{F-M} 粒子, 如表1所示. 每种类型粒子的数量接近于 $N/4$.

对于 B_{Z-R} 粒子和 B_{F-R} 粒子, TP通过比较她的测量结果和它们的初始制备态计算错误率. 如果 B_{Z-R} 粒子的错误率和 B_{F-R} 粒子的错误率都为0, 她们将继续执行协议; 否则, 她们将结束协议.

步骤4: TP从 B_{Z-M} 粒子中随机选出 n 个粒子作为TEST粒子, 并告诉Alice (Bob)所选中的位置. 然后, Alice (Bob)公布这些TEST粒子的测量结果. TP检测它们的错误率. 如果错误率为0, 她们将继续执行协议; 否

图 1 提出的能比较出大小关系的SQPC协议的流程图

Figure 1 The flow chart of the proposed SQPC protocol of size relationship.

表 1 四种粒子及其应用

Table 1 Four kinds of particles and their applications

类型	TP的初始制备基	Alice (Bob)的操作	应用
B_Z-M	MB_Z	MEASURE	窃听检测和隐私比较
B_Z-R	MB_Z	REFLECT	窃听检测
B_F-R	MB_F	REFLECT	窃听检测
B_F-M	MB_F	MEASURE	忽略

则, 她们将结束协议.

步骤5: TP和Alice (Bob)从剩余的 B_Z-M 粒子中挑选出前 n 个粒子用于隐私比较. Alice (Bob)手中的这 n 个选中粒子的测量结果的经典取值被表示为 $S_{A1} = \{S_{A1}^1, S_{A1}^2, \dots, S_{A1}^n\}$ ($S_{B1} = \{S_{B1}^1, S_{B1}^2, \dots, S_{B1}^n\}$). 由于TP自己制备这 n 个选中的粒子, 她能自动地知道 S_{A1} (S_{B1}). 与此同时, TP生成一个经典整数序列 S_{A2} (S_{B2})满足 $S_{A1}^i \oplus S_{A2}^i = S$ ($S_{B1}^i \oplus S_{B2}^i = S$). 这里, 符号 $\oplus$ 代表模 d 加法; S 是一个取值只被TP知道的常数; $S \in \{0, 1, \dots, d-1\}$, $S_{A1}^i, S_{A2}^i, S_{B1}^i, S_{B2}^i \in \{0, 1, \dots, d-1\}$, $i = 1, 2, \dots, n$. 然后, Alice (Bob)根据 K_{AB} 的奇偶性编码自己的秘密消息: 如果 $\text{mod}(K_{AB}^i, 2) = 0$, 令 $m_A^i = x_i$ ($m_B^i = y_i$); 如果 $\text{mod}(K_{AB}^i, 2) = 1$, 令 $m_A^i = (d-1) - x_i$

($m_B^i = (d-1) - y_i$). 之后, Alice (Bob)计算 $R_A^i = S_{A1}^i \oplus m_A^i \oplus K_{AB}^i$ ($R_B^i = S_{B1}^i \oplus m_B^i \oplus K_{AB}^i$). 最后, Alice (Bob)通过经典信道将 R_A (R_B)发送给TP, 其中 $R_A = \{R_A^1, R_A^2, \dots, R_A^n\}$ ($R_B = \{R_B^1, R_B^2, \dots, R_B^n\}$).

步骤6: TP计算 $R_T^i = (R_B^i \oplus S_{B2}^i) \ominus (R_A^i \oplus S_{A2}^i)$, 其中符号 $\ominus$ 表示模 d 减法, $i = 1, 2, \dots, n$. 然后, TP根据以下规则从 R_T^i 产生一个变量 r_i :

$$r_i = \begin{cases} 0, & \text{如果 } R_T^i = 0, \\ -1, & \text{如果 } 0 < R_T^i \leq h, \\ 1, & \text{如果 } h < R_T^i \leq 2h. \end{cases} \quad (2)$$

最后, TP向Alice和Bob公布 r_i .

步骤7: 根据 r_i 和 K_{AB}^i , Alice和Bob通过计算以下公

式得到 x_i 和 y_i 的大小关系, 其中 $i = 1, 2, \dots, n$:

$$R_i = \begin{cases} 0, & \text{如果 } r_i \times (-1)^{\text{mod}(K_{AB}^i, 2)} = 0, \\ -1, & \text{如果 } r_i \times (-1)^{\text{mod}(K_{AB}^i, 2)} = -1, \\ 1, & \text{如果 } r_i \times (-1)^{\text{mod}(K_{AB}^i, 2)} = 1, \end{cases} \quad (3)$$

式中, $R_i = 0$ 意味着 $x_i = y_i$, $R_i = -1$ 意味着 $x_i < y_i$, $R_i = 1$ 意味着 $x_i > y_i$.

3 正确性分析

本节将分析输出结果的正确性. 根据 $S_{A1}^i \oplus S_{A2}^i = S$, $S_{B1}^i \oplus S_{B2}^i = S$, $R_A^i = S_{A1}^i \oplus m_A^i \oplus K_{AB}^i$ 以及 $R_B^i = S_{B1}^i \oplus m_B^i \oplus K_{AB}^i$, 可以得到

$$\begin{aligned} R_T^i &= (R_B^i \oplus S_{B2}^i) \odot (R_A^i \oplus S_{A2}^i) \\ &= (S_{B1}^i \oplus m_B^i \oplus K_{AB}^i \oplus S_{B2}^i) \odot (S_{A1}^i \oplus m_A^i \oplus K_{AB}^i \oplus S_{A2}^i) \\ &= (m_B^i \oplus K_{AB}^i \oplus S) \odot (m_A^i \oplus K_{AB}^i \oplus S) \\ &= m_B^i \odot m_A^i. \end{aligned} \quad (4)$$

根据式(4)以及Alice和Bob的编码规则, 可以得到: 如果 $\text{mod}(K_{AB}^i, 2) = 0$, 那么 $R_T^i = y_i \odot x_i$; 如果 $\text{mod}(K_{AB}^i, 2) = 1$, 那么 $R_T^i = x_i \odot y_i$. 根据式(2)可知, 如果 $h_i^1 \odot h_i^2 = 0$, 那么 $r_i = 0$, 意味着 $h_i^1 = h_i^2$; 如果 $0 < h_i^1 \odot h_i^2 \leq h$, 那么 $r_i = -1$, 意味着 $h_i^1 > h_i^2$; 如果 $h < h_i^1 \odot h_i^2 \leq 2h$, 那么 $r_i = 1$, 意味着 $h_i^1 < h_i^2$. 这里, $h_i^1, h_i^2 \in \{x_i, y_i\}$. 进一步地, 根据式(3), 当

$$\text{mod}(K_{AB}^i, 2) = 0 \text{ 时, 可以得到 } r_i = \begin{cases} 0, & \text{如果 } R_i = 0 \\ -1, & \text{如果 } R_i = -1; \text{ 当} \\ 1, & \text{如果 } R_i = 1 \end{cases}$$

$$\text{mod}(K_{AB}^i, 2) = 1 \text{ 时, 可以得到 } r_i = \begin{cases} 0, & \text{如果 } R_i = 0 \\ -1, & \text{如果 } R_i = 1 \\ 1, & \text{如果 } R_i = -1 \end{cases} \text{ . 因}$$

此, $R_i = 0$ 意味着 $x_i = y_i$; $R_i = -1$ 意味着 $x_i < y_i$; $R_i = 1$ 意味着 $x_i > y_i$. 现在可以得出结论, 本文协议的输出是正确的.

为清晰起见, 用一个例子来进一步验证比较结果的正确性. 假设 $x_i = 2$, $y_i = 4$, $h = 5$, $d = 11$ 和

$\text{mod}(K_{AB}^i, 2) = 1$. Alice (Bob)选中的用于隐私比较的粒子的测量结果对应经典值为 S_{A1}^i (S_{B1}^i). 由于TP自己制备这个选中的粒子, 她能自动知道 S_{A1}^i (S_{B1}^i). TP产生一个经典整数 S_{A2}^i (S_{B2}^i)使得 $S_{A1}^i \oplus S_{A2}^i = S$ ($S_{B1}^i \oplus S_{B2}^i = S$)成立. 这里, S 是一个常数, 且 $S_{A1}^i, S_{A2}^i, S_{B1}^i, S_{B2}^i, S \in \{0, 1, \dots, d-1\}$. 由于 $\text{mod}(K_{AB}^i, 2) = 1$, Alice (Bob)将 x_i (y_i)编码成 $m_A^i = (d-1) - x_i = 8$ ($m_B^i = (d-1) - y_i = 6$). 然后, Alice (Bob)计算 $R_A^i = S_{A1}^i \oplus m_A^i \oplus K_{AB}^i$ ($R_B^i = S_{B1}^i \oplus m_B^i \oplus K_{AB}^i$). 最后, Alice (Bob)将 (R_B^i) 发送给TP. TP计算 $R_T^i = (R_B^i \oplus S_{B2}^i) \odot (R_A^i \oplus S_{A2}^i) = m_B^i \odot m_A^i = 9$. 根据式(2), TP可以得到 $r_i = 1$. TP将 r_i 公布给Alice和Bob. 由于 $r_i \times (-1)^{\text{mod}(K_{AB}^i, 2)} = -1$, 根据式(3), Alice和Bob得到 $R_i = -1$. 因此, Alice和Bob得出 $x_i < y_i$.

4 安全性分析

在这部分, 验证所提出的协议对外部攻击和参与者攻击都是安全的.

4.1 外部攻击

在所提出的协议中, Alice扮演与Bob相同的角色. 不失一般性, 只验证从TP发送给Alice以及返回给TP的粒子的传输安全性. 在这些传输中, Eve可能会发起一些著名的攻击, 如截获-重发攻击、测量-重发攻击以及纠缠-测量攻击等, 来获取关于Alice的秘密消息的一些有用信息.

(1) 截获-重发攻击

为了尝试得到Alice对用于隐私比较的粒子的测量结果, Eve截获从TP发送给Alice的 S_A 的粒子并将她事先制备处于 MB_Z 基的假粒子发送给Alice; 在Alice对假粒子执行她的操作后, Eve截获Alice返回的粒子并将她自己手中的真实粒子发送给TP. 显然, 如果Alice选择进行REFLECT, 不管真实粒子是什么, Eve的攻击将不会被步骤3检测到. 然后, 考虑Alice选择进行MEASURE. 如果真实粒子处于 MB_F 基, 根据表1, 这个粒子将被忽略从而使得Eve的攻击不会被检测到; 如果它处于 MB_Z 基并被选中作为一个TEST粒子, Eve的

攻击在步骤4将以 $(d-1)/d$ 的概率被检测到. 总之, Eve的这种攻击不可避免地被检测到的原因在于两个方面: 一方面, Alice的操作对于Eve来说是随机的; 另一方面, Eve的假粒子很可能与TP制备的真实粒子不同.

(2) 测量-重发攻击

为了尝试得到Alice对用于隐私比较的粒子的测量结果, Eve截获从TP发送给Alice的 S_A 的粒子, 利用 MB_Z 基测量它并将所得量子态发送给Alice. 如果这个原始粒子处于 MB_Z 基, 不管Alice选择什么操作, Eve的攻击将不会被步骤3和4检测到. 然后, 考虑这个原始粒子处于 MB_F 基. 如果Alice选择进行MEASURE, 根据表1, 这个粒子将被忽略从而使得Eve的攻击行为将不会被检测到; 如果Alice选择进行REFLECT, 由于Eve的测量操作会毁坏这个粒子的原始状态, Eve的攻击行为将会在步骤3被检测到. 总之, Eve的这种攻击不可避免地被检测到是由于以下两个原因: 一方面, Eve不知道这个粒子的制备基; 另一方面, Alice的操作对于Eve来说是随机的.

另外, 为了尝试得到Alice对用于隐私比较的粒子的测量结果, Eve可能会发起另一种测量-重发攻击: 她截获从Alice发送给TP的粒子, 利用 MB_Z 基测量它并将所得量子态发送给TP. 与第一种测量-重发攻击一样, 在这种情形下Eve也会不可避免地被检测到.

(3) 纠缠-测量攻击

Eve的这种纠缠-测量攻击可用两个酉操作 $\hat{E}$ 和 $\hat{F}$ 模拟. 这里, $\hat{E}$ 攻击从TP发送给Alice的量子底特, 而 $\hat{F}$ 攻击从Alice返回给TP的量子底特. 并且, $\hat{E}$ 和 $\hat{F}$ 共享一个初始状态为 $|\varepsilon\rangle$ 的共同探测空间. 正如文献[16,17]说明的那样, 共享探测态允许Eve利用从 $\hat{E}$ 获得的知识攻击返回的粒子(如果Eve没有利用这一点, “共享探测态”可以简单地被认为是由两个独立探测态构成的复合系统). Eve使 $\hat{F}$ 依赖于执行 $\hat{E}$ 后的测量的任何攻击都可由 $\hat{E}$ 和 $\hat{F}$ 通过受控门来实现. Eve对 S_A 的粒子发起的纠缠-测量攻击可用图2来表示.

定理1 假设Eve对TP发送给Alice以及返回给TP的粒子施加攻击($\hat{E}, \hat{F}$). 为了这个攻击不在步骤3和4引发错误, Eve的探测态的最终状态应当不仅独立于Alice的操作而且还独立于TP和Alice的测量结果. 这样, Eve得不到关于 S_{A1} 取值的任何信息.

图2 Eve对 S_A 的粒子发起的可由两个酉操作 $\hat{E}$ 和 $\hat{F}$ 建模的纠缠-测量攻击

Figure 2 Eve's entangle-measure attack on the particle of S_A with two unitaries $\hat{E}$ and $\hat{F}$.

证明 在Eve攻击前, 由TP制备的量子底特和Eve的探测态构成的复合系统的全局状态可被表示为 $|T\rangle|\varepsilon\rangle$, 其中 $|T\rangle$ 是从两个集合 MB_Z 和 MB_F 中随机选择出来. 为了方便起见, 用 $|g\rangle$ 和 $|G_g\rangle$ 分别代表集合 MB_Z 的粒子和集合 MB_F 的粒子, 其中

$$|G_g\rangle = F|g\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i g k}{d}} |k\rangle, \quad g = 0, 1, \dots, d-1.$$

① 首先, 考虑TP发送给Alice的粒子在集合 MB_Z 中的情形. $\hat{E}$ 作用在这个粒子和Eve的探测态上的效果可被描述为^[26]

$$\begin{aligned} \hat{E}(|0\rangle|\varepsilon\rangle) &= \alpha_{00}|0\rangle|\varepsilon_{00}\rangle + \alpha_{01}|1\rangle|\varepsilon_{01}\rangle \\ &\quad + \dots + \alpha_{0(d-1)}|d-1\rangle|\varepsilon_{0(d-1)}\rangle, \end{aligned} \quad (5)$$

$$\begin{aligned} \hat{E}(|1\rangle|\varepsilon\rangle) &= \alpha_{10}|0\rangle|\varepsilon_{10}\rangle + \alpha_{11}|1\rangle|\varepsilon_{11}\rangle \\ &\quad + \dots + \alpha_{1(d-1)}|d-1\rangle|\varepsilon_{1(d-1)}\rangle, \end{aligned} \quad (6)$$

⋮

$$\begin{aligned} \hat{E}(|d-1\rangle|\varepsilon\rangle) &= \alpha_{(d-1)0}|0\rangle|\varepsilon_{(d-1)0}\rangle + \alpha_{(d-1)1}|1\rangle|\varepsilon_{(d-1)1}\rangle \\ &\quad + \dots + \alpha_{(d-1)(d-1)}|d-1\rangle|\varepsilon_{(d-1)(d-1)}\rangle, \end{aligned} \quad (7)$$

其中, $|\varepsilon_{gt}\rangle$ 是由 $\hat{E}$ 决定的Eve的探测态, $g, t=0, 1, \dots, d-1$;

对于 $g = 0, 1, \dots, d-1$, 有 $\sum_{t=0}^{d-1} |\alpha_{gt}|^2 = 1$.

在Alice的操作后, Eve对返回给TP的粒子施加 $\hat{F}$.

当Alice选择进行MEASURE时, 根据式(5)–(7), 复合系统的全局状态被坍塌为 $\alpha_{gt}|t\rangle|\varepsilon_{gt}\rangle$, 其中 $g, t=0, 1, \dots$,

$d-1$. 为了使Eve对这个粒子的攻击在步骤4不被TP和Alice发现, Eve施加 $\hat{F}$ 后的复合系统的全局状态应当被演化为

$$\hat{F}(\alpha_{gt}|t\rangle|\varepsilon_{gt}\rangle) = \begin{cases} \alpha_{gg}|g\rangle|F_{gg}\rangle, & \text{如果 } g=t, \\ 0, & \text{如果 } g \neq t, \end{cases} \quad (8)$$

其中蕴含

$$\alpha_{gt} = \begin{cases} \alpha_{gg}, & \text{如果 } g=t, \\ 0, & \text{如果 } g \neq t. \end{cases} \quad (9)$$

当Alice选择进行REFLECT时, 根据式(8)和(9), Eve施加 $\hat{F}$ 后的复合系统的全局状态被演化成

$$\begin{aligned} \hat{F}[\hat{E}(|0\rangle|\varepsilon\rangle)] &= \hat{F}(\alpha_{00}|0\rangle|\varepsilon_{00}\rangle + \alpha_{01}|1\rangle|\varepsilon_{01}\rangle \\ &\quad + \cdots + \alpha_{0(d-1)}|d-1\rangle|\varepsilon_{0(d-1)}\rangle) \\ &= \hat{F}(\alpha_{00}|0\rangle|\varepsilon_{00}\rangle) = \alpha_{00}|0\rangle|F_{00}\rangle, \end{aligned} \quad (10)$$

$$\begin{aligned} \hat{F}[\hat{E}(|1\rangle|\varepsilon\rangle)] &= \hat{F}(\alpha_{10}|0\rangle|\varepsilon_{10}\rangle + \alpha_{11}|1\rangle|\varepsilon_{11}\rangle \\ &\quad + \cdots + \alpha_{1(d-1)}|d-1\rangle|\varepsilon_{1(d-1)}\rangle) \\ &= \hat{F}(\alpha_{11}|1\rangle|\varepsilon_{11}\rangle) = \alpha_{11}|1\rangle|F_{11}\rangle, \end{aligned} \quad (11)$$

$\vdots$

$$\begin{aligned} \hat{F}[\hat{E}(|d-1\rangle|\varepsilon\rangle)] &= \hat{F}(\alpha_{(d-1)0}|0\rangle|\varepsilon_{(d-1)0}\rangle + \alpha_{(d-1)1}|1\rangle|\varepsilon_{(d-1)1}\rangle \\ &\quad + \cdots + \alpha_{(d-1)(d-1)}|d-1\rangle|\varepsilon_{(d-1)(d-1)}\rangle) \\ &= \hat{F}(\alpha_{(d-1)(d-1)}|d-1\rangle|\varepsilon_{(d-1)(d-1)}\rangle) \\ &= \alpha_{(d-1)(d-1)}|d-1\rangle|F_{(d-1)(d-1)}\rangle. \end{aligned} \quad (12)$$

为了使Eve对这个粒子的攻击在步骤3不被TP和Alice发现, 当Alice选择进行REFLECT时, Eve不能改变它的状态. 根据式(10)–(12), 这点是自动满足的.

② 其次, 考虑TP发送给Alice的粒子在集合 MB_F 中的情形. $\hat{E}$ 作用在这个粒子和Eve的探测态上的效果可被描述为

$$\begin{aligned} \hat{E}(|G_g\rangle|\varepsilon\rangle) &= \hat{E}\left[\left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i g k}{d}} |k\rangle\right)|\varepsilon\rangle\right] \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i g k}{d}} \hat{E}(|k\rangle|\varepsilon\rangle). \end{aligned} \quad (13)$$

在Alice的操作后, Eve对返回给TP的粒子施加 $\hat{F}$.

当Alice选择进行REFLECT时, Eve施加 $\hat{F}$ 后的复合系统的全局状态被改变为

$$\hat{F}[\hat{E}(|G_g\rangle|\varepsilon\rangle)] = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i g k}{d}} \hat{F}[\hat{E}(|k\rangle|\varepsilon\rangle)]. \quad (14)$$

根据式(10)–(12), 有 $\hat{F}[\hat{E}(|k\rangle|\varepsilon\rangle)] = \alpha_{kk}|k\rangle|F_{kk}\rangle$, 代入式(14)可得

$$\hat{F}[\hat{E}(|G_g\rangle|\varepsilon\rangle)] = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i g k}{d}} \alpha_{kk}|k\rangle|F_{kk}\rangle. \quad (15)$$

根据逆量子傅里叶变换, 有

$$|k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{-\frac{2\pi i j k}{d}} |G_j\rangle, \quad k=0, 1, \dots, d-1. \quad (16)$$

将式(16)代入式(15)可产生

$$\begin{aligned} \hat{F}[\hat{E}(|G_g\rangle|\varepsilon\rangle)] &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i g k}{d}} \alpha_{kk} \left(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{-\frac{2\pi i j k}{d}} |G_j\rangle \right) |F_{kk}\rangle \\ &= \frac{1}{d} \left(|G_0\rangle \sum_{k=0}^{d-1} e^{\frac{2\pi i (g-0)k}{d}} \alpha_{kk} |F_{kk}\rangle + |G_1\rangle \sum_{k=0}^{d-1} e^{\frac{2\pi i (g-1)k}{d}} \alpha_{kk} |F_{kk}\rangle \right. \\ &\quad \left. + \cdots + |G_{(d-1)}\rangle \sum_{k=0}^{d-1} e^{\frac{2\pi i (g-(d-1))k}{d}} \alpha_{kk} |F_{kk}\rangle \right). \end{aligned} \quad (17)$$

为了使Eve在步骤3不被TP和Alice发现, 对于 $g \neq j$ 以及 $g, j=0, 1, \dots, d-1$, 应满足

$$\sum_{k=0}^{d-1} e^{\frac{2\pi i (g-j)k}{d}} \alpha_{kk} |F_{kk}\rangle = 0. \quad (18)$$

显然, 对于任何 $g \neq j$, 有

$$\sum_{k=0}^{d-1} e^{\frac{2\pi i (g-j)k}{d}} = 0. \quad (19)$$

因此, 根据式(18)和(19)有

$$\alpha_{00}|F_{00}\rangle = \alpha_{11}|F_{11}\rangle = \cdots = \alpha_{(d-1)(d-1)}|F_{(d-1)(d-1)}\rangle = \alpha|F\rangle. \quad (20)$$

③ 将式(20)代入式(8)会产生

$$\hat{F}(\alpha_{gt}|t\rangle|\varepsilon_{gt}\rangle) = \begin{cases} |g\rangle(\alpha|F\rangle), & \text{如果 } g=t, \\ 0, & \text{如果 } g \neq t. \end{cases} \quad (21)$$

将式(20)代入式(10)–(12)可分别得到

$$F[\tilde{E}(|0\rangle|\varepsilon\rangle)] = |0\rangle(\alpha|F\rangle), \quad (22)$$

$$F[\tilde{E}(|1\rangle|\varepsilon\rangle)] = |1\rangle(\alpha|F\rangle), \quad (23)$$

⋮

$$F[\tilde{E}(|d-1\rangle|\varepsilon\rangle)] = |d-1\rangle(\alpha|F\rangle). \quad (24)$$

将式(20)代入式(17)会产生

$$F[\tilde{E}(|G_g\rangle|\varepsilon\rangle)] = |G_g\rangle(\alpha|F\rangle). \quad (25)$$

基于式(21)–(25)可以得出结论, 为了不在步骤3和4引发错误, Eve的探测态的最终状态应当不仅独立于Alice的操作而且还独立于TP和Alice的测量结果. 因此, 如果Eve发起纠缠-测量攻击, 她将得不到关于 S_{A1} 的取值的任何信息.

(4) 特洛伊木马攻击

S_A 的粒子从TP传送到Alice然后又返回TP, 经历了环形传输. 因此, 需考虑Eve发起的特洛伊木马攻击, 如不可见光子窃听攻击^[27]和延迟光子特洛伊木马攻击^[28,29]. 抵抗不可见光子窃听攻击的方法为: Alice在她的设备前安装一个波长滤波器消除不合法光子信号^[29,30]. 抵抗延迟光子特洛伊木马攻击的方法为: Alice利用光子数分割器(Photon Number Splitter: 50/50)将每个样本信号分成两部分并使用正确的测量基测量得到的信号^[29,30]. 只要多光子率高得不合理, 这个攻击就会被发现.

4.2 参与者攻击

2007年, Gao等人^[31]指出不忠诚参与者发起的攻击总是比外部窃听器发起的攻击更加严重. 因此, 必须对参与者攻击更加关注. 关于所提出的协议, 需要考虑两种情形的参与者攻击, 即来自Alice或Bob的攻击以及来自半忠诚TP的攻击.

(1) 来自Alice或Bob的参与者攻击

在所提出的协议中, Alice的角色与Bob的角色是一样的. 不失一般性, 只考虑Bob是不忠诚的, 他被假定具有完全的量子能力. 不忠诚Bob尽他自己最大努力来尝试得到Alice的秘密消息.

当Alice通过经典信道将 R_A^i 发送给TP时, Bob可能会收到它. 尽管Bob自动地知道 K_{AB}^i , 为了从 R_A^i 推导出 m_A^i , 他仍然需要得到 S_{A1}^i . 然而, Bob不能与TP共谋来得到 S_{A1}^i . 因此, 为了得到 S_{A1}^i , Bob不得不对 S_A 的粒子发起主动攻击. 然而, 正如前面所分析的那样, 他不可避免地被Alice和TP当作一个外部攻击者而发现. 总之, Bob没有机会得到 m_A^i . 这等价于Bob无法知道 x_i .

(2) 来自半忠诚TP的参与者攻击

在这个协议中, TP被假设为半忠诚的, 意味着她可以按照自己意愿错误行事但不能与Alice或Bob共谋. 尽管TP知道 S_{A1}^i (S_{B1}^i), 由于缺少 K_{AB}^i , 她仍然无法从 R_A^i (R_B^i)推导出 m_A^i (m_B^i). 因此, TP没有机会得到 x_i (y_i).

5 讨论与结论

由于文献[23]的协议是目前唯一能实现两个经典用户秘密信息大小关系比较的SQPC协议, 将所提出的SQPC协议与它进行详细对比. 对比结果被列在表2中. 文献[32]定义量子比特效率衡量2级系统的量子通信协议的效率. 为了衡量 d 级系统的量子通信协议的效率, 将它修改为量子底特效率, 其定义为 $\eta = \frac{b}{q+c}$, 其中 b , q 和 c 分别是被比较的秘密信息的长度、所消耗的量子底特的数量以及经典通信所涉及的经典信息的长度. 这里忽略窃听检测过程消耗的经典资源. 文献[23]的SQPC协议没有说明采取哪个半量子密钥协商

表 2 本文的SQPC协议与文献[23]的SQPC协议的对比

Table 2 Comparison results of our SQPC protocol and the SQPC protocol of ref. [23]

协议	初始量子资源	量子纠缠交换或酉操作的使用	TP的类型	TP的测量操作	SQKD或SQKA的使用	大小关系的比较	TP是否知道比较结果	量子底特效率
文献[23]	d 级Bell纠缠态	否	半忠诚	d 级Bell纠缠态测量和 d 级单粒子测量	是	是	是	$\frac{1}{24(1+\delta)+3}$
本文的协议	d 级单粒子态	否	半忠诚	d 级单粒子测量	是	是	否	$\frac{1}{24(1+\delta)+3}$

(Semiquantum Key Agreement, SQKA)协议来建立两个经典用户之间预先共享的密钥, 所以用于产生预先共享密钥的量子资源和经典资源也被忽略.

在所提出的协议中, Alice (Bob)的秘密信息的长度是 n , 所以有 $b=n$. TP需要制备 $8n(1+\delta)$ 个初始 d 级单粒子并发送给Alice (Bob). 然后, 当Alice (Bob)选择进行MEASURE时, 她(他)制备 $4n(1+\delta)$ 个新量子底特处于 MB_Z 基并将它们发送给TP. 因此, 有 $q = 8n(1+\delta) \times 2 + 4n(1+\delta) \times 2 = 24n(1+\delta)$. 另外, Alice (Bob)需将 R_A^i (R_B^i)发送给TP, 而TP需将 r_i 公布给Alice和Bob, 其中 $i = 1, 2, \dots, n$, 所以有 $c = n + n + n = 3n$. 因此, 所提出协议的量子底特效率为 $\eta = \frac{n}{24n(1+\delta)+3n} = \frac{1}{24(1+\delta)+3}$.

在文献[23]的SQPC协议中, Alice (Bob)的秘密信息的长度是 n , 所以有 $b=n$. TP需要制备 $8n(1+\delta)$ 个初始 d 级Bell纠缠态并将它们分别发送给Alice和Bob. 然后, 当Alice (Bob)选择进行MEASURE, 她(他)制备 $4n(1+\delta)$ 个新的量子底特处于 Z 基并传送给TP. 因此, 有 $q = 8n(1+\delta) \times 2 + 4n(1+\delta) \times 2 = 24n(1+\delta)$. 另外, Alice (Bob)需将 r_A^i (r_B^i)发送给TP, 而TP需将 c_r^i 公布给

Alice和Bob, 其中 $i = 1, 2, \dots, n$, 所以有 $c=n+n+n=3n$. 因此, 文献[23]的SQPC协议的量子底特效率为

$$\eta = \frac{n}{24n(1+\delta)+3n} = \frac{1}{24(1+\delta)+3}.$$

根据表2, 可以得出结论: (1) 由于 d 级单粒子态的实验制备比 d 级Bell纠缠态的实验制备容易得多, 与文献[23]的SQPC协议相比, 本文的协议降低了初始量子资源的实验制备难度; (2) 由于 d 级单粒子态的实验测量比 d 级Bell纠缠态的实验测量更容易实现, 与文献[23]的SQPC协议相比, 本文的协议降低了TP的实验测量难度; (3) 由于在本文的协议中TP无法知道比较结果, 该协议在比较结果上比文献[23]的SQPC协议具有更好的隐秘性.

总之, 本文提出一个新颖的基于 d 级单粒子态的能安全比较出两个经典用户秘密信息的大小关系的SQPC协议. 该协议能抵抗一系列外部攻击和参与者攻击, 并确保半忠诚TP无法知道具体的比较结果. 此协议仅采用 d 级单粒子态作为初始量子资源, 并只要求TP进行 d 级单粒子测量. 因此, 本协议在初始量子资源的实验制备、TP的实验测量以及TP是否知道比较结果这几个方面比之前唯一能比较出大小关系的SQPC协议[23]具有更好的性能.

参考文献

- 1 Yao A C. Protocols for secure computations. In: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science. Chicago, 1982. 160–164
- 2 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the International Conference on Computers, Systems & Signal Processing. Bangalore, 1984. 175–179
- 3 Yang Y G, Wen Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A-Math Theor*, 2009, 42: 055305
- 4 Tseng H Y, Lin J, Hwang T. New quantum private comparison protocol using EPR pairs. *Quantum Inf Process*, 2012, 11: 373–384
- 5 Chang Y J, Tsai C W, Hwang T. Multi-user private comparison protocol using GHZ class states. *Quantum Inf Process*, 2013, 12: 1077–1088
- 6 Li Y B, Ma Y J, Xu S W, et al. Quantum private comparison based on phase encoding of single photons. *Int J Theor Phys*, 2014, 53: 3191–3200
- 7 Ye C Q, Ye T Y. Circular multi-party quantum private comparison with n -level single-particle states. *Int J Theor Phys*, 2019, 58: 1282–1294
- 8 Xu Q D, Chen H Y, Gong L H, et al. Quantum private comparison protocol based on four-particle GHZ states. *Int J Theor Phys*, 2020, 59: 1798–1806
- 9 Huang X, Zhang S B, Chang Y, et al. Efficient quantum private comparison based on entanglement swapping of Bell states. *Int J Theor Phys*, 2021, 60: 3783–3796
- 10 Guo F Z, Gao F, Qin S J, et al. Quantum private comparison protocol based on entanglement swapping of d -level Bell states. *Quantum Inf Process*, 2013, 12: 2793–2802
- 11 Lin S, Sun Y, Liu X F, et al. Quantum private comparison protocol with d -dimensional Bell states. *Quantum Inf Process*, 2013, 12: 559–568
- 12 Luo Q, Yang G, She K, et al. Multi-party quantum private comparison protocol based on d -dimensional entangled states. *Quantum Inf Process*,

- 2014, 13: 2343–2352
- 13 Ye C Q, Ye T Y. Multi-party quantum private comparison of size relation with d -level single-particle states. *Quantum Inf Process*, 2018, 17: 252
- 14 Song X, Wen A, Gou R. Multiparty quantum private comparison of size relation based on single-particle states. *IEEE Access*, 2019, 7: 142507–142514
- 15 Chen F L, Zhang H, Chen S G, et al. Novel two-party quantum private comparison via quantum walks on circle. *Quantum Inf Process*, 2021, 20: 178
- 16 Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. *Phys Rev Lett*, 2007, 99: 140501, arXiv: [quant-ph/0703107](#)
- 17 Boyer M, Gelles R, Kenigsberg D, et al. Semiquantum key distribution. *Phys Rev A*, 2009, 79: 032341, arXiv: [0812.4835](#)
- 18 Chou W H, Hwang T, Gu J. Semi-quantum private comparison protocol under an almost-dishonest third party. arXiv: [1607.07961](#)
- 19 Ye T Y, Ye C Q. Measure-resend semi-quantum private comparison without entanglement. *Int J Theor Phys*, 2018, 57: 3819–3834
- 20 Lang Y F. Semi-quantum private comparison using single photons. *Int J Theor Phys*, 2018, 57: 3048–3055
- 21 Lin P H, Hwang T, Tsai C W. Efficient semi-quantum private comparison using single photons. *Quantum Inf Process*, 2019, 18: 207
- 22 Ye C Q, Li J, Chen X B, et al. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. *Quantum Inf Process*, 2021, 20: 262
- 23 Zhou N R, Xu Q D, Du N S, et al. Semi-quantum private comparison protocol of size relation with d -dimensional Bell states. *Quantum Inf Process*, 2021, 20: 124
- 24 Yang Y G, Xia J, Jia X, et al. Comment on quantum private comparison protocols with a semi-honest third party. *Quantum Inf Process*, 2013, 12: 877–885
- 25 Krawec W O. Mediated semiquantum key distribution. *Phys Rev A*, 2015, 91: 032323, arXiv: [1411.6024](#)
- 26 Qin H, Dai Y. Dynamic quantum secret sharing by using d -dimensional GHZ state. *Quantum Inf Process*, 2017, 16: 64
- 27 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. *Rev Mod Phys*, 2002, 74: 145–195, arXiv: [quant-ph/0101098](#)
- 28 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A*, 2006, 351: 23–25, arXiv: [quant-ph/0508002](#)
- 29 Deng F G, Zhou P, Li X H, et al. Robustness of two-way quantum communication protocols against Trojan horse attack. arXiv: [0508168](#)
- 30 Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys Rev A*, 2006, 74: 054302, arXiv: [quant-ph/0612016](#)
- 31 Gao F, Qin S J, Wen Q Y, Zhu F C. A simple participant attack on the Brádler-Dušek protocol. *Quantum Inf Comput*, 2007, 7: 329
- 32 Cabello A. Quantum key distribution in the Holevo limit. *Phys Rev Lett*, 2000, 85: 5635–5638, arXiv: [quant-ph/0007064](#)

Semiquantum private comparison of size relationship based on d -level single-particle states

GENG MaoJie, XU TianJie, CHEN Ying & YE TianYu^{*}

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

In this paper, we propose a novel semiquantum private comparison (SQPC) protocol of the size relationship based on d -level single-particle states. This protocol can compare the size relationship of different privacy messages from two classical users with the help of a semi-honest third party (TP), who is permitted to misbehave on her own, but cannot be in collusion with anyone else. The correctness analysis shows that this protocol can gain correct comparison results. The security analysis results reveal that this protocol can resist some famous outside attacks and participant attacks. This protocol only adopts d -level single-particle states as the initial quantum resource, only requires the TP to perform d -level single-particle measurements, and makes the accurate comparison results inaccessible to the TP. Compared with the only existing SQPC protocol of size relationship (Quantum Inf. Process. 20, 124 (2021)), the proposed protocol has advantages in experimental preparation of initial quantum resource, TP's experimental measurements, and TP's knowledge about the comparison results.

semiquantum private comparison, size relationship, d -level single-particle states, semi-honest third party

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

doi: [10.1360/SSPMA-2022-0025](https://doi.org/10.1360/SSPMA-2022-0025)