

动态分等级量子比特共享协议

贾恒越¹, 武霞¹, 张可佳², 朱建明¹, 李洋¹

(1. 中央财经大学信息学院, 北京 100081;

2. 黑龙江大学数学科学学院, 黑龙江 哈尔滨 150080)

摘要: 量子秘密共享是量子密码研究的一个重要分支, 针对多方共享量子比特情况进行研究, 提出一个新的动态量子比特共享协议。此协议中, 参与共享的成员是分等级的, 量子信息的管理者在无需建立新的量子信道的情况下可对秘密重构系统中的参与者进行裁员。裁员后, 管理者通过量子操作可以对量子信息进行更新, 而剩余的有效参与者无需对自己手中的粒子执行额外操作就可完成新信息重构。此外, 还讨论了协议的正确性、安全性及共享成员的等级性。

关键词: 量子比特共享; 分等级; 裁员; 量子隐形传态; 线形 cluster 态

中图分类号: TN918.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00115

Dynamic hierarchical quantum information sharing protocol

JIA Heng-yue¹, WU Xia¹, ZHANG Ke-jia², ZHU Jian-ming¹, LI Yang¹

(1. School of Information, Central University of Finance and Economics, Beijing 100081, China

2. School of Mathematical Science, Heilongjiang University, Harbin 150080, China)

Abstract: Quantum secret sharing (QSS) is one important branch of quantum cryptography. Based on the studies of multi-shared quantum bits, a new dynamic quantum bit sharing protocol was proposed. The participation of the shared members is hierarchical in this protocol. The quantum information leader, in the absence of the establishment of a new quantum channel, can remove some of the participants in the secret reconstruction system. After the layoffs, the leader can also update the quantum information using quantum operations, and the remaining effective participants can recover the new quantum information without performing additional operations. In addition, the correctness, security and the hierarchy of the participants of the protocol were discussed.

Key words: quantum information sharing, hierarchy, removing of participants, quantum teleportation, linear cluster state

1 引言

秘密共享 (SS, secret sharing) 是密码学的重

要分支, 是保护数据安全的基本工具, 在金融信息安全保障技术中具有十分重要的意义。1999年, 量子纠缠被首次用于完成经典信息的共享和

收稿日期: 2016-09-21; 修回日期: 2016-10-25。通信作者: 贾恒越, jiahengyue@163.com

基金项目: 国家自然科学基金资助项目 (No.61309029, No.U1509214, No.61272398); 中央财经大学青年教师发展基金资助项目 (No.QJJ1633); 信息保障技术重点实验室开放基金资助项目 (No.KJ-14-008); 黑龙江省自然科学基金资助项目 (No.A2016007); 黑龙江大学青年基金资助项目 (No.QL201501)

Foundation Items: The National Natural Science Foundation of China (No.61309029, No.U1509214, No.61272398), The Young Teachers Development Fund of Central University of Finance and Economics (No.QJJ1633), The Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-14-008), The Natural Science Foundation of Heilongjiang Province (No.A2016007), Youth Foundation of Heilongjiang University (No.QL201501)

量子信息的分割任务, 即量子秘密共享 (QSS, quantum secret sharing) [1,2]。近年来, 研究人员一直不断地从协议使用的量子态载体、量子操作、通信方式等方面考虑设计出新的 QSS 方案 [3-5], 设备无关和理性参与者情况下的 QSS 取得了一些成果 [6,7]。量子比特是量子信息技术中的基本信息载体, 与经典比特相比具有叠加性、不可克隆性等量子特性, 本文主要针对共享对象为量子信息的情形进行研究。

在一个企业或者机构中的工作人员通常都是存在一定的管理级别或等级体系的, 工作能力或经验较强的参与者会有相对较大的权限或话语权, 在工作事务执行过程中发挥主导作用。与权限相同的协议相比, 分等级的量子信息共享协议更适用于这样的应用场景。2010 年, Wang 等 [8] 首先提出了分等级的量子信息共享协议, 在此类协议中参与者在秘密重构过程中的权限或地位是不同的。随后, 研究人员分别采用不同的量子载体对任意单量子比特信息、两量子比特信息的分等级量子信息共享协议进行了研究 [9-12]。

在实际生活中, 参与完成共同任务的工作组成员很可能会中途退出组织, 从而导致原计划任务无法继续进行或完成。因此, 考虑在秘密信息分发之后参与成员的动态变更问题具有一定的实际意义。换句话说, 在秘密信息分割后, 如何让系统以最小的开销 (通信、计算、时间) 完成自我重建以便能够继续完成任务。对于成员变更问题在理论和实际中都是非常有趣和重要的, 这最早是由 Blakey 等在文献 [13~15] 引入并展开讨论的。近年来, 针对量子秘密共享协议的成员动态变更问题已引起人们的研究兴趣, 在其协议设计及安全分析方面都取得了一定的成果 [16~21]。

最近, Mishra 等 [22] 把动态和分等级的性质相结合, 针对共享经典信息的 QSS 问题给出了解决方案, 而对于分等级的量子信息共享协议的动态问题目前还比较少。本文正是以分等级的量子信息共享协议为研究对象, 考虑允许管理员在秘密分发后对参与成员进行裁员的情况, 基于线形 cluster 态提出了一个动态的多方协议。

2 准备知识

Cluster 态是一类特殊的多粒子纠缠态, 粒子之间的纠缠为 Ising 型交互 [23], 它也是图态中的典型实例, 即其对应的基础图为 d -维网格的一个连通子图, 这种结构使 cluster 态具有很强的反局域性和抗消相干作用 [24]。当维数 $d=1$ 时, 对应的基础图形就成为一个链 (如图 1 所示), 因此也叫做线形 cluster 态 (linear cluster state), 其中每个粒子只与相邻粒子有相互作用。 N 粒子线形 cluster 态的一般表达式可写为

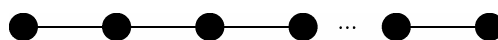


图 1 线形 cluster 态

$$|LC_N\rangle = \prod_{1 \leq i \leq N-1} CZ_{i,i+1} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)^{\otimes N} \quad (1)$$

其中,

$$CZ_{i,i+1} = |00\rangle_{i,i+1} \langle 00| + |01\rangle_{i,i+1} \langle 01| + |10\rangle_{i,i+1} \langle 10| - |11\rangle_{i,i+1} \langle 11|$$

是作用在量子比特 $i, i+1$ 上的受控-Z 门 [25]。

例如, $N=3$ 时, 经计算 cluster 态的表达式可整理为

$$\begin{aligned} |LC_3\rangle &= \frac{1}{\sqrt{2}} (|+\rangle_1 |0\rangle_2 |+\rangle_3 + |-\rangle_1 |1\rangle_2 |-\rangle_3) \\ &= \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 |0\rangle_3 + |1\rangle_1 |1\rangle_2 |1\rangle_3) \end{aligned}$$

在对 1, 3 粒子进行局域么正操作后即可转化为 GHZ 态, 即与 GHZ 态局域么正等价。

Cluster 态因其在量子秘密共享、密集编码、隐形传态, 特别是在量子计算中的应用, 使其成为量子信息处理中比较重要的量子载体。不仅如此, 实验上一些 cluster 态的制备和应用的理论方案已经得到了验证 [26~28]。

本文协议的设计主要是基于奇数量子比特的线形 cluster 态, 为了便于下文分析, 将线形 cluster 态的一般表达式进行了改写, 式(2)即为拥有 $2n+1$ (n 是正整数) 个粒子的线形 cluster 态。

$$|LC_{2n+1}\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{i_1 \in \{0,1\}, 0 \leq j \leq n+1} |i_1, \overline{i_1 \oplus i_2}, i_2, \dots, i_n, \overline{i_n \oplus i_{n+1}}, i_{n+1}\rangle \quad (2)$$

其中,

$$\begin{aligned} |\bar{0}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |\bar{1}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

且 $\oplus$ 表示模 2 加法。由表达式(2)可知, 线形 cluster 态中所有处于偶数位置的量子比特可以由它相邻的量子比特来确定。这种形式可以直观地展示出粒子之间的 Ising 型交互。 $n=1$ 时, cluster 态的表达式为

$$|LC_3\rangle = \frac{1}{2}(|000\rangle + |0\bar{1}1\rangle + |1\bar{1}0\rangle + |101\rangle) \quad (3)$$

$n=2$ 时, 线形 cluster 态的表达式为

$$\begin{aligned} |LC_5\rangle &= \frac{1}{2\sqrt{2}}(|00000\rangle + |000\bar{1}1\rangle + |0\bar{1}1\bar{1}0\rangle + \\ &|0\bar{1}101\rangle + |1\bar{1}000\rangle + |1\bar{1}0\bar{1}1\rangle + |101\bar{1}0\rangle + |10101\rangle) \end{aligned} \quad (4)$$

不难验证, 当表达式(1)用于表示奇数个粒子的量子态时, 与本文给出的表达式(2)是等价的。

本文还将用到单粒子 Hadamard 操作

$$H = |\bar{0}\rangle\langle 0| + |\bar{1}\rangle\langle 1|$$

和两粒子操作

$$\begin{aligned} \text{CNOT}_{ij}^\dagger &= |\bar{0}0\rangle_{ij} \langle \bar{0}0| + |\bar{0}1\rangle_{ij} \langle \bar{0}1| + \\ &|\bar{1}0\rangle_{ij} \langle \bar{1}1| + |\bar{1}1\rangle_{ij} \langle \bar{1}0| \end{aligned}$$

其中, H 算子能将 $|0\rangle$ 态和 $|1\rangle$ 态分别变成 $|\bar{0}\rangle$ 和 $|\bar{1}\rangle$ 态。

3 动态的分等级量子信息共享协议

设管理者拥有秘密量子比特

$$|\varphi\rangle_s = \alpha|0\rangle_s + \beta|1\rangle_s$$

其中, $|\alpha|^2 + |\beta|^2 = 1$, 初始参与者集合记为 $N = \{1, 2, \dots, n\}$ 。由量子态的不可克隆性可知, 最终只有一个参与者能获得重构的秘密量子比特信息。在建立量子信道时, 管理者可以指定粒子分配、共享情况, 因此不失一般性且为叙述方便, 下文协议假设参与者 $x = \left\lfloor \frac{(n+1)}{2} \right\rfloor$ 为重构秘密量子比特的拥有者。

3.1 秘密分发协议

1) 管理者与参与者共享 $2n+1$ 粒子线形 cluster 态

$$\begin{aligned} |LC_{2n+1}\rangle_{1,A_1,2,A_2,\dots,A_n,n+1} &= \frac{1}{\sqrt{2^{n+1}}} \\ &\sum_{i_j \in \{0,1\}, 0 \leq j \leq n+1} |i_1, \overline{i_1} \oplus i_2, i_2, \dots, i_n, \overline{i_n} \oplus i_{n+1}, i_{n+1}\rangle_{1,A_1,2,A_2,\dots,A_n,n+1} \end{aligned}$$

其中, 管理者拥有粒子 $1, \dots, n+1$, 参与者 k 拥有粒子 $A_k (k \in N)$ 。

2) 管理者对手中的粒子执行 H_j 和 CZ_{S_j} 操作, 其中, $j \in N - \{1, x+1\}$, 然后对粒子 $x+1$ 和 S 执行操作 $\text{CNOT}_{x+1,S}^\dagger$ 。

3) 管理者用 $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ 基测量每个粒子 $j \in N - \{1, x+1\}$, 并用经典比特 $d_j \in \{0, 1\}$ 记录测量结果。对于粒子 $x+1$ 和 S , 管理者用 $\{|0\rangle, |1\rangle\}$ 基测量, 测量结果分别记为经典比特 d_{x+1} 和 d_S 。

4) 管理者向所有参与者公布 d_S 、 d_{x+1} 和 $D = d_2 \oplus d_{x+2} \oplus d_n$ 的值。

秘密信息需要重构前, 如果没有参与人员变动, 则执行下面的步骤来重构秘密信息。

3.2 秘密重构协议

1) 参与者 $k \in G_1$ 用 $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ 基测量其手中的粒子, 其他参与者 (x 除外) 用 $\{|0\rangle, |1\rangle\}$ 基测量其各自的粒子, 并把测量结果通过经典比特 $a_k \in \{0, 1\}$ 发送给指定的重构信息参与者 x 。

2) 参与者 x 执行操作 $X^{a_{x+1} \oplus d_S} Z^{1 \oplus d_{x+1} \oplus A \oplus D}$, 其中, $A = \bigoplus_{k \in G_1} a_k$ 。

若在秘密信息重构之前, 由于某种原因有参与者退出或者被裁员, 则需要启动扩展协议进行参与者删除, 协议具体过程如 3.3 节所示。

3.3 裁员协议

为叙述方便, 把参与者集合 N 划分成 3 个组:

$$\begin{aligned} G_1 &= \{k | k \in N, k \neq 1, x, x+1, n\} \\ G_2 &= \{k | k = 1, n\} \\ G_3 &= \{k | k = x, x+1\} \end{aligned}$$

设集合 $L \subset N$ 是管理者想要裁员的名单, 其协议流程如图 2 所示, 具体步骤如下。

步骤 1 管理者公布裁员名单 L , 若满足 $|L \cap G_1| \geq 1$ 执行步骤 2; 否则执行步骤 4。

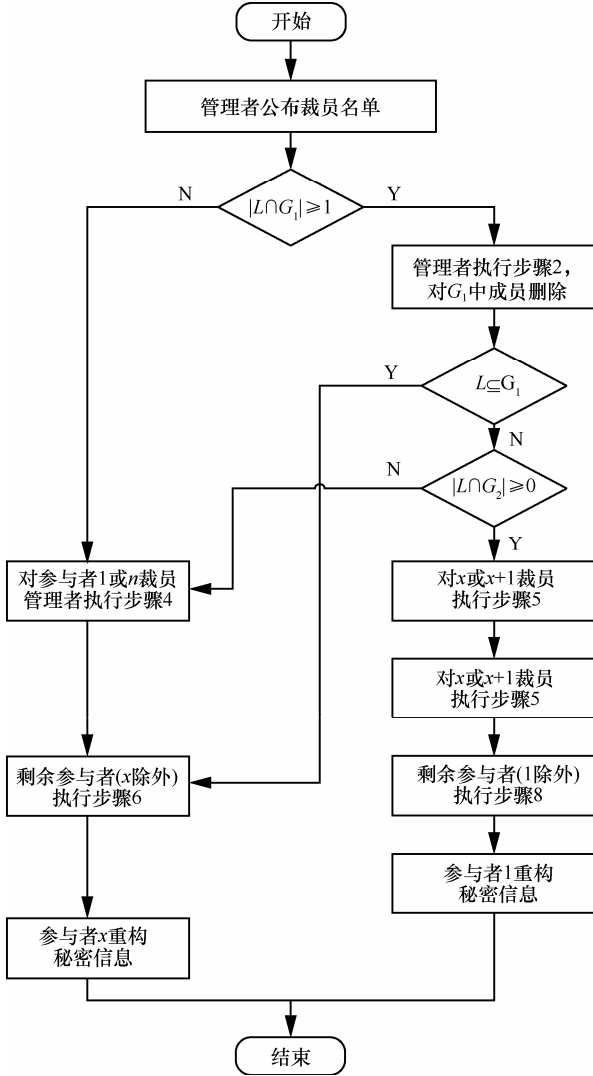


图2 裁员协议流程

步骤 2 若移除参与者 $k(k \in G_1)$ 时, 管理者可以通过更新秘密信息, 从而使被裁员人员的子秘密失效即可。管理者通过局域操作 $Z^{d_k \oplus d_{k+1}}$ 更新秘密量子信息 $|\varphi\rangle_s$ 。利用相同的方式, 管理依次将 $G_1 \cap L$ 中的所有参与者的子密钥失效。如果 $L \subseteq G_1$, 剩余参与者可以执行步骤 6 和步骤 7 来重构秘密信息。若 $L \not\subseteq G_1$, 执行步骤 3。

步骤 3 当 $|L \cap G_2| = 0$ 时, 秘密信息管理者执行步骤 5; 若 $|L \cap G_2| \neq 0$, 执行步骤 4。

步骤 4 为了移除参与者 1(n) 的共享权限, 秘密信息管理者对粒子 1(n+1) 用 $\{|0\rangle, |1\rangle\}$ 基进行测量, 测量结果用经典比特 $d_1(d_{n+1})$ 存储。此外, 管理者还利用局域幺正操作 $Z^{d_1}(Z^{d_{n+1}})$ 对要共享的秘密信息进行更新。倘若 G_2 中的 2 个参与

者都在裁员列表上, 管理者依照这种方法依次进行裁员, 即使他们的子秘密失效。裁员工作结束后, 剩余参与者可依照步骤 6、步骤 7 进行秘密重构。

步骤 5 管理者指定参与者 1 为裁员之后的接收者。如果 $d_2 \neq d_x$, 管理者先对粒子 1 执行操作 $Z^{\dagger} = |+\rangle\langle+| - |-\rangle\langle-|$, 然后对粒子 1、n+1 执行两粒子联合操作 $CZ_{1,n+1}^{\dagger}$, 并用 $\{|0\rangle, |1\rangle\}$ 基分别进行测量, 测量的结果记作 d_1 和 d_{n+1} ($d_1, d_{n+1} \in \{0, 1\}$)。根据测量结果, 秘密信息管理者若要对参与者 x 进行裁员, 则执行 $X^{d_n \oplus d_{n+1}} Z^{d_1 \oplus d_{x+2} \oplus d_n \oplus d_{n+1}}$ 操作; 若删除参与者 $x+1$, 则执行 $X^{d_n \oplus d_{n+1}} Z^{d_1 \oplus d_x \oplus d_n \oplus d_{n+1}}$ 操作。当重构秘密消息时剩余有效参与者执行步骤 8、步骤 9。

步骤 6 对于每个参与者 $j \in G_1 - L$, 分别用 $\{|0\rangle, |1\rangle\}$ 基测量手中的粒子; 其他有效的参与者 (x 除外) 用 $\{|0\rangle, |1\rangle\}$ 基测量。参与者 k ($k \in G_1 \cup G_2 - L$) 的测量结果用经典比特 a_k 记录。

步骤 7 参与者 x 对手中的粒子执行局域幺正操作 $X^{a_{x+1} \oplus d_s} Z^{1 \oplus d_{x+1} \oplus A' \oplus D}$ 即可得到共享的量子秘密信息, 其中 $A' = \bigoplus_{k \in G_1 \cup G_2 - L} a_k$ 。协议终止。

步骤 8 如果管理者要对参与者 x ($x+1$) 进行裁员, 则其余有效的参与者 (1 除外) 用 $\{|0\rangle, |1\rangle\}$ 基进行测量。参与者 k ($k \in G_1 \cup G_3 - L$) 的测量结果用 $a_k \in \{0, 1\}$ 来表示。

步骤 9 基于其余有效参与者的测量结果, 参与者 1 可以通过执行 $X^{a_n} Z^{d_s \oplus d_{x+1} \oplus a_n \oplus A' \oplus D}$ 操作获得管理者的秘密信息, 其中 $A' = \bigoplus_{k \in G_1 \cup G_3 - L} a_k$ 。协议终止。

4 协议分析

下面对上述协议的正确性及裁员功能进行分析。

4.1 秘密分发协议的正确性

定理 1 若参与者均诚实地依照协议执行, 则通过上文中的秘密分发协议能够使管理者有效地实现量子信息共享任务。

证明 参与者与管理者共享 $2n+1$ 粒子线形 cluster 态后, 管理者执行了 H_j (其中 $j \in N - \{1, x+1\}$) 操作, 则作用后的量子态为

$$\begin{aligned}
\pi(i) &= \left(\bigotimes_{j \in N - \{1, x+1\}} H_j \right) |LC_{2n+1}\rangle_{1, A_1, 2, A_2, \dots, A_n, n+1} \\
&= \sum_{\substack{i_i \in \{0,1\} \\ 0 \leq i \leq n+1}} |i_1, \overline{i_1} \oplus i_2, \overline{i_2}, \dots, \overline{i_x}, i_{x+1}, \\
&\quad \overline{i_{x+2}}, \dots, \overline{i_n}, \overline{i_n} \oplus i_{n+1}, i_{n+1}\rangle_{1, A_1, 2, A_2, \dots, A_n, n+1} \\
&= |0\rangle_{x+1} \pi_0(i) + |1\rangle_{x+1} \pi_1(i) \quad (5)
\end{aligned}$$

其中, $\pi_0(i)(\pi_1(i))$ 是 $i_{x+1} = 0(1)$ 时中 $\pi(i)$ 对应的子系统。

管理者执行两粒子 CZ_{sj} , $j \in N - \{1, x+1\}$ 操作之后, 整个系统的状态是

$$\begin{aligned}
&\left(\bigotimes_{j \in [n] - \{1, x+1\}} CZ_{sj} \right) (|\phi\rangle_S \otimes \pi(i)) \\
&= \alpha |0\rangle_S (|0\rangle_{x+1} \pi_0(i) + |1\rangle_{x+1} \pi_1(i)) + \\
&\quad \beta |1\rangle_S (|0\rangle_{x+1} \pi_0(\bar{i}) + |1\rangle_{x+1} \pi_1(\bar{i})) \\
&= |\Phi^+\rangle_{S, x+1} [\alpha \pi_0(i) + \alpha \pi_1(i) + \beta \pi_0(\bar{i}) - \beta \pi_1(\bar{i})] + \\
&\quad |\Phi^-\rangle_{S, x+1} [\alpha \pi_0(i) + \alpha \pi_1(i) - \beta \pi_0(\bar{i}) + \beta \pi_1(\bar{i})] + \\
&\quad |\Psi^+\rangle_{S, x+1} [\alpha \pi_0(i) - \alpha \pi_1(i) + \beta \pi_0(\bar{i}) + \beta \pi_1(\bar{i})] + \\
&\quad |\Psi^-\rangle_{S, x+1} [\alpha \pi_0(i) - \alpha \pi_1(i) - \beta \pi_0(\bar{i}) - \beta \pi_1(\bar{i})] \quad (6)
\end{aligned}$$

其中, $\pi_0(\bar{i})(\pi_1(\bar{i}))$ 表示把 $\pi_0(i)(\pi_1(i))$ 中的量子比特 $|\bar{v}\rangle_j$ ($v \in \{0,1\}$, $j \in N - \{1, x+1\}$) 改成 $|\bar{v} \oplus 1\rangle_j$ 。在管理者的 $CNOT_{x+1, S}^\dagger$ 操作之后, 式(6)中的 $|\Phi^\pm\rangle$ 、 $|\Psi^\pm\rangle$ 态则分别转化为 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ 。另外, 由式(6)可知, 秘密量子比特 $\alpha|0\rangle + \beta|1\rangle$ 包含的信息已被传递到参与者共享的量子系统中, 实现了秘密分割的任务。

4.2 秘密重构协议的正确性

定理 2 若参与者均诚实地依照协议执行, 则通过上文中的秘密重构协议能够使参与者准确恢复出秘密信息。

证明 在秘密重构协议中, 由于量子信息的不可克隆性, 最终只能有一个成员拥有最终的信息。在本协议中, 假定信息最终的拥有者为 x , 其他成员进行协助, 即将自己测量结果对应的经典信息传递给 x 。由线形 cluster 态的纠缠特性及式(5)和式(6)可以确定, $a_k = d_k \oplus d_{k+1}$, 其中 $k \in G_1$ 。

由共享的 cluster 态的纠缠状态, 可分析出量子比特 1 和 A_1 组成的子系统应处于式(7)的状态。

$$\begin{cases} \frac{1}{\sqrt{2}} (|\bar{0}\bar{0}\rangle + (-1)^{d_2} |\bar{1}\bar{1}\rangle)_{1, A_1}, & \text{在 } \pi_0(i) \text{ 或 } \pi_1(i) \text{ 中} \\ \frac{1}{\sqrt{2}} (|\bar{0}\bar{0}\rangle - (-1)^{d_2} |\bar{1}\bar{1}\rangle)_{1, A_1}, & \text{在 } \pi_0(\bar{i}) \text{ 或 } \pi_1(\bar{i}) \text{ 中} \end{cases} \quad (7)$$

类似地, 还可以确定粒子 A_n 和 $n+1$ 的子系统所处的状态

$$\begin{cases} \frac{1}{\sqrt{2}} (|\bar{0}\bar{0}\rangle + (-1)^{d_2} |\bar{1}\bar{1}\rangle)_{A_n, n+1}, & \text{在 } \pi_0(i) \text{ 或 } \pi_1(i) \text{ 中} \\ \frac{1}{\sqrt{2}} (|\bar{0}\bar{0}\rangle - (-1)^{d_2} |\bar{1}\bar{1}\rangle)_{A_n, n+1}, & \text{在 } \pi_0(\bar{i}) \text{ 或 } \pi_1(\bar{i}) \text{ 中} \end{cases} \quad (8)$$

式(7)和式(8)意味着 $a_1 = d_1$ 和 $a_n = d_{n+1}$, 其中 $d_1, d_{n+1} \in \{0,1\}$ 表示粒子 1、 $n+1$ 在 $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ 基下的测量结果。

粒子 x, A_x, A_{x+1} 和 $x+2$ 在经管理员操作后所处的状态也可有相似的方法分析出来, 若在 $\pi_0(i)$ 或 $\pi_1(\bar{i})$ 中, 即

$$\begin{aligned}
&\frac{1}{2} (|\bar{0}\bar{0}\bar{0}\bar{0}\rangle + |\bar{0}\bar{0}\bar{1}\bar{1}\rangle + |\bar{1}\bar{1}\bar{0}\bar{0}\rangle + |\bar{1}\bar{1}\bar{1}\bar{1}\rangle)_{x, A_x, A_{x+1}, x+2} \\
&\text{若在 } \pi_1(i) \text{ 或 } \pi_0(\bar{i}) \text{ 中, 则是} \\
&\frac{1}{2} (|\bar{0}\bar{1}\bar{1}\bar{0}\rangle + |\bar{0}\bar{1}\bar{0}\bar{1}\rangle + |\bar{1}\bar{0}\bar{1}\bar{0}\rangle + |\bar{1}\bar{0}\bar{0}\bar{1}\rangle)_{x, A_x, A_{x+1}, x+2}
\end{aligned}$$

因此, 可以得到粒子 $1, A_1, A_x, A_{x+1}, A_n, n+1$ 组成的子系统和测量结果 $d_s, d_{x+1}, d_x, d_{x+2}$ 之间的对应关系。以 $d_s = d_{x+1} = d_x = d_{x+2} = 0$ 为例, 粒子 $1, A_1, A_x, A_{x+1}, A_n, n+1$ 组成的子系统对应的状态如式(9)所示。

$$\begin{aligned}
&\alpha (|\bar{0}\bar{0}\rangle + (-1)^{d_2} |\bar{1}\bar{1}\rangle)_{1, A_1} (|\bar{0}\bar{0}\rangle + \\
&\quad |\bar{1}\bar{1}\rangle)_{A_x, A_{x+1}} (|\bar{0}\bar{0}\rangle + (-1)^{d_n} |\bar{1}\bar{1}\rangle)_{A_n, n+1} + \\
&\quad \beta (|\bar{0}\bar{0}\rangle - (-1)^{d_2} |\bar{1}\bar{1}\rangle)_{1, A_1} (|\bar{1}\bar{1}\rangle - \\
&\quad |\bar{0}\bar{0}\rangle)_{A_x, A_{x+1}} (|\bar{0}\bar{0}\rangle - (-1)^{d_n} |\bar{1}\bar{1}\rangle)_{A_n, n+1} \quad (9)
\end{aligned}$$

依照基本协议中的步骤, 参与者 1、 $x+1$ 和 n 分别用 $\{|0\rangle, |1\rangle\}$ 基测量它们的粒子。因此, 根据信息管理者和其他成员的测量信息可知 A_x 处于式(10)所示状态。

$$\alpha |0 \oplus d_s \oplus a_{x+1}\rangle_{A_x} - (-1)^{d_{x+1} \oplus d_x \oplus a_1 \oplus a_n} \beta |1 \oplus d_s \oplus a_{x+1}\rangle_{A_x} \quad (10)$$

因为

$$\begin{aligned}
d_x &= (d_2 \oplus d_x \oplus d_{x+2} \oplus d_n) \oplus (d_2 \oplus d_{x+2} \oplus d_n) \\
&= (\bigoplus_{k \in G_1} (d_k \oplus d_{k+1})) \oplus D \\
&= (\bigoplus_{k \in G_1} a_k) \oplus D \\
&= A \oplus D
\end{aligned} \quad (11)$$

由此可知, 参与者 x 可以执行局域幺正操作 $X^{d_s \oplus a_{x+1}} Z^{d_{x+1} \oplus A \oplus D \oplus a_1 \oplus a_n}$ 正确地恢复出管理者要分割的量子信息 $|\phi\rangle$ 。

4.3 裁判员协议的正确性

当管理者对秘密信息进行分割后有删除成员的需求时, 依照裁判员协议进行调整后其余成员仍可以完成信息恢复任务。

定理 3 设 L 为被删除成员集合, 当集合 L 满足条件

$$|L \cap G_2| = 0 \text{ 且 } |L \cap G_3| \leq 1$$

或

$$|L \cap G_3| = 0$$

时, 协议能够对名单 L 上的参与者成功实现裁判员功能, 且剩余有效参与者仍能够完成量子信息重构任务。这里 $|\cdot|$ 表示集合的阶。

证明 在裁判员协议中, 参与共享的成员被分成了 3 个等级, 对不同等级的成员进行移除时所需要的操作不同。在不改变其余成员已有子秘密的情况下, 利用纠缠关系管理者能够通过执行局域操作实现量子秘密信息的更新, 从而使被裁判员的子秘密失效, 让裁判员后的成员组仍可完成秘密共享任务。

由前面分析可知, 对于 $k \in L \cap (G_1 \cup G_2)$, 管理者通过步骤 2 和步骤 4 可以将参与者 k 裁员。换句话说, 参与者 k 的子秘密在管理者更新秘密信息后的秘密重构中没有任何作用。

但是, 如果对参与者 x 或 $x+1$ 进行删除时, 则情况与之不同。为了进行秘密信息重构需要选定新的成员作为最终信息的接收者, 依照协议参与者 1 成为量子信息恢复后的拥有者。

首先考虑 $d_2 = d_x$ 的情况。管理者需要更新其秘密信息, 更新方式取决于两粒子局域操作 $CZ_{1,n+1}^\dagger$ 后, 对粒子 1 和 $n+1$ 的测量结果。倘若共享成员需要重构量子秘密信息时, 只需按照裁判员协议的步骤 8 进行测量即可。当参与者 $x \in L$ 时, 管理者对原秘密信息 $|\phi\rangle$ 执行更新操作

$X^{d_n \oplus d_{n+1}} Z^{d_1 \oplus d_{x+2} \oplus d_n \oplus d_{n+1}}$, 参与者 1 手中的粒子则处于式(12)所示状态。

$$\begin{aligned}
&\alpha |0 \oplus d_n \oplus d_{n+1} \oplus a_n\rangle + \\
&(-1)^{d_s \oplus d_{x+1} \oplus d_1 \oplus d_{x+2} \oplus d_n \oplus d_{n+1} \oplus d_x \oplus a_{x+1} \oplus a_n} \beta |1 \oplus d_n \oplus d_{n+1} \oplus a_n\rangle
\end{aligned} \quad (12)$$

如果 $x+1 \in L$, 管理者的新秘密是 $X^{d_n \oplus d_{n+1}} Z^{d_1 \oplus d_x \oplus d_n \oplus d_{n+1}} |\phi\rangle$, 对应参与者 1 手中粒子的状态为式(13)。

$$\begin{aligned}
&\alpha |0 \oplus d_n \oplus d_{n+1} \oplus a_n\rangle + \\
&(-1)^{d_s \oplus d_{x+1} \oplus d_1 \oplus d_n \oplus d_{n+1} \oplus a_x \oplus a_n} \beta |1 \oplus d_n \oplus d_{n+1} \oplus a_n\rangle
\end{aligned} \quad (13)$$

当 $d_2 \neq d_x$ 时, 管理者在执行两粒子操作 $CZ_{1,n+1}^\dagger$ 前对粒子 1 执行 $Z^\dagger = |+\rangle\langle+| - |-\rangle\langle-|$ 操作可以得到相同的结论。为了能够最终实现对管理者秘密信息重构, 经上述分析可知参与者 1 对其手中粒子执行局域操作 $X^{a_n} Z^{d_s \oplus d_{x+1} \oplus a_n \oplus A' \oplus D}$ 即可。

4.4 共享成员的等级性

在一个企业或机构中, 成员之间存在级别差异是比较常见的现象, 在实际工作进行决策或者执行任务时需要有些成员权限相对较大或者地位较高。在实际执行过程中, 管理者通常选择信用度最高或者最重要的参与者作为最终信息的恢复者(如本文协议中的参与者 x 或参与者 1), 此外往往还需要有监管者的存在(如本文的参与者 $x+1$ 和参与者 n)。

在本文的协议中, 参与者的等级性体现在 G_2 和 G_3 集合中的参与者不能同时离开或者缺席协议秘密信息重构过程, 而且 G_3 中至少有一个成员参与, 协议才能完成最后的秘密恢复。即 G_1 组中的参与者为普通成员, G_2 组中的参与者为中级成员, G_3 组中的参与者为高级成员。3 个组的成员对重构过程的影响作用是不同的, 管理者可以根据实际情况制定参与者级别, 且在共享量子纠缠信道时分配相应的粒子。

4.5 协议的安全性

本文给出了一个可删除参与成员的动态多分等级量子信息共享协议, 由上文正确性计算分析可知, 管理者可以将一个量子比特信息分割给 n 个参与者共享, 且只有在所有参与者都合作的情况下才能够恢复。不仅如此, 依照本文协议利用量子纠缠态的一些纠缠关系, 即使信息分割完成之后, 管理者也可以根据实际工作需要调整, 移除

部分成员。协议实现的本质是利用了量子隐形传态技术,且在共享量子纠缠信道之后其分割秘密、移除参与者时都采用局域操作,因此量子力学基本原理即可保障协议的安全性。对于前期共享量子纠缠的工作可以在传输时插入 decoy 态进行检测窃听,从而保障共享态的安全性。因此,此方案在考虑外部攻击者时可达到理论上安全。对于内部成员合谋的情况,与现有的部分共享量子信息的协议类似不能达到完美的安全性,虽然内部部分参与者合作可能会获得量子信息的振幅等信息,但不能确定秘密信息的完整内容。

5 结束语

对现有的分等级的量子信息共享方案,参与者的离开都会不可避免地影响到量子秘密的重构实现。本文针对这一问题进行了探究,并给出了新的协议。在本文提出的方案中,秘密信息的管理者仅通过对部分粒子的局域操作就可以实现成员删除的需求,同时经过调整后的参与者集合仍能完成量子信息共享功能。

概括起来,本文的分等级量子信息共享协议主要具有以下特点。

1) 根据实际需要,可对不超过 $n-2$ 个参与者在秘密重构阶段开始前进行成员删除。

2) 管理者对部分参与者进行裁员后,更新后的有效参与者集合可以利用现有量子纠缠资源完成秘密信息重构。

3) 参与者授权取消和秘密信息更新都只需要管理者的局域操作就可以完成。利用纠缠态相对相位信息的局域可操作性,管理者对秘密信息进行更新,从而使被移出参与者掌握的信息失去有效性。

与之前的分等级的量子信息共享协议比较,该方案具有裁员功能,因而有更好的灵活性和更好的适用性。考虑成员动态变更问题对密钥的管理有一定的实际意义,本文仅讨论了在分等级量子信息共享中成员删除的需求,如何设计可同时添加、删除成员的协议是值得继续研究的问题。

参考文献:

[1] KARLSSON A, KOASHI M, IMOTO N. Quantum entanglement for secret sharing and secret splitting[J]. Physical Review A, 1999, 59(1):162-168.

[2] HILLERY M, BUŽEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3):1829.

[3] KARIMIPOUR V, ASOUDEH M. Quantum secret sharing and random hopping: using single states instead of entanglement[J]. Physical Review A, 2015, 92(3): 30-36.

[4] LIN S, GUO G D, XU Y Z, et al. Cryptanalysis of quantum secret sharing with d-level single particles[J]. Physical Review A, 2016, 93(6): 23-28.

[5] YANG Y H, GAO F, WU X, et al. Quantum secret sharing via local operations and classical communication[J]. Scientific Reports, 2015(5): 69-76.

[6] YANG X, WEI K, MA H, et al. Measurement-device-independent quantum secret sharing[DB/OL]. http://xueshu.baidu.com/s?wd=paperuri%3A%28f0fd0c618c6c7908ac1c382c4b40a739%29&filter=sc_long_sign&tn=SE_xueshusource_2kduw22v&sc_vurl=http%3A%2F%2Ffarxiv.org%2Fpdf%2F1608.00114&ie=utf-8&sc_us=16717193560532515107.

[7] MAITRA A, DE S J, PAUL G, et al. Proposal for quantum rational secret sharing[J]. Physical Review A, 2015, 92(2): 22-35.

[8] WANG X W, XIA L X, WANG Z Y, et al. Hierarchical quantum information splitting[J]. Optics Communications, 2010:1196-1199.

[9] WANG X W, ZHANG D Y, TANG S Q, et al. Hierarchical quantum information splitting with six-photon cluster states[J]. International Journal of Theoretical Physics, 2010, 49(11): 2691-2697.

[10] WANG X W, ZHANG D Y, TANG S Q, et al. Multiparty hierarchical quantum-information splitting[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2011, 44(3): 35-45.

[11] XU G, WANG C, YANG Y X. Hierarchical quantum information splitting of an arbitrary two-qubit state via the cluster state[J]. Quantum Information Processing, 2014, 13(1): 43-57.

[12] CACHIN C. On-line secret sharing[C]//The 5th IMA Conference on Cryptography and Coding. 1995:190-198.

[13] BLUNDO C, CRESTIB A, SANTISA A D, et al. Fully dynamic secret sharing schemes[J]. Theoretical Computer Science, 1996, 165(2): 407-440.

[14] LI M, POOVENDRAN R. Broadcast enforced threshold schemes with disenrollment[C]//Selected Area on Cryptography (SAC). 2003:1-16.

[15] LI M, POOVENDRAN R. Disenrollment with forward secrecy in threshold schemes[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1676-1682.

[16] JIA H Y, WEN Q Y, GAO F, et al. Dynamic quantum secret sharing[J]. Physics Letters A, 2012, 376(10): 1035-1041.

[17] 贾恒越. 图态的远程制备及在量子密码协议中的应用[D].北京: 北京邮电大学, 2012.

JIA H Y. State diagram of the remote preparation and application in quantum cryptographic protocols[D]. Beijing: Beijing University of Posts and Telecommunications, 2012.

[18] HSU J L, CHONG S K, HWANG T, et al. Dynamic quantum secret sharing[J]. Quantum Information Processing, 2013, 12(1): 331-344.

[19] WANG T Y, LI Y P. Cryptanalysis of dynamic quantum secret sharing[J]. Quantum Information Processing, 2013, 12(5): 1991-1997.

[20] LIAO C H, YANG C W, HWANG T. Dynamic quantum secret

sharing protocol based on GHZ state[J]. Quantum Information Processing, 2014, 13(8): 1907-1916.

- [21] LIU H, MA H, WEI K, et al. Multi-group dynamic quantum secret sharing with single photons[J]. Physics Letters A, 2016, 380(31): 2349-2353.
- [22] MISHRA S, SHUKLA C, PATHAK A, et al. An integrated hierarchical dynamic quantum secret sharing protocol[J]. International Journal of Theoretical Physics, 2015, 54(9): 3143-3154.
- [23] BRIEGEL H J, RAUSSENDORF R. Persistent entanglement in arrays of interacting particles[J]. Physical Review Letters, 2001, 86(5):910-913.
- [24] HEIN M, DÜR W, BRIEGEL H J. Entanglement properties of multipartite entangled states under the influence of decoherence[J]. Physical Review A, 2005,71(3): 32-35.
- [25] HEIN M, EISERT J, BRIEGEL H. Multiparty entanglement in graph states[J]. Physical Review A, 2004, 69(6): 23-29.
- [26] WALTHER P, RESCH K J, RUDOLPH T, et al. Experimental one-way quantum computing[J]. Nature, 2005: 169-176.
- [27] ZHANG A N, LU C Y, ZHOU X Q, et al. Experimental construction of optical multiqubit cluster states from Bell states[J]. Physical Review A, 2006,73(2): 22-33.
- [28] LU C Y, ZHOU X Q, GHNE O, et al. Experimental entanglement of six photons in graph states[J]. Nature, 2007(3): 91-95.

作者简介:



贾恒越 (1983-), 女, 内蒙古海拉尔人, 博士, 中央财经大学讲师, 主要研究方向为量子信息、量子密码协议设计。



武霞 (1987-), 女, 山东临沂人, 博士, 中央财经大学讲师, 主要研究方向为量子信息。



张可佳 (1987-), 男, 黑龙江大庆人, 博士, 黑龙江大学讲师, 主要研究方向为量子密码、量子信息。



朱建明 (1965-), 男, 山西太原人, 中央财经大学教授、博士生导师, 主要研究方向为信息安全、经济信息分析。



李洋 (1981-), 男, 山西太原人, 博士, 中央财经大学副教授, 主要研究方向为电子商务安全、IP 网络安全、移动通信安全。