基于非对称量子通道受控 QOT 量子投票协议*

王郁武† 韦相和 朱兆辉

(淮阴师范学院计算机科学与技术学院, 淮安 223300)

(2013年1月7日收到; 2013年4月16日收到修改稿)

提出一种量子投票协议, 协议基于非对称量子通道受控量子局域幺正操作隐形传输 (quantum operation teleportation, QOT). 由公正机构 CA 提供的零知识证明的量子身份认证, 保证选民身份认证的匿名性. 计票机构 Bob 制造高维 Greenberger-Horne-Zeilinger 纠缠态建立一个高维量子通信信道. 选民对低维的量子选票进行局域幺正操作的量子投票, 是通过非对称基的测量和监票机构 Charlie 的辅助测量隐形传输的. Bob 在 Charlie 帮助下可以通过幺正操作结果得到投票结果. 与其他一般的 QOT 量子投票协议相比, 该协议利用量子信息与传输的量子信道不同维, 使单粒子信息不能被窃取、防止伪造. 选举过程由于有 Charlie 的监督, 使得投票公正和不可抵赖. 由于量子局域幺正操作隐形传输的成功概率是 1, 使量子投票的可靠性得以保证.

关键词: 量子投票, 高维 GHZ 纠缠态, 非对称基测量, 量子操作隐形传输

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.160302

1 引 言

量子投票是以量子密码通信为基础, 利用量子本身的物理特性克服经典密码中存在的安全性问题, 保证选票信息的安全性及参与者身份的合法性, 从而提高投票活动的可靠性. Vaccaro 等 [1] 在 2007 年定义了量子投票协议的标准. 最早的两种量子投票模式由 Hillery [2] 提出, 包括移动式投票方案和分配式投票方案. 以后, 各种量子投票协议 [3−5] 先后被提出. 随着现有通信光纤相匹配的单光子探测器技术的发展 [6], 为单光子量子投票协议的发展奠定了坚实的基础. 在单光子量子通信中, 用纠缠态作为量子信道, 传输量子信息的形式有两种: 一种是传输量子态, 称为量子态隐形传输 (quantum-state teleportation, QST); 另一种是对量子态的局域幺正操作隐形传输, 称为量子操作隐形传输 (quantum operation teleportation, QOT). Bennett 等 [7] 在 1993 年提出了 QST. Huelga 等 [8] 在 2001 年提出 QOT. 以后, 众多的研究人员提出了各种 QST 方案 [9−27] 和 QOT 方案 [28−38]. 近来, 用高维纠缠态作为量子通道传递低维的量子信息称之为非对称量子通道的隐形态传输 [39] 是现在量子通信研究的热点问题之一. 本文提出一种用非对称量子通道, 三方控制的局域幺正操作的 QOT 的量子投票协议. 本协议比用二维纠缠态进行的 QOT 的量子投票协议有一定的优点, 最重要的是单个粒子的信息无法被窃取. 在公正机构 CA 提供的零知识证明的量子身份认证 [40] 帮助下, 解决了选民身份的合法性和匿名性认证的问题.

本文第 2 节介绍了非对称量子通道受控 QOT 的协议; 第 3 节设计了量子投票协议; 第 4 节是量子投票协议正确性和安全性的分析, 首先对量子投票协议的正确性进行分析, 然后对量子投票协议的安全性进行讨论.

2 非对称量子通道受控量子操作传输的协议

2.1 非对称量子通道

设一个 3 维的 Hilbert 空间的 p 粒子与一个 2

* 江苏省教育厅基金 (批准号: 11KJB520002, JHB2012-53) 资助的课题.

† 通讯作者. E-mail: wyw@hytc.edu.cn

维的 Hilbert 空间的粒子 q 组成的最大纠缠态为

$$|\Psi_{00}\rangle_{pq} = 1/\sqrt{2}(|00\rangle + |11\rangle)_{pq}, \tag{1}$$

根据文献 [34, 41—43] 构建一组单粒子操作 $U_{mn}^{(3)}$:

$$\begin{aligned}
U_{00}^{(3)} &= |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|,\\
U_{01}^{(3)} &= |0\rangle\langle 0| - |1\rangle\langle 1| + |2\rangle\langle 2|,\\
U_{10}^{(3)} &= |1\rangle\langle 0| + |2\rangle\langle 1| + |0\rangle\langle 2|,\\
U_{11}^{(3)} &= |1\rangle\langle 0| - |2\rangle\langle 1| + |0\rangle\langle 2|,\\
U_{20}^{(3)} &= |2\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 2|,\\
U_{21}^{(3)} &= |2\rangle\langle 0| - |0\rangle\langle 1| + |1\rangle\langle 2|.
\end{aligned} \tag{2}$$

当 $U_{mn}^{(3)}$ 对三维粒子 p 进行操作非对称态 $|\Psi_{00}\rangle$ 将转换得相应的态分别为

$$\begin{aligned}
U_{00}^{(3)}|\Psi_{00}\rangle &= 1/\sqrt{2}(|00\rangle + |11\rangle) = |\Psi_{00}\rangle,\\
U_{01}^{(3)}|\Psi_{00}\rangle &= 1/\sqrt{2}(|00\rangle - |11\rangle) = |\Psi_{01}\rangle,\\
U_{10}^{(3)}|\Psi_{00}\rangle &= 1/\sqrt{2}(|10\rangle + |21\rangle) = |\Psi_{10}\rangle,\\
U_{11}^{(3)}|\Psi_{00}\rangle &= 1/\sqrt{2}(|10\rangle - |21\rangle) = |\Psi_{11}\rangle,\\
U_{20}^{(3)}|\Psi_{00}\rangle &= 1/\sqrt{2}(|20\rangle + |10\rangle) = |\Psi_{20}\rangle,\\
U_{21}^{(3)}|\Psi_{00}\rangle &= 1/\sqrt{2}(|20\rangle - |10\rangle) = |\Psi_{21}\rangle.
\end{aligned} \tag{3}$$

(3) 式的 6 个态 $|\Psi_{mn}\rangle$ ($m = 0,\ 1,\ 2;\ n = 0,\ 1$) 构成正交的完备的非对称测量基 $\{|\Psi_{mn}\rangle\}$, 满足 $\sum_m\sum_n|\Psi_{mn}\rangle\langle\Psi_{mn}| = I$, $\langle\Psi_{mn}|\Psi_{m'n'}\rangle = \delta_{mm'}\delta_{nn'}$ ($m' = 0,1,2$; $n' = 0,1$).

2.2 受控 QOT 协议

下面对受控 QOT 协议进行具体的描述. 假设 Alice 是进行量子操作的一方, 想要将他的量子操作直接传输给 Bob, Bob 同时要求 Alice 在 Charlie 的同意之下, 才能得到量子操作. 当 Bob 用文献 [44] 方法使 Alice 的粒子 a' 的态为: $|\varphi\rangle_{a'} = (\alpha|0\rangle + \beta|1\rangle)_{a'}$, ($|\alpha|^2 + |\beta|^2 = 1$), a' 的态是二维的 Hilbert 空间的态. Alice 对 a' 的态 $|\varphi\rangle_{a'}$ 的量子操作记为 $U_k|\varphi\rangle_{a'}$. 设 $\{U_k\}$ ($k = 0,1,2$), $\{U_k\} = \{I = |0\rangle\langle 0| + |1\rangle\langle 1|, X = |1\rangle\langle 0| + |0\rangle\langle 1|, Y = \mathrm{i}(-|1\rangle\langle 0| + |0\rangle\langle 1|)\}$. Bob 制造三维的 Hilbert 空间的 3 粒子 Greenberger-Horne-Zeilinger (GHZ) 纠缠态

$$|\phi\rangle_{abc} = 1/\sqrt{3}(|000\rangle + |111\rangle + |222\rangle)_{abc}. \tag{4}$$

将 a, b, c 做如下分配: a 分配给 Alice, c 分配给 Charlie, Bob 自己留 b, 整个系统形式为

$$\begin{aligned}
|\zeta\rangle &= |\phi\rangle_{abc}\otimes(U_k|\varphi\rangle_{a'})\\
&= 1/3\sqrt{2}\Big\{|\Psi_{00}\rangle_{aa'}[(U_k|\varphi\rangle)_b|x_0\rangle_c + (V_{20}^{(3)}U_k|\varphi\rangle)_b|x_1\rangle_c\\
&\quad + (V_{10}^{(3)}U_k|\varphi\rangle)_b|x_2\rangle_c] + |\Psi_{01}\rangle_{aa'}[(U_{01}^{(3)}U_k|\varphi\rangle)_b|x_0\rangle_c\\
&\quad + (U_{01}^{(3)}V_{20}^{(3)}U_k|\varphi\rangle)_b|x_1\rangle_c + (U_{01}^{(3)}V_{10}^{(3)}U_k|\varphi\rangle)_b|x_2\rangle_c]\\
&\quad + |\Psi_{10}\rangle_{aa'}[(U_{20}^{(3)}U_k|\varphi\rangle)_b|x_0\rangle_c\\
&\quad + (U_{20}^{(3)}V_{20}^{(3)}U_k|\varphi\rangle)_b|x_1\rangle_c + (U_{20}^{(3)}V_{10}^{(3)}U_k|\varphi\rangle)_b|x_2\rangle_c]\\
&\quad + |\Psi_{11}\rangle_{aa'}[(U_{01}^{(3)}U_{20}^{(3)}U_k|\varphi\rangle)_b|x_0\rangle_c\\
&\quad + (U_{01}^{(3)}U_{20}^{(3)}V_{20}^{(3)}U_k|\varphi\rangle)_b|x_1\rangle_c\\
&\quad + (U_{01}^{(3)}U_{20}^{(3)}V_{10}^{(3)}U_k|\varphi\rangle)_b|x_2\rangle_c]\\
&\quad + |\Psi_{20}\rangle_{aa'}[(U_{10}^{(3)}U_k|\varphi\rangle)_b|x_0\rangle_c + (U_{10}^{(3)}V_{20}^{(3)}U_k|\varphi\rangle)_b|x_1\rangle_c\\
&\quad + (U_{10}^{(3)}V_{10}^{(3)}U_k|\varphi\rangle)_b|x_2\rangle_c]\\
&\quad + |\Psi_{21}\rangle_{aa'}[(U_{01}^{(3)}U_{10}^{(3)}U_k|\varphi\rangle)_b|x_0\rangle_c\\
&\quad + (U_{01}^{(3)}U_{10}^{(3)}V_{20}^{(3)}U_k|\varphi\rangle)_b|x_1\rangle_c\\
&\quad + (U_{01}^{(3)}U_{10}^{(3)}V_{10}^{(3)}U_k|\varphi\rangle)_b|x_2\rangle_c]\Big\}
\end{aligned} \tag{5}$$

(5) 式中的 $|x_f\rangle$ 形式为

$$|x_f\rangle = \sum_{j=0}^{2}\mathrm{e}^{2\pi\mathrm{i}jf/3}|j\rangle/\sqrt{3}, \quad (f = 0,1,2). \tag{6}$$

称为单粒子测量基, (5) 式中的 $V_{\mu v}^{(3)}$ 形式为

$$V_{\mu v}^{(3)} = \sum_{j=0}^{2}\mathrm{e}^{-2\pi\mathrm{i}j\mu/3}|j\rangle\langle(j+v) \bmod 3|, \quad (\mu, v = 0,1,2). \tag{7}$$

称为三维幺正操作.

Alice 对所具有的粒子 a, a' 进行非对称基 $|\Psi_{mn}\rangle$ 的测量结果为 $|\Psi_{mn}\rangle_{aa'}$, Charlie 如果同意, 则用单粒子测量基 $|x_f\rangle$ 对自己的粒子 c 进行单粒子测量基 $|x_f\rangle$ 的测量结果为 $|x_f\rangle_c$. Alice, Charlie 通过经典信道公布测量结果给 Bob, Bob 知道 Alice, Charlie 的测量结果后, 根据 (5) 式, 知道系统塌陷到 $|\Psi_{mn}\rangle_{aa'}|x_f\rangle_c$ 项中, Bob 对粒子 b 用单粒子操作 $U_{mn}^{(3)}$ 及三维幺正操作 $V_{\mu v}^{(3)}$ 得知 $(U_k|\varphi\rangle)_b$, 量子操作传输成功.

3 量子投票协议

量子投票的参与者有如下几个: 1) 公正机构 CA; 2) 计票机构 Bob; 3) 监票机构 Charlie; 4) 若干选民 Ai. 量子投票过程图如图 1 所示.

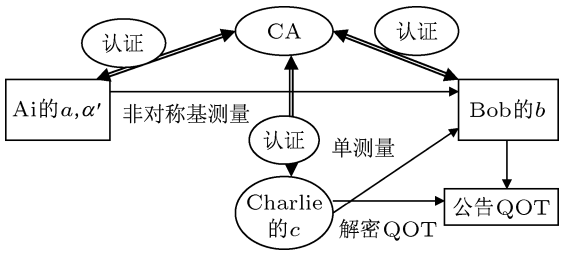

图 1 量子投票过程图

3.1 准备阶段

公正机构 CA 为合法选民 Ai 发放的量子身份证, 设选民人数为 n. CA 同时为监票机构 Charlie 和发票机构 Bob 发放量子身份证.

3.2 投票阶段

第 1 步, 监票机构 Charlie 设立公示栏. 通过公示栏, 可以将经典信息通过经典信道传递, 公示给所有人.

第 2 步, 领取量子选票. 其过程如下: 选民 Ai 到计票机构 Bob 处领取量子选票, Bob 在 CA 的帮助下, 用零知识证明的量子身份认证方法匿名认证选民 Ai 的合法身份 [40]. 认证获得通过后, Bob 用文献 [44] 方法给 Ai 的粒子 a' 制作一张量子选票 $|\varphi\rangle_{a'}=(\alpha|0\rangle+\beta|1\rangle)_{a'}$, $(|\alpha|^2+|\beta|^2=1)$ 并给予编号为 i.

第 3 步, 登记选民. 选民 Ai 到 Charlie 处登记, Charlie 在 CA 的帮助下用上述方法, 认证选民身份. 认证获得通过后, Ai 将自己的编号 i 告知 Charlie. Charlie 制定 i 号量子选票的投票规则. 例: 约定 Ai 对量子选票的局域操作 $U_{\mathrm{i}k}=\{U_1=I,U_2=X,U_3=Y\}=\{$同意, 不同意, 弃权$\}$. 可用类拟于 BB84 协议[45] 加密方法传送给这个选民. 但 Bob 和其他选民不知道这个规则.

第 4 步, 请求投票. 选民 Ai 将 i 告知到 Bob 请求投票, Bob 制备三维的 Hilbert 空间的 GHZ 纠缠态 (4) 式, 将粒子 a 分配给 Ai, 粒子 c 分配给 Charlie, Bob 自己留粒子 b.

第 5 步, Ai 投票. Ai 根据投票规则, 对 a' 进行 $U_{\mathrm{i}k}$ 操作, $U_{\mathrm{i}k}$ 操作完后, 用测量基 $|\Psi_{mn}\rangle$ 测量 a', a, 将结果 $|\Psi_{mn}\rangle_{aa'}$ 公告在 Charlie 设立的公示栏上, Bob 和 Charlie 都可以看到结果 $|\Psi_{mn}\rangle_{aa'}$. Charlie 明确选票的编号 i 后, 用测量基 $|x_f\rangle$ 对 c 进行测量, 将测量结果 $|x_f\rangle_c$ 公告在公示栏, Ai 和 Bob 都可以看到结果 $|x_f\rangle_c$.

第 6 步, Bob 得到 Ai 的局域幺正操作的结果. 根据公示栏上 $|\Psi_{mn}\rangle_{aa'}$ 和 $|x_f\rangle_c$, Bob 通过 (5) 式, 知道自己的粒子 b 塌陷到 $|\Psi_{mn}\rangle_{aa'}|x_f\rangle_c$ 项上, 对粒子 b 进行相关的单粒子操作 $U_{mn}^{(3)}$ 及相关的三维幺正操作 $V_{\mu v}^{(3)}$ 而得到 $(U_k|\varphi\rangle)_b$. 从而知道 Ai 所做的局域幺正操作结果 $U_{\mathrm{i}k}$. 将 Ai 局域幺正操作的结果 $U_{\mathrm{i}k}$ 公布到公告栏上, Ai 和 Charlie 可以看到 $U_{\mathrm{i}k}$.

第 7 步, Bob 这时统计选民的人数 j. 每次投票后, $j=j+1$, 当 $j<n$ 时, 继续下一次投票, $j=n$ 时, 宣布投票结束.

3.3 计票阶段

当 Bob 宣布投票结束后, Charlie 将公示栏上的 $U_{\mathrm{i}k}$ 解密, 公示每个编号 i 的 $U_{\mathrm{i}k}$ 代表的投票结果, Bob 根据这统计出全体投票结果.

4 协议的正确性与安全性分析

4.1 协议正确性分析

对于量子选票的量子局域幺正操作代表的投票信息, 只有 Ai 和 Charlie 知道对量子态么正操作的意义. 在公示解密前, 虽然公示量子局域幺正操作的结果, 但选票信息是隐秘的. 由于采用的是零知识证明的方法 [40] 认证选民 Ai 身份, Bob 只知道 Ai 是第 i 号选民, 无法知道 Ai 选民其他的任何信息. Bob 发放的是量子选票, 而 Ai 对量子态么正操作代表投票信息是没有收据可言. 这就保证了投票过程的匿名性. Charlie 控制测量可以根据自己操作来监督 Bob 计数工作. 因此所有合法选票会被正确统计. 不可能统计不到, 又不可能重复投票, 这就保证了投票过程的正确性. 在 CA 的帮助下, 可追溯参与投票的各个人的身份, 这就保证了投票过程的可追溯性.

4.2 协议安全性分析

攻击者在量子信道上进行攻击, 量子身份证、量子选票 [44] 都是量子态制造, 根据量子不可克隆定理, 攻击者无法伪造量子身份证和量子选票. 传输的量子信息和使用的量子信道不在同维的

Hilbert 空间, 以及有监票机构 Charlie 控制测量, 使得 Ai 的选票信息 (么正操作) 不可能被攻击者窃听. 攻击者在经典信道上进行攻击, 在经典信道上, 传递的信息只是一些指令性的消息, 不涉及投票系统参与者的身份信息、选票信息 (么正操作). 攻击者不可能得到投票系统参与者的身份信息和选票信息. 另外, Ai 和 Bob 投票工作都有 Charlie 监控, 所以双方都不可抵赖投票过程. 公示栏实时显示投票过程的结果, 选民如发现 Bob 公布的么正操作与自己所做的么正操作不符, 可以立即向 Charlie 投诉.

5 结 论

本文提出了非对称量子通道受控 QOT 量子投票协议. 传输的量子信息和量子信道在不同维的 Hilbert 空间, 因此保证了单个粒子信息无法被窃取. 由于协议中选民 Ai 对粒子的量子局域幺正操作代表的选举信息是保密的, 在选举过程中, 这就使得其他选民以及计票机构 Bob 无法根据量子局域幺正操作结果获得与 Ai 投票有关的任何信息. 保证信息无法被窃取. 零知识证明的量子身份认证使得匿名的身份的认证成为可能 [40]. 另外, 该协议的实现涉及量子态制备及测量等, 在目前的实验水平下是比较容易实现的, 且根据 (5) 式可知, 量子局域幺正操作隐形传输成功的概率为 1, 系统具有可靠性. 因此, 本协议具有一定的实用性.

[1] Vaccaro J A, Joseph S, Anthony C 2007 *Phys. Rev.* A **75** 012333

[2] Hillery M 2006 *The International Soeiety for Optieal Engineering* 10.1117/2.1200610.0419

[3] Wen X J, Cai X J 2011 *J. Shandong Univ.* (Natural Science) **46** 9 (in Chinese) [温晓军, 蔡学军 2011 山东大学学报 (理学版) **46** 9]

[4] Yi Z, He G Q, Zeng G H 2009 *Acta Phys.Sin.* **58** 3166 (in Chinese) [易智, 何广强, 曾贵华 2009 物理学报 **58** 3166]

[5] Horoshko D, Kilin S 2011 *Phys. Lett.* A **375** 1172

[6] Wu Q L, Liu Y, Chen W, Han Z F, Wang K Y, Guo G C 2010 *Prog. Phys.* **30** 296 (in Chinese) [吴青林, 刘云, 陈巍, 韩正甫, 王克逸, 郭光灿 2010 物理学进展 **30** 296]

[7] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895

[8] Huelga S F, Vaccaro J A, Chefles A 2001 *Phys. Rev.* A **63** 042303

[9] Cirac J I, Parkins A S 1994 *Phys. Rev.* A **50** R4441

[10] Moussa M H Y 1997 *Phys. Rev.* A **55** R3287

[11] Lee J, Kim M S 2000 *Phys. Rev. Lett.* **84** 4236

[12] Li W L, Li C F, Guo G C 2000 *Phys. Rev.* A **61** 034301

[13] Bowen G, Bose S 2001 *Phys. Rev. Lett.* **87** 267901

[14] Rigolin G 2005 *Phys. Rev.* A **71** 032303

[15] Yao Y, Chua W K 2006 *Phys. Rev. Lett.* **96** 060502

[16] Gordon G, Rigolin G 2006 *Phys. Rev.* A **73** 042309

[17] Muralidharan S, Panigrahi P K 2008 *Phys. Rev.* A **77** 032321

[18] Bouwmeester D, Pan J W, Kmattle, Eibl M, Weinfurter H, Zeilinger A 1997 *Nature* **390** 575

[19] Furusawa A, Sorensen J L, Braustein S L, Fuchs C A, Kimble H J, Polzik E S 1998 *Science* **282** 706

[20] Stemholm S, Bardroff P J 1998 *Phys. Rev.* A **58** 4373

[21] Son W, Lee J, Kim M S, Park Y J 2001 *Phys. Rev.* A **64** 064304

[22] Hsu L Y 2003 *Phys. Lett.* A **311** 459

[23] Roa L, Delgado A, Fuentes-Guridi I 2003 *Phys. Rev.* A **68** 022310

[24] Dai H Y, Zhang M, Li C Z 2004*Phys. Lett.* A **323** 360

[25] Pati A K, Agrawal P 2007 *Phys. Lett.* A **371** 185

[26] Zhan Y B 2007 *Chin. Phys.* **16** 2557

[27] Gulfam Q ul A, Ikram R ul I M 2008 *J. Phys.* B: *At. Mol. Opt. Phys.* **41** 165502

[28] Huelga S F, Plenio M B, Vaccaro J A 2002 *Phys. Rev.* A **65** 042316

[29] Zou X B, Pahlke K, Mathis W 2002 *Phys. Rev.* A **65** 064305

[30] Dür W, Vidal G, Cirac J I 2002 *Phys. Rev. Lett.* **89** 057901

[31] Zhang Y S, Ye M Y, Guo G C 2005 *Phys. Rev.* A **71** 062331

[32] Wang A M 2006 *Phys. Rev.* A **74** 032317

[33] Yao C M 2006 *Chin. Phys. Lett.* **23** 545

[34] Wang A M 2007 *Phys. Rev.* A **75** 062323

[35] Zhao N B, Wang A M 2007 *Phys. Rev.* A **76** 062317

[36] Zhao N B, Wang A M 2008 *Phys. Rev.* A **78** 014305

[37] Yao C M, Cao B F 2009 *Phys. Lett.* A **373** 1011

[38] Zhang Z J, Cheung C Y 2011 *J. Phys.* B: *At. Mol. Opt. Phys.* **44** 165508

[39] Zhan Y B, Zhang Q Y, Wang Y W, Ma P C 2010 *Chin. Phys. Lett.* **27** 010307

[40] Wang Y W, Zhan Y B 2009 *Acta Phys. Sin.* **58** 7668 (in Chinese) [王郁武, 詹佑邦 2009 物理学报 **58** 7668]

[41] Wang J, Chen H Q, Zhang Q, Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese) [王剑, 陈皇卿, 张权, 唐朝京 2007 物理学报 **56** 673]

[42] Fan Q B, Zhang S 2006 *Phys. Lett.* A **348** 160

[43] Zhan Y B, Ma P C, Zhang Q Y 2012 *Inter. J. Quant. Infor.* **10** 1250074

[44] Pati A K 2001 *Phys. Rev.* A **63** 014302

[45] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE Press) p175

Quantum voting protocols based on the non-symmetric quantum channel with controlled quantum operation teleportation*

Wang Yu-Wu† Wei Xiang-He Zhu Zhao-Hui

(*School of Computer Science and Technology, Huaiyin Normal University, Huai'an* 223300*, China*)

(Received 7 January 2013; revised manuscript received 16 April 2013)

Abstract

In the paper, we present a kind of quantum voting protocol, which is based on controlled quantum teleportation of local unitary operations in non-symmetric quantum channel. In this protocol, the umpire CA with zero knowledge proof quantum identity authentication ensures voter's anonymous identity authentication. The counting institution Bob generates a high-dimensional Greenberger-Horne-Zeilinger entangled state to establish a high-dimensional quantum communication channel. Performing the local unitary operation on their low-dimensional quantum ballot, voter's quantum vote is teleportated by asymmetric matrix measurement and scrutineer Charlie auxiliary measuring. With the scrutineer Charlie's help, Bob achieves the voting result by the output of unitary operation. Compared with other general quantum operation teleportation quantum voting protocol, the protocol utilizes the quantum information and transmission of quantum channel, which have different dimensions, so single particle information cannot be stolen, and can prevent forgery. The electoral process is fair and undeniable, owing to Charlie's supervision. Since the success probability of quantum teleportation of local unitary operations is 1, the quantum voting is reliable.

Keywords: quantum voting, high-dimensional entangled state, non-symmetricbasis measurement, quantum operation teleportation

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.160302

* Project supported by Jiangsu Provincial Department of Education, China (Grant Nos. 11KJB520002, JHB2012-53).

† Corresponding author. E-mail: wyw@hytc.edu.cn