基于 d 维三粒子纠缠态的量子投票表决方案

宋秀丽[1],曹耘凡[2],杨 帅[2]
(1. 重庆邮电大学网络空间安全与信息法学院,重庆 400065; 2. 重庆邮电大学计算机科学与技术学院,重庆 400065)

摘 要: 为了突破2 维或3 维 Hilbert 空间限制,本文结合投票表决的实际需求,基于 Shamir (t,n) 门限思想,提出了一个 d 维三粒子纠缠态的量子投票表决方案. 该方案由投票管理中心、投票群组、监票人和计票人四个实体共同完成投票工作. 该方案使用 d 维量子纠缠态增强了适用性,使用单粒子作为投票载体提升了传输效率. 该方案的正确性通过在 IBM 量子云平台上的模拟仿真得以证实. 安全性分析表明,该方案在满足投票方案的安全性需求基础上,能抵抗截获-测量-重发、纠缠测量和伪造攻击. 性能分析表明,随着参与人数的增多,该方案比其他相似的投票方案具有更高的量子比特效率.

关键词: 量子投票; d 维三粒子纠缠态; (t, n) 门限; 量子云平台
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2020)07-1355-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.07.014

Quantum Voting Scheme Based on d Dimensional Three-Particle Entangled State

SONG Xiu-li[1], CAO Yun-fan [2], YANG Shuai [2]
(1. *School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*;
2. *School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: To break through the limitations of two-dimensional or three-dimensional Hilbert space, a quantum voting scheme based on d-dimensional three-particle entangled state was proposed, which was designed by using Shamir (t,n) threshold to meet the actual demand for voting. The scheme consists of four entities: the voting management center, the voting group, the scrutineer and the ballot counter, which work together to complete the voting. In this scheme, a d-dimensional quantum entanglement state is used to enhance the applicability, and the single particle is used as the voting carrier to improve the transmission efficiency. The correctness of the proposed scheme was verified by the experimental simulations on the IBM quantum cloud platform. Security analysis shows that the scheme meets the security requirements of voting schemes, and resists intercept-measure-resend attack, entangle-measure attack, and forgery attack. Performance analysis shows that with the increase of the number of participants, the scheme has higher qubit efficiency than other similar schemes.

Key words: quantum voting; d-dimensional three-particle entangled state; (t,n) threshold; quantum cloud platform

1 引言

在现代社会中,日常生活的各个方面几乎都计算机化和网络化,包括各种情况下的投票表决系统:从国家政府机构的选举到班级议会等相当小的群体决策. 在1981 年,Chaum[1] 提出了第一个匿名网络投票方案. 于1988 年,Chaum[2] 又提出了一种基于 RSA 的无条件安全投票的改进方案. 随后许多经典匿名投票方案被提出,这些方案都是基于计算复杂度或大素数因子分解问题等传统密码学体制设计的[3,4]. 但随着量子计算机的研制和开发,传统投票表决方案的机密性、匿名性和身份验证等信息安全问题难以保证.

为了克服传统网上投票表决方案在量子背景下的局限性,一些研究者借鉴经典网上安全投票表决的思想,提出了基于量子力学原理的量子投票方案[5~12]. 例如,2007 年 Vaccaro 等人[5] 提出了一种可

收稿日期:2019-05-23;修回日期:2020-01-19;责任编辑:李勇锋
基金项目:国家自然科学基金(No. 61772098, No. 61772099, No. 61802039);重庆市科学技术委员会基础科学与前沿技术项目(No. cstc 2018jcyjAX0510)

认证的匿名量子投票方案,随后 2008 年,Li 等人[6]利用了量子纠缠的原理,提出了一种安全匿名投票方案. 2011 年 Horoshko 等人[7]设计了一种以 Bell 态进行匿名验证的投票方案. 2015 年 Cao 等人[8]提出了一种基于 Bell 纠缠态的投票方案,该方案基于传统投票模型,使用单粒子测量完成计票工作. 2016 年 Naseri M 等人[9]提出了一种基于 GHZ 纠缠态的匿名投票表决方案. 该方案中的投票表决者只有两人,当投票人数增多,投票量子载体会相应地增加. 同年,Wang 等人[10]提出了一种由两种纠缠量子态辅助的量子匿名投票协议. 2017 年,刘小华等人[11]提出了一种基于四粒子 GHZ 态的投票方案,该方案设有双监督模式增强了安全性,但如果投票人数较多时,则需要多次重复制备四粒子 GHZ 态,量子制备消耗较大. 同年,Zhang 等人[12]基于量子代理盲签名提出了一个量子投票方案. 该方案既制备 EPR 对,又制备 GHZ 态,导致量子比特效率较低.

上述的投票方案大多数是基于 Bell 态或 GHZ 态设计的,且要求投票者各自保存一个粒子,这导致制备粒子的数目较大,且粒子的传输效率偏低. 针对以上问题,本文将 Shamir(t,n)门限的思想[13]和 d 维三粒子纠缠态的特性相结合,提出了一种新的量子投票表决方案. 该方案使用 d 维量子纠缠态增强适用性,使用单粒子作为投票载体,降低量子态的制备消耗,提升传输效率.

2 提出的量子投票表决方案

提出方案的量子投票表决模型框图如图 1 所示,主要包含四个实体:一是投票群组 Group,负责投票表决;二是投票管理中心 Administrator,负责制备初始纠缠态,并生成和分发私密信息;三是监票人 Alice,负责监督工作,并对投票群体身份进行认证;四是计票人 Bob,负责投票表决统计工作.

在图 1 中,①表示 Administrator 制备 d 维三粒子纠缠态和私密份额,并将粒子分别发送给 Group、Alice 和 Bob,且将私密份额发送给 Group 中的成员. ②表示 Group 中投票参与者的投票过程. ③表示投票完毕后 Group 将粒子发送给 Alice,Alice 对 Group 进行群体身份认证. ④表示 Alice 将粒子发送给 Bob,Bob 进行计票工作.

2.1 初始化阶段

在本阶段,正如投票结构图 1 所示,假设第 k 个群组 G_k 向 Administrator 发起投票申请,Administrator 制备初始量子纠缠态和秘密份额,并将指定的粒子和份额分发给其他各方.

步骤 1 基于 Shamir(t,n)门限思想, Administrator

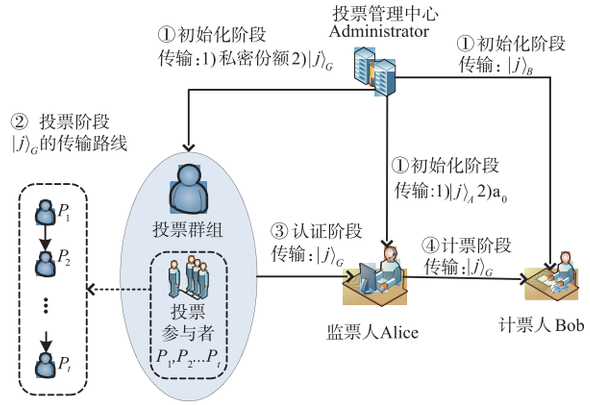

图1 量子投票表决模型框图

首先随机选取一个 $t-1$ 次多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}(\mathrm{mod}\ d)$,其中 $(a_0,a_1,\cdots,a_{t-1})\in Z_d^t$,$a_0$ 作为 G_k 的身份认证码. 然后,Administrator 选择 n 个非零且互不相同的整数 $\{x_l|l=1,2,\cdots,n\}$,计算出 n 个私密份额 $\{(x_l,f(x_l))|l=1,2,\cdots,n\}$. 接着,通过安全量子信道,Administrator 将这 n 个份额分别分发给 G_k 中 n 个成员 $P_1,P_2,\cdots,P_n$,其中每个成员 $P_l(l=1,2,\cdots,n)$ 拥有一个自己的私密份额 $(x_l,f(x_l))$. 另外,他将群体身份认证码 a_0 传送给 Alice.

步骤 2 Administrator 根据 G_k 的群组号 k 制备一个 d 维三粒子纠缠态:$|\psi_0\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}e^{2\pi i\frac{k}{d}j}|j\rangle_G|j\rangle_A|j\rangle_B$. 该纠缠态的制备方法与文献[14,15]中的高维量子纠缠态的制备方法类似. Administrator 首先制备一个 d 维初始态 $|k\rangle_G$,然后对该初始态执行量子傅里叶变换 U_{QFT},接着,制备两个零态 $|0\rangle_A$ 和 $|0\rangle_B$,并以 $|*\rangle_G$ 作为控制粒子,$|0\rangle_A$ 和 $|0\rangle_B$ 作为目标粒子分别执行两次 d 维 CNOT 门变换可制备出三粒子纠缠态 $|\psi\rangle_0$.

进一步,Administrator 将纠缠态 $|\psi\rangle_0$ 中的 $|j\rangle_G$ 作为投票粒子分发给 G_k,将 $|j\rangle_A$ 作为认证粒子分发给 Alice,将 $|j\rangle_B$ 作为计票粒子分发给 Bob.

2.2 群体投票阶段

步骤 3 假设 G_k 的所有成员 $P_1,P_2,\cdots,P_n$ 中授权参与投票的人数为 t 人,约定为 $P_1,P_2,\cdots,P_t$,他们中的每个人 $P_r(r=1,2,\cdots,t)$ 取出自己的私密份额 $(x_r,f(x_r))$,计算私密认证码:

$$s_r=f(x_r)\prod_{1\leqslant v\leqslant t,v\neq r}\frac{x_v}{x_v-x_r}\mathrm{mod}\ d \tag{1}$$

步骤 4 假设首先参与投票的成员是 P_1,则 G_k 将投票粒子 $|j\rangle_G$ 传给 P_1. 当 P_1 确认收到粒子 $|j\rangle_G$ 之后,他根据自己的私密认证码 s_1 生成一个 d 维 Pauli 算子 $U_{s_1,0}$,该算子 $U_{s_1,0}$ 定义如下[16]:

$$U_{s_1,0}=\sum_{j=0}^{d-1}\gamma^{0\cdot j}\,|\,j+s_1\rangle\langle j\,|\,,\gamma=\mathrm{e}^{2\pi i/d}\tag{2}$$

P_1 对粒子$|j\rangle_G$执行 Pauli 算子 $U_{s_1,0}$,得到粒子$|j+s_1\rangle_G$.

步骤 5　P_1 根据自己的表决意向制备一个辅助粒子$|p_1\rangle_1$:

$$|p_1\rangle_1=\begin{cases}|1\rangle\text{赞成}\\|0\rangle\text{反对}\end{cases}\tag{3}$$

P_1 对$|j+s_1\rangle_G\,|p_1\rangle_1$执行 Oracle 算子 O_1,其定义为:

$$O_1\,|j+s_1\rangle_G\,|p_1\rangle_1=\mathrm{e}^{2\pi i\frac{p_1}{d}j}|j+s_1\rangle_G\,|p_1\rangle_1\tag{4}$$

假设 P_1 的表决意向为赞成,那么他制备的辅助粒子为$|1\rangle_1$. 当 P_1 执行完 $U_{s_1,0}$和 O_1 算子之后,投票系统中的三粒子纠缠态$|\psi_0\rangle$演变为$|\psi_1\rangle$:

$$\begin{aligned}|\,\psi_1\rangle&=O_1\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{2\pi i\frac{k}{d}j}U_{s_1,0}\,\Big|j\Big\rangle_G\,|\,j\rangle_A\,|\,j\rangle_B\\&=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{2\pi i\frac{k+1}{d}j}\,\Big|j+s_1\Big\rangle_G\,|\,j\rangle_A\,|\,j\rangle_B\,|\,1\rangle_1\end{aligned}\tag{5}$$

步骤 6　当 P_1 执行完投票表决后,他将投票粒子$|*\rangle_G$传给 P_2,P_2 做与 P_1 类似的操作. P_2 首先对接收到的投票粒子$|*\rangle_G$执行 Pauli 算子 $U_{s_2,0}$,然后制备一个辅助粒子$|p_2\rangle_2$,接着对$|*\rangle_G\,|p_2\rangle_2$执行 Oracle 算子 O_2,将变换后投票粒子$|*\rangle_G$传给 P_3. 授权参与投票人 $P_3,P_4,\cdots,P_t$ 都做与 P_1,P_2 类似的操作. 当所有投票人完成投票表决后,投票系统中的三粒子纠缠态$|\psi_1\rangle$演变为$|\psi_2\rangle$:

$$\begin{aligned}|\,\psi_2\rangle&=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{2\pi i\frac{k+\sum_{r=1}^{t}p_r}{d}j}\,\Big|j+\sum_{r=1}^{t}s_r\Big\rangle_G\\&\otimes|\,j\rangle_A\,\Big|j\Big\rangle_B\,|\,p_1\rangle_1\,|\,p_2\rangle_2\cdots|\,p_t\rangle_t\end{aligned}\tag{6}$$

最后,G_k 通过安全量子信道将变换后的投票粒子$|*\rangle_G$传送给监票人 Alice.

2.3　群体身份认证阶段

步骤 7　当监票人 Alice 确认收到 G_k 传来的投票粒子$|*\rangle_G$后,他根据群组身份认证码 a_0 生成一个 d 维 Pauli 算子 $U_{a_0,0}$,并对自己的粒子$|j\rangle_A$执行 $U_{a_0,0}$酉变换,此时三粒子纠缠态$|\psi_2\rangle$演变为$|\psi_3\rangle$:

$$\begin{aligned}|\,\psi_3\rangle&=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{2\pi i\frac{k+\sum_{r=1}^{t}p_r}{d}j}\,|\,j+\sum_{r=1}^{t}s_r\rangle_G\\&\otimes|\,j+a_0\rangle_A\,|\,j\rangle_B\,|\,p_1\rangle_1\,|\,p_2\rangle_2\cdots|\,p_t\rangle_t\end{aligned}\tag{7}$$

步骤 8　监票人 Alice 以收到的粒子$|*\rangle_G$作为控制粒子,以粒子$|*\rangle_A$作为目标粒子执行一个 d 维 U_{CNOT}变换,此时三粒子纠缠态$|\psi_3\rangle$演变为$|\psi_4\rangle$:

$$\begin{aligned}|\,\psi_4\rangle&=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{2\pi i\frac{k+\sum_{r=1}^{t}p_r}{d}j}\Big(U_{CNOT}\Big(|\,j+\sum_{r=1}^{t}s_r\rangle_G,|\,j+a_0\rangle_A\Big)\Big)\\&\otimes|\,j\rangle_B\,|\,p_1\rangle_1\,|\,p_2\rangle_2\cdots|\,p_t\rangle_t\end{aligned}\tag{8}$$

根据 Shamir(t,n)门限的思想和拉格朗日插值定理,存在等式 $a_0=\sum_{r=1}^{t}s_r \bmod d\,(t\leqslant n)$,因此经过 U_{CNOT}变换之后的量子态$|\psi_4\rangle$也可表示为:

$$\begin{aligned}|\,\psi_4\rangle&=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{2\pi i\frac{k+\sum_{r=1}^{t}p_r}{d}j}\,|\,j+\sum_{r=1}^{t}s_r\rangle_G\,|\,0\rangle_A\,|\,j\rangle_B\\&\otimes|\,p_1\rangle_1\,|\,p_2\rangle_2\cdots|\,p_t\rangle_t\end{aligned}\tag{9}$$

步骤 9　Alice 使用计算基 $B_1=\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$对自己的粒子$|0\rangle_A$进行测量. 如果测量结果为$|0\rangle$,那么授权参与投票人的身份通过认证,否则,认证失败. 如果认证通过,监票人 Alice 将第一个粒子$|*\rangle_G$通过安全信道传输给 Bob,并通知 Bob 进行计票.

2.4　计票阶段

步骤 10　计票人 Bob 使用自己的粒子$|j\rangle_B$作为控制粒子,接收到的粒子$|*\rangle_G$作为目标粒子执行一个 d 维 U_{CNOT}变换,然后 Bob 对自己的粒子$|*\rangle_B$执行逆量子傅里叶变换 $U_{QFT^{-1}}$,得到:

$$U_{QFT^{-1}}\Big(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{2\pi i\frac{k+\sum_{r=1}^{t}p_r}{d}j}\,|\,j\rangle_B\Big)=|\,k+\sum_{r=1}^{t}p_r\rangle_B\tag{10}$$

上述等式(10)的证明可参考文献[15]中逆量子傅里叶变换的证明过程.

进一步,Bob 使用计算基 $B_1=\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$对自己的粒子$|*\rangle_B$进行测量,可得测量结果$|k+\sum_{r=1}^{t}p_r\rangle_B$. 由于 Bob 知道群组号 k,根据$|k+\sum_{r=1}^{t}p_r\rangle_B$,他能计算出投票表决赞成人数 $\sum_{r=1}^{t}p_r$. 如果票数未达到通过数,Bob 宣布方案未通过,否则予以通过.

提出方案中的初始纠缠态$|\psi_0\rangle$由 Administrator 制备,并将其中的三个粒子分别分发给 G_k、Alice 和 Bob,此三粒子纠缠态在上述四个阶段中的演变过程量子线路图如图 2 所示.

在图 2 中,G_k 中的授权成员对粒子$|j\rangle_G$执行了一系列投票表决酉操作,Alice 对粒子$|j\rangle_A$执行酉变换和计算基测量,执行群体身份认证功能,Bob 对粒子$|j\rangle_B$执行逆量子傅里叶变换和计算基测量,并对测量结果进行求和统计.

3　安全性分析

本节将从以下两个方面对提出方案的安全性进行分析:一方面,提出的方案是否具有投票模型的安全属性;另一方面,提出的方案能否抵抗常见的量子攻击.

3.1　投票方案的安全属性

本文所提出的投票方案具有以下安全属性:

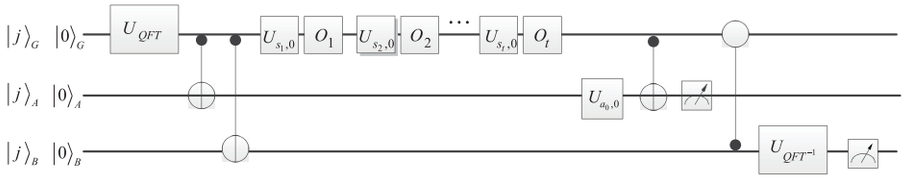

图2 投票方案量子线路图

(1)合法性:Administrator 为 G_k 中每位成员随机分配私密认证码,该认证码不仅可以对投票表决的有效性进行认证,还可以对参与投票者的身份进行认证,保证投票表决的合法性.

(2)公平性:只有监票人 Alice 群体身份认证通过之后,计票员 Bob 才能对表决票进行统计. Alice 监票人角色的设立对计票员 Bob 的权利产生了制约,保障了整个投票过程的公平性.

(3)隐私及匿名性:投票表决信息隐藏在三粒子纠缠态的全局相位中,保证了投票表决信息的隐私性. 每个投票人 P_r 仅知道自己的私密认证码,无法得知他人的身份信息与真实表决信息的联系,保证了投票表决信息的匿名性.

(4)可检测性:在群体身份认证阶段,Alice 对方案的有效性和投票人身份进行了认证. 根据量子塌缩原理,在认证和计票阶段任何企图伪造破坏投票人表决结果的行为都可被检测到.

(5)不可重复性:在投票表决过程中,由于每个投票人根据自己的表决意愿仅仅生成一个辅助粒子,因此如果某个投票人重复投票则需生成更多的辅助粒子,多余辅助粒子在纠缠态中能够被轻易发现,无法重复投票.

3.2 量子攻击安全分析

本节分析提出方案的安全性,论证该方案能否抵抗截获-测量-重发攻击、纠缠-测量攻击和伪造攻击三种常见的量子攻击.

(1)截获-测量-重发攻击

假设存在一个恶意攻击者 Eve,她首先控制量子信道,截获了从 Administrator 到 Group、Alice 和 Bob 信道传输中的任何一个粒子. 然后 Eve 选取计算基 $Z(Z=\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\})$ 对截获的粒子进行测量,她将以 $1/d$ 的概率得到 $|u\rangle(u\in\{0,1,\cdots,d-1\})$. 进一步,她制备一个与截获粒子相同的新粒子,并将此粒子发送给信道传输的接收者. 由于投票表决信息隐藏于三粒子纠缠态的全局相位中,$|u\rangle$ 中并不包含投票人的任何隐私信息. 因此,Eve 在截获-测量-重发攻击中不能获得任何有价值的信息.

(2)纠缠-测量攻击

假设 Eve 截获了投票表决完成之后的粒子 $|j+\sum_{r=1}^{t}s_r\rangle_G$,然后她制备一个辅助粒子 $|e\rangle_a(e\in\{0,1\cdots,d-1\})$,并通过 d 维酉变换 U_{CNOT} 将辅助粒子和截获粒子进行纠缠,其中 $|j+\sum_{r=1}^{t}s_r\rangle_G$ 为控制粒子,$|e\rangle_a$ 为目标粒子. 量子系统态 $|\psi_3\rangle$ 演变为:

$$\begin{aligned}&(U_{CNOT}(|j+\sum_{r=1}^{t}s_r\rangle_G,|e\rangle_a))|\psi_3\rangle\\&=|\psi_3\rangle|e\oplus j+\sum_{r=1}^{t}s_r\rangle_a\end{aligned}\tag{11}$$

假设 Eve 对辅助粒子进行测量,得到 $|e\oplus j+\sum_{r=1}^{t}s_r\rangle$ 的概率为 $1/d$. 其中并不包含投票人的表决信息,Eve 的纠缠-测量攻击也失败了.

(3)伪造攻击

假设攻击者 Eve 假冒授权成员,伪造一个私密认证码 q 参与投票,并生成 Pauli 算子 $U_{q,0}$ 作用到投票粒子 $|j+\sum_{r=1}^{t}s_r\rangle_G$ 上,当投票表决完成之后,该粒子演变为 $|j+\sum_{r=1}^{t}s_r+q\rangle_G$. 由于 $\sum_{r=1}^{t}s_r+q\neq a_0$,所以,当 Alice 使用收到的 $|j+\sum_{r=1}^{t}s_r+q\rangle_G$ 作为控制粒子,自己的 $|j+a_0\rangle_A$ 作为目标粒子执行 U_{CNOT} 变换,自己的粒子演变为:

$$|(j+a_0)\oplus(j+\sum_{r=1}^{t}s_r+q)\rangle_A\neq|0\rangle_A\tag{12}$$

监票人 Alice 对粒子 $|*\rangle_A$ 进行测量,测量结果不为 $|0\rangle_A$,认证不成功,Eve 的伪造攻击又失败了.

4 性能分析与比较

本节将提出的方案和三个类似的量子投票方案[8,9,12]从空间维度、量子比特制备数、量子比特传输数和量子比特效率四个方面进行分析和比较. 为了比较的方便,对于所有方案,我们不考虑经典密钥、经典身份信息、经典份额制备和传输所带来的开销. 比较结果如表 1 所示.

表 1　四个量子投票方案的比较

性能	方案[8]	方案[9]	方案[12]	提出的方案
空间维度	2	2	2	d
量子比特制备数	$4q$	$3n+2m+4w$	$6n$	$(t+3)\lceil\log_2 d\rceil$
量子比特传输数	$3q$	$6n+2m+4w$	$4n$	$(t+4)\lceil\log_2 d\rceil$
量子比特效率	$\frac{n}{4q}$	$\frac{2m}{3n+2m+4w}$	$\frac{n}{6n}$	$\frac{t}{t+3}$

在表 1 中,量子比特效率定义为 $\eta=c/p$,其中 c 代表传输的经典比特(信息位),p 代表制备的量子比特总数,q 与 n 存在关系 $q>n$,m 为制备的单粒子个数,w 为插入的诱骗粒子个数. 从表 1 可看出,仅仅提出的方案处在 d 维 Hilbert 空间,其他方案都处于 2 维 Hilbert 空间. 在 $t\leqslant n$ 条件下,随着 t 和 n 取值的增大,提出方案的量子比特效率是最高的.

5　仿真实验验证

本节利用 IBM 量子云平台实验主要验证投票表决计票过程的正确性,仿真实验如图 3 所示. 由于 IBM 量子云平台还处于测试阶段,有些酉算子在平台上难以模拟验证,例如高维的 Oracle 算子 O_1,因此本次仿真实验将三粒子纠缠态设定在 2 维希尔伯特空间,且只考虑一个投票人生成一个辅助粒子进行投票表决的情况,且省略了群组身份认证过程.

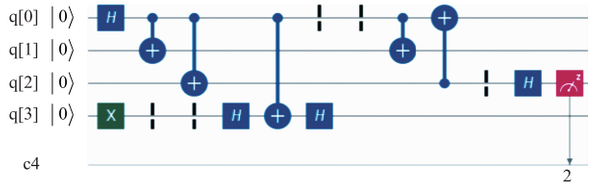

图3　量子投票仿真实验图

在图 3 中,量子寄存器 $q[0]$、$q[1]$ 和 $q[2]$ 分别存放粒子 $|*\rangle_C$、$|*\rangle_A$ 和 $|*\rangle_B$,$q[3]$ 存放投票人 P_1 制备的辅助粒子 $|p_1\rangle_1$,初始设置为赞成,即 $|1\rangle$ 态. 在 2 维 Hilbert 空间下,量子傅里叶变换 U_{QFT} 和逆量子傅里叶算子 $U_{QFT^{-1}}$ 使用 H 门模拟. 根据文献[17],Oracle 算子 O_1 由两个 H 门和一个 CNOT 门组合而成. 一个 H 门和两个 CNOT 门制备出一个 2 维三粒子纠缠态. 用 ibmqx4 作为量子云平台后端服务器,运行 1024 shots 之后,实验结果如图 4 所示.

从图 4 中可以看出,$q[2]$ 中存放的是计票人 Bob 的粒子,它经过逆傅里叶变换 $U_{QFT^{-1}}$ 之后,测量结果为 $|0\rangle$ 的概率为 3.32%,测量结果为 $|1\rangle$ 的概率为 96.68%,接近理论计算的结果. 由此得知,辅助粒子经过 Oracle 算子后将投票信息在纠缠态相位中实现了求和运算.

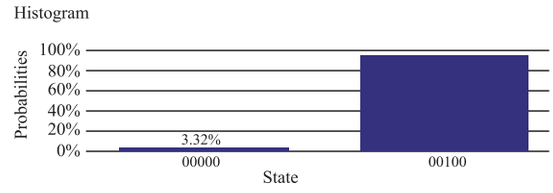

图4　量子投票仿真实验结果图

6　结束语

本文依据 d 维三粒子纠缠态的特征,提出了一种群体投票表决方案,突破了传统的 2 维度和 3 维度 Hilbert 空间的局限性,方案具有较高的普适性和实用性. 本方案能对群组中授权投票人的身份进行群体认证,满足投票方案的安全属性,且能抵抗截获-测量-重发、纠缠测量和伪造攻击三种常见的量子攻击. 该方案的正确性不仅通过理论得以证实,而且在 IBM 量子云平台上模拟验证. 不足之处在于 IBM 量子云平台还处于初级调试阶段,高维的 Oracle 算子 O_1 难以在该平台上模拟验证,只验证了 Hilbert 空间为 2 维的情况.

参考文献

[1] Chaum D L. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Commun ACM, 1981, 24(2): 84 – 90.

[2] Chaum D L. Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA[J]. Advance Cryptology-Eurocrypt, 1988, 88(2): 177 – 182.

[3] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[4] Schnorr C P. Efficient identification and signatures for smart cards (abstract)[A]. Workshop on the Theory & Application of Cryptographic Techniques[C]. Berlin, Heidelberg: Springer, 1989. 239 – 252.

[5] Vaccaro J A, Spring J, Chefles A. Quantum protocols for anonymous voting and surveying[J]. Physical Review A, 2007, 75(1): 012333.

[6] Li Y, Zeng G. Quantum anonymous voting systems based on entangled state[J]. Optical Review, 2008, 15(5): 219

–223.
[7] Horoshko D, Kilin S. Quantum anonymous voting with anonymity check[J]. Physics Letters A, 2011, 375(8): 1172–1175.
[8] Cao H J, Ding L Y, Yu Y F, et al. An electronic voting scheme achieved by using quantum proxy signature[J]. International Journal of Theoretical Physics, 2016, 55(9): 4081–4088.
[9] Naseri M, Gong L H, Houshmand M, et al. An anonymous surveying protocol via Greenberger-Horne-Zeilinger states [J]. International Journal of Theoretical Physics, 2016, 55(10): 4436–4444.
[10] Wang Q L, Yu C H, Gao F, et al. Self-tallying quantum anonymous voting [J]. Physical Review A, 2016, 94(2): 022333.
[11] 刘小华, 温晓军, 范新灿, 等. 一种基于四粒子 GHZ 态的安全量子投票协议[J]. 量子电子学报, 2017, 06: 83–88.
[12] Zhang J L, Xie S C, Zhang J Z. An elaborate secure quantum voting scheme[J]. International Journal of Theoretical Physics, 2017, 56: 3019–3028.
[13] Shamir A. How to share a secret[J]. Commun ACM, 1979, 22(11): 612–613.
[14] Song X L, Liu Y B, Deng H Y, et al. (t, n) Threshold d-level quantum secret sharing [J]. Scientific Reports, 2017, 7(1): 6366.
[15] Shi R H, Mu Y, Zhong H, et al. Secure multiparty quantum computation for summation and multiplication[J]. Scientific Reports, 2016, 6: 19655.
[16] Thas K. The geometry of generalized Pauli operators of N-qudit Hilbert space, and an application to MUBs [A]. IEEE International Conference on Systems, Man, and Cybernetic[C]. IEEE, 2009. 3816–3822.
[17] Majumder A, Mohapatra S, Kumar A. Experimental realization of secure multiparty quantum summation using five-qubit IBM quantum computer on cloud[J/OL]. https://arxiv.org/abs/1707.07460, 2017.

作者简介

宋秀丽(通讯作者) 女, 1972 年生. 博士, 重庆邮电大学副教授, 硕士生导师, 计算机学会会员, IEEE 会员. 研究领域包括量子密码学、量子保密通信、云计算安全和车联网安全.
E-mail: songxl@cqupt.edu.cn

曹耘凡 男, 1991 年生. 硕士研究生, 主要研究方向为量子密码、量子认证.
E-mail: 258334476@qq.com

杨 帅 男, 1995 生. 硕士研究生, 主要研究方向为量子安全多方计算、量子安全多方求和.
E-mail: 865001500@qq.com