DOI: 10.16452/j.cnki.sdkjzk.2022.01.010 文章编号:1672-3767(2022)01-0092-06

基于 d 维纠缠态的安全量子投票协议

陈凯伦,梁向前
(山东科技大学 数学与系统科学学院,山东 青岛 266590)

摘 要:在投票过程中如何保护投票人的隐私是当前量子投票协议设计中的一个重要研究课题。本研究通过对 d 维量子纠缠态进行分析,利用其相位可以隐藏秘密信息的性质,设计一个安全量子投票协议。通过对协议的分析发现,在量子信道中传递选票信息时,协议能够隐藏投票信息,满足投票人对身份信息的安全性和匿名性需求,有效保证投票人的投票信息不被窃取,实现安全匿名投票。

关键词:量子投票方案;安全性;匿名性;d 维纠缠态;量子密码学
中图分类号:TP309 **文献标志码**:A

Secure quantum voting protocol based on d-level entangled state

CHEN Kailun, LIANG Xiangqian
(College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao, Shandong 266590, China)

Abstract: How to protect the privacy of voters in the voting process is an important research topic in the current design of quantum voting protocols. In this paper, a secure quantum voting protocol is designed by analyzing the d-level quantum entangled states and by using its property that the phase can hide the secret information. Through the analysis of the protocol, it is found that the protocol is able to hide the voting information when passing ballot information in the quantum channel, which can meet voters' need for security and anonymity of identity information. Moreover, the proposed protocols can effectively ensure that the voting information of voters is not stolen and achieve the secure and anonymous voting.

Key words: quantum voting protocol; security; anonymity; d-level entangled state; Quantum Cryptography

在设计匿名投票方案的过程中,如何保证投票人投票信息的匿名性是一个关键问题。一个安全的电子投票协议,不仅能够抵御多种方式的攻击,还应该保护投票人信息不被泄露。Chaum[1]在 1981 年首次利用经典密码体制,提出了保护投票人身份的匿名投票协议。随后,诸多学者在投票协议的设计方面进行研究,提出了许多电子投票协议。随着量子计算机的发展,Shor[2]在 1999 年提出了著名的 Shor 算法,在量子计算机帮助下,这一算法使得大整数分解问题变得不再困难,这表明基于计算复杂性的经典密码协议在量子时代易于被攻破。因此,设计能够抵抗量子攻击的安全投票协议具有重要意义。

一个安全的投票方案需要满足以下安全要求[3]:

1) 隐私性。除投票人之外,其他人无法通过投票信息获取投票人的身份信息。

2) 不可重用性。每一张选票只能由投票人使用一次。

收稿日期:2021-04-27
基金项目:山东省自然科学基金项目(ZR2019MF023)
作者简介:陈凯伦(1995—),男,山东潍坊人,硕士研究生,主要从事信息安全理论与应用研究.
E-mail:1293822641@qq.com
梁向前(1969—),男,河南伊川人,副教授,博士,主要从事信息安全理论与应用研究,本文通信作者.
E-mail:xiangqian.liang@163.com

3) 可验证性。每一位投票人的选票是否被正确统计,可由投票人本人核实。

4) 合法性。只有合法的投票人才能投票。

5) 公平性。在投票过程结束之前,没有人能够预先获取投票结果。

2002 年,Christandl 等[4]对隐藏发送人和接收人身份的问题进行研究,提出一种用于经典比特匿名传输和接收的量子协议,开启了在量子信道中传递秘密信息的研究。2007 年,Vaccaro 等[5]提出一个只有两个选项的旅行投票协议,该协议将纠缠态的各个粒子分发到不同的站点并且利用任一站点的不可访问性来保证投票的匿名性和隐私性。之后,Bonanome 等[6]和 Hillery 等[7]对该协议进行改进,修补了可能存在的安全漏洞。2008 年,Okamoto 等[8]基于共轭编码对量子态的使用方式做了改进,设计了更高效的协议。同年,Li 和 Zeng[9]提出了新的量子投票方案,实现在众多候选人中投票。随后,基于不同的量子态,众多专家学者在这一领域做了大量的工作,并提出许多量子投票协议。Jiang 和 He 等[10]利用基于连续变量的量子纠缠态的性质,提出一种安全的量子投票协议,该协议可以保护每个投票人的投票隐私。通过使用多维量子纠缠态、保密的选票和索引号,Wang 等[11]提出一种量子匿名自统计投票协议来保护投票人的隐私。2017 年,Zhang 等[12]设计了一个基于量子代理盲签名的投票协议,对于量子匿名安全投票协议的设计具有启发意义,不少研究人员受到启发,相继提出一些新的、不同类型的量子投票协议[13-24]。

通过对以往方案的总结分析,受到 Zhang 等[25]提出的多方量子秘密共享协议的启发,利用仅通过联合测量才可以从 d 维纠缠态中提取相位信息的性质,本研究设计特殊的选票结构,提出一种基于 d 维纠缠态的安全量子投票协议,在投票过程中,投票人获得选票中心分发的一张可分离的选票,可以在三个不同的地点投票,由计票人在公告栏上宣布投票结果。通过分析,方案满足投票人对隐私保护的安全需求,满足投票方案的安全要求。

1 预备知识

本研究需要应用以下基础理论知识[2,5]:

d 维纠缠态:

$$|\varphi_0\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle|j\rangle|j\rangle|j\rangle。\tag{1}$$

设 x 为整数,对应的相位旋转局部算子 U_x 操作可表示为[28]:

$$U_x=\sum_{j=0}^{d-1}\mathrm{e}^{i\theta j\cdot x}|j\rangle\langle j|,\tag{2}$$

其中 $\theta=\frac{2\pi}{d}$。

对状态为 $|\varphi_0\rangle$ 的任何一个粒子执行 U_x 操作后,状态变为:

$$|\varphi_x\rangle=U_x|\varphi_0\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{i\theta j\cdot x}|j\rangle|j\rangle|j\rangle|j\rangle。\tag{3}$$

对 $|\varphi_x\rangle$ 中任何一个粒子单独测量都不能得到存储在粒子态中的相位信息,当且仅当对量子态 $|\varphi_x\rangle$ 中所有粒子进行联合测量才能得到相位信息[26]。给定可测量算子 $\hat{\mathbf{T}}$,其定义为:

$$\hat{\mathbf{T}}=\sum_{t=0}^{d-1}t|T_t\rangle\langle T_t|,\tag{4}$$

这里,$|T_t\rangle=\frac{1}{\sqrt{d}}\sum_{m=0}^{d-1}\mathrm{e}^{i\theta m\cdot t}|m\rangle|m\rangle|m\rangle|m\rangle$,满足 $\langle T_s|T_t\rangle=\delta_{st}$。该理论最早由 Vaccaro 提出并应用到量子安全协议的设计中[5,9]。

本研究使用 $\hat{\mathbf{T}}$ 算子来提取在 $|\varphi_x\rangle$ 中编码的信息,并且当 $x=0,\cdots,d-1$ 时,式(3)所表示的量子态是可观测量算子 $\hat{\mathbf{T}}$ 的全部特征态,$|T_t\rangle\langle T_t|$ 是对应算子 $\hat{\mathbf{T}}$ 的本征值 t 的投影算子。

2 量子安全匿名投票协议

2.1 协议中的符号表示

为了描述方便,本研究用 MC 表示投票管理中心(manage center),用 Bob_1、Bob_2 和 Bob_3 表示选票收集

站,Charlie 表示计票人,Alice 表示投票人,Q_D 代表纠缠态的第四粒子组成的序列,B_N 为纠缠态的前 3 个粒子序列组成的未进行投票的选票,B_{1N*}、B_{2N*} 和 B_{3N*} 分别代表拆分开之后进行投票后的选票,B_{1E}、B_{2E} 和 B_{3E} 分别为选票收集站 Bob_1、Bob_2 和 Bob_3 进行加解密操作之后的选票。

2.2 投票过程

量子投票过程如图 1 所示,具体分为 4 个阶段。

2.2.1 初始阶段

1) 投票管理中心(MC)验证投票人 Alice 的身份并确认 Alice 的合法性。若 Alice 身份合法,MC 为 Alice 随机生成唯一的投票 ID 号,记为序列 $P_{MC}\in\{0,1\}^{5m}$,这里 m 表示 ID 号的位数。否则,Alice 被禁止投票。

2) Bob_1、Bob_2 和 Bob_3 分别与合法的投票人 Alice 通过 QKD 协议共享会话密钥 K_{B_1A}、K_{B_2A} 和 $K_{B_3A}\in\{0,1\}^N$,这里 $N=n+m$,n 表示投票信息长度。

3) Bob_1、Bob_2 和 Bob_3 分别与 Charlie 共享会话密钥 K_{B_1C}、K_{B_2C} 和 $K_{B_3C}\in\{0,1\}^N$。

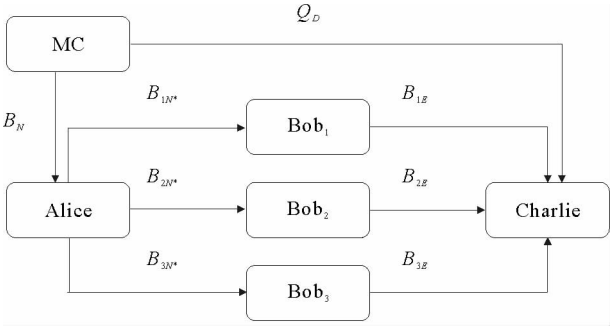

图 1 量子投票过程图

Fig. 1 Diagram of the quantum voting process

2.2.2 选票分配阶段

1) MC 准备 N 个 d 维纠缠态 $|\varphi_0\rangle_i=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_{A_i}|j\rangle_{B_i}|j\rangle_{C_i}|j\rangle_{D_i}$,$i=1,2,\cdots,N$。本研究利用 $d=2^5$ 维纠缠态来设计协议。MC 将每个纠缠态的第一、二、三、四粒子顺序取出分别构成量子序列:

$$\begin{aligned}Q_A&=\{q_A^i,i=1,2,\cdots,N\},\\Q_B&=\{q_B^i,i=1,2,\cdots,N\},\\Q_C&=\{q_C^i,i=1,2,\cdots,N\},\\Q_D&=\{q_D^i,i=1,2,\cdots,N\}。\end{aligned}\tag{5}$$

2) MC 将前三个量子序列 $\{Q_A,Q_B,Q_C\}$ 打包为一个序列 $B_N=\{Q_A,Q_B,Q_C\}$ 发送给 Alice,MC 保留序列 Q_D。这里要说明的是,发送的序列中需要插入诱饵粒子来确保传输的安全性,具体操作方法可参考文献[14]。如果检测双方通过窃听检测,证明无窃听行为发生,协议可以继续,否则需要重新执行协议。

2.2.3 投票阶段

1) Charlie 建立一个公告栏。

2) Alice 通过计算收到的量子数来确认选票序列 B_N 的完整性。Alice 根据自己的投票内容生成二进制投票信息 $M=\{m_1,m_2,\cdots,m_{5n}\}\in\{0,1\}^{5n}$,然后合并序列 M 和 P_{MC},得到序列 $M^*=M\|P_{MC}=\{m_1,m_2,\cdots,m_{5n},\cdots,m_{5(n+m)}\}$,之后 Alice 使用算子 U_x 将信息 M^* 编码到选票 B_N 上。为了方便,下文中记 $n+m=N$,其具体编码规则如下:

$$X_i=2^4\times m_{5i-4}+2^3\times m_{5i-3}+2^2\times m_{5i-2}+2^1\times m_{5i-1}+2^0\times m_{5i},i=1,2,\cdots,N。\tag{6}$$

Alice 根据上式计算 X_i,随机选择 x_A^i、x_B^i、x_C^i,要求选取的数值符合规则 $x_A^i+x_B^i+x_C^i\equiv X_i \bmod d$。对于每个对应的 X_i,Alice 使用 $U_{x_A^i}$、$U_{x_B^i}$ 和 $U_{x_C^i}$ 分别作用于三个不同的粒子 $\{q_A^i,q_B^i,q_C^i\}(i=1,2,\cdots,N)$ 上,通过操作后得到的选票记为 $B_N{}^*=\{Q_A{}^*,Q_B{}^*,Q_C{}^*\}$,其包含投票信息和投票 ID 号。

3) Alice 将选票 $B_N{}^*$ 分为三部分,每个部分可以分别表示如下:

$$\begin{aligned}B_{1N}&=\{q_A^i{}^*,i=1,2,\cdots,N\},\\B_{2N}&=\{q_B^i{}^*,i=1,2,\cdots,N\},\\B_{3N}&=\{q_C^i{}^*,i=1,2,\cdots,N\}。\end{aligned}\tag{7}$$

4) Alice 用 K_{B_1A}、K_{B_2A} 和 $K_{B_3A}\in\{0,1\}^N$ 分别加密选票 B_{1N}、B_{2N} 和 B_{3N},得到加密后的选票,用量子序列的形式分别描述为 $B_{1N}{}^*=\{E_{K_{B1A}}(B_{1N})\}$、$B_{2N}{}^*=\{E_{K_{B2A}}(B_{2N})\}$ 和 $B_{3N}{}^*=\{E_{K_{B3A}}(B_{3N})\}$。加密

方法为:如果 $K_{B_jA}^i=1(j=1,2,3)$,选择 $a^i\equiv1\bmod d$;如果 $K_{B_jA}^i=0(j=1,2,3)$,选择 $a^i\equiv(d-1)\bmod d$。根据每个 $K_{B_jA}^i$,Alice 将算子 U_{a^i} 作用在粒子 $\{q^{i*}\}$ 上来获得 $\{q^{i*}_e\}$,$i=1,2,\cdots,N$。

5) Alice 通过安全信道分别将 $B_{1N}{}^*$、$B_{2N}{}^*$ 和 $B_{3N}{}^*$ 发送给 Bob_1、Bob_2 和 Bob_3。

2.2.4 计票阶段

1) Bob_1、Bob_2 和 Bob_3 接收量子序列 $B_{1N}{}^*$、$B_{2N}{}^*$ 和 $B_{3N}{}^*$。Bob_1 用 K_{B_1A} 解密选票 $B_{1N}{}^*$ 获得 $B_{1N}=\{q_A^{i}{}^*,i=1,2,\cdots,N\}$;同样 Bob_2 用 K_{B_2A} 解密选票 $B_{2N}{}^*$ 获得 $B_{2N}=\{q_B^{i}{}^*,i=1,2,\cdots,N\}$;$\mathrm{Bob}_3$ 用 K_{B_3A} 解密选票 $B_{3N}{}^*$ 获得 $B_{3N}=\{q_C^{i}{}^*,i=1,2,\cdots,N\}$。解密规则为:如果 $K_{B_jA}^i=1$,选择 $a^i\equiv(d-1)\bmod d$;如果 $K_{B_jA}^i=0$,选择 $a^i\equiv1\bmod d$。对于每个 $K_{B_jA}^i$,使用 U_{a^i} 算子作用于 $\{q^{i*}_e\}$,就会获得 $\{q^{i*}\}$,$j=1,2,3$;$i=1,2,\cdots,N$。接下来 Bob_1、Bob_2 和 Bob_3 分别使用与 Charlie 的通讯密钥 K_{B_1C}、K_{B_2C} 和 K_{B_3C} 加密 B_{1N}、B_{2N} 和 B_{3N},可以获得加密后的选票:

$$\begin{aligned}B_{1E}&=\{E_{K_{B1C}}(B_{1N})\},\\B_{2E}&=\{E_{K_{B2C}}(B_{2N})\},\\B_{3E}&=\{E_{K_{B3C}}(B_{3N})\}。\end{aligned}\tag{8}$$

依据加密规则:如果 $K_{B_jC}^i=1$,选择 $a^i\equiv(d-1)\bmod d$;如果 $K_{B_jC}^i=0$,选择 $a^i\equiv1\bmod d$。对于每个 $K_{B_jC}^i$,使用 U_{a^i} 算子作用于 $\{q^{i*}_e\}$,就会获得 $\{q^{i*}\}$,$j=1,2,3$;$i=1,2,\cdots,N$。

2) Bob_1、Bob_2 和 Bob_3 将量子序列 B_{1E}、B_{2E} 和 B_{3E} 无错误的发送给 Charlie。

3) Charlie 接收到量子序列之后,由 Bob_1、Bob_2 和 Bob_3 通知投票管理中心 MC,Alice 已经完成投票,并且选票已经发送给 Charlie。MC 将粒子序列 Q_D 和 P_{MC} 通过量子安全信道发送给 Charlie。

4) 在使用通信密钥 K_{B_1C}、K_{B_2C} 和 K_{B_3C} 分别解密 B_{1E}、B_{2E} 和 B_{3E} 之后,利用 MC 传输的第四个量子序列 Q_D,Charlie 可以获得完整的选票:

$$B_{N_f}=\{q_A^{i}{}^*,q_B^{i}{}^*,q_C^{i}{}^*,q_D^{i},i=1,2,\cdots,N\},\tag{8}$$

同样的解密规则为:如果 $K_{B_jC}^i=1$,选择 $a^i\equiv(d-1)\bmod d$;如果 $K_{B_jC}^i=0$,选择 $a^i\equiv1\bmod d$。对于每个 $K_{B_jC}^i$,使用算子 U_{a^i} 作用于 $\{q^{i*}_e\}$,就会获得 $\{q^{i*}\}$,$j=1,2,3$;$i=1,2,\cdots,N$。通过这种方式 Charlie 会获得如下量子态:

$$|\varphi_{x_A^k+x_B^k+x_C^k}\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{i\theta j\cdot(x_A^k+x_B^k+x_C^k)}\,|j\rangle_{A_k}|j\rangle_{B_k}|j\rangle_{C_k}|j\rangle_{D_k},k=1,2,\cdots,N。\tag{9}$$

通过测量算子 $\hat{\mathbf{T}}$ 测量后,Charlie 获得信息:

$$X_k\equiv x_A^k+x_B^k+x_C^k\bmod d\equiv\langle\varphi_{x_A^k+x_B^k+x_C^k}|\hat{\mathbf{T}}|\varphi_{x_A^k+x_B^k+x_C^k}\rangle,k=1,2,\cdots,N。\tag{10}$$

5) Charlie 通过将 X_k 转换为二进制数 m_{5k-4}、m_{5k-3}、m_{5k-2}、m_{5k-1}、m_{5k} 来获取信息 $M^{*'}$,即 Charlie 得到了 M' 和 $P_{\mathrm{MC}}{}'$。如果 $P_{\mathrm{MC}}{}'=P_{\mathrm{MC}}$,Charlie 在公告板上公布相应的投票 ID 号 P_{MC} 和投票信息 M';否则 Charlie 拒绝这次投票。

3 安全性分析

3.1 隐私性

在量子投票协议中,隐私性主要表现为:除了投票人自己,没有人可以通过投票信息获取投票人身份信息,也不能通过投票人身份信息获取投票人的投票信息。只有确保选票的安全,才能确保投票人的隐私安全。本部分分析投票过程中的安全性和隐私性,具体讨论在选票分配阶段和投票阶段泄露投票人信息的可能性。

作为一个外部窃听者 Eve,存在两种攻击方式。

一种是在选票分配阶段,Eve 伪装成合法投票人窃取选票并发送给投票人。考虑 Eve 截获了序列 B_N 中的任意粒子数 x 的情况。假设协议中使用的诱饵粒子的比例为 ξ_0。如果 $x<N=n+m$,则所有 x 粒子都在选票信息序列中而不在诱饵粒子序列中的概率为:

$$\begin{aligned}p_e&=\binom{N}{x}\Big/\binom{N+N\xi_0}{x}=\frac{N!}{(N-x)!}\,\frac{(N+N\xi_0-x)!}{(N+N\xi_0)!}=\prod_{n=N}^{N-x+1}\frac{n}{n+N\xi_0},\\p_e&\sim O\left(\left(\frac{1}{\xi_0}\right)^x\right)。\end{aligned}\tag{11}$$

如果诱饵粒子的比例 ξ_0 足够大,则概率接近“0”。此时,Eve 截获选票中有用的粒子的概率几乎为 0。在窃听检查的安全保护下,这种攻击是失败的。

另一种方法是在投票阶段截取选票,即 Eve 有可能截获 Alice 发送的粒子。在这种情况下,约化密度矩阵与未执行操作前相同:

$$\boldsymbol{\rho}^{A_i}=\mathrm{tr}_{B_iC_iD_i}(\boldsymbol{\rho}^{A_iB_iC_iD_i})=\frac{1}{d}\sum_{n=0}^{d-1}|j\rangle_{A_iA_i}\langle j|。\tag{12}$$

可以知道,Eve 不能从截获的粒子上获得任何有效信息。同样的,考虑 Eve 截获两个或三个粒子的情况下,根据约化密度矩阵可以得知 Eve 依然不能获得任何有效信息。根据量子 Fourier 变换的性质,Eve 只有对纠缠态的所有粒子进行联合测量才能获得其相位信息,然而这是不可能实现的,因此 Eve 无法获得 Alice 的投票信息。

另外,考虑投票过程中其他参与者试图获得整个投票信息的情况。由于参与者可以获得部分投票信息,因此在获取全部投票信息方面具有一定的优势。但是通过对协议中参与者攻击的安全性分析,只有 MC 或 Charlie 可以同时访问所有的粒子。但对于 MC 来说,他无权参与投票阶段。同样,对 Charlie 来说,Alice 的真实身份是绝对保密的,因为他只被允许在计票阶段得知 Alice 的秘密投票 ID 号序列 P_{MC}。在此基础上,由于多个投票站的存在,Charlie 无法直接联系投票人,这不仅保证了投票人的合法性,也保护了投票人的身份信息不被泄露。因此,多个投票站可以有效防止合谋攻击。

分析结果表明,攻击者获取的信息不会威胁到投票人的隐私性。

3.2 不可重用性

在该协议中,MC 是高度可信的。在投票阶段,当 MC 接收到投票者的身份信息后,MC 负责验证投票者身份的合法性,并检查是否是第一次投票。如果是第一次投票,量子序列(量子选票)以及 ID 号被发送给投票人,否则投票人没有权利进行投票。通过这种方式,可以保证投票人没有重复投票。

3.3 可验证性

每个投票人都有专属的唯一的投票序列号 P_{MC},由 MC 分配,投票人身份信息和投票序列号 P_{MC}是一对一的对应关系。投票人完成投票后,计票员 Charlie 将在公告栏上公布唯一的 P_{MC}及其相应的投票结果 M'。每个投票人都可以查看公告板,以确定投票信息是否正确地被统计。由于每个合法投票者都有一个唯一的 P_{MC},并且选票信息中包含唯一的 P_{MC},计票人 Charlie 可以在投票和计票阶段通过比较 P_{MC}来验证每个投票者身份的有效性。

3.4 合法性

参与投票的投票人需要在初始阶段将身份信息发送给 MC 进行认证。认证合法后,MC 再给每个合法投票人生成唯一的 ID 号并向其发送可用于投票的粒子序列。若投票人不满足投票条件,那么将无法执行此投票协议。另外,投票人只有一次投票机会并且要对自己的选票负责。

3.5 公平性

每个投票人都有平等的投票机会,每一张选票都独立。在投票阶段,每个投票人可以根据自己的意愿进行投票,不能从其他投票人那里获得投票信息。在计票阶段,每一位投票人的投票信息都会得到正确的统计。根据 d 维纠缠态的性质,计票人 Charlie 只有在获得完整的量子序列时才能计算投票结果。因此,在投票过程结束之前,任何人不能获得投票结果,从而保证了投票的公平性。

4 结论

本研究提出一个量子安全投票协议,协议执行过程中,d 维纠缠态的特性可以有效保护投票人隐私信息。每个合法投票人只有一张选票,以保证投票的公平性和不可重用性。在投票阶段,投票人把选票分成三部分,拆分他们的隐私信息,使得任何单独获得部分选票的投票站都无法获得投票人的有效信息。该协议容易推广到使用多个选票收集站的场景上,可确保选票在传输过程中的安全性。经过分析,方案保证了投票人的隐私信息在投票过程中不被窃取。此外,本研究提出的保护隐私思想对量子秘密共享等领域的研究也具有一定参考价值。

参考文献:

[1]CHAUM D.The dining cryptographers problem:Unconditional sender and recipient untraceability[J].Journal of Cryptology,1988,1(1):65-75.

[2]SHOR P W.Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J].SIAM Review,1999,41(2):303-332.

[3]SCHNEIER B.Applied cryptography:protocols,algorithms,and source code in C[M]. Wiley,1995.

[4]CHRISTANDL M,WEHNER S.Quantum anonymous transmissions[C]// International Conference on the Theory and Application of Cryptology and Information Security.Berlin,Heidelberg:Springer,2005:217-235.

[5]VACCARO J A,SPRING J,CHEFLES A.Quantum protocols for anonymous voting and surveying[J].Physical Review A,2005,75(1):10064-10070.

[6]BONANOME M,BUŽEK V,HILLERY M,et al.Toward protocols for quantum-ensured privacy and secure voting[J].Physical Review A,2011,84(2):290-296.

[7]HILLERY M,ZIMAN M,BUŽEK V,et al.Towards quantum-based privacy and voting[J].Physics Letters A,2006,349(1-4):75-81.

[8]OKAMOTO T,SUZLIKI K,TOKUNAGA Y.Quantum voting scheme based on conjugate coding[J].NTT Technical Review,2008,6(1):1-8.

[9]LI Y,ZENG G.Quantum anonymous voting systems based on entangled state[J].Optical Review,2008,15(5):219-223.

[10]JIANG L,HE G,NIE D,et al.Quantum anonymous voting for continuous variables[J].Physical Review A,2012,85(4):9335-9340.

[11]WANG Q,YU C,GAO F,et al.Self-tallying quantum anonymous voting[J/OL].Physical Review A,2016,94(2).DOI:10.1103/PhyRevA.94.022333.

[12]ZHANG J L,XIE S C,ZHANG J Z.An elaborate secure quantum voting scheme[J].International Journal of Theoretical Physics,2017,56(10):3019-3028.

[13]LIU W J,WANG F,JI S,et al.Attacks and improvement of quantum sealed-bid auction with EPR pairs[J].Communications in Theoretical Physics,2014,61(6):686-690.

[14]WANG S L,ZHANG S,WANG Q,et al.Fault-tolerant quantum anonymous voting protocol[J].International Journal of Theoretical Physics,2019,58(3):1008-1016.

[15]TIAN J H,ZHANG J Z,LI Y P.A voting protocol based on the controlled quantum operation teleportation[J].International Journal of Theoretical Physics,2016,55(5):2303-2310.

[16]HOROSHKO D,KILIN S.Quantum anonymous voting with anonymity check[J].Physics Letters A,2011,375(8):1172-1175.

[17]XUE P,ZHANG X.A simple quantum voting scheme with multi-qubit entanglement[J].Scientific Reports,2017,7(1):7586.

[18]SHI R H,QIN J Q,LIU B,et al.Anonymous quantum voting protocol based on Chinese remainder theorem[J].The European Physical Journal D,2021,75(1):1-7.

[19]NIU X F,ZHANG J Z,XIE S C,et al.An improved quantum voting scheme[J].International Journal of Theoretical Physics,2018,57(10):3200-3206.

[20]WANG J,XU G B,JIANG D H.Quantum voting scheme with greenberger-horne-zeilinger states[J].International Journal of Theoretical Physics,2020,59(8):2599-2605.

[21]WANG Q,LIU J,LI Y,et al.Quantum bell states-based anonymous voting with anonymity trace[J].Quantum Information Processing,2021,20(4):1-21.

[22]LI Y R,JIANG D H,ZHANG Y H,et al.A quantum voting protocol using single-particle states[J].Quantum Information Processing,2021,20(3):1-17.

[23]LIU B X,JIANG D H,LIANG X Q,et al.A novel quantum voting scheme based on BB84-state[J/OL].International Journal of Theoretical Physics(2021).DOI:10.1007/s10773-021-04760-w.

[24]JIANG D H,WANG J,LIANG X Q,et al.Quantum voting scheme based on locally indistinguishable orthogonal product states[J].International Journal of Theoretical Physics,2020,59(12):436-444.

[25]ZHANG Z,LI Y,MAN Z.Multiparty quantum secret sharing[J/OL].Physical Review A,2005,71(4):DOI:10.1103/physreva.71.044301.

[26]JIA H Y,WEN Q Y,SONG T T,et al.Quantum protocol for millionaire problem[J].Optics Communications,2011,284(1):545-549.

(责任编辑:刘西奎)