多中心高效量子安全投票方案

张启帆[1],孙 莹[1],李艳俊[1,2*]
(1. 北京电子科技学院密码科学与技术系,北京 100070;
2. 中国电子科技集团公司第十五研究所信息产业信息安全测评中心,北京 100083)

摘 要: 投票是现代社会的一种重要的决策方式. 本文利用量子游走和半量子技术提出了多中心高效量子安全投票方案. 该方案由多个选民、多个量子中心等构成. 该方案使用半量子技术降低了设施成本,便于实现;多个量子中心分别并行计算,环形结构和星形结构相结合,减少了中心节点的通信压力,投票、计票更加高效,适用于大量人数投票的场景;量子中心之间汇总计票时,初始量子资源使用两粒子乘积态,制备简单且仅需进行单粒子测量,操作方便,降低了计票难度. 该方案可有效检测和抵抗多种攻击,保证安全性.

关键词: 量子投票;多中心并行计算;量子游走;半量子密钥分发;d维量子系统
基金项目: 北京市自然科学基金(No.4234084)
中图分类号: TP309;O413 **文献标识码:** A **文章编号:** 0372-2112(2025)06-1996-11
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240895

Multi-Center Efficient Quantum Secure Voting Scheme

ZHANG Qi-fan[1], SUN Ying[1], LI Yan-jun[1,2*]
(1. *Department of Cryptographic Science and Technology, Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*;
2. *Information Industry Information Security Evaluation Center, The* 15*th Research Institute of China Electronics Technology Group Corporation, Beijing* 100083, *China*)

Abstract: Voting is an important decision-making method in modern society. This paper propose an efficient multi-centre quantum-secure voting scheme using quantum walk and semi-quantum techniques. This scheme consists of multiple voters, multiple quantum centres, etc. This scheme uses semi-quantum techniques to reduce the equipment cost and facilitate the implementation; Multiple quantum centers are computed in parallel, and the combination of ring and star structures reduces the communication pressure on the central nodes, making voting and vote counting more efficient and suitable for scenarios with a large number of people voting; When summarizing vote counting between quantum centers, the initial quantum resources use two-particle product states, which are easy to prepare and require only single-particle measurements, making the operation convenient and reducing the difficulty of vote counting. This system can effectively detect and resist various attacks, thus ensuring security.

Key words: quantum voting; multi-center parallel computing; quantum walk; semi-quantum key distribution; d dimensional quantum system
Foundation Item(s): Beijing Natural Science Foundation (No.4234084)

1 引言

在当今社会,投票已经成为一种重要的决策方式,电子投票也逐渐突显出其重要性. 随着量子计算机的开发和研制,传统投票协议的机密性、匿名性等安全问题面临挑战,根据海森堡测不准原理[1]和量子不可克隆定理[2]等,量子密码学可以确保量子通信过程的绝对安全性,量子投票的研究应运而生. 2006年,Hillery等人[3]提出了两种投票模式:移动式投票方案和分布式投票方案,旨在弥补经典方案中的安全性不足. 随后,Vaccaro等人[4]在2007年定义了量子投票协议的标准,为量子投票方案的进一步研究奠定了基础. 2020年,宋秀丽等人[5]设计了基于d维三粒子纠缠态的量子投票方案,突破了2维或3维Hilbert空间限制. 还有一些量

收稿日期:2024-10-07;修回日期:2025-03-26;责任编辑:覃怀银
*通讯作者:李艳俊

子投票协议相继被提出[6~12]. 然而,量子计算机不完全成熟和量子资源昂贵等因素限制了量子投票在实际场景中的应用. 经典的量子协议中,所有的参与者都需要具备完整的量子能力,这增加了协议的实际应用难度. 2007 年,Boyer 等人[13]提出了半量子密钥分发(Semi-Quantum Key Distribution,SQKD)方案,并在2008年扩展了这个结果[14],提出了两种SQKD方案,并证明了完全鲁棒性. 在半量子协议中,参与者分为量子通信方和经典通信方,经典通信方只需要具备限定的量子能力,就可以与量子通信方进行通信,它与量子协议具有同等的安全性,且需要的量子资源更少,更适用于如今量子技术的发展水平. 此后,半量子技术迅速发展,包括半量子投票在内的半量子密码协议不断被提出[15~22]. 在投票方面,2021 年,Qiu 等人[16]提出了一种基于环签名的半量子投票方案. 2022 年,张妍等人[18]提出了一种基于单粒子用于问卷调查的半量子投票协议. 2024 年,Qiu 等人[20]对基于环签名的半量子投票方案进行了改进. 半量子技术的研究和应用,降低了量子技术的实现成本,兼容性高,使得现有的经典通信基础设施能够逐步过渡到量子通信,随着量子技术的不断发展,半量子投票协议有望在未来的投票系统中发挥重要作用.

安全多方求和允许多个参与方在不泄露各自私有秘密的情况下,联合计算出他们私有秘密之和. 量子游走是经典随机游走在量子力学中的模拟,是一种利用量子力学性质产生的随机过程. 这两种技术是量子和半量子密码协议中经常用到的技术. 如,2022 年,冯雁等人[9]设计了基于量子傅里叶变换求和的量子投票协议,将傅里叶变换、安全多方求和应用到量子投票中. 2023 年,李佩珊等人[19]提出一种第三方 TP 只需制备单量子比特就可对多个资源受限的参与方进行秘密求和的半量子协议. 2024 年,石润华等人[12]设计了基于量子行走公钥加密的电子投票方案,将量子行走即量子游走应用到了量子投票中.

基于半量子密码协议的发展和安全多方求和、量子游走等技术的原理,本文提出一种多中心高效量子安全投票方案,与其他传统方案比较,该方案具有以下优点:

(1)半量子密钥分发协议允许经典用户和全量子用户间通信,降低了设施成本,便于实现.

(2)多个量子中心分别并行计算各自负责的选民的票数,且结合了环形结构和星形结构,减少了中心节点的通信压力,投票、计票更加高效,适用于大量人数投票的场景. 例如,总统选举投票时,可在多地设置量子中心,选民可在当地使用经典操作进行投票,再由当地的量子中心计票,最后进行量子中心间的汇总计票.

(3)量子中心之间汇总计票时,初始量子资源使用两粒子乘积态而非纠缠态,通过对量子态施加单向演化算子实现计票,制备简单,操作方便,降低了计票难度,提高了计票效率,便于方案的实现.

2　基本知识

2.1　半量子密钥分发

半量子密钥分发的基本思想是利用量子力学的特性来确保通信的安全性,即使窃听者能够拦截和测量部分量子态,也无法在不被察觉的情况下完全复制和重传这些量子态.

本文对经典操作的定义为,经典选民只能执行以下操作:制备 $\bar{Z}$ 基状态 $\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$;用 $\bar{Z}$ 基 $\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$ 测量;直接返回量子比特;重新排序量子比特. 所需制备的 d 维单粒子叠加态为

$$|w\rangle=\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}|l\rangle \tag{1}$$

其中,每个 $|l\rangle$ 都是 d 维基态,$l\in\{0,1,\cdots,d-1\}$,对每个 d 维基态 $|l\rangle$ 执行傅里叶变换后状态变为

$$F|l\rangle=\frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}\xi^{l\delta}|\delta\rangle \tag{2}$$

其中,$\xi=\mathrm{e}^{\frac{2\pi i}{d}}$. 设置两组正交基 $V_1=\left|l\right\rangle_{l=0}^{d-1}$ 和 $V_2=F\left|l\right\rangle_{l=0}^{d-1}$,这两组测量基也可以被表示为 $\bar{Z}$ 基和 $\bar{X}$ 基:

$$\bar{Z}=|0\rangle,|1\rangle,\cdots,|d-1\rangle \tag{3}$$

$$\bar{X}=F|0\rangle,F|1\rangle,\cdots,F|d-1\rangle \tag{4}$$

2.2　量子游走

量子游走是经典随机游走的量子版本. Aharonov 等人[23]于 1993 年将经典随机游走理论扩展到了量子力学领域,提出了量子游走模型. 量子游走可以分为离散时间量子游走和连续时间量子游走. 离散时间位于直线上的量子游走系统是由记录游走粒子位置的游走系统和决定游走粒子方向的硬币系统所构成[24]. 以抛硬币为例,如果是掷出正面,就向右走一步;如果是反面,则向左走一步. 在量子世界里,是立刻向两个方向移动,像波一样展开.

量子游走态可以用 $|\psi\rangle=|p\rangle\otimes|c\rangle$ 来表示,$|p\rangle$ 表示游走粒子量子态,$|c\rangle$ 表示硬币粒子量子态,在接下来的方案中,$p\in(-d,d)$ 并且 $c\in\{0,1\}$. 可以用演化算子 $\boldsymbol{U}=\boldsymbol{S}\cdot(\boldsymbol{I}\otimes\boldsymbol{C})$ 来描述量子游走态的每步演化,其中 $\boldsymbol{U}$ 是酉算子,$\boldsymbol{S}$ 为全局移动算子,$\boldsymbol{I}$ 为 H_p 的单位算子,$\boldsymbol{C}$ 为 H_C 的硬币算子,作用于硬币粒子空间,这里选择的 $\boldsymbol{C}$ 为哈达玛矩阵:

$$\boldsymbol{C}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{5}$$

假定硬币粒子的$|0\rangle$态表示游走粒子向右走，硬币粒子的$|1\rangle$态表示游走粒子向左走. $\boldsymbol{C}$作用到硬币粒子可得到如下结果：

$$\boldsymbol{C}|0\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right),\boldsymbol{C}|1\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right) \tag{6}$$

$\boldsymbol{S}$是全局移动算子，负责控制游走粒子朝着相应的方向移动一步，定义为

$$\boldsymbol{S}=\sum_i|i+1\rangle\langle i|\otimes|0\rangle\rangle\langle 0|+\sum_i|i-1\rangle\langle i|\otimes|1\rangle\langle 1| \tag{7}$$

则有

$$\boldsymbol{S}\left(|i\rangle\otimes|0\rangle\right)=|i+1\rangle\otimes|0\rangle \tag{8}$$

$$\boldsymbol{S}\left(|i\rangle\otimes|1\rangle\right)=|i-1\rangle\otimes|1\rangle \tag{9}$$

其中，i为H_p中的位置，$\boldsymbol{U}$的逆算子被定义为

$$\boldsymbol{U}^{-1}=\left[\boldsymbol{S}\cdot\left(\boldsymbol{I}\otimes\boldsymbol{C}\right)\right]^{-1}=\left(\boldsymbol{I}\otimes\boldsymbol{C}^{-1}\right)\cdot\boldsymbol{S}^{-1} \tag{10}$$

移动算子$\boldsymbol{S}$的逆$\boldsymbol{S}^{-1}$为

$$\boldsymbol{S}^{-1}=\sum_i|i-1\rangle\langle i|\otimes|0\rangle\langle 0|+\sum_i|i+1\rangle\langle i|\otimes|1\rangle\langle 1| \tag{11}$$

假设对初始量子游走态$|\psi_0\rangle=|p\rangle\otimes|c\rangle=|0\rangle\otimes|0\rangle$施加$k$次$\boldsymbol{U}$后得到：

$$\boldsymbol{U}^k|\psi_0\rangle=\left[\boldsymbol{S}\cdot\left(\boldsymbol{I}\otimes\boldsymbol{C}\right)\right]^k|\psi_0\rangle \tag{12}$$

然后对游走粒子量子态进行$\left\{|-(d-1)\rangle,|-(d-2)\rangle,\cdots,|-1\rangle,|0\rangle,|1\rangle,\cdots,|d-1\rangle\right\}$基测量，其将以一定概率被坍塌到某位置.

如果直线双向量子游走(Two-Direction Quantum Walks on a Line，TDQWL)系统向左右两端延伸的游走路线被首尾相连成一个圆，那么其将被转化为圆上量子游走(Quantum Walks on a Circle，QWC)系统.

定义$\boldsymbol{T}_k$算子为$\boldsymbol{T}_k=\sum_i|(i+k)\bmod d\rangle\langle i|$，其中mod为求模运算，那么单向移动算子$\boldsymbol{S}_o$及其逆$\boldsymbol{S}_o^{-1}$分别为

$$\boldsymbol{S}_o=\boldsymbol{T}_1\otimes|0\rangle\langle 0|\ +\boldsymbol{T}_0\otimes|1\rangle\langle 1| \tag{13}$$

$$\boldsymbol{S}_o^{-1}=\boldsymbol{T}_{-1}\otimes|0\rangle\langle 0|\ +\boldsymbol{T}_0\otimes|1\rangle\langle 1| \tag{14}$$

$\boldsymbol{S}_o$的作用变为

$$\boldsymbol{S}_o\left(|i\rangle\otimes|0\rangle\right)=\left|(i+1)\bmod d\right\rangle\otimes|0\rangle \tag{15}$$

$$\boldsymbol{S}_o\left(|i\rangle\otimes|1\rangle\right)=|i\rangle\otimes|1\rangle \tag{16}$$

从而得到单向演化算子$\boldsymbol{U}_o$及其逆$\boldsymbol{U}_o^{-1}$分别为

$$\boldsymbol{U}_o=\boldsymbol{S}_o\cdot\left(\boldsymbol{I}_d\otimes\boldsymbol{C}\right) \tag{17}$$

$$\boldsymbol{U}_o^{-1}=\left[\boldsymbol{S}_o\cdot\left(\boldsymbol{I}_d\otimes\boldsymbol{C}\right)\right]^{-1}=\left(\boldsymbol{I}_d\otimes\boldsymbol{C}^{-1}\right)\cdot\boldsymbol{S}_o^{-1} \tag{18}$$

如果再对该系统施加若干次$\boldsymbol{U}_o$以使量子态只朝一个方向移动，就会产生基于圆上的单向量子游走系统(One-Direction Quantum Walks on a Circle，ODQWC).

对初始量子游走态$|\psi_0\rangle=|0\rangle\otimes|0\rangle$作用一次单向演化算子$\boldsymbol{U}_o=\boldsymbol{S}_o\cdot\left(\boldsymbol{I}_d\otimes\boldsymbol{C}\right)$. 首先哈达玛门$\boldsymbol{C}$作用于硬币粒子的$|0\rangle$状态：

$$\boldsymbol{C}|0\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right) \tag{19}$$

得到的状态与位置粒子的$|0\rangle$状态结合：

$$\begin{aligned}|0\rangle\otimes\boldsymbol{C}|0\rangle&=|0\rangle\otimes\left(\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right)\\&=\frac{1}{\sqrt{2}}\left(|0\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle\right)\end{aligned} \tag{20}$$

$\boldsymbol{S}_o$作用于$\frac{1}{\sqrt{2}}\left(|0\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle\right)$得到：

$$\begin{aligned}\boldsymbol{U}_o^1|\psi_0\rangle&=\boldsymbol{S}_0\left(\frac{1}{\sqrt{2}}\left(|0\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle\right)\right)\\&=\frac{1}{\sqrt{2}}\left(|1\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle\right)\end{aligned} \tag{21}$$

同理，施加两次单向演化算子后，量子态为

$$\begin{aligned}\boldsymbol{U}_o^2|\psi_0\rangle=\frac{1}{2}&\left(|2\rangle\otimes|0\rangle+|1\rangle\otimes|0\rangle\right.\\&\left.+|1\rangle\otimes|1\rangle-|0\rangle\otimes|1\rangle\right)\end{aligned} \tag{22}$$

3 多中心高效量子安全投票方案

假设多个选民需要在不透露各自选票的前提下借助量子中心完成计票. 记量子可信中心为TP，并定义TP是半诚实的，即在执行过程中，TP必须遵循方案的步骤且不能与任何选民串通，但是它可能会试图通过收集相关信息来获取选民的选票内容. 为了减少TP通信压力，引入多个TP，在传统的星形粒子传输结构的基础上引入环形的粒子传输结构，将环形结构和星形结构相结合，以实现多中心高效量子安全投票方案，如图1、图2及图3所示.

假设各选民拥有相同但不完全的量子能力，仅能进行经典操作；TP作为量子通信中心，拥有制备任意量

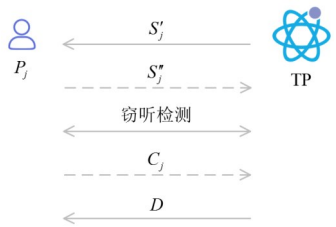

图1 多中心高效量子安全投票方案TP内求和结构图

图2　多中心高效量子安全投票方案量子中心求和结构图

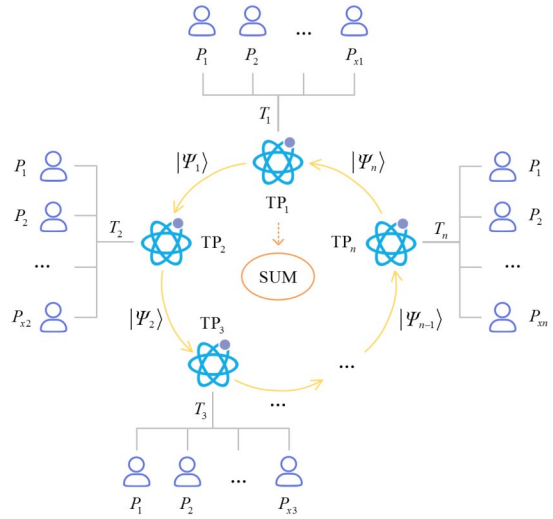

图3　多中心高效量子安全投票方案总结构图

子态和执行任意量子门操作的完全量子能力. 各选民与TP之间采用半量子密钥分发方案[25]进行通信,TP之间采用基于ODQWC的能实现整数求和的量子安全多方求和协议进行通信[24]. 并且所有选民之间以及选民与TP之间通过认证的量子信道和经典信道进行通信,通信信道有理想的物理安全保护,不存在信息泄露问题. 基于半量子密钥分发协议和单向量子游走,本文提出了多中心高效量子安全投票方案.

定义模加运算符$\oplus$为$a\oplus b=(a+b)\bmod d$,定义模减运算符$\ominus$如下:当$a>b$时,定义为$a\ominus b=(a-b)\bmod d$;当$a<b$时,定义为$a\ominus b=(a+d-b)\bmod d$.

假设有L个候选人,候选人序号分别为$1,2,\cdots,L$. 某个TP有$x(x>2)$个具有半量子能力的选民$P_j(1\leqslant j\leqslant x)$,每个选民有长度为$L$的选票$V_j$,即$V_j=\left(v_j^1,v_j^2,\cdots,v_j^L\right)$,$v_j^i\in\{0,1\}$,$1\leqslant i\leqslant L$,若选民$P_j$对候选人$i$投票,则$v_j^i=1$,否则$v_j^i=0$. 希望在不泄露选民选票内容的情况下,在半诚实TP的帮助下完成计票,票数和记为$T=\left(t^1,t^2,\cdots,t^L\right)$,即计算模$d$之和:

$$\begin{aligned}T&=V_1\oplus V_2\oplus\cdots\oplus V_n\\&=\left(v_1^1\oplus v_2^1\oplus\cdots\oplus v_x^1,v_1^2\oplus v_2^2\oplus\cdots\oplus v_x^2,\right.\\&\quad\left.\cdots,v_1^L\oplus v_2^L\oplus\cdots\oplus v_x^L\right)\\&=\left(t^1,t^2,\cdots,t^L\right)\end{aligned}\tag{23}$$

其中,d为大于x的有原根的大数. 在协议开始前,x个选民使用扩展的半量子密钥分发方案[25],预先共享长度为L的密钥$K=\left(k^1,k^2,\cdots,k^L\right)$,$k^i\in\{0,1,\cdots,d-1\}$. TP随机指定一个选民$P_j$,该选民选定$d$的一个原根$\gamma$,公开$\gamma\oplus k^1$的值,其余选民用自己的密钥$K$计算出原根$\gamma=\gamma\oplus k^1\ominus k^1$.

原根设m是正整数,a是整数,若a模m的阶等于$\varphi(m)$,则称a为模m的一个原根,其中$\varphi(m)$表示m的欧拉函数.

3.1　TP内求和阶段

步骤S1. 量子中心TP准备x组长度为$2L$的d维量子比特序列$S_j=\left(q_j^1,q_j^2,\cdots,q_j^{2L}\right)$,其中每个量子比特的状态为$|w\rangle$. TP产生$x$组长度为$2L$的诱骗粒子序列$B_j$,每个量子比特都随机取自式(3)和式(4)中$\{\bar{Z},\bar{X}\}$基中的状态. 随后,TP将每组诱骗粒子$B_j$随机插入到每组量子比特序列$S_j$中形成新的长度为$4L$的序列$S_j'$,分别发送给选民$P_j$.

步骤S2. 选民P_j对收到的每个量子比特随机选择以下两种操作之一. 直接将收到的量子比特返回给TP,记为操作R;对收到的量子比特执行$\bar{Z}$基测量,并根据测量结果制备新的量子比特发送给TP,记为操作M. 最终生成长度为$4L$的量子比特序列S_j''发送给TP. 序列$\mathrm{G_pre}_j=\left(\mathrm{g_p}_j^1,\mathrm{g_p}_j^2,\cdots,\mathrm{g_p}_j^{2L}\right)$记录所有的$\bar{Z}$基测量结果,$\mathrm{g_p}_j^i\in\{0,1,\cdots,d-1\}$. 因为选民$P_j$随机选择操作$R$或操作$M$,执行操作$M$的概率为$\frac{1}{2}$,因此序列$\mathrm{G_pre}_j$的长度为$2L$.

步骤S3. TP与选民P_j协同检测序列S_j''传输的安全性. 选民P_j公开在步骤S2对每个量子比特选择的操作;TP通过半量子密钥分发方案生成的密钥加密数据进行传输等安全的方式单独告知选民P_j诱骗粒子的位置和状态. TP根据选民P_j告知的操作检查S_j''. 当P_j选择操作R时,TP选择对应的测量基对量子比特进行测量,测量结果应该与TP准备的初始量子比特相同,否则存在窃听,TP终止方案;当P_j选择操作M时,TP对量子比特执行$\bar{Z}$基测量,测量结果应与P_j的测量结果一致,否则存在窃听,TP终止方案. 如果错误率高于预先设定的阈值,方案将被终止. 选民P_j和TP对每个量子比特的检测过程详见表1. 如果检测通过,TP和选民P_j分别丢弃$\mathrm{G_pre}_j$中的诱骗粒子,将P_j实行M操作返回的非诱骗粒子的量子比特执行$\bar{Z}$基测量的结果整理形成长度为L的序列$G_j=\left(g_j^1,g_j^2,\cdots,g_j^L\right)$.

步骤S4. 选民P_j计算$C_j^i=g_j^i\oplus v_j^i\oplus\gamma^{k^i+j}$并发送给TP. TP计算$D^i=C_1^i\oplus C_2^i\oplus\cdots\oplus C_x^i\ominus g_1^i\ominus g_2^i\ominus\cdots\ominus g_x^i$并发送给每位选民. 每个选民$P_j$根据预先共享的密钥$K$和原根$\gamma$计算每位候选人的票数之和$t^i=D^i\ominus\gamma^{k^i+1}\ominus\gamma^{k^i+2}\ominus\cdots\ominus\gamma^{k^i+x}$. TP随机指定一个选民$P_j$

公开候选人票数 $T=\left(t^1,t^2,\cdots,t^L\right)$.

表 1 选民 P_j 操作和 TP 对量子态测量关系表

TP制备的初始态(S_j'中状态)	选民P_j操作	选民P_j返回的量子态(S_j''中状态)	TP测量基	TP测量结果
$\|0\rangle$	R	$\|0\rangle$	$\bar{Z}$	$\|0\rangle$
$\|1\rangle$		$\|1\rangle$		$\|1\rangle$
$\cdots$		$\cdots$		$\cdots$
$\|d-1\rangle$		$\|d-1\rangle$		$\|d-1\rangle$
$F\|0\rangle$		$F\|0\rangle$	$\bar{X}$	$F\|0\rangle$
$F\|1\rangle$		$F\|1\rangle$		$F\|1\rangle$
$\cdots$		$\cdots$		$\cdots$
$F\|d-1\rangle$		$F\|d-1\rangle$		$F\|d-1\rangle$
$\|0\rangle$	M	$\|0\rangle$	$\bar{Z}$	$\|0\rangle$
$\|1\rangle$		$\|1\rangle$		$\|1\rangle$
$\cdots$		$\cdots$		$\cdots$
$\|d-1\rangle$		$\|d-1\rangle$		$\|d-1\rangle$
$F\|0\rangle$		μ_0		μ_0
$F\|1\rangle$		μ_1		μ_1
$\cdots$		$\cdots$		$\cdots$
$F\|d-1\rangle$		μ_{d-1}		μ_{d-1}

注:其中 $\mu_0,\mu_1,\cdots,\mu_{d-1}\in\left\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\right\}$. 如,假设选民对 $F|0\rangle$ 进行 $\bar{Z}$ 基测量后结果 $\mu_0=|1\rangle$,则 TP 根据选民 P_j 公开的操作用 $\bar{Z}$ 基测量后结果应当同样为 $\mu_0=|1\rangle$.

3.2 量子中心求和阶段

步骤 S5. 假设存在 $n(n>2)$ 个量子中心 $\mathrm{TP}_a(1\leqslant a\leqslant n)$,其中 TP_1 负责制备初始量子游走态且被假定为不能与其他任何人共谋. 每个量子中心 TP_a 有长度为 L 的选票 $T_a=\left(t_a^1,t_a^2,\cdots,t_a^L\right)$, $t_a^i\in\{0,1,\cdots,d-1\}$, $1\leqslant a\leqslant n$. 希望在不泄露 T_a 内容的前提下得到 $\mathrm{SUM}=T_1+T_2+\cdots+T_n=\left(\mathrm{sum}^1,\mathrm{sum}^2,\cdots,\mathrm{sum}^L\right)$ 的正确计票结果. TP_1 制备 Q 份长度为 L 的都处于 $|0\rangle\otimes|0\rangle$ 的初始量子游走态的量子态序列,每份量子态序列记为 $\left|\Psi_0\right\rangle=\left\{\left|\psi_0^1\right\rangle,\left|\psi_0^2\right\rangle,\cdots,\left|\psi_0^L\right\rangle\right\}$.

步骤 S6. TP_1 用自己的选票 $\left(t_1^1,t_1^2,\cdots,t_1^L\right)$ 对每份量子态序列进行编码. 对于自己的比特序列 T_1 中的每一位 t_1^i,TP_1 对相应位置的量子游走态 $\left|\psi_0^i\right\rangle$ 应用 $\boldsymbol{U}_o$ 算子 $t_1^i+f_1^i$ 次,即 $\left|\psi_1^i\right\rangle=\boldsymbol{U}_o^{t_1^i+f_1^i}\left|\psi_0^i\right\rangle$,其中 f_1^i 为 TP_1 产生的随机数,$f_1^i\geqslant 0$. 编码后的每份量子态序列为

$$\begin{aligned}\left|\Psi_1\right\rangle&=\left\{\left|\psi_1^1\right\rangle,\left|\psi_1^2\right\rangle,\cdots,\left|\psi_1^L\right\rangle\right\}\\&=\left\{\boldsymbol{U}_o^{t_1^1+f_1^1}\left|\psi_0^1\right\rangle,\boldsymbol{U}_o^{t_1^2+f_1^2}\left|\psi_0^2\right\rangle,\cdots,\boldsymbol{U}_o^{t_1^L+f_1^L}\left|\psi_0^L\right\rangle\right\}\end{aligned}\tag{24}$$

然后 TP_1 制备 λ 个诱骗粒子,每个粒子都随机取自式(3)和式(4)中 $\left\{\bar{Z},\bar{X}\right\}$ 基中的状态,并将诱骗粒子随机插入 Q 份 $\left\{\left|\psi_1^1\right\rangle,\left|\psi_1^2\right\rangle,\cdots,\left|\psi_1^L\right\rangle\right\}$ 中,将这个新序列传递给 TP_2. TP_1 和 TP_2 共同进行窃听检测. TP_1 告知 TP_2 诱骗粒子的位置和制备基,TP_2 用相应的测量基对其测量,将测量结果告知 TP_1. TP_1 将诱骗粒子初始状态和收到的测量结果进行对比,如果错误率高于预先设定的阈值,方案将被终止. 否则,方案继续.

步骤 S7. 每个量子中心按照同样的规则依次对量子态序列进行编码. 对于从 TP_{a-1} 收到的每份量子态序列,双方进行窃听检测,通过后,TP_a 去掉诱骗粒子,并利用自己的比特序列 $\left(t_a^1,t_a^2,\cdots,t_a^L\right)$ 和随机数 $\left(f_a^1,f_a^2,\cdots,f_a^L\right)$ 对 Q 份量子态序列进行编码,然后将编码后的量子态序列随机插入自己的诱骗粒子传送给 TP_{a+1}. 最后 TP_n 编码后每份量子态序列为

$$\begin{aligned}\left|\Psi_n\right\rangle&=\left\{\left|\psi_n^1\right\rangle,\left|\psi_n^2\right\rangle,\cdots,\left|\psi_n^L\right\rangle\right\}\\&=\left\{\boldsymbol{U}_o^{t_1^1+t_2^1+\cdots+t_n^1+f_1^1+\cdots+f_n^1}\left|\psi_0^1\right\rangle,\right.\\&\quad\boldsymbol{U}_o^{t_1^2+t_2^2+\cdots+t_n^2+f_1^2+\cdots+f_n^2}\left|\psi_0^2\right\rangle,\\&\quad\left.\cdots,\boldsymbol{U}_o^{t_1^L+t_2^L+\cdots+t_n^L+f_1^L+\cdots+f_n^L}\left|\psi_0^L\right\rangle\right\}\end{aligned}\tag{25}$$

将诱骗粒子插入后返回给 TP_1.

步骤 S8. TP_n 和 TP_1 共同进行窃听检测. $\mathrm{TP}_a(2\leqslant a\leqslant n)$ 通过量子安全直接通信将自己的 $\left(f_a^1,f_a^2,\cdots,f_a^L\right)$ 发送给 TP_1. TP_1 对从 TP_n 处收到的 Q 份量子态序列中的每一位 $\left|\psi_n^i\right\rangle$ 都施加 $f_1^i+f_2^i+\cdots+f_n^i$ 次 $\boldsymbol{U}_o^{-1}$,即 $\left|\psi_{n+1}^i\right\rangle=\left(\boldsymbol{U}_o^{-1}\right)^{f_1^i+f_2^i+\cdots+f_n^i}\left|\psi_n^i\right\rangle=\boldsymbol{U}_o^{t_1^i+t_2^i+\cdots+t_n^i}\left|\psi_0^i\right\rangle$. TP_1 对 Q 份量子态序列的每个 $\left|\psi_{n+1}^i\right\rangle$ 的游走粒子进行单粒子 $\bar{Z}$ 基测量,得到测量结果序列. TP_1 统计第 i 位的测量结果中出现了哪些位置,统计结果中位置的最大值即为第 i 位候选人的总票数 sum^i. 例如,对 Q 份量子态序列,如果测得的 Q 个 $\left|\psi_{n+1}^1\right\rangle$ 的结果中位置的最大值为 5,则 1 号候选人获得的总票数 sum^1 为 5. 最后,TP_1 将票数 SUM 公开.

4 方案正确性说明

在选民与 TP 的半量子求和阶段,不考虑检测传输安全的窃听检测环节,假设有 L 个候选人,3 个经典选民 P_1、P_2、P_3,选票分别为 V_1、V_2、V_3. 3 个选民预先共享一个密钥 K 和原根 γ.

TP 生成量子比特序列 S_j 并发送给选民. 选民选择操作直接反射(R)或测量(M).

TP 对返回的量子比特进行测量,得到结果 G_1、G_2、G_3. 选民分别计算并公开 $C_1=V_1\oplus\gamma^{K+1}\oplus G_1$、$C_2=$

$V_2\oplus\gamma^{K+2}\oplus G_2$、$C_3=V_3\oplus\gamma^{K+3}\oplus G_3$. TP已知$C_j$和$G_j$的值,计算模$d$之和$D$:

$$\begin{aligned}D&=C_1\oplus C_2\oplus C_3\ominus G_1\ominus G_2\ominus G_3\\&=\left(V_1\oplus\gamma^{K+1}\oplus G_1\right)\oplus\left(V_2\oplus\gamma^{K+2}\oplus G_2\right)\\&\quad\oplus\left(V_3\oplus\gamma^{K+3}\oplus G_3\right)\ominus G_1\ominus G_2\ominus G_3\\&=\left(V_1\oplus\gamma^{K+1}\right)\oplus\left(V_2\oplus\gamma^{K+2}\right)\oplus\left(V_3\oplus\gamma^{K+3}\right)\\&=\left(V_1\oplus V_2\oplus V_3\right)\oplus\left(\gamma^{K+1}\oplus\gamma^{K+2}\oplus\gamma^{K+3}\right)\end{aligned}\tag{26}$$

TP将D发送给每位选民,选民收到后计算

$$\begin{aligned}T&=D\ominus\left(\gamma^{K+1}\oplus\gamma^{K+2}\oplus\gamma^{K+3}\right)\\&=\left(V_1\oplus V_2\oplus V_3\right)\oplus\left(\gamma^{K+1}\oplus\gamma^{K+2}\oplus\gamma^{K+3}\right)\\&\quad\ominus\left(\gamma^{K+1}\oplus\gamma^{K+2}\oplus\gamma^{K+3}\right)\\&=V_1\oplus V_2\oplus V_3\end{aligned}\tag{27}$$

得到3个选民的票数之和T.

在量子中心求和阶段,不考虑窃听检测,对初始态$|0\rangle$施加$\boldsymbol{U}_o^r$操作后,得到的位置值最大的状态为$|r\rangle$,即对初始态$|0\rangle$施加$\boldsymbol{U}_o^{t_1^i+t_2^i+\cdots+t_n^i+f_1^i+f_2^i+\cdots+f_n^i}$操作及$\left(\boldsymbol{U}_o^{-1}\right)^{f_1^i+f_2^i+\cdots+f_n^i}$操作后,得到的位置值最大的状态为$\left|t_1^i+t_2^i+\cdots+t_n^i\right\rangle$.

量子中心TP_1制备Q份长度为L的都处于$|0\rangle\otimes|0\rangle$的初始量子游走态的量子态序列,每份量子态序列记为$\left\{|0\rangle,|0\rangle,\cdots,|0\rangle\right\}$. 量子中心$\mathrm{TP}_1$用自己的选票$T_1$及随机数对每份量子态序列进行编码,并将其传输给$\mathrm{TP}_2$,依此类推,每个量子中心$\mathrm{TP}_a$用自己的选票$T_a=\left(t_a^1,t_a^2,\cdots,t_a^L\right)$和随机数$\left(f_a^1,f_a^2,\cdots,f_a^L\right)$对接收到的量子游走态施加单向演化算子$\boldsymbol{U}_o^{t_a^i+f_a^i}$,最后传输回$\mathrm{TP}_1$. TP_1对去掉随机数的量子游走态进行$\bar{Z}$基测量,测得游走粒子位置的最大值,即为候选人获得的总票数$\mathrm{SUM}=T_1+T_2+\cdots+T_n$.

5　方案实例

本节通过具体实例进一步验证方案的正确性. 假设有3个选民Alice、Bob和Carol,负责对他们的选票进行计票的量子中心为TP_1,d为5.

首先Alice、Bob和Carol通过安全的半量子密钥分发协议共享密钥$K=3041$,原根$\gamma=2$. Alice的选票$V_\mathrm{A}=1011$,Bob的选票$V_\mathrm{B}=1100$,Carol的选票$V_\mathrm{C}=0110$.

TP_1准备诱骗粒子,并随机插入到序列S_A、S_B、S_C中生成新的序列S_A'、S_B'、S_C',分别发送给3个选民. TP_1与选民共同检测传输安全性,如果检测到窃听则方案终止. 这里的操作只是为了检测传输安全性,对结果并不产生影响,故不再赘述. 设3个选民的$\bar{Z}$基测量结果为$G_\mathrm{A}=1234$,$G_\mathrm{B}=0243$,$G_\mathrm{C}=4210$.

选民与TP_1共同计算票数. 选民Alice、Bob和Carol计算并公开$C_j^i=g_j^i\oplus v_j^i\oplus\gamma^{k^i+j}$.

Alice加密:$C_\mathrm{A}^i=g_\mathrm{A}^i\oplus v_\mathrm{A}^i\oplus\gamma^{k^i+1}$,$C_\mathrm{A}=3414$.

Bob加密:$C_\mathrm{B}^i=g_\mathrm{B}^i\oplus v_\mathrm{B}^i\oplus\gamma^{k^i+2}$,$C_\mathrm{B}=3231$.

Carol加密:$C_\mathrm{C}^i=g_\mathrm{C}^i\oplus v_\mathrm{C}^i\oplus\gamma^{k^i+3}$,$C_\mathrm{C}=3101$.

TP_1计算

$$\begin{aligned}D&=C_\mathrm{A}\oplus C_\mathrm{B}\oplus C_\mathrm{C}\ominus G_\mathrm{A}\ominus G_\mathrm{B}\ominus G_\mathrm{C}\\&=3414\oplus3231\oplus3101\\&\quad\ominus1234\ominus0243\ominus4210\\&=4114\end{aligned}\tag{28}$$

并将其发送给每位选民.

通过密钥K和原根γ,每个选民都可以求出票数T:

$$t^i=D^i\ominus\gamma^{k^i+1}\ominus\gamma^{k^i+2}\ominus\gamma^{k^i+3},\ T=2221\tag{29}$$

即1、2、3号候选人的票数为2,4号候选人的票数为1.

不考虑窃听检测,假设有3个量子中心TP_1、TP_2、TP_3,选票分别为T_1、T_2、T_3. TP_1制备Q份长度为4的都处于$|0\rangle\otimes|0\rangle$的初始量子游走态的量子态序列,每份量子态序列记为$\left\{|0\rangle,|0\rangle,|0\rangle,|0\rangle\right\}$.

TP_1用自己的选票$T_1=2221$和随机数3411将量子态序列编码为$\left\{|5\rangle,|6\rangle,|3\rangle,|2\rangle\right\}$,将这些量子态序列传输给$\mathrm{TP}_2$,依此类推,每个量子中心用自己的选票和随机数对量子态序列施加单向演化算子,最后传输回TP_1. 假设最后传输回TP_1之后去掉随机数的量子态序列为$\left\{|5\rangle,|8\rangle,|4\rangle,|3\rangle\right\}$,$\mathrm{TP}_1$对每份量子态序列进行$\bar{Z}$基测量,测得的游走粒子位置的最大值分别为5、8、4、3,即1号候选人获得的总票数sum^1为5,2号候选人获得的总票数sum^2为8,3号候选人获得的总票数sum^3为4,4号候选人获得的总票数sum^4为3. 最后,TP_1将票数$\mathrm{SUM}=\{5,8,4,3\}$公开.

6　安全性分析

本方案可有效检测测量重发攻击、截获重发攻击、纠缠测量攻击等,有效抵抗双CNOT门攻击、TP攻击、TP_a发起的攻击等,保证安全性.

6.1　测量重发攻击

在本节中讨论测量重发攻击,不诚实的参与者尝试通过拦截、测量并重新发送量子比特来获取其他选民的选票信息.

6.1.1　TP内求和阶段

恶意的参与者(例如P_1)可能会试图拦截TP发送给其他参与者的量子比特,并对这些截获的量子态进行$\bar{Z}$基测量,从而获得测量结果. 然后,他们根据获得的测量结果,制备出与原始量子态相匹配的新量子比特. 最后,将这些新制备的量子态转发给目标选民,企图掩盖自己的拦截行为.

当选民选择执行操作M时,攻击者简单地重发测

量后的量子态,这种恶意行为可能不会被立刻察觉. 然而,如果选民选择执行操作R,TP可以通过对接收到的量子比特进行$\bar{X}$基测量来检测是否存在窃听行为. 如果测量结果为初始态,则表明没有攻击者的存在. 但是,由于攻击者之前已经通过$\bar{Z}$基测量破坏了量子态的原始状态,TP有很大的概率得到与初始态不同的测量结果. 这种测量结果的差异可以用来检测攻击者的存在和恶意行为. 例如,假设TP发送的初始态是$F|0\rangle$,P_1拦截并执行$\bar{Z}$基测量,这会将量子态坍缩到$|0\rangle,|1\rangle,\cdots,|d-1\rangle$中某一个. 如果$P_1$测量得到$|0\rangle$并发送这个状态,当选民选择操作$R$且TP执行$\bar{X}$基测量时,TP有很大的概率测量得到$F|0\rangle,F|1\rangle,\cdots,F|d-1\rangle$中某一个,从而发现了$P_1$的攻击.

6.1.2 量子中心求和阶段

假设攻击者Eve截获参与者TP_a发送给TP_{a+1}的粒子序列. Eve随机选择$\bar{Z}$基或$\bar{X}$基对截获的粒子序列进行测量. Eve将测量结果作为新的粒子序列,发送给TP_{a+1}. 对于单个诱骗粒子,Eve选择正确基的概率是$\frac{1}{2}$. 如果Eve选择了错误的测量基,其测量结果可能与原始状态不一致,攻击会被TP_a和TP_{a+1}的窃听检测过程发现,对于d维量子系统而言,在d个可能的基中,只有1个是正确的基,所以Eve的攻击被发现的概率是$\frac{1}{2}\times\frac{d-1}{d}=\frac{d-1}{2d}$. 而对于$\lambda$个粒子而言,Eve的攻击有$1-\left(\frac{d+1}{2d}\right)^{\lambda}$的概率被检测到. 当$\lambda$趋近于无穷大时,这个概率趋近于1. 这意味着,当使用足够多的粒子时,Eve的测量重发攻击几乎肯定会被发现.

6.2 截获重发攻击

在本节中讨论截获重发攻击,不诚实的参与者尝试通过拦截和重新发送量子比特来获取其他选民的选票信息. 以下是截获重发攻击的详细分析.

6.2.1 TP内求和阶段

恶意的选民(例如P_1)可能会拦截TP发送给其他选民的量子比特,并将这些截获的量子态保存下来,然后随机制备新的量子态,发送给目标选民. 当目标选民将量子比特返回给TP时,恶意参与者会再次拦截这些量子态,并将先前截获并保存的原始量子比特重新发送给TP. 通过对这些原始量子比特执行$\bar{Z}$基测量,恶意参与者企图推断出目标选民所选择的操作类型. 在量子比特的传输过程中,TP插入了一些诱骗粒子,其位置和状态对恶意参与者来说是未知的. 因此,恶意参与者无法区分自己拦截的量子比特是诱骗粒子还是真正携带信息的量子态. 当目标选民选择操作M时,由于恶意参与者在第二次拦截后发送的是原始的量子态,TP在执行窃听检测时有很大的概率得到与预期不同的测量结果,从而发现攻击行为的存在.

6.2.2 量子中心求和阶段

假设攻击者Eve截获了参与者TP_a发送给TP_{a+1}的粒子序列,并将这些粒子保留在自己手中. 然后Eve准备了一组假粒子序列,这些粒子随机处于$\bar{Z}$基或$\bar{X}$基中,然后将这些假粒子序列发送给TP_{a+1}. 在量子通信中,窃听检测是通过诱骗粒子来实现的. 对于一个诱骗粒子,Eve对其施加的攻击会以$\frac{d-1}{d}$的概率被TP_a和TP_{a+1}进行的窃听检测过程检测到. 对于λ个诱骗粒子,Eve对它们施加的攻击会以$1-\left(\frac{1}{d}\right)^{\lambda}$的概率被$\mathrm{TP}_a$和$\mathrm{TP}_{a+1}$进行的窃听检测过程检测到. 当$\lambda$趋近于正无穷时,这个概率趋近于1. Eve的截获重发攻击能被发现的原因在于制备的假粒子的状态有可能与真实诱骗粒子的状态不一致.

6.3 双CNOT攻击

在本节讨论双CNOT门攻击的情况. 恶意选民P_1试图在半量子求和阶段通过执行两次CNOT门操作来获取其他诚实选民的选票信息而不被发现. 假设以下情景:首先,TP准备了多个$|w\rangle$状态的量子比特,并将它们分配给假设的3个"经典的"选民P_1、P_2、P_3. 每个选民接收到的量子比特序列分别为S_1、S_2、S_3. P_1拦截发送给P_2的量子比特,并将其与自己的辅助量子比特(初始状态为$|0\rangle$)进行CNOT操作. 这个操作使得TP发送的量子比特和P_1的辅助量子比特之间产生了纠缠,形成了新的量子系统状态:

$$|\omega\rangle_1=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{TE} \tag{30}$$

其中,T代表TP的量子比特,E代表P_1的辅助量子比特.

P_2随机选择执行操作R或M,将新的量子序列发送给TP. P_1再次拦截P_2返回给TP的量子比特,并执行第二次CNOT门操作. 这次操作中,P_2的量子比特作为控制比特,P_1的辅助量子比特作为目标比特. 当P_2选择操作R时,第二次CNOT门操作后系统状态恢复为初始状态$|w\rangle_T\otimes|0\rangle_E$. TP无法通过常规的窃听检测发现$P_1$的攻击,但$P_1$也无法从辅助量子比特中获取$P_2$任何的选票信息. 当$P_2$选择操作$M$并进行$\bar{Z}$基测量时,系统的状态根据$P_2$的测量结果坍缩为$|00\rangle_{TE}$或$|11\rangle_{TE}$. P_1的第二次CNOT门操作使得无论系统坍缩为哪个状态辅助量子比特都变为$|0\rangle$,P_1仍无法从辅助量子比特中获取P_2的选票信息. 所以尽管P_1尝试通过双CNOT门攻击来获取P_2的选票信息,但这种攻击最终不会成功.

这表明该方案能够有效抵抗双CNOT门攻击,确保选民的选票信息安全.

6.4 纠缠测量攻击

Eve对TP发送给选民P_j或TP_a发送给TP_{a+1}的粒子施加纠缠测量攻击,即其对TP或TP_a发送出的粒子和自己的探测粒子施加酉操作U_E,然后对自己的探测粒子进行测量试图得到有用的信息. 为了不被TP和P_j或TP_a和TP_{a+1}进行的窃听检测过程检测到,Eve的探测粒子的最终态必须独立于TP发送给选民P_j或TP_a发送给TP_{a+1}的粒子,从而使得Eve无法获得任何有用信息. 以Eve攻击TP_a发送给TP_{a+1}的粒子为例,证明如下:

(1)用$|r\rangle$表示TP_a发送给TP_{a+1}的处于$\bar{Z}$基的粒子. Eve对$|r\rangle$和$|\theta\rangle$施加U_E后,全局复合系统变为$U_E\left(|r\rangle|\theta\rangle\right)=\sum_{r'=0}^{d-1}\alpha_{rr'}|r'\rangle|\theta_{rr'}\rangle$,其中$|\theta_{rr'}\rangle(r,r'=0,1,\cdots,d-1)$是Eve的探测态,$\sum_{r'=0}^{d-1}\left|\alpha_{rr'}\right|^2=1$. 为了不被窃听检测过程检测到,应有对$r\neq r'$,$\alpha_{rr'}=0$成立,则$U_E\left(|r\rangle|\theta\rangle\right)=\alpha_{rr}|r\rangle|\theta_{rr}\rangle$,$r=0,1,\cdots,d-1$. (2)用$|Y_r\rangle=F|r\rangle=\frac{1}{\sqrt{d}}\sum_{\tau=0}^{d-1}\mathrm{e}^{\frac{2\pi i\tau r}{d}}|\tau\rangle$表示$\mathrm{TP}_a$发送给$\mathrm{TP}_{a+1}$的处于$\bar{X}$基的粒子,$r=0,1,\cdots,d-1$. Eve对$|Y_r\rangle$和$|\theta\rangle$施加$U_E$后,全局复合系统变为$U_E\left(|Y_r\rangle|\theta\rangle\right)=\frac{1}{\sqrt{d}}\sum_{\tau=0}^{d-1}\mathrm{e}^{\frac{2\pi i\tau r}{d}}U_E\left(|\tau\rangle|\theta\rangle\right)$,即$\frac{1}{\sqrt{d}}\sum_{\tau=0}^{d-1}\mathrm{e}^{\frac{2\pi i\tau r}{d}}\alpha_{\tau\tau}|\tau\rangle|\theta_{\tau\tau}\rangle$. 经过离散量子傅里叶逆变换可得到$|\tau\rangle=\frac{1}{\sqrt{d}}\sum_{\sigma=0}^{d-1}\mathrm{e}^{-\frac{2\pi i\sigma\tau}{d}}|Y_\sigma\rangle$,则$U_E\left(|Y_r\rangle|\theta\rangle\right)=\frac{1}{d}\sum_{\tau=0}^{d-1}\sum_{\sigma=0}^{d-1}\mathrm{e}^{\frac{2\pi i\tau(r-\sigma)}{d}}\alpha_{\tau\tau}|Y_\sigma\rangle|\theta_{\tau\tau}\rangle$. 为了不被窃听检测过程检测到,应有对$r\neq\sigma$和$r,\sigma=0,1,\cdots,d-1$,$\sum_{\tau=0}^{d-1}\mathrm{e}^{\frac{2\pi i\tau(r-\sigma)}{d}}\alpha_{\tau\tau}|\theta_{\tau\tau}\rangle=0$成立,且$\sum_{\tau=0}^{d-1}\mathrm{e}^{\frac{2\pi i\tau(r-\sigma)}{d}}=0$,则$\alpha_{00}|\theta_{00}\rangle=\alpha_{11}|\theta_{11}\rangle=\cdots=\alpha_{(d-1)(d-1)}|\theta_{(d-1)(d-1)}\rangle=\alpha'|\theta'\rangle$. (3)结合(1)与(2)可得,$U_E\left(|r\rangle|\theta\rangle\right)=\alpha'|r\rangle|\theta'\rangle$,$U_E\left(|Y_r\rangle|\theta\rangle\right)=\alpha'|Y_r\rangle|\theta'\rangle$. 因此,为了不被窃听检测过程检测到,Eve的探测粒子的最终态必须独立于TP_a发送给TP_{a+1}的粒子,从而使得Eve无法获得任何有用信息. 同理,Eve的探测粒子的最终态必须独立于TP发送给选民P_j的粒子.

6.5 TP攻击

半诚实的TP需要按照方案步骤执行操作,且不允许与其他选民合谋. TP只能通过收集公共信息来尝试推算选民的选票信息,而不能主动偏离方案或与他人共谋. 以下是TP攻击的详细分析.

TP对选民选票的主动攻击是否安全主要依赖于选民进行密钥分发的协议的安全性. 如使用文献[25]的半量子密钥分发方案,则可抵抗TP的测量攻击、伪造攻击和集体攻击等. TP的被动攻击主要通过收集公共信息以推测选票信息. 在方案的步骤S3中,TP知道选民所选择的操作. 这使得TP能够了解到序列G_j的信息. 在步骤S4中,所有选民会公开他们的C_j值,并与TP共同计算出选票票数之和. 尽管TP可以获取g_j^i和C_j^i的值,但由于TP不知道选民之间共享的密钥K和原根γ的具体值,他无法直接从这些信息中推导出各个选民的具体选票内容. 而方案设计中也包括了多个步骤,如诱骗粒子的使用,这些都是为了增加任何外部或内部攻击者(包括TP)获取足够信息以推断选民选票内容的难度. 如果选民之间共享的密钥K和原根γ得到妥善保护,TP无法破解各选民的选票信息,保证了方案的安全性.

6.6 TP_a发起的攻击

6.6.1 单个TP_a发起的攻击

(1)假设恶意参与者TP_2完成与TP_1的窃听检测后,试图用$\bar{Z}$基测量粒子序列的游走粒子以获得TP_1的选票信息. 但TP_2不知道f_1^i,因此无法获得TP_1的选票信息. (2)假设恶意参与者TP_β攻击TP_a发送给TP_{a+1}的粒子序列$(\beta\neq a,a+1)$,由于不知道诱骗粒子的位置和制备基,会被窃听检测发现. (3)假设恶意参与者TP_{a+2}截获并保留TP_a发送给TP_{a+1}的粒子序列,将事先制备的都处于$|0\rangle\otimes|0\rangle$状态的假量子游走态序列发给$\mathrm{TP}_{a+1}$,试图在自己与$\mathrm{TP}_{a+1}$完成窃听检测后用$\bar{Z}$基测量$\mathrm{TP}_{a+1}$编码后的量子游走态的游走粒子得到$\mathrm{TP}_{a+1}$的选票信息. 但该过程必定被$\mathrm{TP}_a$和$\mathrm{TP}_{a+1}$之间的窃听检测发现;且$\mathrm{TP}_{a+2}$不知道$f_{a+1}^i$,因此无法获得$\mathrm{TP}_{a+1}$的选票信息.

6.6.2 共谋攻击

本文假定TP_1不能与其他任何人共谋,且如果$\mathrm{TP}_2,\mathrm{TP}_3,\cdots,\mathrm{TP}_n$联合起来,很容易在$\mathrm{TP}_1$公布票数时推断出$\mathrm{TP}_1$的选票信息$T_1$. 因此以下仅讨论共谋人数在$n-2$以内的共谋攻击. 假设除$\mathrm{TP}_1$以外的参与者中$n-2$个恶意参与者试图联合起来得到$\mathrm{TP}_1$和$\mathrm{TP}_a$的选票信息.

(1)对于TP_1,假设TP_2完成与TP_1的窃听检测后,包括TP_2在内的$n-2$个恶意参与者试图用$\bar{Z}$基测量粒子序列的游走粒子以获得TP_1的选票信息T_1. 但恶意参与者不知道f_1^i,因此无法获得TP_1的选票信息.

(2)对于TP_a,假设TP_{a-1}将事先制备的都处于$|0\rangle\otimes|0\rangle$状态的假量子游走态序列发给$\mathrm{TP}_a$,完成窃

听检测后，TP_a将用选票信息T_a和随机数f_a^i编码后的粒子序列发给TP_{a+1}. TP_{a+1}和TP_a通过窃听检测后，包括TP_{a-1}和TP_{a+1}在内的$n-2$个恶意参与者试图用$\bar{Z}$基测量粒子序列的游走粒子以获得TP_a的选票信息T_a. 但恶意参与者不知道f_a^i，因此无法获得TP_a的选票信息.

7 讨论与总结

本节讨论本文方案的性能并与其他星形结构的方案进行对比，如表2所示. 量子通信效率计算公式为$\eta=\frac{c}{q}$，其中c表示求和的私有比特数，q表示传输的量子比特数，不计算用于窃听检测的诱骗粒子.

与文献[8]相比，本文方案为半量子，允许经典用户参与. 与文献[8]、文献[17]和文献[20]相比，本文方案量子资源制备、量子操作、量子测量简单，且量子通信效率在人数较多、范围更大时更高. 与文献[20]相比，本文方案通信复杂度更低. 本文方案与文献[19]、文献[24]的安全多方求和方案相似，下面与这两个方案进行详细比较. 与文献[19]相比.(1)文献[19]使用星形结构，节点数量较多时，TP处理数据压力大，增加了系统的负担，可能导致延迟. 本文方案结合了环形结构和星形结构，进行多层级计算，减少了中心节点的通信压力，更适合选民人数较多的情况.(2)本文与文献[19]都是基于半量子安全多方求和，文献[19]的方案求和时模加密钥本身，但本文求和时模加γ^{k^i+j}. 各选民的密钥相同，且选票中只有0和1两个值，TP知道每个选民的G_j，因此如果仅将密钥和选票模加，TP可以对比每个C_j同一位置的值，推测出选民的选票信息. 如果模加γ^{k^i+j}，每个选民加的值不同，TP推测不出选票信息. 文献[19]中SMSQS2协议并未丢弃诱骗粒子并将其用于计算，本文方案丢弃了诱骗粒子. 因此本文方案安全性更高. 与文献[24]相比.(1)本文方案允许经典用户参与.(2)文献[24]使用环形结构，数据需要经过每个节点最终返回TP_1，在大规模投票中，容易发生延迟；每次操作仅有两个节点参与计算，其余节点闲置，系统运行效率低；如果某个选民节点出现故障，该节点之后的选票无法被统计. 本文方案结合了环形结构和星形结构，更适用于大规模投票. 例如，在进行全国范围的投票时，可以在首都设置TP_1，在几个其他城市分别设置量子中心，参与投票的选民可在当地使用经典操作进行投票，再由当地的量子中心计票，最后汇总计票. 在TP内求和阶段，TP同时统计多个选票，系统运行效率高，且仅负责本组，计算压力较小；如果某个选民节点出现故障，不影响其他选民票数的计算；选民为经典用户，增减节点相对容易. 在量子中心求和阶段，每个量子中心负责的选民数量可以根据需求设置，可根据选民数量变化程度增减量子中心节点，可根据需求扩展为3层或更多层级计算，具有较高的可扩展性和灵活性，便于管理.

表2 本文方案与同类方案的比较

方案	是否为半量子	初始量子资源	参与方信息维度	量子操作	量子测量方法	量子通信效率	通信复杂度
文献[8]	否	d维纠缠态	d维	编码操作及加解密操作U_x	d维纠缠态联合测量	$\frac{L}{4x(L+m)}$	$O(Lx)$
文献[17]	是	2维GHZ态	2维	/	2维单粒子测量和GHZ态测量	$\frac{2}{3x(32+d+\delta)}$	$O(Lx)$
文献[20]	是	2维GHZ态	2维	/	GHZ态测量	$\frac{1}{x^2}$	$O(x^2)$
本文方案	是	d维单粒子、d维单粒子与2维单粒子的乘积态	d维	单向演化算子U_o及其逆U_o^{-1}	d维单粒子测量	$\frac{1}{3x+2Q}$	$O(Lx)$

注：其中L表示投票信息长度，m表示选民ID号的位数[8]，x表示选民人数，d、δ为常数[17]，Q表示量子中心制备的量子态序列的份数.

综上所述，本文利用量子游走和半量子技术提出了多中心高效量子安全投票方案，该方案安全高效，便于实现和管理，更适用于大规模投票. 目前，量子计算本身仍处于科学探索阶段，尽管量子计算领域取得了诸多研究进展，但这些成果主要集中在科研层面，距离实际应用还有一定差距，在实际应用中可能面临一些挑战. 未来，半量子密码、量子游走等技术有望进一步应用到密码方案设计中，推动量子计算技术的成熟和应用场景的拓展.

参考文献

[1] BUSCH P, HEINONEN T, LAHTI P. Heisenberg's uncertainty principle[J]. Physics Reports, 2007, 452(6): 155-176.

[2] WOOTTERS W K, ZUREK W H. A single quantum cannot be cloned[J]. Nature, 1982, 299: 802-803.

[3] HILLERY M. Quantum voting and privacy protection: First steps[J]. SPIE Newsroom, 2006, 1: 1-21.

[4] VACCARO J A, SPRING J, CHEFLES A. Quantum protocols for anonymous voting and surveying[J]. Physical Re-

view A, 2007, 75: 012333.

[5] 宋秀丽, 曹耘凡, 杨帅. 基于d维三粒子纠缠态的量子投票表决方案[J]. 电子学报, 2020, 48(7): 1355-1360.
SONG X L, CAO Y F, YANG S. Quantum voting scheme based on d dimensional three-particle entangled state[J]. Acta Electronica Sinica, 2020, 48(7): 1355-1360. (in Chinese)

[6] 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, 34(6): 721.
LIU X H, WEN X J, FAN X C, et al. A secure quantum voting protocol based on four-particle GHZ-state[J]. Chinese Journal of Quantum Electronics, 2017, 34(6): 721. (in Chinese)

[7] 秦加奇, 石润华, 张瑞. 基于受控量子安全直接通信的量子投票协议[J]. 量子电子学报, 2018, 35(5): 558.
QIN J Q, SHI R H, ZHANG R. Quantum voting protocol based on controlled quantum secure direct communication[J]. Chinese Journal of Quantum Electronics, 2018, 35(5): 558. (in Chinese)

[8] 陈凯伦, 梁向前. 基于d维纠缠态的安全量子投票协议[J]. 山东科技大学学报(自然科学版), 2022, 41(1): 92-97.
CHEN K L, LIANG X Q. Secure quantum voting protocol based on d-level entangled state[J]. Journal of Shandong University of Science and Technology (Natural Science), 2022, 41(1): 92-97. (in Chinese)

[9] 冯雁, 王蕊聪. 基于量子傅里叶变换求和的量子投票协议[J]. 计算机科学, 2022, 49(5): 311-317.
FENG Y, WANG R C. Quantum voting protocol based on quantum Fourier transform summation[J]. Computer Science, 2022, 49(5): 311-317. (in Chinese)

[10] 彭宇辰, 孙莹, 李艳俊. 基于N粒子GHZ态的量子匿名投票协议[J]. 北京电子科技学院学报, 2022, 30(1): 86-93.
PENG Y C, SUN Y, LI Y J. Quantum anonymous voting protocol based on N-qubit GHZ states[J]. Journal of Beijing Electronic Science and Technology Institute, 2022, 30 (1): 86-93. (in Chinese)

[11] 谢四江, 毛贲豪. 双向隐私保护量子投票协议[J]. 北京工业大学学报, 2023, 49(6): 694-702.
XIE S J, MAO B H. Two-way privacy-protected quantum voting protocol[J]. Journal of Beijing University of Technology, 2023, 49(6): 694-702. (in Chinese)

[12] 石润华, 邓佳鹏, 于辉, 等. 基于量子行走公钥加密的电子投票方案[J]. 信息网络安全, 2024, 24(5): 732-744.
SHI R H, DENG J P, YU H, et al. Electronic voting scheme based on public key cryptography of quantum walks[J]. Netinfo Security, 2024, 24(5): 732-744. (in Chinese)

[13] BOYER M, KENIGSBERG D, MOR T. Quantum key distribution with classical bob[J]. Physical Review Letters, 2007, 99(14): 140501.

[14] BOYER M, GELLES R, KENIGSBERG D, et al. Semi-quantum key distribution[J]. CoRR, 2008, 1: 1-13.

[15] ZOU X F, QIU D W. Three-step semiquantum secure direct communication protocol[J]. Science China Physics, Mechanics & Astronomy, 2014, 57(9): 1696-1702.

[16] QIU C, ZHANG S B, CHANG Y, et al. Electronic voting scheme based on a quantum ring signature[J]. International Journal of Theoretical Physics, 2021, 60(4): 1550-1555.

[17] ZHANG C, HUANG Q, LONG Y X, et al. Secure three-party semi-quantum summation using single photons[J]. International Journal of Theoretical Physics, 2021, 60(9): 3478-3487.

[18] 张妍, 王明明. 基于单粒子的半量子投票协议[J]. 计算机与数字工程, 2022, 50(6): 1274-1277.
ZHANG Y, WANG M M. Semi-quantum voting protocol based on single-qubits[J]. Computer & Digital Engineering, 2022, 50(6): 1274-1277. (in Chinese)

[19] 李佩珊, 陈灵丽, 谢勇, 等. 高效的安全多方半量子求和协议[J]. 密码学报, 2023, 10(4): 786-795.
LI P S, CHEN L L, XIE Y, et al. Efficient secure multi-party semi-quantum summation protocols[J]. Journal of Cryptologic Research, 2023, 10(4): 786-795. (in Chinese)

[20] QIU S J, XIN X J, ZHENG Q, et al. Security analysis and improvements on a semi-quantum electronic voting protocol[J]. International Journal of Theoretical Physics, 2024, 63(3): 79.

[21] TIAN Y, ZHANG N, YE C Q, et al. Different secure semi-quantum summation models without measurement[J]. EPJ Quantum Technology, 2024, 11(1): 35.

[22] QIU S J, XIN X J, ZHENG Q, et al. Semi-quantum voting protocol with decentralization of vote verification and traceability[J]. Quantum Information Processing, 2024, 23(12): 402.

[23] AHARONOV Y, DAVIDOVICH L, ZAGURY N. Quantum random walks[J]. Physical Review A, 1993, 48(2): 1687-1690.

[24] 王锦涛, 李霞, 叶天语. 基于圆上单向量子游走的量子安全多方求和协议[J]. 中国科学: 物理学 力学 天文学, 2024, 54(4): 86-97.
WANG J T, LI X, YE T Y. A quantum secure multi-party summation protocol based on one-direction quantum walks on a circle[J]. Scientia Sinica (Physica, Mechanica & Astronomica), 2024, 54(4): 86-97. (in Chinese)

[25] CHEN L L, LI Q, LIU C D, et al. Efficient mediated semi-quantum key distribution[J]. Physica A: Statistical Mechanics and Its Applications, 2021, 582: 126265.

作者简介

张启帆 女,2001年10月出生于山西省临汾市. 现为北京电子科技学院硕士研究生. 主要研究方向为量子密码、量子区块链.
E-mail: a4424736670@163.com

孙 莹 女,1982年3月出生于山东省青岛市. 现为北京电子科技学院副教授. 主要研究方向为量子计算与密码协议.
E-mail: sunybesiti@foxmail.com

李艳俊 女,1979年2月出生于山西省晋城市. 现为中国电子科技集团公司第十五研究所高级工程师. 主要研究方向为密码协议设计分析、商用密码测评.
E-mail: liyjwuyh@163.com