计算机科学
COMPUTER SCIENCE

基于量子傅里叶变换求和的量子投票协议

冯雁，王蕊聪

引用本文

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 Yan, WANG Rui-cong. Quantum Voting Protocol Based on Quantum Fourier Transform Summation[J]. Computer Science, 2022, 49(5): 311-317.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210300058

基于量子傅里叶变换求和的量子投票协议

冯　雁[1,3]　王蕊聪[1,2]
1 北京电子科技学院网络空间安全系　北京 100070
2 西安电子科技大学计算机科学与技术学院　西安 710126
3 中国科技大学网络空间安全学院　合肥 230026
(fengy@besti.edu)

摘　要　针对传统电子投票存在用户信息易被窃取,而现有量子投票普遍计算效率较低的问题,提出了一种基于量子傅里叶变换求和与向量编码结合的量子投票协议,各方通过量子傅里叶变换将自己的保密数值以单粒子态的形式纠缠叠加到发起方手中进行投票,并通过向量编码实现对候选者票数的保密排序,由获胜者公布票数及排名。通过 IBM 提供的量子计算模拟器对协议量子傅里叶变换求和的正确性进行了验证。通过理论分析证明了协议在面对截取-重发攻击、纠缠测量攻击、共谋攻击以及监听方-候选者攻击这 4 类攻击时均有较好的安全性,且与现有同类型量子投票方案相比,协议的效率较高。

关键词:电子投票;量子傅里叶变换求和;向量编码;量子投票;IBM Q Experience
中图法分类号　TN918.1

Quantum Voting Protocol Based on Quantum Fourier Transform Summation

FENG Yan[1,3] and WANG Rui-cong[1,2]
1 Department of Cyberspace Security,Beijing Electronic Science and Technology Institute,Beijing 100070,China
2 School of Computer Science and Technology,Xidian University,Xi'an 710126,China
3 School of Cyber Science and Technology,University of Science and Technology of China,Hefei 230026,China

Abstract　To solve the problem that the user information is easy to be stolen in the traditional electronic voting,and the existing quantum voting generally has low computational efficiency,a quantum voting protocol based on the combination of quantum Fourier transform summation and vector coding is proposed. In the protocol,each particpant uses quantum Fourier transform to entangle their secret values into the hands of the initiator in the form of a single particle state to vote,and the secret ranking of candidates' votes is realized by vector coding,finally the winner announces the number of votes and ranking. The correctness of the quantum Fourier transform summation in the protocol is verified by the quantum computing simulator provided by IBM. Through theoretical analysis,it is proved that the protocol has good security against four kinds of attacks which are intercept-resend attack,entanglement measurement attack,collusion attack,monitor and candidate attack,and the efficiency of the protocol is higher than the existing quantum voting schemes of the same type.

Keywords　Electronic voting,Quantum Fourier transform summation,Vector coding,Quantum voting,IBM Q Experience

1　引言

作为一种对安全多方计算的实际应用问题,电子投票在现实工作和生活中扮演着非常重要的角色,小到班级干部的选举和村民代表的选举,大到国家领导人的选举,因此拥有一种高效且安全的投票系统就显得极为重要。自电子投票相关概念被提出后,国内外学者纷纷对保密投票协议开展了深入研究。1981 年,David 等[1]基于混合网与 RSA 公钥体制提出了第一个电子投票协议,该协议允许电子邮件系统隐藏参与者的通信对象以及通信内容。之后,学术界在对电子投票展开大量研究的同时发现,在计算机计算能力不断增强的大背景下,经典电子投票协议安全性保障不大的问题逐渐显露,2005 年文献[2]提出了量子投票这一概念,其首次将量子密码学的知识运用到投票过程中,为传统投票提供了新的思路。2006 年,Hillery[3]则根据量子现有的通信方式,为了弥补传统投票方案中安全性的不足,提出了两种投票模型,一种是分配式投票模型,另一种是移动式投票模型。Vaccaro 等则相应地在文献[4]中首次定义了量子投票需要满足的 4 项基本

到稿日期:2021-03-05　返修日期:2021-07-03
基金项目:国家重点研发计划(2018YFE0200600);安徽省量子通信与量子计算机重大项目引导性项目课题(AHY180500)
This work was supported by the National Key R&D Program of China(2018YFE0200600) and Anhui Province Guidance Project of Quantum Communication and Quantum Computer Major Projects(AHY180500).
通信作者:王蕊聪(1193238657@qq.com)

准则，并提出了比较投票的概念，即每次仅限于两个投票者参与，通过比较两个投票者投票操作的异同来判断投票信息，这种方案主要用于二进制投票，投 1(支持)或 0(反对)两种操作。根据 4 项基本准则，研究者们在量子投票方向[5-7]展开了大量研究，弥补了上述方案的不足，扩大了投票者的参与功能。为减小操作复杂度，还出现了基于量子纠缠态[8-10]的匿名投票方案。例如，Liu 等于 2017 年基于四粒子多重态提出了一种新的安全量子投票协议[11]。与以往的协议相比，该协议角色全面且都能实质性地参与投票的相关活动，避免了使用复杂的量子指纹函数，在技术上易于实现；但该方案收集投票时需要执行多次协议，效率较低。2020 年，Song 等为了突破三维 Hilbert 空间的限制，基于 *Shamir*(t,n)门限思想，设计了基于 d 维三粒子纠缠态的量子投票方案[12]，该方案不仅增强了协议适用性，并且以单粒子为投票载体提升了传输效率；但该方案在小基数投票时效率较低，且无法防止内部参与者的合谋攻击。

本文受文献[13]中关于向量编码以及文献[14]中基于量子傅里叶变换的安全多方量子求和[15-17]的启发，将向量编码与安全多方量子求和方法相结合，提出了一种新型量子投票协议，该协议不仅能够满足量子投票的基本安全性，且一轮即可收集到所有参与者的投票，简单、安全且效率较高。

2 预备知识

2.1 安全性定义

安全多方计算一般研究的是半诚实参与者模型下的保密计算问题。半诚实参与者执行协议的主要特点是会诚实执行协议所要求的步骤，但会尝试对自己的输入和得到的中间数据进行推导并窃取保密信息。如果参与者无法获得保密信息，则认为协议过程是安全的。协议的安全性定义如图 1 所示。

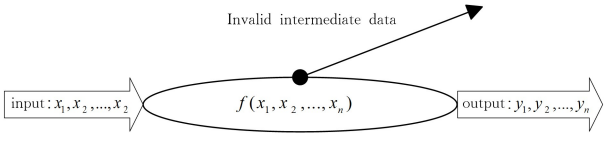

图 1 安全性定义

Fig. 1 Security definition

根据文献[18]中关于协议的安全性定义可知，在半诚实参与者模型下，如果存在 n 元计算函数 f(f_i 表示第 $i\in\{1,2,\cdots,n\}$个计算结果)使得概率多项式时间算法 S 成立，则认为协议是安全的。概率多项式时间算法 S 的表达式如下：

$$\{S(x_i,f_i(x_1,x_2,\cdots,x_n)),f(x_1,x_2,\cdots,x_n)\}\overset{c}{\equiv}\{v_i^{\pi}(x_1,x_2,\cdots,x_n),O^{\pi}(x_1,x_2,\cdots,x_n)\} \tag{1}$$

其中，$x_i\in\{x_1,x_2,x_3,\cdots,x_n\}$是 n 名参与者 $P_1,P_2,P_3,\cdots,P_n$ 的秘密数据，π 表示计算该函数的协议，执行协议 π 时 P_i 得到的中间数据 r_i 及所有信息可记为 v_i^{π}，即$(x_i,r_i,m_i^1,\cdots,m_i^t)$，其中 m_i^j 表示参与者 P_i 第 j 次收到的信息。在执行完协议 π 之后，协议最终输出信息记为 O^{π}。在协议执行过程中，半诚实参与者 P_i 希望在不泄露自身保密数据的情况下安全地得到函数结果 f_i。

2.2 安全多方量子排序

本方案使用基于量子求和的安全多方量子排序协议[19]来对投票和结果进行排序，各方根据排序结果公布排名即可。该协议中，n 名参与者 $P_1,P_2,P_3,\cdots,P_n$ 分别拥有保密数值 $s_1,s_2,s_3,\cdots,s_n$，且保密数值各不相等。协议中通过向量编码将排序转化为求和方式进行，各参与者可在不泄露自身保密数值的情况下获得自己的数值在整个序列中保密排序后的位置。

安全多方量子排序协议的具体向量编码规则为：$P_1,P_2,P_3,\cdots,P_n$ 各自拥有秘密 $s_i\in\{1,2,\cdots,n\}$，每个参与者将各自的秘密数值 s_i 用一个长度为 N 的向量表示为 $\boldsymbol{V}_i=(x_{i1},x_{i2},\cdots,x_{in})$，如果 $1\leqslant j<s_i$，则 $x_{ij}=0$；若 $j\geqslant s_i$，则 $x_{ij}=1$，其中 $1\leqslant j\leqslant n$，如 $s=3,n=8$，则根据向量编码规则表示为 $\boldsymbol{V}_i=(0,0,1,1,1,1,1,1)$，当 $s_i=1$ 时，该向量用 $\boldsymbol{V}_i=(1_{i1},1_{i2},\cdots,1_{in})$表示。

只要选定一位发起方按向量的列进行保密求和，求和后将该结果公布即可。根据量子傅里叶变换以及纠缠态纠缠交换的本质，求和过程具体如下：首先，由多方量子求和的发起方对准备的随机态进行初始化傅里叶变换，并将辅助态$|j\rangle_t$发送给第一个参与者，由该参与者对$|j\rangle_t$进行 D_j 操作。D_j 操作符定义为：

$$D_j:|j\rangle_t|x_i\rangle\rightarrow|j\rangle_tU^j|x_i\rangle \tag{2}$$

$$U|x_i\rangle=e^{2\pi i\frac{x_i}{N}}|\boldsymbol{x}_i\rangle \tag{3}$$

式(2)中，下标 t 代表该粒子发送到量子信道中，$|j\rangle_t$ 表示辅助态，该辅助态由发起方生成并发送给对应的参与者，每位参与者都会传递$|j\rangle_t$，用于辅助求和计算。$|\boldsymbol{x}_i\rangle$即为算符 U 的一个特征值为 $e^{2\pi i\frac{x_i}{N}}$ 的特征向量。

发起方将$|j\rangle_t$发送给第一个参与者，该参与者对$|j\rangle_t$进行 D_j 操作后再发送给下一位参与者，每个参与者执行相同的过程，最后一个参与者将$|j\rangle_t$返还给发起方，由发起方执行傅里叶逆变换，最终取得多方参与者和的取模结果 $\sum_{k=1}^{n}x_k \bmod N$，其中 N 表示所有参与排序数值的最大值。理论上，发起方需要求取 N 列的和，获得数字序列：$\sum_{i=1}^{n}x_{i1} \bmod N$，$\sum_{i=1}^{n}x_{i2} \bmod N$，$\sum_{i=1}^{n}x_{i3} \bmod N$，$\sum_{i=1}^{n}x_{i4} \bmod N$，$\cdots$。发起方将该数字序列公布，该序列即为 s_i 的由小至大的升序排序序列，各参与者寻找自己对应的序列号 s_i，该序列号对应的数值即为各参与者的排名。

3 量子投票协议

本投票协议主要由三方参与者构成，包括投票者、候选者以及监听方。各参与者的具体任务如下：

(1)投票者。每个投票者都有投票的权利，可以对候选者进行投票，但是单个投票者支持的票数不得超过候选人数的一半。

(2)候选者。候选者参与投票协议过程，可以被投票者投票，但是不具备投票权利，需要参与排序计算。

(3)监听方。用于监听候选者是否存在作弊行为，一般从投票者中随机选取，也可以单独使用半诚实第三方进行监听。

假设在一次投票选举活动中，共有 n 个投票者(半诚实)，所有的投票者需要对 m 名候选者进行投票选举，并选出前 k 名候选者作为投票获胜者。投票、计票在各个投票者之间是保密的，并且他们都会保证自己选票的投出，每个投票者对候选者的选票可用 0 或 1 表示(其中，1 表示为该候选者投出一票，0 为弃权或不投该候选者)。m 位候选者将会得到自己的票数，随即参与排序协议，进行保密排序，最后由前 k 名候选者公布结果。

协议由 n 个投票者 $P_1,P_2,P_3,\cdots,P_n$(半诚实)和 m 个候选者 $C_i\in\{C_1,C_2,\cdots,C_m\}$以及两个监听方 P_k,P_0 组成，每个投票者拥有各自的秘密选票 $|x\rangle_i$，且 $|x\rangle_i\in\{|x_1\rangle_i,|x_2\rangle_i,|x_3\rangle_i,\cdots,|x_m\rangle_i\}$。协议执行过程如下：监听方 P_k,P_0 均可在参与者中随机选取，也可由半诚实第三方担任，P_k 主要在步骤 5 中防止投票者作弊以及在步骤 10 中恢复数据，防止候选者在排序过程中传输虚假信息。监听方 P_0 主要防止候选者在排序过程中进行窃听等作弊行为。

3.1　投票准备阶段

步骤 1　候选者 C_i 准备一个 n-bit 长的基态 $|x_0\rangle_h$(其中 n 为投票者的个数)，并且 $|x_0\rangle_h$ 是 C_i 的私有态，C_i 对 $|x_0\rangle_h$ 应用量子傅里叶变换得到纠缠态 $|\phi_1\rangle=QFT\ |x_0\rangle_h=\frac{1}{N}\sum_{j=0}^{N-1}e^{2\pi i\frac{x_0}{N}j}|j\rangle_h$，准备另一个 n-bit 的辅助态 $|0\rangle_t$，对 $|\phi_1\rangle|0\rangle_t$ 执行 n 个 CNOT 门后并对该量子纠缠态执行一个 C_i 选定的随机 U 操作，得到纠缠态 $|\phi_2\rangle=U\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{x_0}{N}j}|j\rangle_h\ |j\rangle_t$。

3.2　投票阶段

步骤 2　由系统随机轮转选定一个序号 k，候选者选择该序号的投票者作为监听方 P_k，C_i 此时将准备好的纠缠态 $|\phi_2\rangle$ 发送给选定的监听方 P_k，P_k 将 $|\phi_2\rangle$ 中的辅助量子态 $|j\rangle_t$ 通过默认量子信道发送给投票者 P_1。

步骤 3　投票者 P_1 接收到辅助量子态 $|j\rangle_t$，首先准备自己的私有选票粒子态 $|x_i\rangle_1$；然后对 $|j\rangle_t\ |x_i\rangle_1$ 应用一个操作符 D_j(其中 $|x_i\rangle_1$ 即为操作符 D_j 的一个特征值为 $e^{2\pi i\frac{x_j}{N}}$ 的特征向量)，投票者 P_1 将私有粒子 $|x_i\rangle_1$ 保留，并将 $|j\rangle_t$ 通过量子信道发送给下一个投票者 P_2，投票者 P_2 重复执行 P_1 的步骤，依次类推，直至 n 个投票者均完成投票操作。根据量子态纠缠的性质，监听方 P_k 手中的纠缠态 $|\phi_2\rangle$ 会纠缠交换成 $|\phi_3\rangle=U\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}|j\rangle_h\ |j\rangle_t\ |x_i\rangle_1\cdots|x_i\rangle_n$。

步骤 4　投票者 P_n 投票结束后，需要将 $|j\rangle_t$ 发送给监听方 P_k，P_k 认证投票结束，并对 $|\phi_3\rangle$ 执行 n 个 CNOT 门，得到 $|\phi_4\rangle=U\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}|j\rangle_h\ |0\rangle_t|x_1\rangle\cdots|x_n\rangle$。

3.3　票数统计阶段

步骤 5　监听方 P_k 在适当测量基上测量第二个 n-bit 位的粒子($|j\rangle_t$)，如果测量 n 个 bit 位的结果均为 $|0\rangle$，则继续下一步，否则认为可能有第三方攻击者窃取并修改了中间数据，立即结束本次交互。本次协议无效，从步骤 1 重新开始执行协议。

步骤 6　P_k 将傅里叶逆变换应用于纠缠态 $|\phi_4\rangle$，得到 $|\phi_5\rangle=U|\omega\rangle=U\sum_{k=1}^{n}x_k\bmod N$。$P_k$ 将自己手中目前持有的量子态发送给 C_i，C_i 对其执行之前选定的随机 U 操作对应的逆操作 U^{-1}，得到 $U^{-1}U|\omega\rangle=\sum_{k=1}^{n}x_k\bmod N$。因此，当投票者、候选者按步骤诚实地执行该协议时，候选者 $C_2,C_3,\cdots,C_m$ 将会正确地得到多方参与者投票和的取模结果 $\sum_{i=1}^{n}x_{i2}\bmod N$，$\sum_{i=1}^{n}x_{i3}\bmod N,\sum_{i=1}^{n}x_{i4}\bmod N,\cdots$。

3.4　票数排序阶段

步骤 7　由上述步骤可知，$C_1,C_2,\cdots,C_m$ 得到各自的投票和 $s_i\in\{1,2,\cdots,m\}$，每个候选者将各自的秘密数值 s_i 按照 2.2 节使用的向量编码规则对自己的保密数值进行向量编码；每个候选者可得到 $V_i=(x_{i1},x_{i2},\cdots,x_{in})$(其中 n 为候选者的个数)。

步骤 8　首先监听方 P_0 准备一个 m-bit 长的随机的基态 $|x_0\rangle_h$，$m=\log_2 N$(其中 N 为上述的向量长度)且 $|x_0\rangle_h$ 是 P_0 的私有态，然后 P_0 对 $|x_0\rangle_h$ 应用量子傅里叶变换得到 $|\phi_1\rangle$。P_0 再准备另外一个 m-bit 的辅助态 $|0\rangle_t$，并对 $|\phi_1\rangle|0\rangle_t$ 执行 m 个 CNOT 门得到 $|\varphi_2\rangle$。每个候选者 C_i 都根据自己的向量 $\boldsymbol{V}_i=(\boldsymbol{x}_{i1},\boldsymbol{x}_{i2},\cdots,\boldsymbol{x}_{in})$ 准备 n 个私有粒子态 $|x_1\rangle_i,|x_2\rangle_i,|x_3\rangle_i,\cdots,|x_n\rangle_i$。之后执行步骤 2－步骤 5，$P_0$ 得到 $|\phi_5\rangle$，并对第一个 m-bit 粒子执行量子傅里叶逆变换，得到 $|\omega\rangle=\sum_{k=1}^{n}x_k\bmod N$。

步骤 9　监听方 P_0 针对 $C_1,C_2,\cdots,C_m$ 各自拥有的向量 $\boldsymbol{V}_i=(\boldsymbol{x}_{i1},\boldsymbol{x}_{i2},\cdots,\boldsymbol{x}_{in})$ 按列重复执行步骤 8，则 P_0 最终可获得一段数字序列：$\sum_{i=1}^{n}x_{i1}\bmod N,\sum_{i=1}^{n}x_{i2}\bmod N,\sum_{i=1}^{n}x_{i3}\bmod N,\sum_{i=1}^{n}x_{i4}\bmod N,\cdots$。$P_0$ 公布这段数字序列，序列即为 s_i 由小至大的升序排序序列，各候选者寻找自己对应的序列号 s_i，该序列号对应的数值即为各候选者的排名。

步骤 10　前 k 名候选者主动公布自己的票数以及排名，并且同时公布之前选择的随机 U 操作及 U^{-1} 操作。前 k 名候选者对应之前选择的随机监听方 P_k 公布自己拥有的量子态 $|\phi_5\rangle$，并对自己手中的量子态执行 U^{-1} 操作，得到 $\sum_{k=1}^{n}x_k\bmod N$ 后公布，与各候选者公布的票数进行核对。如果核对正确，则认为协议过程安全，否则认为该候选者没有诚实执行排序步骤 7—步骤 9，判定该候选者的票数无效。如果有参与者不信任监听方 P_k 计算的结果，可自行通过对量子态 $|\phi_5\rangle$ 执行 U^{-1} 操作，以进行核对。

3.5　关键计算

3.5.1　U 操作的选取

协议的步骤 1 中，监听加密所用到的 U 算子应该如何选取，以及选取后应如何进行恢复操作是协议的关键计算之一。根据投票协议可知，选择加密算子 U 参与计算后，在候选者公布投票结果时需要同时公布采用的加密算子以及对应的逆操作，以便监听方 P 恢复出需要的信息，并与候选者公布的投票信息进行核对，以防止候选者排序过程中发生作弊。U 算子和对应的逆操作如表 1 所列。

表 1 U 算子和 U^{-1} 算子的矩阵形式

Table 1 Matrix form of U operator and U^{-1} operator

Operator matrix form	U operator	U^{-1} operator
$\boldsymbol{X}=\begin{bmatrix}0&1\\1&0\end{bmatrix}$	$\boldsymbol{X}$	$\boldsymbol{X}$
$\boldsymbol{Y}=\begin{bmatrix}0&-i\\i&0\end{bmatrix}$	$\boldsymbol{Y}$	$-\frac{1}{i^2}\boldsymbol{Y}$
$\boldsymbol{Z}=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$	$\boldsymbol{Z}$	$\boldsymbol{Z}$
$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$	$\boldsymbol{H}$	$\boldsymbol{H}$
$\boldsymbol{I}=\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\boldsymbol{I}$	$\boldsymbol{I}$

U 算子主要从基础酉操作$\{\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z},\boldsymbol{H},\boldsymbol{I}\}$中由候选者进行随机选择，解密算子采用表 1 中对应的 U^{-1} 操作即可，也可将以上基础酉操作的复合操作作为 U 算子，例如将酉操作 XZ 作为 U 算子，解密算子即为 $U^{-1}=Z^{-1}X^{-1}$。

3.5.2 量子傅里叶变换及逆变换

协议中的安全多方量子求和主要基于量子傅里叶变换来完成。根据文献[17]中对该量子傅里叶变换的定义，对未知量子态$|x\rangle$进行傅里叶变换的定义为：

$$QFT:|x\rangle\rightarrow\frac{1}{N}\sum_{y=0}^{N-1}e^{2\pi i\frac{x}{N}y}|y\rangle \tag{4}$$

对量子态$|y\rangle$进行傅里叶逆变换的定义为：

$$QFT^{-1}:|y\rangle\rightarrow\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-2\pi i\frac{y}{N}x}|x\rangle \tag{5}$$

且存在右边定义：

$$\sum_{y=0}^{N-1}e^{2\pi i\frac{x}{N}y}=\begin{cases}0, & \text{if } x\neq 0 \bmod N\\ N, & \text{if } x=0 \bmod N\end{cases} \tag{6}$$

因此，步骤 6 中$|\phi_4\rangle$经过傅里叶逆变换得到$|\phi_5\rangle$的计算式如下：

$$\begin{aligned}
&QFT^{-1}U\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}|j\rangle_h\right)\\
&=U\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}QFT^{-1}|j\rangle_h\\
&=U\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}\left(\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}e^{2\pi i\frac{j}{N}j}|l\rangle_h\right)\\
&=U\frac{1}{N}\sum_{j=0}^{N-1}\sum_{l=0}^{N-1}e^{2\pi i\frac{(\sum_{k=1}^{n}x_k)-l}{N}j}|l\rangle_h\\
&=U(\frac{1}{N}\sum_{j=0}^{N-1}|\sum_{k=0}^{n}x_k \bmod N\rangle_h+\frac{1}{N}\sum_{j=0\wedge l\neq\sum_{k=1}^{n}x_k \bmod N}^{N-1}\\
&(\sum_{j=0}^{N-1}e^{2\pi i\frac{(\sum_{k=1}^{n}x_k)-l}{N}j})|l\rangle_h)\\
&=U(|\sum_{k=0}^{n}x_k \bmod N\rangle_h+\frac{1}{N}\sum_{j=0\wedge l\neq\sum_{k=1}^{n}x_k \bmod N}^{N-1}0\cdot|l\rangle_h)\\
&=U|\sum_{k=0}^{n}x_k \bmod N\rangle_h
\end{aligned} \tag{7}$$

3.6 实验结果

本文的实验重点是关于量子安全多方求和计算到逻辑电路的实现。本协议为 n(投票者)选 m(候选者)的量子投票，在 IBMQ 平台上，以 $n=8$，$m=3$ 为例，即由 8 个投票者(P_1，P_2，…，P_8)为 3 个候选者(A，B，C)投票，每个投票者有小于等于 2 票的投票权，设置投票规模如表 2 所列(其中，1 表示为该候选者投出一票，0 为弃权或不投该候选者)。投票者投票完成后，候选者通过排序电路实现对收集到的票数的保密排序，并由第一名候选者公布自己的排名、票数以及选定的 U 操作，由实验过程中提前选定的监听方通过 U 操作解密，实现对第一名候选者的票数核对，最终完成投票。

表 2 参与者候选者投票规模

Table 2 Voting scale of participants and candidates

Participants/Candidates	A	B	C
P_1	0	1	0
P_2	1	0	1
P_3	1	1	0
P_4	0	1	1
P_5	1	1	0
P_6	0	1	0
P_7	1	0	0
P_8	0	0	1

实验结果如图 2 所示。由发起排序的候选者公布结果，每位候选者根据自己的票数查看排名，此处 A 票数为 4，则根据图 2 查看横坐标 4 对应的纵坐标数值是 2，因此 A 在 3 人中的排名为 2。同理，B 票数为 5，排名为 3，C 的票数为 3，排名为 1。由于此排名是按照由小到大的顺序排序的，候选者只需将自己的排名逆置，从而得到自己的票数从大到小的实际排名($B=5$，$A=4$，$C=3$)，A 的排名即为 2，B 的排名为 1，C 的排名为 3。因此，B 的票数最多，B 可公布自己的票数和排名。

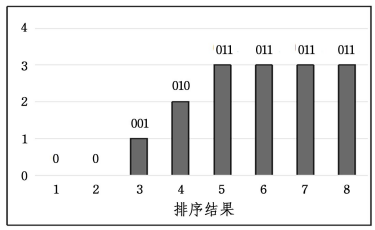

图 2 排序后的投票结果

Fig. 2 Sorted voting results

4 协议的安全性分析

本协议中，协议安全主要指数据隐私和计算过程的安全性，即投票者、候选者数据(量子态信息)的隐私安全性，以及所有参与计算的参与者计算过程的安全性。本节重点分析计算过程中量子态纠缠时是否安全，以及不诚实参与者如果进行攻击，协议是否可以检测到该攻击以保证投票协议过程的安全性。

(1)截取-重发攻击

协议采用对步骤 1 中的辅助量子比特进行检测，来避免截取-重发攻击。在协议中，投票者事实上并没有将自己的私有数据通过量子信道传送，而是将自己的私有态通过 D_j 操作与初始量子系统进行复合，得到纠缠态，再根据适当的傅里叶

逆变换操作来得到求和结果。假设有攻击者通过量子信道获取到 P 发送的中间数据，攻击者得到的中间数据只有 $|j\rangle_t$，攻击者一旦对其进行测量，该量子复合系统就会发生纠缠交换，P 手中拥有的量子态会塌缩。在步骤 5 中，P 对复合系统进行 CNOT 门还原，再对 $|j\rangle_t$ 进行测量，理论上，如果没有攻击者攻击，则可以测得 $|j\rangle_t$ 为 $|0\rangle_t$，但是由于攻击者发起攻击，使之前的数据塌缩，P 可以正确获得 $|j\rangle_t$ 刚好为 $|0\rangle_t$ 的概率为 $1/2^N$，因此 P 基本可认为手中的数据是绝对安全的，因为 P 有 $(1-1/2^N)$ 的概率会发现信息被窃取，可以立即停止当前协议，废除数据，重新开始协议并进行计算。同理，攻击者对 P_1 及其他参与者采取这样的攻击都适用上述分析，因此协议可以抵御截取-重发攻击。

(2)纠缠测量攻击

纠缠测量攻击分两种情况进行分析：1)投票者对协议过程中收到的中间数据进行攻击；2)投票者对投票者进行攻击。

1)P_1 测量辅助量子比特 $|j\rangle_t$，显然他可以以相同概率 1/2 得到 $|j\rangle$($j\in\{0,1\}$)，然而测量结果 j 与 P 手中的纠缠态没有关系，也无法推导出更多数据，因此这样的攻击无效。

2)在将 D_j 操作算子应用于辅助比特 $|j\rangle_t$ 后，P_2 再次测量它。P_2 知道 P_1 的秘密状态 $|x_1\rangle$ 已经演化成与基于量子傅里叶变换的辅助态 $|j\rangle_t$ 相同的状态。因此，他可以在辅助态 $|j\rangle_t$ 上执行量子傅里叶逆变换，期望提取 $|x_1\rangle$。其攻击描述如下：

$$
\begin{aligned}
&QFT^{-1}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{x_1}{N}\right)j}|j\rangle_h|j\rangle_t\\
&=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{x_1}{N}\right)j}|j\rangle_h QFT^{-1}|j\rangle_t\\
&=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i(\frac{x_1}{N})j}|j\rangle_h\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{-2\pi i\frac{j}{N}l}|l\rangle_t\right)\\
&=\frac{1}{N}\sum_{l=0}^{N-1}\sum_{j=0}^{N-1}e^{2\pi i\frac{x_1-l}{N}j}|j\rangle_h|l\rangle_t
\end{aligned}
\tag{8}
$$

通过上述推导，P_2 如果测量辅助态，则会以等概率 1/2 得到 $|l\rangle_t$($l\in\{0,1\}$)。这意味着 P_2 无法获得任何关于 P_1 的秘密信息，因为他不能从具有下标 h 和 t 的纠缠量子系统的部分量子位中提取全局相位信息。事实上，任何局部酉算子都是这样，除非直接测量，否则部分量子位不能完全分离复合系统的纠缠。因此，P_2 即使执行这种攻击，也无法得到任何关于 P_1 的私密信息 $|x_1\rangle$，因此纠缠测量攻击无效。

(3)共谋攻击

假设存在两个不诚实的投票者相互共谋，想要获得其他投票者的选票或者组织其他投票者参与投票。例如，投票者 P_1 和 P_3 不想投票者 P_2 参与投票，在协议步骤 3 中，P_1 可以跳过 P_2，将需要传送的量子态 $|j\rangle_t$ 直接发送给 P_3，同时，为避免 P_2 发现这样的攻击行为，P_1 伪造一个 $|j\rangle_t$ 发送给 P_2，P_2 执行完投票操作后会继续将该量子态发送给 P_3，P_3 可以根据 P_2 发送给自己的内容进行对应 $|j\rangle_t$ 的逆操作，从而获得 P_2 的选票，之后继续按照 P_1 发送的量子选票进行操作，并继续往下发送。这样的攻击方式虽然能够获得 P_2 的选票，但是会被发起方察觉。因为在协议最开始时发起人不仅对手中的量子态进行了傅里叶变换，还添加了 n-bit 的 $|0\rangle_t$ 作为辅助量子，并对 $|\varphi_1\rangle|0\rangle_t$ 执行了 CNOT 门作为安全检测手段，在恢复协议时，会再次执行 CNOT 门来抵消之前的 CNOT 门，将辅助量子恢复成 $|0\rangle_t$。显然，如果 P_1 和 P_3 执行共谋攻击，将会导致辅助量子态 $|j\rangle_t$ 从 P_1(不含 P_1)往后的每一位无法正确恢复成 $|0\rangle$，只能按概率分布成 0 或 1，因此监听方会发现这样的攻击，并且可以根据无法正确恢复成 $|0\rangle$ 的位置来判断攻击者的编号，有较大概率可以锁定共谋的攻击者，因此此攻击无效。

(4)监听方、候选者攻击

由于规定所有参与方都是半诚实的，即会诚实地执行协议步骤，但其会试图通过中间数据窃取选票信息，或伪造部分信息来影响最终结果。监听方和候选者在协议计算过程中接触到的纠缠态是无法从中单独提取投票者信息的[19]，因此监听方和候选者无法窃取投票信息。

如果监听方 P_k 试图伪造或者破坏投票，其可操作的步骤为步骤 6 和步骤 10，他可以在步骤 6 中发送假的量子态 $|\phi_5\rangle$，这会导致步骤 6 中候选者执行 U^{-1} 操作几乎无法得出正确结果，因此可认定监听方试图破坏投票。同理，步骤 10 中监听方如果公布假的量子态 $|\phi_5\rangle$ 也会导致无法计算出正确结果。由于监听方的量子态和候选者的 U^{-1} 操作都会被公布，因此对监听方操作结果有怀疑的任意参与方均可自行计算核对。如果对计算结果存在怀疑，认为监听方作弊，则可作为发起方重新对该候选者执行投票协议。

如果候选者试图伪造或破坏投票，其可操作的是步骤 7 或步骤 10。在步骤 7 中，所有候选者需要对自己的票数进行向量编码，并参与排序，此处候选者可以伪造自己的投票并参与排序。在步骤 10 中，监听方执行 U^{-1} 操作后在核对票数时能够发现该候选者作弊。或者候选者在步骤 10 中伪造 U^{-1} 操作，但这会导致监听方对 $|\phi_5\rangle$ 进行 U^{-1} 操作时几乎无法得出正确的结果，候选者的目的应该是希望监听方核对的结果与自己公布的一致，伪造 U^{-1} 操作无法得到正确结果。协议中的监听方是随机选取的匿名投票者，但如果不可避免地出现了监听方候选者的合谋攻击，则可由对结果产生怀疑的参与方作为发起方，再次执行协议，对该候选者进行投票，这样虽然会消耗一定的资源，但能够更好地保证协议的安全性。

此外，根据协议在各方的安全性来分析本协议与其他量子投票的安全性情况。首先本协议满足文献[5]提出的关于量子投票应该满足的 4 项基本准则：匿名性、唯一性、全隐私性以及无收据性。在此基础上，本协议使用安全多方量子求和来组织投票，可以防止投票者对同一候选者的多次投票，实现了不可重用性，且本协议在传输过程中由于量子态相互纠缠，使得在实现投票者匿名投票的同时，也使得投票是可验证的，进一步防止了不诚实候选者参与排序时上传虚假票数。与经典的两种量子投票协议进行对比，主要对可验证性、匿名性、不可重用性以及是否可以抵抗量子攻击中几种常用的攻击手段等方面进行具体比较，结果如表 3 所列。

表 3 协议安全性对比分析

Table 3 Comparison and analysis of protocol security

Protocol	Verifiability	Anonymity	Immobility	Quantum channel detection	Resistance to collusive attacks	Resistance to entangle measurement attacks
Vaccaro's[5]	No	Yes	No	No	Yes	Yes
Li's[6]	No	Yes	No	No	No	Yes
This protocol	Yes	Yes	Yes	Yes	Yes	Yes

5 协议的效率分析

本节选取可进行效率对比的两种经典的具有代表性的量子投票方案进行对比分析，根据文献[20]，量子安全投票的效率由以下公式得出：

$$\eta=\frac{c}{q+b}\times\frac{1}{t} \tag{9}$$

其中，c 是要传输的秘密信息，q 是传输过程中会用到的量子比特数，b 是传输过程中要用到的经典比特数，t 是计算票数的轮次。

在文献[21]提出的 TZL 量子投票方案中，采用了四量子纠缠 GHZ 态，由三方通信组成，在投票过程中由监听方认证投票者的身份，然后制备量子票$|+\rangle$，随后提出了基于受控量子安全直接通信的投票协议，使用了三量子纠缠 GHZ-like 态作为量子通道，减少了资源的浪费，且考虑到了投票过程中被攻击的可能性。本协议则直接使用量子傅里叶变换来进行纠缠交换，在极大提高安全性的同时，也从计算轮次方面提高了协议效率。在 TZL 方案中，传输的秘密信息 c 为 1，即投票信息(赞成 1，反对 0)。而量子比特数 q 为 5，除了监听方制备的四量子 GHZ 纠缠态，还有投票者已有的量子态 b，该方案所用到的经典比特数 b 为 7。其次，计算完一轮票数需要进行 n 次该协议，因此效率 $\eta_{TZL}=\frac{c}{q+b}\times\frac{1}{t}=\frac{1}{5+7}\times\frac{1}{n}=\frac{1}{12n}$。而文献[22]提出的基于受控量子安全直接通信的投票协议，在传输信息的模式上与 TZL 方案相同，但是在效率方面有所改进，可以不考虑信道检测所耗费的量子态，传输的秘密信息 c 为 2，可传输两位经典比特，即投票信息(赞成 11，反对 00，弃权 10/01)，因为需要两个三量子 GHZ-like 态，所以用到的量子比特数 q 为 6，其经典比特数为 8，计算完一轮票数需要进行 n 次该协议，因此效率为：

$$\eta_{TZL^{改}}=\frac{c}{q+b}\times\frac{1}{t}=\frac{2}{6+8}\times\frac{1}{n}=\frac{1}{7n}。$$

反观本协议，传输秘密信息 c 为 n，即投票信息(赞成 1，反对/弃权 0)。而基于傅里叶变换的投票没有用到经典比特，而用到的量子比特数 q 为投票者数量和被投票的候选者之和 $n+1$。本方案中计算完一轮票数只需要执行 1 次本协议，但是秘密信息 c 需要被传递 n 次，根据式(9)可得本协议的效率为 $\eta_{QFT}=\frac{c}{q+b}\times\frac{1}{t}=\frac{n}{n+1+0}\times\frac{1}{n}=\frac{1}{n+1}$。协议效率的具体比较结果如表 4 所列。

表 4 协议效率的对比分析

Table 4 Comparison and analysis of protocol efficiency

Protocol	Need ballots	Quantum resources	Measuring operation	Communication method	Efficiency
TZL's protocol[21]	Yes	GHZ	GHZ states analysis	QOT	$1/12n$
Modified TZL Protocol[22]	No	GHZ-like	Bell states analysis	CDSDC	$1/7n$
This protocol	No	QFT entangled states	Direct projection analysis	Based on QFT entangled superposition	$1/(n+1)$

在解决问题时，传统算法的复杂度需要考虑时间复杂度和空间复杂度，但是在量子通信中，由于是分布式系统，因此强调参与者之间交换信息的次数及信息数据量的多少，即通信复杂度。通信次数越少，通信数据量越低，则认为通信复杂度越低。从表 4 可以看出，本文提出的量子投票协议在量子比特数的利用率上大幅高于另外两种投票协议，而之前的量子投票协议方案大多是基于多粒子纠缠态，即通过多方验证的方式来传递一位投票者的选票，每增加一个投票者就增加一轮协议的通信次数，这在大型投票活动中的效率上是十分不利的，其不仅使计算复杂度大幅提升，而且投票者增多后，通信复杂度也会大幅提升，计算时间也会随着投票者数量的增多而大幅增加。而本文的协议在通信过程中，无论人数多少，每个人只需要进行一次通信交换，相比现有的量子投票协议，通信复杂度已经大大降低。

此外，还有轮次复杂度指标，即协议完成所需计算量需要执行协议的次数。在完成计算的前提下尽可能降低轮次复杂度是保证信息安全的一个非常重要的措施，这对于非局域空间下的信息交换非常重要。表 4 中的 TZL 和改进 TZL 量子投票协议，一轮次只能收集一个投票者的投票，随着投票者数量的增多，需要不断地重复执行协议，这还没有包括如果存在攻击者需要废除当前进行的协议而需重新执行的情况。反观本文的量子投票协议，随着投票者数量的增加，只需要提供投票者数量对应的量子比特，协议仍然是一轮可收集到所有人的投票。由此看来，本文投票协议应用前景明显优于另外两种协议。

结束语 本文基于量子傅里叶变换求和，设计出了一种安全多方量子投票协议，可求取多方参与者的投票，从而获得投票和，并通过向量编码方式将排序转化为求和问题来取得投票排序结果，该排名只需公布即可。相比其他量子投票协议，本协议只需执行 $O(n)$ 轮次就能完成投票，一定程度上降低了通信及计算开销。在 IBM Q 平台上对协议核心的量子求和方案进行了验证，可知协议正确有效。同时，理论分析了

协议的安全性，在量子投票模式下能够抵御恶意攻击者的截取-重发攻击，以及 $n-2$ 名以下参与者的联合攻击等。

与现有量子投票方案相比，本文协议虽然在效率方面有较大的提高，但由于消耗的量子比特数较多，因此实际应用时对量子计算机的计算能力要求较高。未来，如何在保证协议安全性的同时更高效地使用量子比特，可能是协议改进的一个重要研究方向。

参 考 文 献

[1] DAVID C. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-90.

[2] CHRISTANDL M, WEHNER S. Quantum Anonymous Transmissions[C]// Proceedings of 11th ASIACRYPT. Berlin: Springer, 2005: 217-235.

[3] HILLERY M. Quantum voting and privacy protection: first steps[J]. SPIENewsroom, 2006, 10: 1117.

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

[5] DU G, ZHOU B M, MA C G, et al. A Secure Quantum Voting Scheme Based on Orthogonal Product States[J]. International Journal of Theoretical Physics, 2021, 60(4): 1374-1383.

[6] WANG Q. Application of blind signature in electronic voting system based on coding [J]. Digital World, 2020, 179(9): 5-6.

[7] YANG Y T, ZHAO Y, ZHANG Q L, et al. Homomorphic Weighted Electronic Voting System Based on SEAL Library [J]. Chinese Journal of Computers, 2020, 43(4): 711-723.

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

[9] YAN P L, ZHOU F X, WANG T Y, et al. Novel Quantum Voting Protocol with Eight-Qubit Cluster Entangled State[J]. International Journal of Theoretical Physics, 2020, 59(9): 2671-2680.

[10] 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.

[11] 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): 721-726.

[12] SONG X L, CAO Y F, YANG S. Quantum voting scheme based on D-dimensional three-particle entangled states [J]. Acta Electronica Sinica, 2020, 48(7): 1355-1360.

[13] QIAN X Q. Research on secure multiparty sorting [D]. Hefei: Anhui University, 2013.

[14] SHI R H, MU Y, ZHONG H, et al. Secure Multiparty Quantum Computation for Summation and Multiplication[J]. Scientific Reports, 2016, 6(1): 1-9.

[15] YANG H Y, YE T Y. Secure multi-party quantum summation based on quantum Fourier transform[J]. Quantum Information Processing, 2018, 17(6): 1-17.

[16] DU J Z, CHEN X B, WEN Q Y, et al. Secure multiparty quantum summation [J]. Acta physica Sinica, 2007, 56(11): 6214-6219.

[17] YE T Y, HU J L. Quantum Safe Multiparty Sum Based on the Mutual Unbiased Basis of D-order Quantum Systems and Its Applications [J]. Science China: Physics, Mechanics and Astronomy, 2021, 51 (2): 88-95.

[18] OVERILL R E. Review: Foundations of Cryptography, Volume II: Basic Applications[J]. Journal of Logic and Computation, 2005, 15(3): 405-405.

[19] WANG R C, FENG Y. Secure multi-party quantum sorting protocol based on quantum summation [J]. Chinese Journal of Quantum Electronics, 2021, 38(3): 354-364.

[20] QIN J Q. Design and analysis of quantum voting protocol based on multi-body entangled states [D]. Hefei: Anhui University, 2019.

[21] 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.

[22] THAPLIYAL K, SHARMAR D, PATHAK A. Analysis and improvement of Tian-Zhang-Li voting protocol based on controlled quantum teleportation[J]. arXiv: 2016, 1602.00791.

FENG Yan, born in 1979, postgraduate, associate professor. Her main research interests include cryptography, network security, and quantum communication network security system.

WANG Rui-cong, born in 1995, postgraduate. Her main research interests include network security and quantum cryptography.

（责任编辑：柯颖）