基于 BB84 态的量子匿名一票否决协议

石润华，于辉，柯唯阳，徐小桐
（华北电力大学控制与计算机工程学院，北京 102206）

摘 要：为了构造无条件安全的一票否决协议，首先定义了一个安全多方计算原子协议，即安全多方析取。借助量子云，提出了量子安全多方析取协议，使用 BB84 态作为量子资源，且只需单光子操作和测量。针对现有绝大多数量子投票协议需对高维空间粒子执行复杂的操作和测量从而导致可实现性较差的缺陷，利用所提出的量子安全多方析取协议来解决一票否决投票问题，提出了基于量子云的量子匿名一票否决协议。进一步，对协议去中心化处理，提出了一种不需要第三方协助的量子匿名一票否决协议。相较于目前类似协议，所提协议所需量子资源少且操作简单，具有较好的可实现性。在半诚实模型下，对所提协议进行了安全性证明，利用量子完备加密和经典一次一密进行秘密信息编码，保证了协议的无条件安全，既满足了一票否决场景下的投票需求，又保护了投票者的绝对隐私。最后，使用 IBM Qiskit 进行了仿真实验，实验结果验证了所提协议的正确性和可行性。

关键词：一票否决；量子匿名投票；单光子操作；无条件安全
中图分类号：TN918.1
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022157

Quantum anonymous one-vote veto protocol based on BB84 states

SHI Runhua, YU Hui, KE Weiyang, XU Xiaotong
School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China

Abstract: In order to construct unconditionally secure one-vote veto protocol, a primitive protocol of secure multiparty computations was defined, i.e., secure multiparty disjunction. Furthermore, by introducing a quantum cloud, a quantum secure multiparty disjunction (QSMD) protocol was proposed. BB84 states were took as quantum resources and only single-photon operations and measurements were needed. To avoid the flaws of infeasibility, i.e., most of existing quantum voting protocols need to perform operations and measurements in high-dimensional Hilbert space, a quantum anonymous one-vote veto protocol with a quantum cloud (QAOVC) was designed by using the QSMD protocol. In addition, to decentralize, a quantum anonymous one-vote veto (QAOV) protocol without any third party was presented. Compared with related protocols, the proposed protocols require less quantum resources and simpler operations, so they have better feasibility. Under the semi-honest model, quantum perfect encryption and classical one-time pad can ensure the unconditional security of the proposed protocols, i.e., it can completely meet secure requirements of one-vote veto and perfectly protect the privacy of the voters. Finally, simulation experiments are implemented on IBM Qiskit, and the experimental results show that the protocols are correct and feasible.

Keywords: one-vote veto, quantum anonymous voting, single-photon operator, unconditional security

0 引言

投票是日常生活中一项重要活动，重要事项表决以及选举都采取投票制。纸质投票因受时间地点限制，不适用于大规模投票场景。电子投票因具有高效性和便捷性，逐渐取代了纸质投票，成为表决的主流方式。电子投票[1]利用互联网传输经典密码学算法加密后的投票信息，目前提出的电子投票协

收稿日期：2022−05−07；**修回日期：**2022−08−04
基金项目：国家自然科学基金资助项目（No.61772001）
Foundation Item: The National Natural Science Foundation of China (No.61772001)

议大多基于盲签名[2]和组签名[3]技术。最著名的电子投票协议是 Fujioka 等[4]提出的 FOO（Fujioka Okamoto Ohta）算法，它是一种基于盲签名、比特承诺技术以及数字签名技术的电子投票协议。然而，这些电子投票协议的共同特点是安全性基于未被证明的假设，因此只能保证计算安全。

随着量子通信和量子计算机的发展，计算速度越来越快，求解数学困难性问题的复杂性大幅降低，从而对经典密码学的安全构成了威胁，量子密码学[5]也因此得到越来越多的关注。量子投票[6]利用量子密码学对投票信息进行编码，其安全性受量子力学原理保证，理论上具有无条件的安全性，并且可以检测信道中的窃听行为。Hillery 等[7]对投票进行分类，提出了移动式投票和分配式投票 2 种投票模式。Vaccaro 等[8]提出了比较投票，根据 2 个人的投票来判断他们的操作是否相同。在比较投票和移动式投票的基础上，匿名投票被提出[9]。在其研究基础上，许多学者都提出自己的量子投票方案[10-12]。

具有一票否决功能的投票协议是指：若有至少一个投票者反对，决议被否决，但任何投票者都无法知道谁投了反对票，从而保护了投票者的隐私。该投票场景主要用于防止少数服从多数，经典电子投票领域已产生许多研究成果。Kiayias 等[13]提出了一种基于 DDH（decisional Diffie-Hellman）假设和零知识证明的投票方案。仲红等[14]提出了一种半诚实模型下的电子投票方案，主要利用多精度运算和安全多方求和。杨志勇等[15]提出了一种不需要可信第三方的基于安全多方求和的一票否决方案。延吉红等[16]提出了一种安全高效的投票方案，使当串谋人数小于 n–1 时，方案满足完全保密性。此外，在经典密码算法的基础上出现了安全性更高的量子一票否决协议。Rahaman 等[17]提出了一种多粒子 GHZ （Greenberger-Horne-Zeilinger）态先验纠缠的量子匿名一票否决（QAOV, quantum anonymous one-vote veto）协议，该协议以泄露部分投票隐私为代价，当偶数票同意或者奇数票反对即可实现投票结果，然而，由于多粒子 GHZ 态制备困难，其可实现性不好。Wu 等[18]提出了一种基于量子位和 Pauli 运算 Z 和 X 的量子匿名一票否决协议，使用的量子资源和量子操作较简单。然而，该协议利用一个半诚实的服务器作为投票管理中心来制备量子态和生成并分发子秘密（即子密钥），辅助投票者完成投票过程，因此服务器的不诚实行为可能窃取投票者的隐私信息，实际上该协议需要可信的第三方。总之，现有投票协议主要存在以下挑战。

1) 所用量子资源为多粒子纠缠态，且需要进行高维空间的量子测量，操作困难，协议的可实现性差。

2) 投票者需要制备量子资源，增加了投票者的负担。

3) 以泄露部分投票隐私为代价实现投票结果。

4) 存在可信第三方，但在现实中完全可信的第三方是很难找到的。

此外，随着 Google 量子霸权[19]的验证（即针对特定问题的计算能力超越经典超级计算机，又称“量子优越性”），现在的量子计算设备计算速度越来越快，但因其昂贵的计算成本而未得到普及。另一方面，各种量子云平台的出现（如 IBM 量子实验）使普通用户也可以执行量子计算。鉴于此，本文引入诚实且好奇的量子云，设计量子安全多方析取协议，其中量子云制备所需量子资源和实施所有量子测量，从而使其他参与者的量子处理能力达到最小要求，仅需执行简单的单光子操作（Pauli 算子和 Hadamard gate 操作）；并将此协议用于解决一票否决投票问题，提出了基于量子云的量子匿名一票否决（QAOVC, quantum anonymous one-vote veto with a quantum cloud）协议。进一步地，进行去中心化处理，本文提出一种不需要第三方协助的量子匿名一票否决协议。协议均以 BB84 态单光子[20]为量子资源，并进行简单的单光子操作和单光子测量。协议不仅满足匿名性、合法性、可验证性等较完备的投票安全属性，且耗费量子资源少，量子操作及测量的复杂性低，具有更好的可实现性。

1 预备知识

本节主要介绍单光子操作：Pauli 算子和 Hadamard gate 操作。

1.1 Pauli 算子

Pauli 算子可以看作二维 Hilbert 空间上的 2 个基向量 $|0\rangle$ 和 $|1\rangle$ 的外积算子[21]，本文所用到的 $\boldsymbol{U}_Y$ 算子外积为 $|0\rangle\langle 1|-|1\rangle\langle 0|$，其密度矩阵如式(1)所示，$\boldsymbol{U}_Y$ 算子对基底 $\{|+\rangle,|-\rangle,|0\rangle,|1\rangle\}$ 进行变换如式(2)所示。

$$\boldsymbol{U}_Y = iY = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{1}$$

$$\begin{aligned}\boldsymbol{U}_Y|0\rangle &\to -|1\rangle\\ \boldsymbol{U}_Y|1\rangle &\to |0\rangle\\ \boldsymbol{U}_Y|-\rangle &\to -|+\rangle\\ \boldsymbol{U}_Y|+\rangle &\to |-\rangle\end{aligned} \tag{2}$$

1.2 Hadamard gate 操作

Hadamard gate 操作（简称 $\boldsymbol{H}$ 门操作）的密度矩阵如式(3)所示，其效果是对量子比特的状态做基底的变换，进行基底 $\{|0\rangle,|1\rangle\}$ 与 $\{|+\rangle,|-\rangle\}$ 间相互转换，变换过程如式(4)所示。

$$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{3}$$

$$\begin{aligned}\boldsymbol{H}|0\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}=|+\rangle\\ \boldsymbol{H}|1\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix}=|-\rangle\end{aligned} \tag{4}$$

此外，$\boldsymbol{H}$ 和 $\boldsymbol{U}_Y$ 变换还满足如下性质。

$$\begin{aligned}\boldsymbol{H}^2 &= \boldsymbol{I}\\ \boldsymbol{U}_Y{}^2 &= -\boldsymbol{I}\\ \boldsymbol{H}\boldsymbol{U}_Y\boldsymbol{H} &= -\boldsymbol{U}_Y\\ \boldsymbol{H}\boldsymbol{U}_Y &= -\boldsymbol{U}_Y\boldsymbol{H}\end{aligned} \tag{5}$$

2 量子安全多方析取协议

随着量子计算的发展，量子设备的计算能力越来越强，但由于其成本昂贵，并未得到普及。为此，本文引入了量子云，提出了一个可行的量子安全多方析取（QSMD, quantum security multiparty disjunction）协议，使参与者仅需执行简单的单光子操作，降低了参与者的负担。

2.1 协议模型

定义 1　QSMD 协议。假设协议中有 m 个参与者 $P_1,P_2,\cdots,P_m$，每个参与者 P_i 有一个秘密输入 x_i ($x_i\in\{0, 1\}$)。执行 QSMD 协议后，输出结果为 $x_1\vee x_2\vee\cdots\vee x_m$（此处“$\vee$”表示逻辑或，$0\vee 0=0$，$0\vee 1=1$，$1\vee 0=1$，$1\vee 1=1$）。此外，协议满足以下安全目标。

1) 正确性。如果所有参与者都诚实地执行协议，则最后的结果 $x_1\vee x_2\vee\cdots\vee x_m$ 是正确的。

2) 公平性。每个参与者都是平等的，都能以同等概率得到结果 $x_1\vee x_2\vee\cdots\vee x_m$。

3) 隐私性。除参与者 P_i 外，没有任何参与者能知道其秘密输入 x_i。

在协议中，量子云制备单光子并对其进行测量，其他参与者只需执行简单的单光子操作。此外，假设协议中所有参与者都是诚实且好奇的，即每个参与者都诚实地执行协议，但是对其他参与者的秘密信息 x_i 感兴趣，类似于经典的半诚实模型。假设参与者 P_i 和 P_{i+1}（$i=1,2,\cdots,m$；P_{m+1} 代表量子云）之间存在量子认证通道，且实现环境是无噪声、无粒子丢失和设备性能完美的。最后量子云负责输出结果。符号定义如表 1 所示。

表 1　　**符号定义**

符号	含义
x_i	参与者的秘密输入（投票者 Alice$_i$ 的投票信息）
$\boldsymbol{X}_i$	根据 x_i 生成的满足 $x_i=\boldsymbol{X}_i[1]\vee\boldsymbol{X}_i[2]\vee\cdots\vee\boldsymbol{X}_i[k]$ 的随机数构成的数组
$\boldsymbol{R}_i$	决定单光子是否执行 $\boldsymbol{H}$ 门变换的随机数构成的数组
$\boldsymbol{S}_i$	决定单光子是否执行 $\boldsymbol{U}_Y$ 算子变换的随机数构成的数组
t	量子云总共需生成的单光子数
h	用于身份认证的单光子数
k	用于传递信息的单光子数
q	用于窃听检测的单光子数
ID	身份认证信息
result	所有投票者身份认证信息异或的正确结果
r	量子云计算的投票者身份认证信息异或的结果
c_i	Alice$_i$ 保存到量子云（区块链）的承诺值
r_i	随机整数
ph	单光子
w	QSMD 协议的输出（投票结果）
d	制备单光子的轮数

2.2 协议描述

步骤 1　所有参与者 $P_i(i=1,2,\cdots,m)$ 共同确认小整数 k（例如，$k=10$，其错误的概率为 $\delta\approx\frac{1}{2^{10}}$），它与成功得到结果 $x_1\vee x_2\vee\cdots\vee x_m$ 的概率有关。

步骤 2　每个参与者 P_i 生成自己的秘密信息 $x_i(x_i\in\{0, 1\},\ i=1,2,\cdots,m)$，并根据秘密信息 x_i 生成一个长度为 k 且满足 $x_i=\boldsymbol{X}_i[1]\vee\boldsymbol{X}_i[2]\vee\cdots\vee\boldsymbol{X}_i[k]$ 的随机私密数组 $\boldsymbol{X}_i(\boldsymbol{X}_i[j]\in\{0, 1\},\ 1\leqslant j\leqslant k)$。

步骤 3　每个参与者 P_i 随机生成 2 个长度为 $t(t=2(k+q))$ 的数组 $\boldsymbol{R}_i$ 和 $\boldsymbol{S}_i$（$\boldsymbol{R}_i[j]\in_R\{0, 1\}$ 且 $\boldsymbol{S}_i[j]\in_R\{0, 1\}$，$1\leqslant j\leqslant t$）。

步骤 4 量子云制备 t 个 BB84 态的单光子 $\mathrm{ph}_1,\mathrm{ph}_2,\cdots,\mathrm{ph}_t(\mathrm{ph}_j\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\},j=1,2,\cdots,t)$ 并记录其初始状态，然后，将单光子通过认证的量子通道发送给参与者 P_1。

步骤 5 参与者 P_1 执行以下步骤。

{
for $j=1$ to t do {
if $\boldsymbol{S}_1[j]=1$，对第 j 个单光子 ph_j 执行 $\boldsymbol{H}$ 门变换
if $\boldsymbol{R}_1[j]=1$，对第 j 个单光子 ph_j 执行 $\boldsymbol{U}_Y$ 算子变换}}

步骤 6 参与者 P_1 通过认证的量子通道将 t 个单光子发送给 P_2。

步骤 7 参与者 P_2 收到 P_1 发送的单光子后，根据 $\boldsymbol{S}_2[j]$ 和 $\boldsymbol{R}_2[j]$ 对其进行相应操作，随后将单光子通过认证的量子通道发送给 P_3。收发单光子过程执行 m 次，最后 P_m 将单光子发回量子云。

得到上一参与者发送的单光子后，参与者 P_i 执行以下步骤。

{
for $j=1$ to t do {
if $\boldsymbol{S}_i[j]=1$，对第 j 个单光子 ph_j 执行 $\boldsymbol{H}$ 门变换
if $\boldsymbol{R}_i[j]=1$，对第 j 个单光子 ph_j 执行 $\boldsymbol{U}_Y$ 算子变换}}

步骤 8 量子云收到单光子后，对每个单光子以初始基进行测量并记录。

步骤 9 后处理。

1) 每个参与者 P_i 公开它的数组 $\boldsymbol{S}_i[j]$ ($j=1,2,\cdots,t$)。

2) 所有参与者 P_i 选出满足有效条件 $\sum_{i=1}^{m}\boldsymbol{S}_i[j]\bmod 2=0$ 的 j。根据预备知识可知，满足有效条件的第 j 个单光子 ph_j 的基不变。

3) 所有参与者保存满足有效条件的事件 j，其余的事件丢弃（概率约为 $\frac{1}{2}$）。

4) 约有 $k+q$（约为 $\frac{t}{2}$）个有效事件，所有参与者随机选择 k 个事件用来传递信息，其余 q 个事件则用来进行窃听检测。

5) 对于 q 个用于检测窃听的事件，所有参与者要求量子云公开相应检测光子的初始态和测量结果，继而所有参与者也公开对应的数组 $\boldsymbol{R}_i[j]$。通过所有公开信息可以确定是否存在不诚实行为或窃听者。经过有效条件的判定，若用于窃听检测的单光子 ph_j 与初始状态匹配，则继续执行下一步；否则认为存在窃听，放弃 QSMD 协议的执行。

例如，假设第 j 个单光子 ph_j 是一个窃听检测事件，如果满足 $\sum_{i=1}^{m}\boldsymbol{R}_i[j]\bmod 2=0$，那么这个单光子的测量结果应该与初始状态相同；否则，与初始状态不同。

步骤 10 假设用来计算最后结果的 k 个编码事件与 t 个单光子中第 $g_1,g_2,\cdots,g_k$ 个事件相对应，每个参与者 P_i 计算且公开

$$\boldsymbol{X}_i^*[g_j]=(\boldsymbol{X}_i[j]+\boldsymbol{R}_i[g_j])\bmod 2 \tag{6}$$

其中，$g_j\in\{1,2,\cdots,t\}$，$j\in\{1,2,\cdots,k\}$。

步骤 11 量子云计算 $\boldsymbol{X}^*[\mathrm{g}_j]$ ($j=1,2,\cdots,k$)

$$\boldsymbol{X}^*[g_j]=\sum_{i=1}^{m}\boldsymbol{X}_i^*[g_j]\bmod 2 \tag{7}$$

量子云执行以下操作。

{
1)令 $w=0$
2) for $j=1$ to k do {
if 单光子ph_{g_j}的测量结果与其初始状态不同// 等价于$\sum_{i=1}^{m}\boldsymbol{R}_i[g_j]\bmod 2=1$，$w=(\boldsymbol{X}^*[g_j]+1)\bmod 2$
else $w=\boldsymbol{X}^*[g_j]$
if $w=1$, return (w)}
return(0)}

3 基于量子云的量子匿名一票否决协议

本节将 QSMD 协议用于解决一票否决场景下的投票问题，增加了对投票者的身份认证和对投票信息的承诺，使投票协议满足合法性及可验证性，提出了 QAOVC 协议。

3.1 协议模型

假定协议中 m 个投票者 $\mathrm{Alice}_1,\mathrm{Alice}_2,\cdots,\mathrm{Alice}_m$ 对决议进行投票，每个投票者 Alice_i 对决议的秘密选票 x_i 可用 0 或 1 表示，其中，0 表示支持决议，1 表示反对决议。执行 QAOVC 协议后，投票结果为

$w = x_1 \vee x_2 \vee \cdots \vee x_m$（0 表示决议通过，1 表示决议被否决）。QAOVC 协议除了满足安全多方析取协议的安全假设以及安全目标外，还满足可验证性，即任意一个投反对票的投票者都可以验证他的选票是否被正确计算在内。QAOVC 协议模型框架如图 1 所示，其中，$H^{S_i[j]}U_y^{R_i[j]}$ 表示投票者 Alice$_i$ 对单光子 ph$_j$ 进行的单光子操作。投票协议包含以下两类参与者。

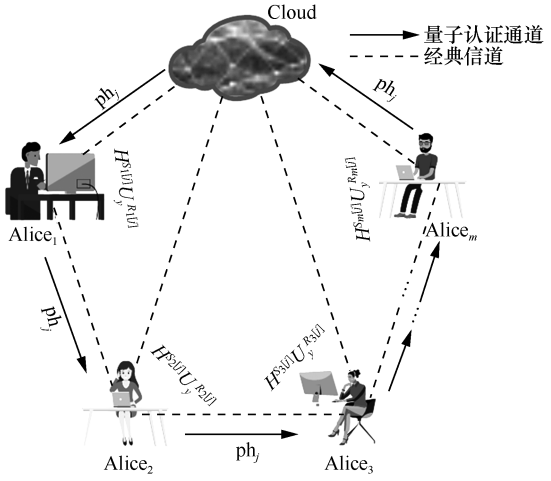

图 1　QAOVC 协议模型框架

1) 量子云 Cloud。半诚实的参与者，假定其不与其他投票者串谋，主要负责验证投票者身份、制备并测量 BB84 态单光子、统计选票结果并公布，保存投票者投票信息的承诺值。

2) 投票者 Alice。半诚实的投票者，负责对决议进行表决，具有一票否决的权利。

3.2　协议描述

3.2.1　初始化阶段

步骤 1　所有投票者 Alice$_i$($i = 1,2,\cdots,m$) 共同确认整数 k，生成自己的秘密选票 x_i 以及对应的随机私密数组 $\boldsymbol{X}_i$，随机生成 2 个长度为 t 的数组 $\boldsymbol{R}_i$ 和 $\boldsymbol{S}_i$，其中 $t = 2(h+k+q)$。

步骤 2　量子云事先准备一组长度为 h 的身份认证信息 $\mathbf{ID}_i[j]$ ($i = 1,2,\cdots,m; j = 1,2,\cdots,h$)，并将身份认证结果保存在数组 $\mathbf{result}[j]$ ($j = 1,2,\cdots,h$)中，且满足式(8)；然后利用面对面或其他安全的方式，如 QKD（quantum key distribution），为每个投票者 Alice$_i$ 分配一个身份认证信息数组 $\mathbf{ID}_i[j]$。

$$\mathbf{result}[j] = \mathbf{ID}_1[j] \oplus \mathbf{ID}_2[j] \oplus \cdots \oplus \mathbf{ID}_m[j] \quad (8)$$

步骤 3　每个投票者 Alice$_i$ 随机选择一个整数 $r_i \in \{0, 1\}$ 并计算 $c_i = H(r_i \oplus H(r_i \oplus x_i))$，其中 H 为安全的哈希函数；然后投票者 Alice$_i$ 将 c_i 通过经典信道发送给量子云，即投票者 Alice$_i$ 将秘密选票 x_i 承诺给量子云，但是量子云在不知道 r_i 的情况下是不能解密出秘密选票的。

3.2.2　量子执行阶段

按照 2.2 节的步骤 4~步骤 8 制备 t 个单光子并执行。

3.2.3　经典后处理阶段

执行 2.2 节的后处理阶段，选出 $h+k+q$（约为 $\frac{t}{2}$）个有效事件，所有投票者随机选择 h 个事件用来验证身份，k 个事件用来传递信息，其余 q 个事件则用来进行窃听检测。

3.2.4　身份认证及窃听检测阶段

步骤 1　假设用来认证身份的 h 个事件与 t 个单光子中的第 $l_1, l_2, \cdots, l_h$ 个单光子相对应，每个投票者 Alice$_i$ 计算

$$\boldsymbol{Y}_i[l_j] = (\mathbf{ID}_i[j] + \boldsymbol{R}_i[l_j]) \bmod 2 \quad (9)$$

其中，$j \in \{1,2,\cdots,h\}$ 且 $l_j \in \{1,2,\cdots,t\}$，计算完成后投票者将 $\boldsymbol{Y}_i[l_j]$ 公开。

步骤 2　量子云计算 $\boldsymbol{Y}[l_j](j = 1,2,\cdots,h)$ 如下

$$\boldsymbol{Y}[l_j] = \sum_{i=1}^{m} \boldsymbol{Y}_i[l_j] \bmod 2 \quad (10)$$

量子云执行以下操作。

{

1) 令 $r = 0$

2) for $j = 1$ to h do {

if 单光子ph$_{l_j}$的测量结果与其初始状态不同// 等价于$\sum_{i=1}^{m} \boldsymbol{R}_i[l_j] \bmod 2 = 1$，$r = (\boldsymbol{Y}[l_j]+1) \bmod 2$

else $r = \boldsymbol{Y}[l_j]$

if $r \neq \mathbf{result}[j]$，return(“身份认证失败”)}

return (“身份认证成功”)}

若身份认证成功则继续执行下一步，否则放弃此次投票。

步骤 3　对于 q 个用于窃听检测的事件，所有投票者公开对应的数组 $\boldsymbol{R}_i[j]$。量子云通过所有公开信息可以确定是否存在不诚实行为或者窃听。经过有效条件的判定，若用于窃听检测的单光子 ph$_j$ 与初始状态匹配，则继续执行下一步；否则认为存在窃听，放弃此次投票。

例如，假设第 j 个单光子 ph_j 是一个窃听检测事件，如果满足 $\sum_{i=1}^{m}\boldsymbol{R}_i[j]\bmod 2=0$，那么这个单光子的测量结果应该与初始状态相同；否则，与初始状态不同。

3.2.5 投票及计票阶段

假设用来计算最后结果的 k 个编码事件与 t 个单光子中第 $g_1,g_2,\cdots,g_k$ 个事件相对应，每个投票者计算且公开

$$\boldsymbol{X}_i^*[g_j]=(\boldsymbol{X}_i[j]+\boldsymbol{R}_i[g_j])\bmod 2 \tag{11}$$

其中，$g_j\in\{1,2,\cdots,t\}$，$j\in\{1,2,\cdots,k\}$。

量子云计算 $\boldsymbol{X}^*[g_j]$（$j=1,2,\cdots,k$），即

$$\boldsymbol{X}^*[g_j]=\sum_{i=1}^{m}\boldsymbol{X}_i^*[g_j]\bmod 2 \tag{12}$$

量子云执行以下操作。

{

1) 令 $w=0$

2) for $j=1$ to k do {

if 单光子ph_{g_j} 的测量结果与其初始状态不同// 等价于$\sum_{i=1}^{m}\boldsymbol{R}_i[g_j]\bmod 2=1$，$w=(\boldsymbol{X}^*[g_j]+1)\bmod 2$

else $w=\boldsymbol{X}^*[g_j]$

if $w=1$,return (w)}

return(0)}

若有投票者投反对票，则量子云的计算结果应为 1，表示决议被否决；否则决议通过。

3.2.6 验证阶段

假设投票者 Alice_i 投了反对票，而量子云公布的投票结果为通过时，则投票者 Alice_i 可以使用量子匿名通信技术[22-24]广播中断信号，并向量子云公开随机数 r_i，对初始化阶段存放在量子云的承诺信息 c_i 进行验证。若经验证投票结果正确，则投票结束；否则，量子云对投票结果进行改正。

4 量子匿名一票否决协议

量子云负责验证身份、收集选票、制备并测量单光子、公布结果的工作，中心化程度非常高，存在较高的安全威胁，也存在单点失效的风险。实际上，即使量子云不可信，也得不到投票者的任何隐私信息。所以，可以去掉量子云，将它的工作平摊给每个投票者，以达到去中心化的目的。本节提出了一种不需要第三方协助的 QAOV 协议。

4.1 协议模型

本节提出的 QAOV 协议同样满足 QAOVC 的安全目标以及安全假设，在执行完 QAOV 协议后，投票结果依然为 $x_1\vee x_2\vee\cdots\vee x_m$，只是将量子云的工作平摊给每个投票者，并且引入区块链保存投票者的承诺。QAOV 协议模型如图 2 所示。协议主要包含以下参与者。

1) 投票者 Alice。半诚实的投票者，负责对决议进行表决，制备单光子并测量。

2) 区块链。保存承诺值。

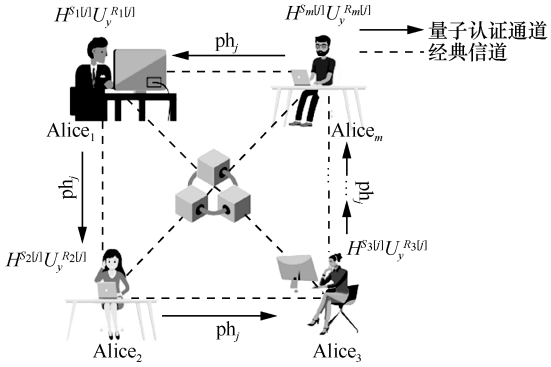

图 2 QAOV 协议模型

4.2 协议描述

4.2.1 *初始化阶段*

步骤 1 所有投票者 Alice_i 共同确认整数 k。

步骤 2 所有投票者通过面对面或其他安全的方式（如 QKD）事先准备一组长度为 h 的身份认证信息 $\mathbf{ID}_i[j]$，并将身份认证结果保存在数组 $\mathbf{result}[j]$ 中；然后为每个投票者 Alice_i 分配一个身份认证信息 $\mathbf{ID}_i[j]$。

步骤 3 每个投票者 Alice_i 确定自己的秘密选票 x_i 及其对应的随机私密数组 $\boldsymbol{X}_i$，生成随机秘密数组 $\boldsymbol{R}_i$ 和 $\boldsymbol{S}_i$。

步骤 4 每个投票者 Alice_i 随机选择一个整数 $r_i\in\{0,1\}$ 并计算 $c_i=H(r_i\oplus H(r_i\oplus x_i))$；然后将 c_i 保存到区块链。即投票者 Alice_i 将秘密选票 x_i 承诺给区块链，但是区块链在不知道 r_i 的情况下是不能解密出投票信息的。

4.2.2 *量子执行阶段*

记录量子执行轮数 $d=1$（$1\leqslant d\leqslant\dfrac{2(k+q+h)}{m}$，假设 $k+q+h$ 为 m 的整数倍），每个投票者 Alice_i 制备一个 BB84 态的单光子 $\mathrm{ph}_{m(d-1)+i}$ 并记录其初始状

态，根据 $\boldsymbol{S}_i[m(d-1)+i]$ 和 $\boldsymbol{R}_i[m(d-1)+i]$ 对单光子执行相应的单光子操作；然后通过认证的量子通道将单光子发送给 Alice_{i+1}。

Alice_{i+1} 收到单光子后，对其执行相应的单光子操作，然后通过认证的量子通道将单光子发送给 Alice_{i+2}。每个单光子的收发过程都执行 m 次，最后将单光子发回其制备者手中，用初始基进行测量并记录，至此，第一轮量子执行结束，进入下一轮，共需执行 $\dfrac{2(k+q+h)}{m}$ 轮。第 j 个单光子的量子执行阶段如图 3 所示。

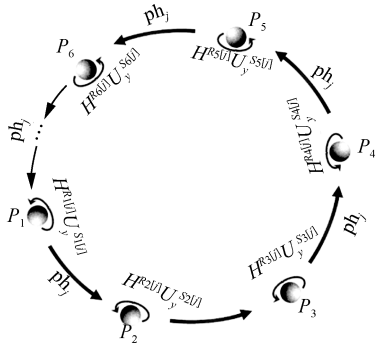

图 3　第 j 个单光子的量子执行阶段

4.2.3　经典后处理阶段

与 3.2.3 节一致，所有投票者随机选出 $h+k+q$ 个有效事件。

4.2.4　身份认证及窃听检测阶段

步骤 1　假设用来认证身份的 h 个事件与 t 个单光子中的第 $l_1,l_2,\cdots,l_h$ 个单光子相对应，每个投票者 Alice_i 计算 $\boldsymbol{Y}_i[l_j]$（$j\in\{1,2,\cdots,h\}$）并公开。

步骤 2　制备第 l_j 个单光子的投票者 $\text{Alice}_{l_j \bmod m}$ 计算 $\boldsymbol{Y}[l_j]$ 并进行身份认证，若身份认证成功，则继续进行下一步；否则，放弃此次投票。

步骤 3　窃听检测，过程与 3.2.4 节步骤 3 的检测程序相同。

4.2.5　投票及计票阶段

假设用来计算最后结果的 k 个编码事件与 t 个单光子中第 $g_1,g_2,\cdots,g_k$ 个相对应，每个投票者 Alice_i 计算 $\boldsymbol{X}_i^*[g_j]$ 并公开，制备第 g_j 个单光子的投票者 $\text{Alice}_{g_j \bmod m}$ 计算 $\boldsymbol{X}^*[g_j]$（$j=1,2,\cdots,k$）以及 w。若 $w=1$，则决议被否决；否则，决议通过。

4.2.6　验证阶段

假设投票者 Alice_i 投了反对票，公布的投票结果为通过，则投票者 Alice_i 可以使用量子匿名通信技术广播中断信号，并对区块链公开随机数 r_i，对初始化阶段存放在区块链的承诺信息 c_i 进行验证。若经验证投票结果正确，则投票结束；否则，对投票结果进行改正。

5　分析与实验

本节首先分析了量子安全多方析取协议的正确性，并证明当所有的参与者都诚实执行协议时，所述协议是无条件安全的；其次，分析了投票方案所满足的安全属性；最后，将所提协议与其他协议从量子资源、通信复杂度以及效率等方面做对比，并使用 IBM Qiskit 对所述协议进行仿真实验，实验结果表明，所提协议具有正确性。

5.1　正确性

本文提出的 QAOVC 协议和 QAOV 协议的正确性是由 QSMD 协议的正确性保证的，以下将对 QSMD 协议的正确性进行分析。

定理 1　假设有 m 个输入，其中 1 的个数为 $p(p\leqslant m)$，如果 $p=0$ 或 1，协议正确执行；如果 $p\geqslant 2$，则可能输出错误结果 0，其概率为 $\delta\approx\dfrac{1}{2^k}$（当 k 足够大时可忽略不计）。

证明

1)　假设量子云生成的单光子 ph_j 的初始态为 $|\psi\rangle_j$，执行协议后发送回量子云的状态为 $|\varphi\rangle_j$，可表示为

$$|\varphi\rangle_j=(-1)^{l}U_Y^{\sum_t R_t[j]}H^{\sum_t S_t[j]}|\psi\rangle_j \tag{13}$$

如果 j 满足有效条件 $\sum_{i=1}^{m}S_i[l_j]\bmod 2=0$，则

$$|\varphi\rangle_j=(-1)^{l}U_Y^{\sum_t R_t[j]}|\psi\rangle_j \tag{14}$$

从式(2)和式(14)可知，对于有效事件，最终状态与初始状态的基相同，如果 U_Y 变换执行偶数次，则除了多一个全局相位因子外其状态不变；否则，状态改变，但维持同一个基。

从式(11)和式(12)易得

$$\begin{aligned}\boldsymbol{X}^*[g_j]&=\sum_{i=1}^{m}\boldsymbol{X}_i^*[g_j]\bmod 2=\\&\sum_{i=1}^{m}(\boldsymbol{X}_i[j]+\boldsymbol{R}_i[g_j])\bmod 2=\\&\sum_{i=1}^{m}\boldsymbol{X}_i[j]\bmod 2+\sum_{i=1}^{m}\boldsymbol{R}_i[j]\bmod 2\end{aligned} \tag{15}$$

量子云可通过公开信息计算 $\sum_{i=1}^{m}\boldsymbol{X}_i[j]\bmod 2$，即

$$w=\boldsymbol{X}^*[g_j]+\sum_{i=1}^{m}\boldsymbol{R}_i[j]\bmod 2=\sum_{i=1}^{m}\boldsymbol{X}_i[j]\bmod 2 \tag{16}$$

2) 进一步考虑以下几种情况，m 个输入 $x_1,x_2,\cdots,x_m$，其中 1 的个数为 p

情况 1 $p=0$

所有 $\boldsymbol{X}_i[j]$ 均为 0，即 $w=\sum_{i=1}^{m}\boldsymbol{X}_i[j]\bmod 2=0$。计算结果表示输出正确，与假设符合，所以结果正确。

情况 2 $p=1$

假设任意一个参与者 P_i 的输入为 1，即 $X_{i^*}\neq 0$，且至少存在一个 j 使 $w=\sum_{i=1}^{m}\boldsymbol{X}_i[j]\bmod 2=1$。计算结果与假设符合，所以结果正确。

情况 3 $p=2$

假设 2 个参与者 P_{i_1} 和 P_{i_2} 投反对票，即 $x_{i_1}=1$且 $x_{i_2}=1$，可知 $\boldsymbol{X}_{i_1}\neq 0$ 且 $\boldsymbol{X}_{i_2}\neq 0$（共有 $\left(2^k-1\right)\left(2^k-1\right)$种情况）。如果 $\boldsymbol{X}_{i_1}=\boldsymbol{X}_{i_2}$，则 $w=0$，共有 2^k-1 种情况，则错误的概率为

$$\delta=\frac{2^k-1}{(2^k-1)(2^k-1)}=\frac{1}{2^k-1} \tag{17}$$

显然，当 k 足够大时，$\delta\approx 0$。例如，$k=6$ 时，$\delta=0.015\,78$；$k=10$ 时，$\delta=0.000\,98$。

情况 4 $p=3$

假设有这样的 k 行（对应 $j=1,2,\cdots,k$）和 p 列（对应 p 个数组 X_i），其中每列至少有一个 1 且每行有 0 个 1 或者 2 个 1，$w=\sum_{i=1}^{m}\boldsymbol{X}_i[j]\bmod 2=0$，然而，$x_1\vee x_2\vee\cdots\vee x_m=1$，所以通过 1 在每行可能的位置，可以推断出协议错误的概率满足以下条件

$$\delta<\frac{(\mathrm{C}_3^0+\mathrm{C}_3^2)^k}{(2^k-1)(2^k-1)(2^k-1)}$$

$$\delta<\frac{4^k}{(2^k-1)(2^k-1)(2^k-1)}\approx\frac{1}{2^k} \tag{18}$$

当 k 足够大时，$\delta\approx 0$。例如，$k=6$ 时，$\delta=0.016\,38$；$k=10$ 时，$\delta<0.000\,98$。

依次类推，可得 p 取其他值的情况，即

$$\delta<\frac{(\mathrm{C}_p^0+\mathrm{C}_p^2+\mathrm{C}_p^4+\cdots+\mathrm{C}_p^{2\left\lfloor\frac{p}{2}\right\rfloor})^k}{(2^k-1)^p}$$

$$\delta<\frac{(2^{p-1})^k}{(2^{k-1})^p}\approx\frac{1}{2^k} \tag{19}$$

已知 $\mathrm{C}_p^0+\mathrm{C}_p^1+\mathrm{C}_p^2+\cdots+\mathrm{C}_p^p=2^p$ 且 $\mathrm{C}_p^i=\mathrm{C}_{p-1}^{i-1}+\mathrm{C}_{p-1}^i$。因此，当 k 足够大时，δ 可忽略不计，即所述协议是正确的。

5.2 安全性

本文提出的 QAOVC 协议和 QAOV 协议的安全性主要是由 QSMD 协议的安全性保证的，所以，在定理 2 中将证明 QSMD 协议在半诚实模型下是无条件安全的。

定理 2 若所有参与者都诚实执行协议时，则所述协议是无条件安全的。

证明 单光子在量子认证通道传递信息时，根据随机数组 $\boldsymbol{R}_i$ 和 $\boldsymbol{S}_i$ 执行单光子操作来进行加密，此时数组未公开是私密数组。如果输入态和输出态都是混合态，则本文提出的量子投票协议是无条件安全的。不失一般性，以第 j 个随机的单光子 ph_j 为例，其输入态为

$$\rho_{\mathrm{in}}(\mathrm{ph}_j)=[\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|] \tag{20}$$

在执行完相应操作后，输出态为

$$\begin{aligned}
&\rho_{\mathrm{out}}(\mathrm{ph}_j)=\\
&\frac{1}{4}\left[U_Y^0H^0\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]+\\
&\frac{1}{4}\left[U_Y^0H^1\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]+\\
&\frac{1}{4}\left[U_Y^1H^0\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]+\\
&\frac{1}{4}\left[U_Y^1H^1\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]=\\
&\frac{1}{4}\left[\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]+\\
&\frac{1}{4}\left[\left(\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|)+\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|\right)\right]+\\
&\frac{1}{4}\left[\left(\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|-\rangle\langle -|+\frac{1}{4}|+\rangle\langle +|\right)\right]+\\
&\frac{1}{4}\left[\left(\frac{1}{4}|-\rangle\langle -|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|0\rangle\langle 0|\right)\right]=\\
&\frac{1}{4}\left[\left(|0\rangle\langle 0|+|1\rangle\langle 1|+|+\rangle\langle +|+|-\rangle\langle -|\right)\right]=\\
&\frac{1}{4}\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\right]=\\
&\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\frac{I}{2}
\end{aligned} \tag{21}$$

由式(21)可知，输出态为最大混合态，所有参与者都不能得到除自己以外其他参与者所选择的秘密信息，因此该协议使用的量子完备加密是信息理论安全的。

在执行完 q 个单光子的窃听检测后，每个投票者 P_i 公开 $\boldsymbol{R}_i[l_j]$，它是随机且私密的，显然这是经典的一次一密[25]。

综上所述，量子完备加密[26]和一次一密保证了在半诚实模型下协议是无条件安全的。然而，一个不诚实的参与者 P_{i-1} 可能会与参与者 P_{i+1} 联合窃取 P_i 的秘密信息，分析如下。

不诚实参与者 P_{i-1} 在收到 t 个单光子后，制备 t 个贝尔态粒子 $\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}$，并将光子 b 发送给 P_i，自己保留光子 a。参与者 P_i 收到光子 b 后对其进行 $U_Y{}^{R_i[j]}H^{S_i[j]}$ 变换如下

$$U_Y{}^0H^0\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}=\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}} \tag{22}$$

$$U_Y{}^0H^1\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}=\frac{|0+\rangle_{ab}+|1-\rangle_{ab}}{\sqrt{2}} \tag{23}$$

$$U_Y{}^1H^0\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}=\frac{|01\rangle_{ab}-|10\rangle_{ab}}{\sqrt{2}} \tag{24}$$

$$U_Y{}^1H^1\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}=\frac{|0-\rangle_{ab}+|1+\rangle_{ab}}{\sqrt{2}} \tag{25}$$

参与者 P_{i+1} 收到单光子 b 后，由于与 P_{i-1} 联合窃听，他将单光子发送给 P_{i-1}，对 2 个光子 (a,b) 进行贝尔态测量即可推测出 P_i 的私密数据（如果测量结果为 $\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}$，则 $\boldsymbol{R}_i[j]=0$ 且 $\boldsymbol{S}_i[j]=0$）。所以，为了抵抗这种攻击，用 q 个单光子进行窃听检测，显然，它可以保证所有参与者的诚实性，且可抵抗外部窃听者，这类似于 QKD[27]中的诱骗态。

根据上面的分析可知，如果各方都诚实地执行协议，就会正确地输出最终的结果。在所提协议中，所有参与者都是完全对等的且执行相同的程序。因此，所提 QSMD 协议可以实现公平性。此外，与大多数现有的量子安全多方计算一样，所提 QSMD 协议需要经过认证的量子信道，可以保证量子资源和参与者身份的真实性。原则上可以将量子认证技术[28]和经典认证技术[29]结合起来，在量子信道中实现各种认证。

5.3　投票协议满足的安全属性

本文提出的 QAOVC 协议和 QAOV 协议均满足以下安全属性。

5.3.1　匿名性

在 QAOVC 协议中，所有投票者都可得到一个唯一的 ID，身份认证成功后即可使用匿名 ID 进行投票，因此投票者的真实身份不能被除自己以外的任何投票者知道（注意，验证者仅验证所有投票者合法或存在不合法的投票者）。此外，在上述 2 个协议中只公布决议通过与否（即投票的最终结果），无法知道是谁投了反对票以及投反对票的人数，在 QAOVC 协议中，结果由量子云计算后公布；在 QAOV 协议中，所有投票者共同计算投票结果，因此所提协议满足匿名性。

5.3.2　合法性

在投票协议中，需要核实投票者身份信息，只有合法投票者才能够进行投票。在 QAOVC 协议中，初始化阶段，每个投票者都可得到量子云准备的身份认证信息，并将其异或的正确结果保存在数组 **result** 中；身份认证阶段，会对投票者的合法性进行验证，只有当所有投票者的身份认证信息异或的结果与事先保存在数组 **result** 中的结果符合时，才能进行投票。在 QAOV 协议中，所有投票者通过面对面或其他安全的方式（例如 QKD）准备一组身份认证信息，并将结果保存，同样对身份认证信息进行核实，身份合法即可投票。

5.3.3　公平性

各投票者都是等价的，在投票前任何投票者都不能获取部分投票记录或其他投票者的有用信息，且他们以同等的概率得到投票结果。本文所提协议中，投票者利用量子完备加密对量子资源进行编码，即根据随机数组 $\boldsymbol{R}_i$ 和 $\boldsymbol{S}_i$ 执行单光子操作来进行加密，并通过后选择的方式选出满足有效条件的单光子用于对投票信息的编码，且在协议中传递投票信息的单光子处于最大混合态，因此投票信息不会泄露给其他投票者。在 QAOVC 协议中，投票信息在量子云计算后进行公布，且假定量子云不与其他投票者串谋，从而避免了投票信息的泄露；在 QAOV 协议中，每个投票者均需制备相同个数的单光子，并对传递的信息进行统计后公开，计算并公布投票结果过程需投票者共同执行。因此，协议具有公平性。

5.3.4　可验证性

任意一个投反对票的投票者都可以验证他的选票是否被正确计算。根据 5.1 节的正确性分析，如果每个参与者都诚实地执行协议，则投票结果正确；当投票结果错误时，任何投反对票的投票者均

可中断协议，对结果进行验证。在 QAOVC 协议中，投票者需向量子云公布随机数 r_i，对存放在量子云的承诺信息 c_i 进行验证；在 QAOV 协议中，投票者需向区块链公开随机数 r_i，对存放在区块链的承诺信息 c_i 进行验证。实际上，当所有投票者均同意决议时，可验证性被隐藏，为解决这种情况，可引入可信第三方来监督量子云（区块链）。

5.4 通信性能比较

根据前文分析易得，所提协议具有较完备的安全属性，本节将从量子资源、通信复杂度以及效率等方面与其他协议进行对比分析。假设 m 个投票者，对 n 个决议进行表决，所提协议中每对一个决议进行表决，量子云需制备 t $(t=2(h+k+q))$ 个单光子，其中 k 个用来传递投票信息，总共传递 $2n(h+k+q)$ 个单光子，通信复杂度为 $O(kn)$，效率为 $\eta=\dfrac{q}{2(h+k+q)}$。所提协议与其他协议的比较如表 2 所示。

由表 2 易得，所提协议使用的量子资源较易制备，同时使用的量子操作较为简单，具有良好的可行性。此外，本文提出的 QAOVC 协议引入了第三方量子云作为投票中心，负责制备投票所需量子资源，并计算最终投票结果，且投票者仅需执行简单的单光子操作，降低了投票者负担；QAOV 协议在 QAOVC 协议的基础上进行去中心化处理，将量子云的工作平摊给投票者，投票结果由所有投票者共同计算，避免了 QAOVC 协议单点失效的风险，具有更好的安全性和隐私性。

5.5 仿真实验

为了更好地理解，在 IBM Qiskit 平台对所提 QSMD 协议进行仿真实验，假设参与者的人数 $m=6$，量子云制备 6 个单光子，分别为 $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|0\rangle,|+\rangle\}$，具体线路如图 4 所示。在 IBM Qiskit 上仿真 1 024 次后，用初始基对单光子进行测量，经典测量结果为 010100，概率为 100%。显然，实验结果与公式推导结果一致。综上所述，所提协议是正确的。

表 2 所提协议与其他协议的比较

协议	量子资源	没有第三方	是否窃听检测	不泄露投票者隐私	投票者不需要制备量子态	通信复杂度
文献[17]	多粒子 GHZ 态	√	×	×	√	$O(n^2)$
文献[18]	单光子	×	√	×	×	$O(n^2)$
文献[30]	单光子	×	√	×	√	$O(n^2)$
文献[31]	四粒子比特簇态	×	√	√	√	$O(mn)$
QAOVC 协议	单光子	×	√	√	√	$O(kn)$
QAOV 协议	单光子	√	√	√	×	$O(kn)$

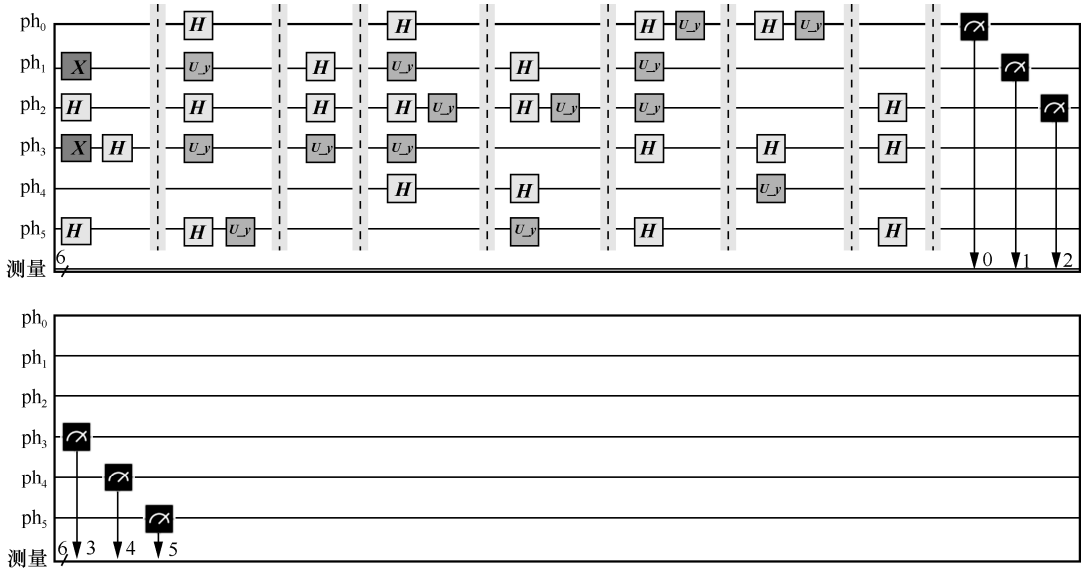

图 4 具体线路

k 取不同值时错误率与输入中 1 的个数 p 的关系如图 5 所示。在模拟实验中，假设有 10 个参与方，对每个 k 共同计算 QSMD 协议 60 000 次，每次输入都是随机的。从图 5 可以看出，错误率主要取决于 $p \geqslant 2$ 时 k 的取值，当 $k = 10$ 时，错误率近似等于 0。总之，仿真实验验证了所提 QSMD 协议的正确性和可行性。

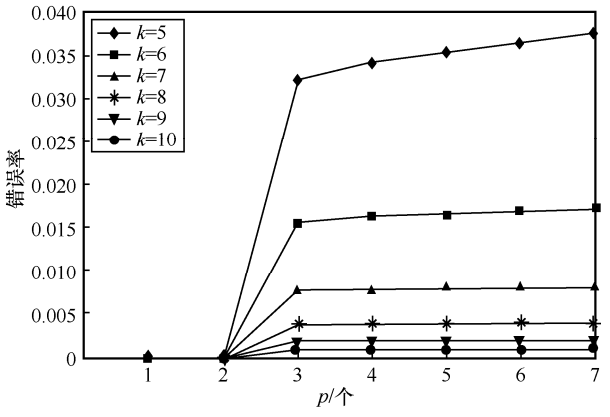

图 5　k 取不同值时错误率与 p 的关系

所提协议中没有考虑量子噪声和光子损失，与已有抗噪容错的量子协议类似，可以在实际应用中增加单光子的数量 t，并采用量子容错（例如 decoherence-free states）或经典的纠错技术来避免这些问题。此外，当参与者相距较远时，可以在每一方部署一个量子中继器，用基于隐形传态的方式转发未知状态的光子。

综上所述，所提协议具有较好的可行性。

6　结束语

本文首先设计了一个新颖的量子安全多方计算基础协议，即量子安全多方析取协议，进一步提出了一种基于 BB84 态的有量子云协助的匿名一票否决协议。该协议以单光子作为量子资源，投票者只需进行简单的单光子操作，且使用的量子资源更少，具有良好的可行性。在所述协议中，利用量子完备加密与经典一次一密结合保证了协议的无条件安全，且满足较为完备的投票安全属性。在此基础上进行去中心化处理，提出了一种不需要第三方协助的量子匿名投票一票否决协议。相较于现有的量子一票否决协议，所提协议降低了投票者的负担，同时不泄露投反对票的总人数，更好地保护了投票者的隐私。所提协议使用单光子作为量子资源，然而现有技术水平无法制备完美的单光子，为此可使用弱相干脉冲代替所述协议中的单光子，使协议具有更好的可行性。

此外，作为一个基础协议，量子安全多方析取协议可应用于安全计算布尔函数或其他更复杂的安全多方计算任务中。

参考文献：

[1] 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.

[2] KONG W, SHEN J, VIJAYAKUMAR P, et al. A practical group blind signature scheme for privacy protection in smart grid[J]. Journal of Parallel and Distributed Computing, 2020, 136: 29-39.

[3] KUNDU N, DEBNATH S K, MISHRA D. A secure and efficient group signature scheme based on multivariate public key cryptography[J]. Journal of Information Security and Applications, 2021, 58: 102776.

[4] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections[M]. Berlin: Springe, 1993.

[5] ABIDIN S, SWAMI A, RAMIREZ-ASÍS E, et al. Quantum cryptography technique: a way to improve security challenges in mobile cloud computing (MCC)[J]. Materials Today: Proceedings, 2022, 51: 508-514.

[6] 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: 20.

[7] HILLERY M. Quantum voting and privacy protection: first steps[J]. SPIE Newsroom, 2006, 1598: 2006.

[8] VACCARO J A, SPRING J, CHEFLES A. Quantum protocols for anonymous voting and surveying[J]. Physical Review A, 2007, 75: 012333.

[9] XU Q J, ZHANG S Y. Improvement of the security of quantum protocols for anonymous voting and surveying[J]. Science China Physics, Mechanics and Astronomy, 2010, 53(11): 2131-2134.

[10] XU Y P, GAO D Z, LIANG X Q, et al. Semi-quantum voting protocol[J]. International Journal of Theoretical Physics, 2022, 61(3): 1-12.

[11] 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.

[12] ZHANG S, WANG S L, WANG Q, et al. Quantum anonymous voting protocol with the privacy protection of the candidate[J]. International Journal of Theoretical Physics, 2019, 58(10): 3323-3332.

[13] KIAYIAS A, YUNG M. Non-interactive zero-sharing with applications to private distributed decision making[C]//International Conference on Financial Cryptography. Berlin: Springer, 2003: 303-320.

[14] 仲红, 黄刘生, 罗永龙. 基于安全多方求和的多候选人电子选举方案[J]. 计算机研究与发展, 2006, 43(8): 1405-1410.
ZHONG H, HUANG L S, LUO Y L. A multi-candidate electronic voting scheme based on secure sum protocol[J]. Journal of Computer Research and Development, 2006, 43(8): 1405-1410.

[15] 杨智勇, 唐西林, 杨长海. 一个基于安全多方求和的一票否决协议[J]. 计算机应用与软件, 2009, 26(4): 109-111.
YANG Z Y, TANG X L, YANG C H. A private vote protocol based on se-

cure sum[J]. Computer Applications and Software, 2009, 26(4): 109-111.
[16] 延吉红, 刘忆宁, 刘方, 等. 一种安全高效的一票否决电子选举方案[J]. 计算机工程与应用, 2012, 48(15): 93-96, 158.
YAN J H, LIU Y N, LIU F, et al. Improved unanimous election voting scheme[J]. Computer Engineering and Applications, 2012, 48(15): 93-96, 158.
[17] RAHAMAN R, KAR G. GHZ correlation provides secure anonymous veto protocol[J]. arXiv Preprint, arXiv: 1507. 00592, 2015.
[18] WU S Y, SUN W Q, WANG Q L, et al. A secure quantum protocol for anonymous one-vote veto voting[J]. IEEE Access, 2021, 9: 146841-146849.
[19] ARUTE F, ARYA K, BABBUSH R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.
[20] ANUSUYA D V, KALAIVANI V. Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications[J]. Personal and Ubiquitous Computing, 2021, 25: 1-11.
[21] NIELSEN M A, CHUANG I L. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2012.
[22] MENICUCCI N C, BARAGIOLA B Q, DEMARIE T F, et al. Anonymous broadcasting of classical information with a continuous-variable topological quantum code[J]. Physical Review A, 2018, 97(3): 032345.
[23] CHRISTANDL M, WEHNER S. Quantum anonymous transmissions[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2005: 217-235.
[24] 马鸿洋, 张鑫, 徐鹏翱, 等. 基于循环码和信息压缩融合的量子保密通信算法[J]. 通信学报, 2020, 41(3): 190-196.
MA H Y, ZHANG X, XU P G, et al. Quantum secure communication algorithm based on cyclic code and information compression[J]. Journal on Communications, 2020, 41(3): 190-196.
[25] ZHOU S H. A real-time one-time pad DNA-chaos image encryption algorithm based on multiple keys[J]. Optics & Laser Technology, 2021, 143: 107359.
[26] BOYKIN P O, ROYCHOWDHURY V. Optimal encryption of quantum bits[J]. Physical Review A, 2003, 67(4): 042317.
[27] 王华, 赵永利. 量子密钥分发城域光组网技术前瞻[J]. 通信学报, 2019, 40(9): 168-174.
WANG H, ZHAO Y L. Overview of quantum key distribution metropolitan optical networking technology[J]. Journal on Communications, 2019, 40(9): 168-174.
[28] SHI R H, MU Y, ZHONG H, et al. Quantum private set intersection cardinality and its application to anonymous authentication[J]. Information Sciences, 2016, 370/371: 147-158.
[29] SHI R H, MU Y, ZHONG H, et al. Secure multiparty quantum computation for summation and multiplication[J]. Scientific Reports, 2016, 6: 19655.
[30] LIU B X, JIANG D H, LIANG X Q, et al. A novel quantum voting scheme based on BB84-state[J]. International Journal of Theoretical Physics, 2021, 60(4): 1339-1349.
[31] 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.

[作者简介]

石润华（1974− ），男，安徽安庆人，博士，华北电力大学教授、博士生导师，主要研究方向为经典量子密码算法、协议及其应用。

于辉（1998− ），女，满族，河北唐山人，华北电力大学硕士生，主要研究方向为量子投票协议。

柯唯阳（1996− ），男，陕西宝鸡人，华北电力大学硕士生，主要研究方向为测量设备无关的密码学、量子投票协议。

徐小桐（1997− ），女，河北武安人，华北电力大学硕士生，主要研究方向为量子投票协议。