第 58 卷 第 5 期 2009 年 5 月
1000-3290/2009/58(05)/3166-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.5,May,2009

基于双模压缩态的量子投票协议*

易 智† 何广强 曾贵华

(上海交通大学电子工程系区域光纤通信网与新型光通信系统国家重点实验室,上海 200240)

(2008 年 9 月 9 日收到;2008 年 10 月 7 日收到修改稿)

提出了一种基于双模压缩态的基本量子投票协议,该协议通过随机选择信号加载的方式,充分利用量子信号测不确定性原理实现了分布式投票系统.并在此基础上分析可能遇到的攻击.双模压缩态的模间关联性保证了该方案的安全性.

关键词:量子投票协议,双模压缩态,不确定性原理

PACC:4250,4230Q,0365

1. 引 言

选举和投票是现代民主社会的一个重要标志.通过网络的分布式投票系统将可以极大地方便投票.在经典网络通信下,投票信息很容易被窃听,这就失去了投票的匿名性;投票信息同样很容易被修改,最后的投票结果就不可信.即使是使用 RSA 签名[1]等依赖于数学难题手段也将面临严峻的挑战.但是,以量子物理学为基础的量子通信的安全性由量子力学的基本规律保证,而且量子不确定性原理和量子不可克隆定理保证了量子通信对窃听的可检测性[3—7].

连续变量量子密码采用高斯态(相干态和压缩态)作为信号载波,采用光场的正则振幅和正则相位作为信号载波的可观测物理量,通过振幅和相位调制把信号加载到量子载波上,采用散粒噪声限制的零差接收机检测量子信号[8—28].相对于基于单光子发生与检测技术的离散变量量子通信,连续变量量子通信实现相对简单,单信号所能传输的信息量较高[8].双模压缩态是一种连续变量纠缠态,双模压缩态的模间关联性对于量子通信信号的检测十分有用.本文提出了一种基于双模压缩态的量子投票方案.

本文第 2 节介绍了基于双模压缩态的量子投票协议的工作过程.第 3 节首先分析量子投票协议的匿名性,然后针对投票协议可能遇到的攻击,给出篡改信息攻击的物理模型,最后分析本文提出的量子投票协议如何检测攻击者.

2. 投票协议描述

2.1. 流程描述

在这个协议中,Alice 代表双模压缩态的制备者,Bob 代表可信任的计票中心.有 N 个投票人(V_0-V_{N-1})以及 M 个候选人(C_0-C_{M-1}).该协议模型如图 1 所示.每个合法的投票人只有一票且必须投票给一个候选人,为使简化讨论,本文将弃权也视为投给一个候选人[1)].

为了保证协议安全性和投票人的匿名性,完成一次完整的投票,需要多轮 Alice→Voters→Bob 的过程.为了方便描述,每一轮都有唯一的代号 Round.第一轮投票 Round =" ";除第一轮外,本轮的代号都是在上一轮结束后由 Bob 确定.Bob 通过设置轮次计数器 Round Counter 的值来通知 Alice 以及所有投票者本轮的轮次.

在每一轮 Alice→Voters→Bob 的过程中有如下

* 国家自然科学基金(批准号:60472018,60801051)资助的课题.

† E-mail:yiyimm515@sjtu.edu.cn

1) 弃权意味着投票者不选择任何一名已有的候选人,但是这也是投票者的一种选择.于是 Bob 在已有的候选人基础上添加一个虚拟的候选人.如果投票者决定弃权,那么他就将票投给虚拟的候选人.最后 Bob 在计票的时候统计虚拟候选人的票数就可以得出弃权的人数.

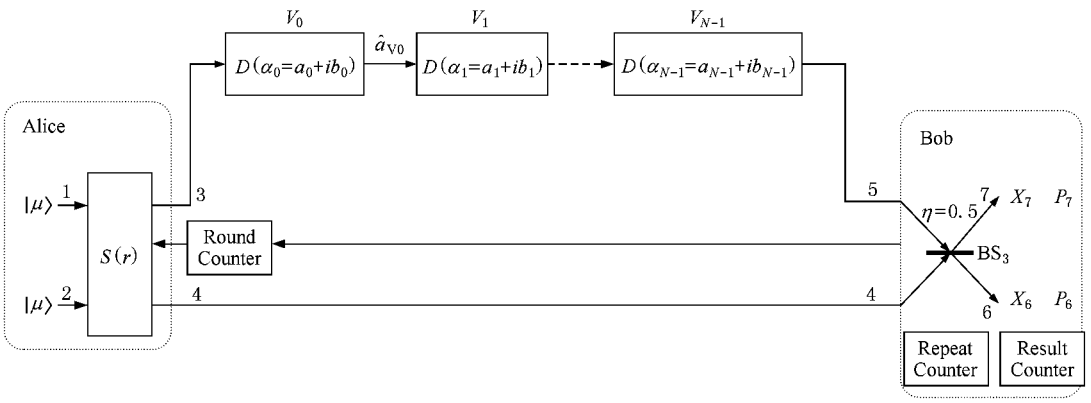

图 1　基于双模压缩态的量子投票方案($\hat{S}(\pm r)$为双模压缩算符；$\hat{D}(\alpha)$为平移算符；BS 为光束分离器)

3 步：

第 1 步　Alice 将双模压缩算符 $\hat{S}(r)$作用于光学模 $\hat{a}_1$ 和 $\hat{a}_2$，产生纠缠光学模 $\hat{a}_3$ 和 $\hat{a}_4$. 制备完成之后，Alice 将制备的 $\hat{a}_3$ 发送给第一个投票人 V_0.

第 2 步　V_0 及以后每一个投票者都应用平移算符 $\hat{D}(\alpha_i = a_i p_i + \mathrm{i}a_i(1-p_i), p_i = 0,1)$作用于模 $\hat{a}_3(a_i = (N+1)^{I_i}, I_i$ 表示 V_i 投票给候选人 $C_{I_i}, I_i \sim (0, M-1), p_i = 0$ 表示 V_i 将投票信息加载在 $\hat{a}_3$ 的 P 上，$p_i = 1$ 表示 V_i 将投票信息加载在 $\hat{a}_3$ 的 X 上)，最终产生模 $\hat{a}_5$.

第 3 步　Bob 通过光束分离器把 BS(分光比为 η)合成光学模 $\hat{a}_4$ 和 $\hat{a}_5$，产生光学模 $\hat{a}_6$ 和 $\hat{a}_7$. 当 $\eta = \frac{1}{2}$，Bob 选择测量基(X_6, P_7). Bob 通过计算(X_6, P_7)的值，可以得出有 $\mathrm{Voter}X_{\mathrm{Round}}$名投票者将信息加载在 $\hat{a}_3$ 的 X 上，$\mathrm{Voter}P_{\mathrm{Round}}$名投票者将信息加载在 $\hat{a}_3$ 的 P 上. 之所以选择测量基(X_6, P_7)，以及如何通过(X_6, P_7)获得 $\mathrm{Voter}X_{\mathrm{Round}}$和 $\mathrm{Voter}P_{\mathrm{Round}}$，下文介绍物理过程时将详细说明. Bob 获得 $\mathrm{Voter}X_{\mathrm{Round}}$和 $\mathrm{Voter}P_{\mathrm{Round}}$后，针对以下不同情况作出相应的处理.

1)如果 $\mathrm{Voter}X_{\mathrm{round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$(如同时成立，以 X 优先)，Bob 通过设置轮次计数器 Round Counter 的值为 Round +“ X ”或 Round +“ P ”通知唯一将投票信息加载在 X 或 P 上的投票者再投 1 次票. 同时将 Repeat Counter 的值加 1(初始值为 0). Bob 此时的目的就是通过设置轮次计数器的值，使得唯一的投票者连续进行 T 次投票(T 的具体值将在安全性分析中说明).

如果 Repeat Counter 的值达到 T，Bob 将(X_6 或 P_7)上测到的值乘以$\sqrt{2}$并加到 Result Counter，并将 Repeat Counter 置 0；Bob 通知参加本轮投票的另外 $\mathrm{Voter}P_{\mathrm{Round}}$或 $\mathrm{Voter}X_{\mathrm{Round}}$名投票者进行下轮投票，记下轮投票的轮次为 Round +“ P ”或 Round +“ X ”.

如果 Repeat Counter 的值在未达到 T 前，Bob 计算出 $\mathrm{Voter}X_{\mathrm{Round}} + \mathrm{Voter}P_{\mathrm{Round}} \neq 1$，则 Bob 认为系统中存在恶意攻击者 EVE.

2)如果 $\mathrm{Voter}X_{\mathrm{Round}} = 0$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 0$，Bob 通知参加本轮投票无效，所有投票者重新投票.

3)如果 $\mathrm{Voter}X_{\mathrm{Round}} > 1$，Bob 通过设置计数器 Counter 的值为(Round +“ X ”)通知参加本轮投票的 N_x 名将投票信息加载在 X 上的投票者再投 1 次票；而参加本轮投票的 $\mathrm{Voter}P_{\mathrm{Round}} > 1$ 名将投票信息加载在 P 上的投票者在没有收到 Bob 通知前不要做任何操作，并且 Bob 通知他们后进行的投票轮次将记为 Round +“ P ”.

投票者通过下轮次判断是否参加该轮投票. 例如，Round =“ XXP ”，那么所有随机选择加载信息在 X 或 P 上顺序为 XXP 的投票者参加下轮投票，而其他人不参加. 直到轮次符合为止. 对于合法的投票者，在下轮投票中，投票者不能修改他们的本轮的投票信息即 $a_i = (N+1)^{I_i}$，但是他们可以重新随机的选择 p_i，来确定投票信息是加载在 X 上还是 P 上.

投票的终点是通过条件 $\mathrm{Voter}X_{\mathrm{Round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$ 而遍历所有投票者. 当所有投票结束，如果 Bob 没有确认发现 EVE，那么 Result Counter 的值就是最后的投票结果.

Bob 根据协议的流程可以得到每轮结果可以用树状图表示，如图 2.

在“ ”轮(第一轮)所有投票者投票结束后，Bob 通知所有投票者 在“ ”轮选择将信号加载在 $\hat{a}_3$ 的 X

上的投票者参加轮次为“ X ”的投票轮次，其余的投票者参加轮次为“ P ”的投票轮次. 然后设置轮次计数器 Round Counter 的值为“ X ”，开始轮次为“ X ”的投票. 一直到轮次为 ”XXX ”的投票结束后，Bob 发现只剩下一名投票者，并且 Bob 通过使该名投票者连续投 T 次票确认是合法的投票者之后，将投票结果计入 Result Counter，并将轮次计数器 Round Counter 的值为“ XXP ”. 当“ XXP ”轮投票结束后，Bob 设置轮次计数器 Round Counter 的值为“ XP ”；“ XPP ”轮投票结束后，Bob 设置轮次计数器 Round Counter 的值为“ P ”直到“ PPP ”轮投票结束后，Bob 确认所有投票结束，最终 Result Counter 的结果就是投票结果[2].

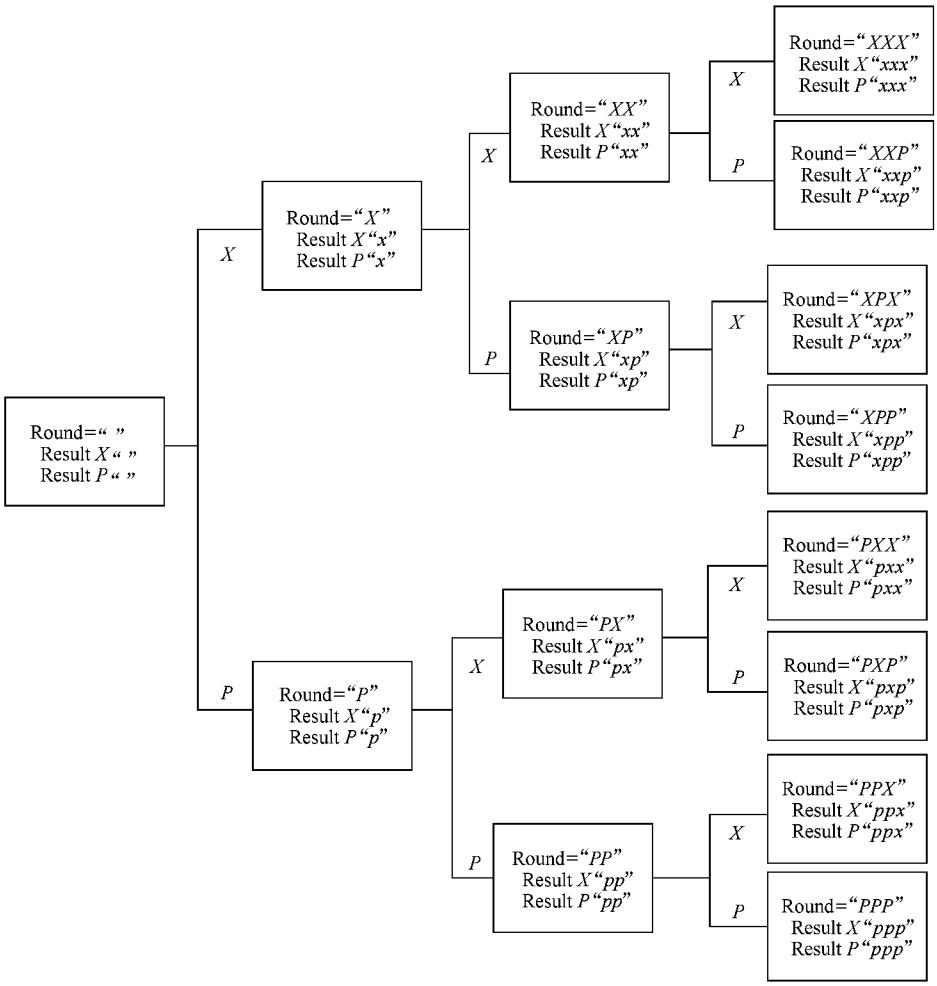

图 2 投票结果树状图

2.2. 物理过程

Alice 将双模压缩算符 $\hat{S}(r)$ 作用于光学模 $\hat{a}_1$ 和 $\hat{a}_2$，产生纠缠光学模 $\hat{a}_3$ 和 $\hat{a}_4$. 利用双模压缩效应制备纠缠态的过程如下，双模压缩算符为

$$S(r) = \exp[r(\hat{a}_1^{\dagger}\hat{a}_2^{\dagger} - \hat{a}_1\hat{a}_2)]. \tag{1}$$

双模压缩变换为

$$\begin{aligned}\hat{a}_3 &= \hat{S}^{\dagger}(r)\hat{a}_1\hat{S}(r)\\ &= \hat{a}_1\cosh(r) + \hat{a}_2^{\dagger}\sinh(r),\\ \hat{a}_4 &= \hat{S}^{\dagger}(r)\hat{a}_2\hat{S}(r)\\ &= \hat{a}_2\cosh(r) + \hat{a}_1^{\dagger}\sinh(r),\end{aligned} \tag{2}$$

分别定义正则振幅 $X = \frac{1}{2}(\hat{a} + \hat{a}^{\dagger})$，$P = \frac{1}{2\mathrm{i}}(\hat{a} - \hat{a}^{\dagger})$ 则二者满足不确定性关系 $\Delta X\Delta P = \frac{1}{4}$，根据(2)式，可得如下关系：

2) 也可能出现“ $XXPX$ ”和“ $XXPP$ ”等轮次. Bob 在确认某个轮次只有一名合法的投票者之后，就将轮次计数器 Round Counter 的值设为树图的最近一条分支.

$$\begin{aligned} X_3 &= X_1\cosh(r) + X_2\sinh(r),\\ P_3 &= P_1\cosh(r) - P_2\sinh(r),\\ X_4 &= X_2\cosh(r) + X_1\sinh(r),\\ P_4 &= P_2\cosh(r) - P_1\sinh(r), \end{aligned} \tag{3}$$

显然

$$\begin{aligned} &\lim_{r\to\infty}(X_3 - X_4) = 0,\\ &\lim_{r\to\infty}(P_3 + P_4) = 0. \end{aligned} \tag{4}$$

即应用 $\hat{S}(r)$时，X_3 与 X_4 正相关，P_3 与 P_4 负相关[2].

V_0 应用平移算符 $\hat{D}(\alpha_0 = a_0p_0 + \mathrm{i}a_0(1-p_0)$，其中 $p_0 = 0,1)$作用于模 $\hat{a}_3$. $p_0 = 0$ 表示 V_0 将投票信息加载在 $\hat{a}_3$ 的 P 上，$p_0 = 1$ 表示 V_0 将投票信息加载在 $\hat{a}_3$ 的 X 上. 平移算符 $\hat{D}(\alpha) = \exp(\hat{\alpha}\hat{a}_3^{\dagger} - \alpha^{*}\hat{a}_3)$作用于模 $\hat{a}_3$ 产生变换 $\hat{a}_{V0} = \hat{D}^{\dagger}j(\alpha_0)\hat{a}_3\hat{D}(\alpha_0) = \hat{a}_3 + \alpha_0$，因为 a_0 为实数，则

$$X_{V0} = X_3 + a_0p_0,\ P_{V0} = P_3 + a_0(1-p_0), \tag{5}$$

那么最终有

$$\begin{aligned} X_5 &= X_3 + a_0p_0 + a_1p_1 + a_2p_2 + \cdots\\ &\quad + a_{N-1}p_{N-1},\\ P_5 &= P_3 + a_0(1-p_0) + a_1(1-p_1)\\ &\quad + a_2(1-p_2) + \cdots + a_{N-1}(1-p_{N-1}). \end{aligned} \tag{6}$$

Bob 通过光束分离器把 BS(分光比为 η)合成光学模 $\hat{a}_4$ 和 $\hat{a}_5$，产生光学模 $\hat{a}_6$ 和 $\hat{a}_7$. 那么有

$$\begin{aligned} X_7 &= \sqrt{\eta}X_4 + \sqrt{1-\eta}X_5,\\ P_7 &= \sqrt{\eta}P_4 + \sqrt{1-\eta}P_5,\\ X_6 &= \sqrt{\eta}X_5 - \sqrt{1-\eta}X_4,\\ P_6 &= \sqrt{\eta}P_5 - \sqrt{1-\eta}P_4. \end{aligned} \tag{7}$$

当 $\eta = \frac{1}{2}$，Bob 选择测量基(X_6, P_7)，因为

$$\begin{aligned} X_6 &= \sqrt{\frac{1}{2}}X_5 - \sqrt{1-\frac{1}{2}}X_4\\ &= \sqrt{\frac{1}{2}}(X_5 - X_4)\\ &= \sqrt{\frac{1}{2}}(X_3 - X_4)\\ &\quad + \sqrt{\frac{1}{2}}(a_0p_0 + a_1p_1 + a_2p_2 + \cdots + a_{N-1}p_{N-1}),\\ P_7 &= \sqrt{\frac{1}{2}}P_4 + \sqrt{1-\frac{1}{2}}P_5\\ &= \sqrt{\frac{1}{2}}(P_5 + P_4)\\ &= \sqrt{\frac{1}{2}}(P_3 + P_4)\\ &\quad + \sqrt{\frac{1}{2}}[a_0(1-p_0) + a_1(1-p_1)\\ &\quad + a_2(1-p_2) + \cdots + a_{N-1}(1-p_{N-1})]. \end{aligned} \tag{8}$$

当 $r\to+\infty$ 时，由(4)式可以得出

$$\begin{aligned} \lim_{r\to\infty}X_6 &= \sqrt{\frac{1}{2}}(a_0p_0 + a_1p_1 + a_2p_2 + \cdots + a_{N-1}p_{N-1}),\\ \lim_{r\to\infty}P_7 &= \sqrt{\frac{1}{2}}[a_0(1-p_0) + a_1(1-p_1)\\ &\quad + a_2(1-p_2) + \cdots + a_{N-1}(1-p_{N-1})]. \end{aligned} \tag{9}$$

令

$$\begin{aligned} \mathrm{Result}X_{\mathrm{Round}} &= (a_0p_0 + a_1p_1 + a_2p_2 + \cdots + a_{N-1}p_{N-1}),\\ \mathrm{Result}P_{\mathrm{Round}} &= a_0(1-p_0) + a_1(1-p_1)\\ &\quad + a_2(1-p_2) + \cdots + a_{N-1}(1-p_{N-1}), \end{aligned} \tag{10}$$

$$\begin{aligned} \mathrm{Result}_{\mathrm{Round}} &= \mathrm{Result}X_{\mathrm{Round}} + \mathrm{Result}P_{\mathrm{Round}}\\ &= a_0 + a_1 + a_2 + \cdots + a_{N-1}, \end{aligned} \tag{11}$$

因为

$$a_k = (N+1)^{I_k},\ k \sim (0, N-1), I_k \sim (0, M-1), \tag{12}$$

所以

$$\mathrm{Result}_{\mathrm{Round}} = \sum_{k=0}^{N-1}(N+1)^{I_k},\ I_k \sim (0, M-1), \tag{13}$$

同时 $\mathrm{Result}_{\mathrm{Round}}$ 也可以表示成

$$\mathrm{Result}_{\mathrm{Round}} = \sum_{j=0}^{M-1}v_j(N+1)^j, \tag{14}$$

其中

$$\begin{aligned} v_0 &= \mathrm{Result}_{\mathrm{Round}}\%(N+1),\\ v_j &= (\mathrm{Result}_{\mathrm{Round}}\%(N+1)^{j+1})/(N+1)^j, \end{aligned} \tag{15}$$

“%”表示求余，“/”表示整除.

(14)式中 v_j 表示 j 次子项的系数. 因为即使所有投票者选择同一个候选人 $C[j]$，

$$\mathrm{Result} = \mathrm{N}(\mathrm{N}+1)^j < (N+1)^{j+1}. \tag{16}$$

所以 v_j 就表示投票者中选择 $\hat{D}(\alpha = (N+1)^j)$ 的个数，也即候选人 $C[j]$ 获得的票数. 那么同时也就有 $\mathrm{Voter}_{\mathrm{Round}} = \sum_{j=0}^{N-1}v_j$. 从 $\mathrm{Result}X_{\mathrm{Round}}$ 和 $\mathrm{Result}P_{\mathrm{Round}}$，根据(12)—(15)式，同样可以计算出 $\mathrm{Voter}X_{\mathrm{Round}}$ 和 $\mathrm{Voter}P_{\mathrm{Round}}$.

3. 投票者的匿名性与协议的安全性分析

3.1. 匿名性分析

首先，Alice 只是信号的产生者，投票者对于 Alice 是匿名的.

其次，根据(3)以及光学模 $\hat{a}_1$ 和 $\hat{a}_2$ 无关，所以

$$\lim_{r\to\infty}\cosh^2(r) = \infty \quad \lim_{r\to\infty}\sinh^2(r) = \infty,$$
$$\lim_{r\to\infty}(\Delta X_3^2) = \lim_{r\to\infty}[\Delta X_1^2\cosh^2(r) + \Delta X_2^2\sinh^2(r)] = \infty,$$
$$\lim_{r\to\infty}(\Delta P_3^2) = \lim_{r\to\infty}[\Delta P_1^2\cosh^2(r) + \Delta P_2^2\sinh^2(r)] = \infty. \tag{17}$$

由(17)式可以看出，X_3，P_3 由于是不可预知的，于是 $\hat{a}_3$ 是不可以预知的.对于任意 V_i $(i \geqslant 1)$ 即使能够测量出经过 $V_i - V_{i-1}$ 修改的 $\hat{a}_3$，但是由于 X_3，P_3 是不确定的，所以 V_i 都无法获得 $V_i - V_{i-1}$ 加载的投票信息，也无法确定 $V_i - V_{i-1}$ 的投票信息是加载在 X 或是 P.所以投票者之间是匿名的.

最后，由于 Bob 获得的测量结果 $\mathrm{Result}_{\mathrm{Round}} = a_0 + a_1 + a_2 + \cdots + a_{N-1}$ 是一个求和的结果，所以 Bob 无法通过 $\mathrm{Result}_{\mathrm{Round}}$ 获得 a_i 的具体值.即使在一些投票轮次出现 $\mathrm{Voter}X_{\mathrm{Round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$，但是由于这个唯一的投票者是通过投票者自己多轮随机选择出现的，Bob 无法确认投票者的具体身份信息.因此，投票者对于 Bob 也是匿名的.

综上所述，该协议保证了投票者的匿名性.

3.2. 安全性分析

攻击者对该投票协议可能采取 2 种攻击方式：1)恶意破坏投票即主动攻击，与密码学中任何一个协议一样，解决主动攻击依赖于认证技术.2)篡改投票结果即被动攻击，下面主要分析这种攻击方式.

攻击者可能来至于不诚实的投票者或投票者之外的任意攻击者.对于不诚实的投票者，可以将其投票信息分为 2 部分，即遵守协议的部分以及不遵守协议的部分.由于系统是一个串联加和的过程，Bob 也无法区分各个不诚实的投票者的投票信息中不遵守规则的部分，所以对于 Bob，可以将 Alice→Voters→Bob 中间所有不遵守投票规则的投票信息视为一个统一的整体 EVE.如图 3 所示.

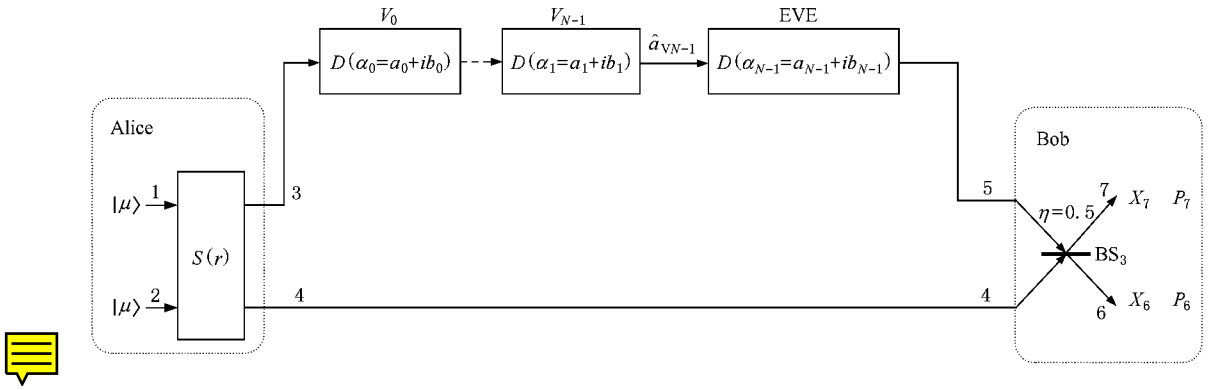

图 3 有攻击者的基于双模压缩态的量子投票方案($\hat{S}(\pm r)$为双模压缩算符；$\hat{D}(\alpha)$为平移算符；BS 为光束分离器)

直观上，Eve 最可能采用与投票者相同的投票方式篡改光学模 $\hat{a}_{VN-1}$ 所携带的信息.对于 EVE，篡改信息最理想的情况是应用平移算符

$$\hat{D}(\alpha_{\mathrm{E}} = [e_{nX}(N+1)^n + ie_{nP}(N+1)^n] - \sum_{m=0,m\neq n}^{N-1}[e_{mX}(N+1)^m + \mathrm{i}e_{mP}(N+1)^m])$$

作用于模 $\hat{a}_{VN-1}$，即对于 C_n 加上 $e_{nX} + e_{nP}$ 票，其余候选者 $C_{m,m\neq n}$ 减去 $e_{mX} + e_{mP}$ 票.

显然必须满足

$$e_{nX} + e_{nP} = \sum_{m=0,m\neq n}^{N-1}(e_{mX} + e_{mP}). \tag{18}$$

对于 EVE 来至于多个部分(多个不诚实投票者和外部攻击者)的组合的情况，EVE 要满足(18)式是十分困难的.

如果 EVE 不能保证满足(18)式，Bob 就能发现投票结果所体现的投票人数和实际投票人数是不符的，即存在 EVE.

EVE 除了保证每次投票都能满足(18)式，而且 EVE 不能修改投票信息，而且必须遵守 Bob 确定的轮次.这是因为协议要求

$$\mathrm{Result}X_{\mathrm{Round}} = \mathrm{Result}X_{\mathrm{Round}+\text{“}X\text{”}} + \mathrm{Result}P_{\mathrm{Round}+\text{“}X\text{”}},$$
$$\mathrm{Result}P_{\mathrm{Round}} = \mathrm{Result}X_{\mathrm{Round}+\text{“}P\text{”}} + \mathrm{Result}P_{\mathrm{Round}+\text{“}P\text{”}},$$

$$\mathrm{Voter}X_{\mathrm{Round}} = \mathrm{Voter}X_{\mathrm{Round}+\text{“}X\text{”}} + \mathrm{Voter}P_{\mathrm{Round}+\text{“}X\text{”}},$$
$$\mathrm{Voter}P_{\mathrm{Round}} = \mathrm{Voter}X_{\mathrm{Round}+\text{“}P\text{”}} + \mathrm{Voter}P_{\mathrm{Round}+\text{“}P\text{”}}. \quad (19)$$

(19)式也可以通过图 2 清楚地看出. EVE 若修改投票信息或不遵守 Bob 的轮次要求，Bob 通过前后轮次的结果对比的差异就能确认 EVE 的存在. EVE 只能通过选择 X 或 P 或者同时选择 X 和 P(因为 EVE 可能一次投多张票)来获得最有利的地位.

如果 EVE 既保证每次投票都能满足(18)式，而且不修改投票信息，同时还遵守 Bob 的轮次要求，那么在出现 $\mathrm{Voter}X_{\mathrm{Round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$ 情况前，Bob 是无法判断 EVE 是否存在. 但是，因为投票的是通过 $\mathrm{Voter}X_{\mathrm{Round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$ 的条件而遍历所有投票者，所以无论 EVE 如何获得有利地位，只要存在 EVE，那么 EVE 的投票信息最终隐藏在 $\mathrm{Voter}X_{\mathrm{Round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$ 的情况中. 通过协议的描述，Bob 通过设置 Round Counter 的值，使得唯一的投票者(其中可能包括 EVE)进行 T 次投票. 对于每一次投票，因为合法投票人 V_i 只会将投票信息加在 X_3 或 P_3 的一项上，EVE 若不被发现，唯一的可能是 EVE 选择的减少一票的候选人恰和 Vi 选择的候选人相同，并且 EVE 和 V_i 同时选择将信息加在 X_3 或同时选择将信息加在 P_3 上，所以 EVE 攻击成功的概率为 $\frac{1}{2}\times\frac{1}{M}$. 进行 T 次投票，EVE 攻击成功的概率为

$$P(T) = \frac{1}{M}\left(\frac{1}{2}\right)^{\mathrm{T}}. \quad (20)$$

所以，对于 EVE 如果对于 C_n 加上 $e_{nX}+e_{nP}$ 票，那么就必须将 $e_{nX}+e_{nP}$ 票隐藏在 $e_{nX}+e_{nP}$ 次 $\mathrm{Voter}X_{\mathrm{Round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$ 的情况中，任何一次 EVE 被发现，EVE 就攻击失败，那么 EVE 被发现的概率

$$P = 1 - [P(T)]^{e_{nX}+e_{nP}}. \quad (21)$$

3.3. 预防攻击

通过安全性分析可以看出，如果每次对于 $\mathrm{Voter}X_{\mathrm{Round}} = 1$ 或 $\mathrm{Voter}P_{\mathrm{Round}} = 1$ 的情况，都能正确的鉴别是否存在 EVE，那么就可以将 EVE 的投票信息从结果中除去. 那么成功预防攻击的概率

$$P = [1 - P(T)]^{e_{nX}+e_{nP}}. \quad (22)$$

4. 结　论

本文提出了一种基于双模压缩态的量子投票协议，量子信号的不确定性原理以及双模压缩态的模间关联性保证了协议的安全性. 对于该协议的匿名性分析表明量子投票协议可以保证投票人的匿名性，而安全性分析则表明该方案能有效抵御被动攻击方式.

[1] Lai J, Fan Y S 2003 *Chin. J. of Computers* **30** 124 (in Chinese) [赖　瑾、范玉顺 2003 计算机科学 **30** 142]

[2] He G Q, Yi Z, Zhu J, Zeng G H 2007 *Acta Phys. Sin.* **56** 6427 (in Chinese) [何广强、易　智、朱　俊、曾贵华 2007 物理学报 **56** 6427]

[3] Zeng G H 2006 *Quantum Cryptography* (Beijing: Science Press) (in Chinese) [曾贵华 2006 量子密码学(科学出版社)]

[4] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[5] Lo H K, Chau H F 1999 *Science* **283** 2050

[6] Shor P W, Preskill J 2000 *Phys. Rew. Lett.* **85** 441

[7] Mayers D 2001 *J. ACM* **48** 351

[8] Braunstein S L, Loock P van 2005 *Rev. Mod. Phys.* **77** 513

[9] Ralph T C 1999 *Phys. Rev.* A **61** 010303 (R)

[10] Ralph T C 2000 *Phys. Rev.* A **62** 062306

[11] Hillery M 2000 *Phys. Rev.* A **61** 022309

[12] Reid M D 2000 *Phys. Rev.* A **62** 062308

[13] Gottesman D, Preskill J 2001 *Phys. Rev.* A **63** 022309

[14] Cerf N J, Lévy M, Assche G. Van 2001 *Phys. Rev.* A **63** 052311

[15] Silberhorn C, Ralph T C, Lutkenhaus N, Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901

[16] Silberhorn C, Korolkova N, Leuchs G 2002 *Phys. Rev. Lett.* **88** 167902

[17] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[18] Grosshans F, Assche G Van, Wanger J *et al* 2003 *Nature* (London) **421** 238

[19] Weedbrook C, Lance A M, Bowen W P *et al* 2004 *Phys. Rev. Lett.* **93** 170504

[20] Weedbrook C, Lance A M, Bowen W P *et al* 2003 *Phys. Rev.* A **73** 022316

[21] Lance A M, Symul T, Sharma V *et al* 2005 *Phys. Rev. Lett.* **95** 180503

[22] He G Q, Zhu J, Zeng G H 2006 *Phys. Rev.* A **73** 012314

[23] Grosshans F, Cerf N J 2004 *Phys. Rev. Lett.* **92** 047905

[24] Iblisdir S, Assche G Van, Cerf N J 2004 *Phys. Rev. Lett.* **93** 170502
[25] Navascués M, Bae J, Cirac J I *et al* 2005 *Phys. Rev. Lett.* **94** 01050
[26] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504
[27] Grosshans F, Cerf N J 2005 *Quantum Information and Communication* **3** 535
[28] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733

Quantum voting protocol using two-mode squeezed states*

Yi Zhi† He Guang-Qiang Ze Gui-Hua
(*Shanghai Jiaotong University*, *Shanghai* 200240, *China*)
(Received 9 September 2008; revised manuscript received 7 October 2008)

Abstract

A basic quantum voting protocol using two-mode squeezed states is proposed firstly in this paper. This protocol makes use of the uncertainty principle by using random-selection, possible attack modes are then analyzed. The mode-mode correlation of two-mode squeezed states guarantees the security of the protocol.

Keywords: quantum voting, two-mode squeezed state, uncertainty principle
PACC: 4250, 4230Q, 0365

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60472018, 60801051).
† E-mail: yiyimm515@sjtu.edu.cn