Quantum anonymous voting for continuous variables

Lang Jiang,[1] Guangqiang He,[1,*] Ding Nie,[2] Jin Xiong,[1] and Guihua Zeng[1]

[1]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Key Lab on Navigation and Location-based Service, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240, China*

[2]*Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana 46556, USA*

(Received 9 November 2011; published 9 April 2012)

A series of quantum voting protocols of continuous variables is proposed. Three methods are employed to ensure that the quantum voting obeys some desirable rules. Entanglement is used to keep voters away from the voting results. We enable voters to operate identically to represent the same vote to prevent the tallyman from gaining information about individual voters. We also propose an effective scheme to prevent voters from voting more than once. In both two-valued and multivalued ballot protocols, several specific constraints are set to meet the rules.

DOI: 10.1103/PhysRevA.85.042309 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

With the development of technology, society automatization and computation becomes a general trend. This trend expanded into nearly all aspects of our lives, including such subtle areas as the voting procedure in various contexts: from governmental elections to decision making in rather small groups like councils. As a result, a lot of protocols for electronic voting have been proposed and successfully applied in the last decade [1]. The protocols belong to the scope of the science of cryptography, because they meet the information security problems of confidentiality, authentication, and data integrity. In modern electronic voting systems, information security is ensured by public-key cryptography and secrecy is guaranteed under conditions of limited computational resources. With the development of quantum computers this condition is no longer secured, which inspires us to develop unconditionally secure voting schemes and protocols. An effective means to solve this is to use quantum systems as information carriers, as proven by the unconditional quantum key distribution [2,3].

In this paper, we describe quantum protocols for voting and for the related task of surveying. Surveying and voting are the same in many respects. The biggest difference between voting and surveying is the value of the vote. The value of the vote in surveying is not restricted to a binary yes or no but may take any integer value. As such, surveying corresponds to collecting estimates of some numerical quantity. The identities of the people who make each bid are kept private and the sum of the bids is made public. On the other hand, voting includes comparative voting and binary-valued and multivalued ballots. For comparative voting, we consider two parties voting on a question with a yes or no answer. The aim is not to determine the tally itself, but to determine whether both parties voted identically without knowing the value of each of the votes. We show that it is possible to encode the voting information in an entangled state [4]. In binary-valued and multivalued ballots, we consider more than two voters voting for two or more parties. The collective result is made public and the the identities of voters are kept secret [5–7] just like in surveying. But the values of the votes are binary.

The paper is organized as follows. We devote Sec. II to the description of our protocols. Subsequently we describe protocols for comparative voting and anonymous surveying. In Sec. III, we discuss adaptations of the protocol for an anonymous ballot for binary-valued ballots and the relationship between the privacy of a vote and the ability for a voter to cheat by making multiple votes. We then introduce multiple-valued ballots and compare them to binary-valued ballots. The conclusions are drawn in Sec. IV.

II. FUNDAMENTAL QUANTUM ANONYMOUS VOTING PROTOCOLS

To describe the voting protocols, we will use terms such as "voters,", "votes," and "tallyman" in the following discussion. Before examining our voting protocols, we should first find the property that a desirable voting satisfies. Based on quantum protocols for anonymous voting and surveying [8], we set a number of general rules.

(R1) The vote of each voter should be kept secret from all other voters.

(R2) The tallyman calculating the collective quantity should not be able to gain information about the voting of individual voters.

(R3) The votes should be receipt-free. This is, it should be impossible for a voter to prove how they voted to a third party, even if they wanted to. This rule thwarts vote buying and prevents coercion of the voter.

(R4) A voter may not make more than one vote, that is, the value of each vote should not count as more than one vote.

In some cases, some people, such as the ballot agency where the voters register their votes, will assist the voting protocols. They should not gain any information in their assistance. Thus, apart from these rules, an additional rule should also be obeyed.

(R5) People who assist the voting processing may exist, but they should not gain any more information than the tallyman.

No one could get more information than the tallyman with entangled states as the carrier. In our discussion we will not consider rule (R5). We call a ballot that satisfies the rules (R1)–(R3) but not (R4) an anonymous survey.

*Corresponding author: gqhe@sjtu.edu.cn

In the following discussion, we will use the Heisenberg picture to describe the continuous-variable quantum state. The "position" and "momentum" are the canonical quantum quadratures of a single-mode electromagnetic field defined as $\hat{x} = \frac{1}{2}(\hat{a} + \hat{a}^\dagger)$ and $\hat{p} = \frac{1}{2i}(\hat{a} - \hat{a}^\dagger)$. Thus $\hat{x}$ and $\hat{p}$ obey the Heisenberg uncertainty relation $\Delta\hat{x}\,\Delta\hat{p} \geqslant \frac{1}{4}$. Now we examine the two fundamental schemes: the comparative ballot and anonymous surveying.

A. Comparative ballot

The first voting protocol we describe is a simple comparative one, which is called a comparative ballot. This protocol involves two voters, Alice and Bob, voting on a binary-valued question, a question whose answer is a binary digit (for example, a "yes" or "no" question). Such a ballot involves only two voters, so it is easy for both of them to make the conjecture about the other vote based on the tallyman's result and their own vote. So the comparative ballot does not satisfy rule (R1), but only rules (R2)–(R4). The tallyman's duty is to examine whether they agree on the question, in other words, to detect whether they have cast the same vote. However, the tallyman should not gain any information about the individual vote of either Alice or Bob.

To achieve the latter goal of the tallyman, the initial ballot state should satisfy two requirements: (1) the state cannot introduce too much noise in the final measurement by the tallyman and (2) the quadratures of single modes making up the state cannot be fully decided. Entanglement is a solution to the problem. In our protocol we employ the continuous-variable Einstein-Podolsky-Rosen (EPR) state [9] as the initial ballot state. The EPR state is expressed in Heisenberg operators as

$$\begin{aligned}
\hat{x}_1 &= \frac{1}{\sqrt{2}}e^{+r}\hat{x}_1^{(0)} + \frac{1}{\sqrt{2}}e^{-r}\hat{x}_2^{(0)},\\
\hat{p}_1 &= \frac{1}{\sqrt{2}}e^{-r}\hat{p}_1^{(0)} + \frac{1}{\sqrt{2}}e^{+r}\hat{p}_2^{(0)},\\
\hat{x}_2 &= \frac{1}{\sqrt{2}}e^{+r}\hat{x}_1^{(0)} - \frac{1}{\sqrt{2}}e^{-r}\hat{x}_2^{(0)},\\
\hat{p}_2 &= \frac{1}{\sqrt{2}}e^{-r}\hat{p}_1^{(0)} - \frac{1}{\sqrt{2}}e^{+r}\hat{p}_2^{(0)},
\end{aligned} \tag{1}$$

where the superscript "(0)" denotes initial vacuum modes.

To begin with, the two modes 1 and 2 in Eqs. (1) are sent to Alice and Bob, respectively. A voter makes a yes vote by applying a local rotation transformation $\hat{x} \to -\hat{x}$, $\hat{p} \to -\hat{p}$ on the possessed mode. A no vote is cast by simply doing no change on the mode. After voting, the tally man collects the two modes $\hat{x}_1', \hat{p}_1'$ and $\hat{x}_2', \hat{p}_2'$, measures the position of both modes, and then reduces them to classical results x_1' and x_2'. From the classical results we can identify whether Alice and Bob have cast the same vote. Now we will explain how the outcomes of the measurements reveal the votes. We assume r in Eqs. (1) satisfies $r \to \infty$ in the following discussion. Under this condition, the EPR state in Eqs. (1) is an eigenstate of total momenta $p_1 + p_2 = 0$ with relative positions $x_1 - x_2 = 0$. When Alice and Bob cast the same votes, the two modes either remain unchanged or both are rotated. This will result in no change of relative positions $x_1' - x_2' = 0$. When Alice and Bob cast different votes, one of the modes will be rotated while the other will not. In this case, the relative positions will no longer be zero but the sum of positions $x_1' + x_2' = 0$. Because the tallyman cannot decide the outcome of position measurement of the initial ballot modes [see Eqs. (1)], the infinite exponent in the first term of $\hat{x}_1$ and $\hat{x}_2$ will make x_1 and x_2 completely unpredictable, and the information of individual votes will be concealed. In short, we can decide whether the two voters agree by examining whether the classical positions satisfy $x_1' - x_2' = 0$ or $x_1' + x_2' = 0$.

Admittedly, the two above conditions can be simultaneously satisfied. That is when $x_1' = x_2' = 0$. However, when $r \to \infty$, the possibility occurs that $x_1' = x_2' = 0$ is zero, and thus will not worry us. What matters is when r is a large but finite value. Under this condition, an error of $e^{-r}/\sqrt{2}$ should be considered when the tallyman makes the decision. Therefore, the deciding condition must be changed to $x_1' - x_2' = 0 \pm e^{-r}/\sqrt{2}$ and $x_1' + x_2' = 0 \pm e^{-r}/\sqrt{2}$. In addition, the possibility that x_1' and x_2' satisfy both conditions is no longer zero. Another similar procedure may solve this problem.

An alternative scheme, which simply changes the position measurements by the tallyman into momentum measurements, also works. When $r \to \infty$, the tallyman only has to examine whether $p_1' + p_2' = 0$, which implies that two votes are the same, or $p_1' - p_2' = 0$, which implies that two votes are different.

B. Anonymous survey

In preceding protocol, the restriction exists that the answer is binary-valued. In many cases, however, the answer to a question is an integer, or more generally, a real number. The goal of an anonymous survey is to find the voter's opinion about such a question. An anonymous survey satisfies rules (R1)–(R3) but not rule (R4).

Suppose n people take part in a quantum anonymous survey. Again we employ continuous-variable EPR states in Eqs. (1) in our scheme. Instead of rotation operation, we take advantage of a displacement operation defined in this survey as

$$\hat{D}_k(\alpha,\beta) : \begin{cases} \hat{x}_k \to \hat{x}_k + \alpha, \\ \hat{p}_k \to \hat{p}_k + \beta. \end{cases} \tag{2}$$

The subscript k means the operation on mode k; α and β can be arbitrary real numbers.

In this protocol, the tallyman keeps one mode (mode 1) to himself and sends the other mode (mode 2) to the voters. Voters can only apply operations on mode 2. Assume the value of voter i is v_i, voter i can register the vote by applying an $\hat{D}_2(v_i,0)$ operation on mode 2. Therefore, we get the relationship $\hat{x}_2^{(i)} = \hat{x}_2^{(i-1)} + v_i$, where $\hat{x}_2^{(i)}$ is mode 2 after the ith voter has registered. After all n people have cast their votes, mode 2 is expressed as

$$\begin{aligned}
\hat{x}_2^{(n)} &= \frac{1}{\sqrt{2}}e^{+r}\hat{x}_1^{(0)} - \frac{1}{\sqrt{2}}e^{-r}\hat{x}_2^{(0)} + \sum_{i=1}^{n} v_i,\\
\hat{p}_2^{(n)} &= \frac{1}{\sqrt{2}}e^{-r}\hat{p}_1^{(0)} - \frac{1}{\sqrt{2}}e^{+r}\hat{p}_2^{(0)}.
\end{aligned} \tag{3}$$

Then mode 2 is sent back to the tallyman, who performs position measurements on both modes 1 and 2. By calculating

the difference between the classical outcomes x_1 and $x_2^{(n)}$, the tallyman can gain information about the sum of all voters' answers to the survey $\sum_{i=1}^{n} v_i$, with an error of $e^{-r}/\sqrt{2}$. Under the condition of $r \to \infty$, we can get the exact result of the survey.

III. QUANTUM ANONYMOUS VOTING EXTENSION AND CHEATING DEFENSE

In this section we will introduce voting protocols as an extension of the basic schemes in Sec. II. For general voting, it involves n voters, whose votes can only be one of the m given choices (candidates). But for both of the two basic schemes, the disadvantages are evident. The comparative ballot is feasible only for two voters. If n voters participate in the voting, the ballot state must be expanded to an n-partite GHZ state, which is hard to prepare. A greater difficulty is that the measurement can only imply the individual votes, rather than the desired collective results. In contrast, an anonymous survey has neither problem: we only need easily prepared m couples of EPR states, since the choice number m is much smaller than the number of voters n (especially in a nationwide election); the choice by each voter will be cast on the same mode, so the measurement results will be the sum of all voters. The tallyman can only get a collective result so he cannot get personal information. The voter can just access one part of the EPR state, so voters cannot know other voters' situations. However, a disadvantage needs to be noted: in the extension of an anonymous survey, cheating by voting more than one vote must be prohibited.

In the rest of this section, we will introduce two protocols: a simpler binary-valued ballot, which has only two candidates, and a more complex multivalued ballot, which we will discuss for the condition of m candidates. With regard to cheating, we do not consider the situation in which the voters want to destroy the ballot. We only consider that the ballot is effective according to our rules, i.e., the voter should not be found in the cheating process.

A. Binary-valued ballot

The binary-valued ballot requires the vote to be a binary digit rather than a real number. Such a ballot is useful in a democratic election with only two candidates. Each voter can make a vote for one candidate, and voters have the right to decline to vote (which is a specific case of multivalued ballot). Without loss of generality, a binary-valued ballot can be simplified to a "yes" or "no" vote.

Anonymous surveys can be used for a binary-valued ballot: voters can cast a unit value v_0 to vote yes, or do nothing (or cast a zero value) to vote no. After all n voters have completed their operation, the tallyman measures the total displacement which indicates the number of yes votes. The number of no votes can be calculated from the number of yes votes and the number of voters. But an anonymous survey cannot prevent voters from casting more than one vote. A voter may cheat by casting $m \times v_0$ to vote yes m times.

To defend against this kind of cheating, the protocol must be further developed. Since the above problem occurs when we only measure yes votes but do not detect the no votes directly, a scheme (Fig. 1) that records both kinds of votes will solve the problem.

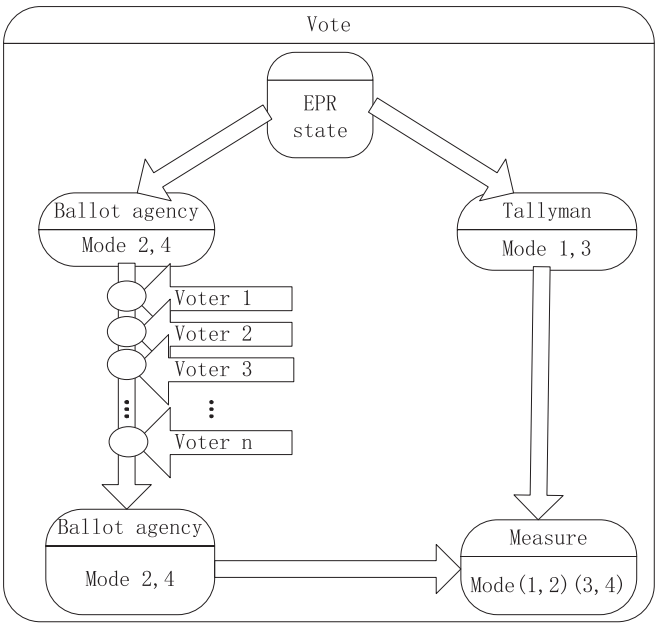

FIG. 1. Two-valued ballot process with two couples of EPR states.

In this protocol, we employ as our ballot states two couples of EPR states:

$$
\begin{aligned}
\hat{x}_1 &= \frac{1}{\sqrt{2}} e^{+r} \hat{x}_1^{(0)} + \frac{1}{\sqrt{2}} e^{-r} \hat{x}_2^{(0)}, \\
\hat{p}_1 &= \frac{1}{\sqrt{2}} e^{-r} \hat{p}_1^{(0)} + \frac{1}{\sqrt{2}} e^{+r} \hat{p}_2^{(0)}, \\
\hat{x}_2 &= \frac{1}{\sqrt{2}} e^{+r} \hat{x}_1^{(0)} - \frac{1}{\sqrt{2}} e^{-r} \hat{x}_2^{(0)}, \\
\hat{p}_2 &= \frac{1}{\sqrt{2}} e^{-r} \hat{p}_1^{(0)} - \frac{1}{\sqrt{2}} e^{+r} \hat{p}_2^{(0)},
\end{aligned}
\tag{4}
$$

$$
\begin{aligned}
\hat{x}_3 &= \frac{1}{\sqrt{2}} e^{+r} \hat{x}_3^{(0)} + \frac{1}{\sqrt{2}} e^{-r} \hat{x}_4^{(0)}, \\
\hat{p}_3 &= \frac{1}{\sqrt{2}} e^{-r} \hat{p}_3^{(0)} + \frac{1}{\sqrt{2}} e^{+r} \hat{p}_4^{(0)}, \\
\hat{x}_4 &= \frac{1}{\sqrt{2}} e^{+r} \hat{x}_3^{(0)} - \frac{1}{\sqrt{2}} e^{-r} \hat{x}_4^{(0)}, \\
\hat{p}_4 &= \frac{1}{\sqrt{2}} e^{-r} \hat{p}_3^{(0)} - \frac{1}{\sqrt{2}} e^{+r} \hat{p}_4^{(0)}.
\end{aligned}
\tag{5}
$$

These two couples of EPR states are eigenstates of total momenta $p_1 + p_2 = 0$ and $p_3 + p_4 = 0$ with relative positions $x_1 - x_2 = 0$ and $x_3 - x_4 = 0$ when $r \to \infty$. The tallyman keeps modes 1, 3 and sends modes 2, 4 to the voters. Voters cast a yes vote by applying $\hat{D}_2(v_0,0)$ operation and a no vote by the $\hat{D}_4(v_0,0)$ operation, where v_0 is the unit value of a vote. After all n voters have completed, the tallyman collects modes 2 and 4, $\hat{x}_2^{(n)}$ and $\hat{x}_4^{(n)}$. Then he measures the position of all four modes and reduces them to the classical result x_1, $x_2^{(n)}$, x_3, and $x_4^{(n)}$, then he calculates the yes and no votes. Under the condition of $r \to \infty$, the number of each kind of vote is

expressed as

$$n_{\text{yes}} = \frac{x_2^{(n)} - x_1}{v_0}, \quad n_{\text{no}} = \frac{x_4^{(n)} - x_3}{v_0}. \tag{6}$$

The sum of two numbers should be equal to the number of voters, i.e., $n_{\text{yes}} + n_{\text{no}} = n$. If the result does not satisfy the relationship, someone must have cheated. Also, when r in Eqs. (6) is a finite number, an error of $e^{-r}/\sqrt{2}$ will be introduced to the identical relationship among x_1, x_2 and x_3, x_4. Therefore, Eqs. (6) are transformed to

$$n_{\text{yes}} = \frac{x_2^{(n)} - x_1}{v_0} \pm \frac{e^{-r}}{\sqrt{2}v_0}, \quad n_{\text{no}} = \frac{x_4^{(n)} - x_3}{v_0} \pm \frac{e^{-r}}{\sqrt{2}v_0}. \tag{7}$$

Since the ballot result is required to be deterministic and unambiguous, the amount of error $e^{-r}/\sqrt{2}v_0$ should be controlled to less than $\frac{1}{2}$. Thus, a restriction is set to v_0: $v_0 > \sqrt{2}e^{-r}$. Because of inaccurate measurement and the introduced error, the numbers n_{no} or n_{yes} may not be integers. We round them to the nearest whole number and then consider them as before. If $n_{\text{no}} + n_{\text{yes}} \neq n$, then voter cheating has occurred.

However, voters can still cheat in this scheme. Suppose voter i wants to vote two yes votes, he can apply $\hat{D}_2(2v_0,0)$ on mode 2. At the same time, he can also apply $\hat{D}_4(-v_0,0)$ on mode 4 because a voter has access to both modes 2 and 4. Even if there are some restrictions to prevent them from operating on both modes, he can still connive with another voter j. If voter i operates $\hat{D}_2(3v_0,0)$ on mode 2 and voter j operates $\hat{D}_4(-v_0,0)$ on mode 4, then two voters can vote yes three times and at the same time reduce the no votes by one. To prevent this kind of cheating, we have a further developed scheme.

Improvement method. When a voter votes, he makes a more complicated displacement on the vote mode (modes 2 and 4). We bring in a new operator defined as

$$\hat{D}_{0k}(\alpha,\beta) = \hat{D}_k(e^{\alpha},e^{\beta}) : \begin{cases} \hat{x}_k \rightarrow \hat{x}_k + e^{\alpha}, \\ \hat{p}_k \rightarrow \hat{p}_k + e^{\beta}. \end{cases} \tag{8}$$

The voter can only adjust the value of α or β to vote. When a voter k makes a yes or no vote, modes 2 and 4 become

$$\begin{aligned} x_2^{(k)} &= \hat{D}_{02}(v_k,0)x_2^{(k-1)} = x_2^{(k-1)} + e^{v_k} \\ x_4^{(k)} &= \hat{D}_{04}(v_k,0)x_4^{(k-1)} = x_4^{(k-1)} + e^{v_k}. \end{aligned} \tag{9}$$

Here v_k is dependent on the voter; and for one vote, v_i should be a constant v_0. After all voters have voted, modes 2 and 4 become

$$\begin{aligned} \hat{x}_2^{(n)} &= \frac{1}{\sqrt{2}}e^{+r}\hat{x}_1^{(0)} - \frac{1}{\sqrt{2}}e^{-r}\hat{x}_2^{(0)} + \sum_{i=1}^{n} e^{v_i}, \\ \hat{p}_2^{(n)} &= \frac{1}{\sqrt{2}}e^{-r}\hat{p}_1^{(0)} - \frac{1}{\sqrt{2}}e^{+r}\hat{p}_2^{(0)}, \\ \hat{x}_4^{(n)} &= \frac{1}{\sqrt{2}}e^{+r}\hat{x}_1^{(0)} - \frac{1}{\sqrt{2}}e^{-r}\hat{x}_2^{(0)} + \sum_{i=1}^{n} e^{v_i}, \\ \hat{p}_4^{(n)} &= \frac{1}{\sqrt{2}}e^{-r}\hat{p}_1^{(0)} - \frac{1}{\sqrt{2}}e^{+r}\hat{p}_2^{(0)}. \end{aligned} \tag{10}$$

Here v_i is the ith vote. We suppose $r \rightarrow \infty$. And the number of yes and no votes can be expressed as

$$n_{\text{yes}} = \frac{x_2^{(n)} - x_1}{e^{v_0}}, \quad n_{\text{no}} = \frac{x_4^{(n)} - x_3}{e^{v_0}}. \tag{11}$$

If every voter voted and no one cheated, the number of voters should equal the sum of the number of yes and no votes ($n = n_{\text{yes}} + n_{\text{no}}$). The new introduced operation is to stop voters from casting negative votes.

First we consider the case that all the voters have voted and discuss if our design can detect all the cheating. When just a single voter cheated, for example, the voter voted $\hat{D}_{0(2i)}(3v_0,0)$ or $\hat{D}_{0(2i)}(-v_0,0)$ ($i = 1, 2$). This kind of cheating can be easily detected by examining $n = n_{\text{yes}} + n_{\text{no}}$. For the operation $\hat{D}_{0(2i)}(v_0 + \ln 2,0)$, there would be two votes. It also can be detected by examining $n = n_{\text{yes}} + n_{\text{no}}$. The cheating by more than one voter can be detected in a similar way.

Second there are voters making no vote. If a voter makes no vote but another voter votes twice, the detecting system could not find this kind of cheating. However, if we think of making a no vote as a third choice, this cheating can be found. It is the multivalued ballot and will be discussed below. In conclusion, if ($n = n_{\text{yes}} + n_{\text{no}}$), there was no cheating; otherwise, some one cheated.

Also, when r in Eqs. (11) is a finite number, an error of $e^{-r}/\sqrt{2}$ will be introduced to the equal relationship among x_1, x_2 and x_3, x_4. Therefore, Eqs. (11) are changed to

$$n_{\text{yes}} = \frac{x_2^{(n)} - x_1}{e^{v_0}} \pm \frac{e^{-r}}{\sqrt{2}e^{v_0}}, \quad n_{\text{no}} = \frac{x_4^{(n)} - x_3}{e^{v_0}} \pm \frac{e^{-r}}{\sqrt{2}e^{v_0}}. \tag{12}$$

Considering that the result should be deterministic and unambiguous, the amount of error $e^{-r}/\sqrt{2}e^{v_0}$ should be controlled to less than $\frac{1}{2}$. Thus, a restriction is set to v_0: $v_0 > \ln(\sqrt{2}e^{-r})$. The improved method also has the problem that the number n_{no} or n_{yes} may not be an integer. We round it to the nearest whole number and then consider it as before. If $n_{\text{no}} + n_{\text{yes}} \neq n$ there is voter cheating. But it is possible to make a wrong judgment too, with each voter making one vote exactly, but $n_{\text{no}} + n_{\text{yes}} \neq n$. To reduce this kind of mistake we should improve the measurement accuracy.

B. Multivalued ballot

The difference between binary-valued and multivalued ballots lies in the fact that the first one has two choices while the other has m ($m > 2$) choices. Still, there are n voters participating in the ballot. This time we also need a ballot agency to assist voting. Considering there are m choices for each voter, we employ m couples of EPR states, with an eigenstate of total momenta $p_{2(i+1)} + p_{2i+1} \rightarrow 0$ with relative positions $x_{2(i+1)} - x_{2i+1} \rightarrow 0$ ($i = 0,1,2,\ldots,m-1$) when $r \rightarrow \infty$ for every pair of modes. In the voting process (Fig. 2), the tallyman keeps modes $(2i+1)$ and the rest of the m modes, mode $(2i+2)$, are sent to the ballot agency, where the voters cast their votes. We implement the improved

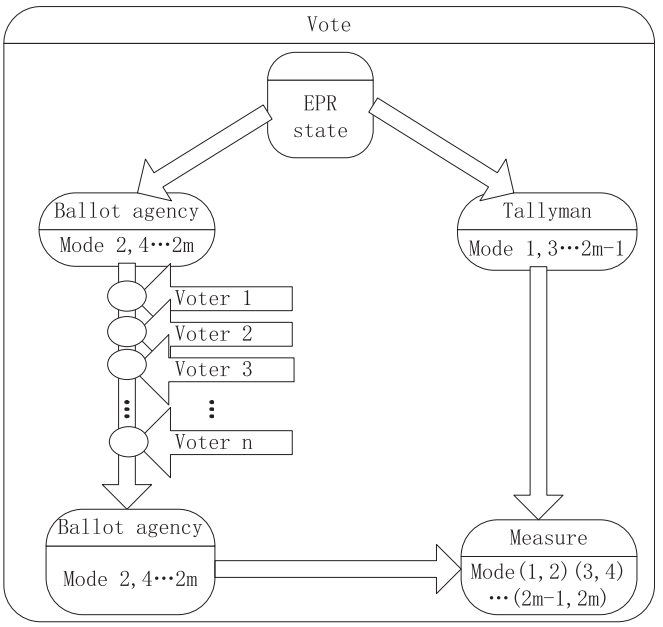

FIG. 2. m-valued ballot process with m couples of EPR states.

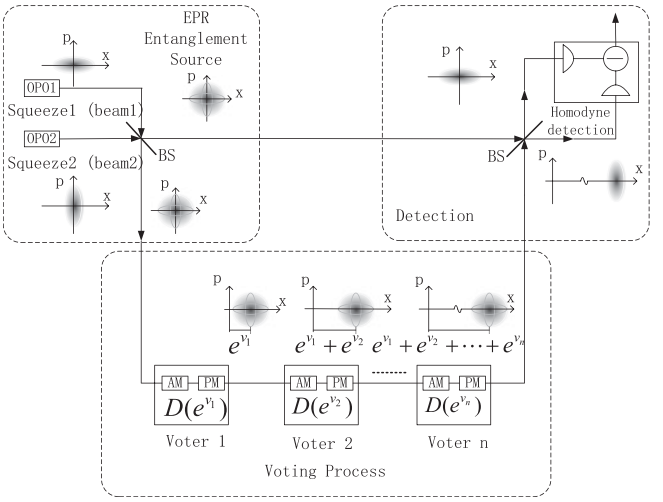

FIG. 3. Experimental setup for ballot. OPO: optical parametric oscillator, BS: 50:50 beam splitter, AM: amplitude modulator, and PM: phase modulator.

displacement operation in this protocol. Again, the voters are required to submit m position modes for all m choices. To vote for the kth choice, the voter would make an e^{v_0} displacement on the position of the $2k$th mode. The jth voter wants to make a vote on the kth mode, then $x_k^j = D_{0k}(v_j)x_k^{j-1}$ $[D_{0k}(v) = D_{0k}(v,0) = D_k(e^v,0)]$. Like the two-valued ballot, we have two situations.

First, all voters have voted. After all voters have finished the voting, we could get the number of each candidate's votes:

$$\begin{aligned} n_2 &= \frac{x_2^{(n)} - x_1}{e^{v_0}}, \\ n_4 &= \frac{x_4^{(n)} - x_3}{e^{v_0}}, \\ &\vdots \\ n_{2m} &= \frac{x_{2m}^{(n)} - x_{2m-1}}{e^{v_0}}. \end{aligned} \tag{13}$$

Then we can judge whether there are voters cheating by comparing the number of votes and the number of voters. If $\sum_{i=1}^{m} n_{2i} = n$, there is no cheating, otherwise someone has cheated in the voting.

Second, there is the case of a voter making no vote. If we know that not every voter has used his/her vote, we cannot examine cheating by the method above. But we could set the option of making a no vote as the $(m+1)$th choice. Then we could detect cheating and also find the number of voters who have given up voting.

When r is a large but finite value, an error of $e^{-r}/\sqrt{2}$ should be considered when the tallyman makes the decision, as for the two-valued ballot. And the situation in which the number n_{no} or n_{yes} may not be an integer should be considered too.

We also think about the how to make our proposal become reality and we give a basic experimental graph of a ballot in Fig. 3. The figure includes three parts: entanglement source, voting process, and detecting system. EPR states were sent to the voting part and detecting part separately. In the voting process voters make a displacement on the amplitude or phase to vote. And the tallyman compares the two parts of EPR states to get the voting result in the detecting part.

IV. CONCLUSIONS

In the paper we discuss two-valued and multivalued ballots. Entangled state of continuous variables was used as the information carrier to ensure the privacy and anonymity of each voter. Part of the entangled state was sent to tallyman and the other was sent to the ballot agency where voters can vote. After all votes have been cast, the tallyman collects the collective data and calculates the number of the votes. For the quality of entanglement the voters are unable to gain information of others and the tallyman just knows the collective quantity of votes. We introduce the special operation $D_{0k}(\alpha,\beta)$ to stop voters from casting multiple votes. With the new operation, voters cannot make negative votes, and thus are unable to cheat without being discovered.

We also considered some other securities, which we will detect at the beginning of the ballot if the system works well. We detect the entanglement source randomly, then we decide if we choose the rest of the source as m couples of EPR states. In the case of a dishonest tallyman, the tallyman could just give some data arbitrarily without considering the real data. So the tallyman should perform all the operations under public surveillance.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61102053, No. 61170228, No. 60970109, and No. 60801051) and SJTU PRP (Grants No. T030PRP18001 and No. T030PRP19035).

[1] D. Gritzalis, *Secure Electronic Voting* (Kluwer, Dordrecht, Netherlands, 2003).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
[4] Y. G. Yang and Q. Y. Wen, J. Phys. A **42**, 055305 (2009).
[5] M. Bonanome, V. Buzek, M. Hillery, and M. Ziman, Phys. Rev. A **84**, 022331 (2011).
[6] D. Horoshko and S. Kilin, Phys. Lett. A **375**, 1172 (2011).
[7] M. Hillery, M. Ziman, V. Buzek, and M. Bielikova, Phys. Lett. A **349**, 75 (2006).
[8] J. A. Vaccaro, J. Spring, and A. Chefles, Phys. Rev. A **75**, 012333 (2007).
[9] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).