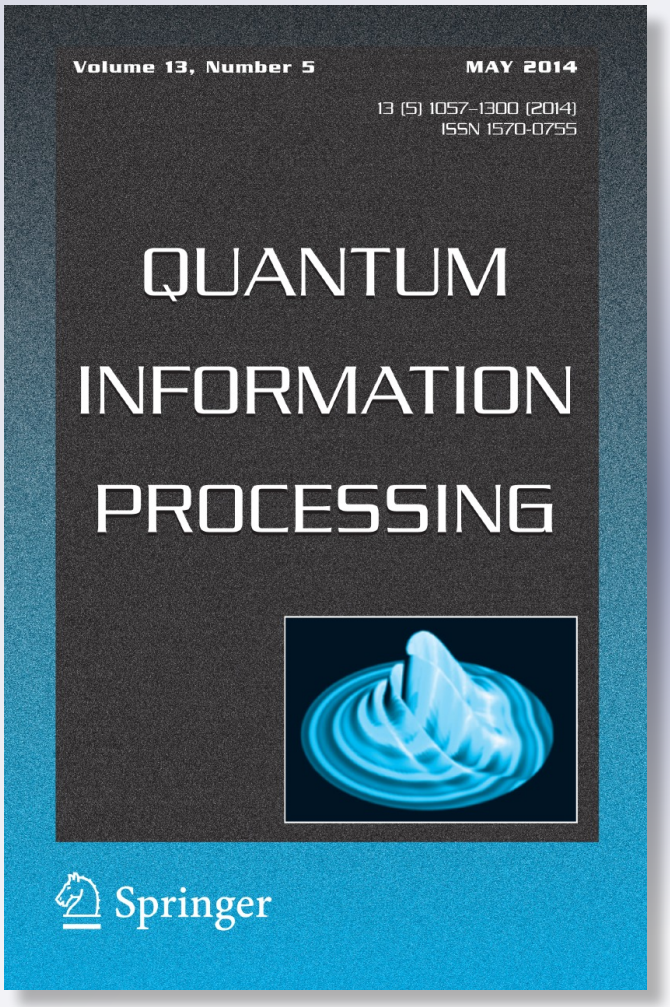
Quantum secret sharing with continuous variable graph state

Yadong Wu, Runze Cai, Guangqiang He & Jun Zhang

Quantum Information Processing

ISSN 1570-0755
Volume 13
Number 5

Quantum Inf Process (2014)
13:1085-1102
DOI 10.1007/s11128-013-0713-7



Springer

Quantum Inf Process (2014) 13:1085–1102
DOI 10.1007/s11128-013-0713-7

Quantum secret sharing with continuous variable graph state

Yadong Wu · Runze Cai · Guangqiang He · Jun Zhang

Received: 1 October 2013 / Accepted: 5 December 2013 / Published online: 17 December 2013

Abstract In this paper, we study several physically feasible quantum secret sharing (QSS) schemes using continuous variable graph state (CVGS). Their implementation protocols are given, and the estimation error formulae are derived. Then, we present a variety of results on the theory of QSS with CVGS. Any (k, n) threshold protocol of the three specific schemes satisfying $\frac{n}{2} < k \leq n$, where n denotes the total number of players and k denotes the minimum number of players who can collaboratively access the secret, can be implemented by certain weighted CVGS. The quantum secret is absolutely confidential to any player group with number less than threshold. Besides, the effect of finite squeezing to these results is properly considered. In the end, the duality between two specific schemes is investigated.

Keywords Quantum secret sharing · Continuous variables · Graph state

Y. Wu (✉) · R. Cai · J. Zhang
Joint Institute of UMich-SJTU, Shanghai Jiao Tong University,
Shanghai 200240, China
e-mail: wuyadong301@sjtu.edu.cn

R. Cai
e-mail: cairunze@sjtu.edu.cn

J. Zhang
e-mail: zhangjun12@sjtu.edu.cn

J. Zhang
Key Laboratory of System Control and Information Processing (Ministry of Education),
Shanghai 200240, China

G. He
State Key Laboratory of Advanced Optical Communication Systems and Networks, and Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
e-mail: gqhe@sjtu.edu.cn

1 Introduction

Quantum cryptography provides an entirely new approach to achieve the communication security by taking advantage of quantum mechanics principles [1]. Among various quantum cryptography schemes, quantum secret sharing (QSS) is a general multipartite information security scheme that attracted extensive research interests [2–7]. It allows a dealer to distribute an encoded secret, which may be a string of bits or qubits, among a number of players in such a manner that only certain sufficient number of players can collaboratively reconstruct the secret, and fewer players cannot access any information about the secret. QSS has its origin in classical information theory. The first QSS scheme was given in [2] utilizing GHZ states. Reference [3] studied the theory of threshold schemes to share quantum secrets. Reference [4] further investigated the theory of QSS, e.g., schemes with general access structures, and sharing classical secrets using quantum states.

On the other hand, graph state [8] has been extensively studied in applications, such as quantum error correction [9], entanglement purification [10], entanglement measurement [8], and Bell inequality [11]. It is a special type of multi-particle entangled state that can be represented by a mathematical graph, where each vertex denotes a qubit, and each edge denotes an Ising interaction.

In recent years, QSS with graph state was introduced in [5] to treat three kinds of threshold QSS schemes in a unified graph state approach and to propose embedded protocols in large graph states. Reference [6] generalized the results to prime dimensions, and Ref. [7] investigated non-threshold schemes in the graph state formalism.

All these results are based on the discrete variable formalism. However, any discrete variable quantum communication protocol requires the generation and detection of single photon, which is difficult to implement in practical experiments. The essential steps in quantum communication, i.e., preparation, modulation, and measurement, can be efficiently implemented in quantum optics utilizing the continuous variable quadratures of the quantized electromagnetic fields [22]. For example, an entangled state can be prepared by squeezed lights and linear optics, and the shift amount in the quadrature phase space can be measured by a homodyne detection. Experimental demonstrations of QSS with continuous variables were reported in Refs. [12,13].

Thus, we are interested in the implementation of QSS using continuous variable graph state (CVGS). CVGS was first introduced in [14] as the Gaussian analogue of discrete variable graph state. It is a multi-particle entangled quantum state that can be associated with a mathematical graph, where each vertex denotes a qumode and each edge denotes a quantum non-demolition coupling between two qumodes. It has the nice property that any local Gaussian operation on a CVGS can be associated with a geometric transformation on its graph representation [15]. CVGS has been shown to be useful in universal quantum computation [16,17] and blind quantum computation [18]. In addition, CVGS also finds applications in quantum communications, e.g., Ref. [19] proposed a protocol to realize quantum teleportation between two parties.

In this paper, we study the implementations and properties of four QSS schemes with CVGS. According to secret and communication channel types, we can differentiate eight QSS schemes. Among all these schemes, we are interested in four of them,

because the other four are either physically infeasible or insecure. These schemes extend the works in [5,6] into the CVGS domain.

For each QSS scheme using CVGS, we design an implementation protocol for the dealer and players to follow so that the players may collaborate to estimate the secret. The mean value and variance of the estimation error are calculated explicitly. Based on these analytic formulae, we can derive the conditions for unbiased estimation, which means that the difference between the expectation of the estimator and the real parameter being estimated is zero. Furthermore, the parameters in the implementation protocol can be tuned to minimize the error variance, namely, the variance of the unbiased estimator. In the extremal case of infinite squeezing, it is shown that the condition that a set of players perfectly estimate the secret can be transformed to the consistency of a set of linear equations. By perfectly estimating the secret, we mean that the players obtain a zero-variance unbiased estimator for the secret.

Then, we focus on the investigation of threshold schemes. In QSS, a (k, n) threshold protocol refers to the case when k players or more can reconstruct the secret collaboratively, and any set of fewer than k players cannot get any information about the secret. For continuous variable case, we would like to explain threshold protocols in an equivalent way: Any k or more players can estimate the secret perfectly, and any set of fewer than k players cannot estimate the secret within a finite error bound. We show that for three schemes, an arbitrary (k, n) threshold protocol with $\frac{n}{2} < k \leq n$ can be implemented using a weighted CVGS prepared with infinitely squeezed qumodes. For two schemes, these protocols cover all the physically feasible cases, and we also reveal the duality between two schemes. An interesting observation is that for the scheme with quantum secret, private distribution channel, and quantum player–player channel, the threshold protocol for two noncooperative player groups is exclusive, meaning that if one group can perfectly estimate the secret qumode, the other cannot estimate either quadrature of the secret qumode within a finite error bound. The security of the quantum secret is thus guaranteed. However, the definition of threshold scheme works only in the ideal case of infinite squeezing. In experiments, we utilize finite squeezed lights to prepare CVGSs. So, we analyze the effect of finite squeezing to the threshold schemes.

This paper is organized as follows. Section 2 provides a brief introduction on QSS schemes and CVGS. Three QSS schemes with CVGS are investigated in Sects. 3, 4, and 5, respectively. We conclude the paper in Sect. 6.

2 Background

In this section, we give a brief introduction of QSS schemes and CVGS.

In a QSS protocol, there are one dealer and n players as illustrated in Fig. 1. The dealer has a secret that is encoded into either a string of real numbers or qumodes. We assume that the string is shared one by one, and at a time, one real number or one qumode is shared. In each round, the dealer encodes the number or qumode into a prepared quantum state and subsequently distributes it to all the players through either private or public channels. With this quantum state under disposal, a group of players can either apply local operations to their own states and then exchange

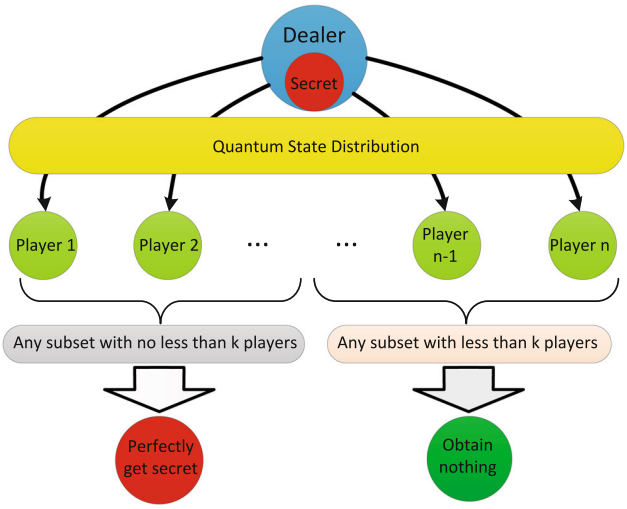


Fig. 1 QSS (k, n) threshold protocol

classical information, or take joint operations to their states. Based on the information circulated around, the task for these players is to reconstruct the secret.

We can classify QSS into eight schemes according to their secret type (classical or quantum), dealer–player distribution channel (private or public), and player–player communication channel (classical or quantum). Acronyms can be used to denote these eight schemes in the following way: The first "C" or "Q" denotes the secret type; "Pvt" or "Pub" denotes the dealer–player distribution channel; the second "C" or "Q" denotes the player–player communication channel; each scheme is characterized by the combination of these three acronyms in this order. Among all these eight schemes, QPubC and QPvtC are physically infeasible because it is impossible to recover unknown quantum information from classical information. Moreover, QPubQ and CPubQ are insecure because the eavesdropper can disguise his/her identity to modify the information on public channel. Therefore, we will investigate only the four schemes in Table 1:

CPvtC: *classical* secret sharing with *private* quantum channels between the dealer and the players, and *classical* channels connect each pair of players;
QPvtQ: *quantum* secret sharing with *private* quantum channels between the dealer and the players, and *quantum* channels connect each pair of players;
CPubC: *classical* secret sharing with *public* quantum channels between the dealer and the players, and *classical* channels connect each pair of players;
CPvtQ: *classical* secret sharing with *private* quantum channels between the dealer and the players, and *quantum* channels connect each pair of players.

Among all these four schemes, CPvtC has no clear advantages over the classical secret sharing—it just use the CVGS formalism to solve a classical information problem. On the other hand, CPubC and CPvtQ schemes both share the classical secret, but they also take advantage of the quantum features. Specifically, CPubC scheme can

Table 1 Feasible QSS schemes

	Secret type	Dealer–Player channel	Player–Player channel
CPvtC	Classical	Private	Classical
QPvtQ	Quantum	Private	Quantum
CPubC	Classical	Public	Classical
CPvtQ	Classical	Private	Quantum

protect the classical secret from eavesdropping, and CPvtQ scheme can double the efficiency of encoding. Different from these three schemes, QPvtQ is a pure quantum scheme parallel to classical secret sharing.

In particular, we are interested in (k, n) threshold protocols, which correspond to the case when it requires at least k players to estimate the secret perfectly, and any set with less than k players cannot estimate the secret within a finite error bound. This procedure is shown in Fig. 1.

Furthermore, we will use CVGS to implement QSS schemes. A CVGS is an entangled multi-qumode state that can be represented by an undirected graph. Denote the adjacency matrix of this graph as G, whose element G_{ij} represents the interaction gain of the coupling between qumode i and j. If G_{ij} takes only binary values 0 or 1, it is an unweighted CVGS; otherwise, it is a weighted CVGS.

In a QSS scheme, the dealer needs to prepare a CVGS and then to encode the secret into that CVGS. At the beginning, the dealer has n vacuum states each with the position $X_i^{(0)}$ and the momentum $P_i^{(0)}$, where both $X_i^{(0)}$ and $P_i^{(0)}$ are random variables with standard Gaussian distribution. The dealer then squeezes the momentum and at the same time amplifies the position of each qumode, obtaining squeezed vacuum states:

$$P_j = e^{-r_j} P_j^{(0)}, \quad X_j = e^{r_j} X_j^{(0)}, \tag{1}$$

Here, r_j is the squeezing parameter for qumode j. Juxtapose X_j's and P_j's in a vector form:

$$v_{(n)} = \left[X_1 \ \ldots \ X_n \ P_1 \ \ldots \ P_n\right]^{\mathrm{T}}. \tag{2}$$

where the subscript (n) indicates the number of the qumodes, and the superscript T denotes the transpose of the vector. Now, apply a quantum non-demolition (QND) coupling with interaction gain G_{ij} to the pair (i, j) [14]. This establishes a connection between qumode i and j in the graph, and the resulting quadratures are $(X_i, P_i + G_{ij}X_j)$ and $(X_j, P_j + G_{ij}X_i)$, respectively. After a series of such QND coupling operations, the final quadratures can be written as

$$X_j^G = X_j, \quad P_j^G = P_j + \sum_{l=1}^{n} G_{jl} X_l. \tag{3}$$

Letting

$$v_{(n)}^G = \left[\, X_1^G \ \ldots \ X_n^G \ \ P_1^G \ \ldots \ P_n^G \,\right]^{\mathrm{T}}.$$

We can rewrite Eq. (3) in a compact form as

$$v_{(n)}^G = \begin{bmatrix} I & 0 \\ G_{(n)} & I \end{bmatrix} v_{(n)}, \tag{4}$$

where $G_{(n)}$ is the adjacency matrix of the n-qumode graph state.

In the next three sections, we will investigate the implementations of the CPvtC, QPvtQ, and CPubC schemes in Table 1. We point out that the CPvtQ scheme can be implemented by super-dense coding [20] and is indeed a quantum data hiding scheme [21]. Since the methodology is similar, we will focus on the first three. For simplicity, we set $\hbar = 1$ throughout this paper.

3 Case 1: CPvtC scheme

In this section, we study the CPvtC scheme, in which the dealer encodes a *classical* secret into a CVGS and then distributes the qumodes to the players through *private* channels, and finally, the players exchange information via *classical* channels so as to reconstruct the secret. We will derive the condition to perfectly estimate the secret under infinite squeezing, discuss the implementation of a (k, n) CPvtC threshold scheme on CVGS, and finally discuss the effect of finite squeezing.

Assume that the classical secret the dealer holds is a real number γ. The dealer starts from encoding the secret into a CVGS by applying a momentum displacement operation $Z(c_j\gamma) = e^{ic_j\gamma\hat{x}}$ [17] to qumode j with quadratures (X_j^G, P_j^G), where c_j, γ are real numbers and $\hat{x}$ is the position operator. The momentum of qumode j is shifted to $P_j^G + c_j\gamma$. Let $c = [\,c_1 \ \ldots \ c_n\,]^{\mathrm{T}}$. Then, the shifted momenta for all the qumodes can be written as a vector $c\gamma$. The dealer distributes qumode j to player j and publishes the vector c to all the players. Now, player j has the quadratures $(X_j^G, P_j^G + c_j\gamma)$ under disposal.

To recover the secret, player j can take the following actions:

1. Let
$$P_j^D = P_j^G + c_j\gamma. \tag{5}$$
Apply the operator $\exp\left\{-i\frac{\beta_j}{2\alpha_j}(\hat{P}_j^D)^2\right\}$ to the quadratures (X_j, P_j^D) so that the new quadratures are $\left(X_j + \frac{\beta_j}{\alpha_j}P_j^D, P_j^D\right)$.
2. Measure the position to get $\mathcal{M}\left(X_j + \frac{\beta_j}{\alpha_j}P_j^D\right)$, where $\mathcal{M}(\cdot)$ is a measurement operation that results in a random variable.
3. Scale the measurement result by α_j and obtain
$$\begin{aligned}\mu_j &= \alpha_j\mathcal{M}\left(X_j + \frac{\beta_j}{\alpha_j}P_j^D\right) \\ &= \mathcal{M}(\alpha_j X_j + \beta_j P_j^D).\end{aligned} \tag{6}$$
The last equality is because $\mathcal{M}(\cdot)$ is a linear operation.

The players can then exchange their μ_j by classical communications. We now show that with these μ_j, each player can use the sum of μ_j to estimate the secret γ. From Eqs. (2)–(6), the estimation error e can be calculated as

$$\begin{aligned} e &= \sum_{j=1}^{n} \mu_j - \gamma \\ &= \mathcal{M}\left(\left[a^{\mathrm{T}} \mid b^{\mathrm{T}}\right]\left(\left[\begin{array}{c|c} I & 0 \\ \hline G_{(n)} & I \end{array}\right] v_{(n)} + \left[\begin{array}{c} \mathbf{0} \\ \hline c \end{array}\right]\gamma\right)\right) - \gamma \\ &= \mathcal{M}\left(\left[a^{\mathrm{T}} + b^{\mathrm{T}} G_{(n)} \mid b^{\mathrm{T}}\right] v_{(n)}\right) + (b^{\mathrm{T}} c - 1)\gamma, \end{aligned} \tag{7}$$

where $a = [\,\alpha_1 \ \ldots \ \alpha_n\,]^{\mathrm{T}}$, $b = [\,\beta_1 \ \ldots \ \beta_n\,]^{\mathrm{T}}$ and $\mathbf{0} = [\,0 \ \ldots \ 0\,]^{\mathrm{T}}$.

The mean value of the estimation error is

$$\mathbb{E}\, e = \mathbb{E}\, \mathcal{M}\left(\left[a^{\mathrm{T}} + b^{\mathrm{T}} G_{(n)} \mid b^{\mathrm{T}}\right] v_{(n)}\right) + \left(b^{\mathrm{T}} c - 1\right)\gamma.$$

Since $\mathbb{E}\,\mathcal{M}(X_j) = \mathbb{E}\,\mathcal{M}(P_j) = 0$, we have $\mathbb{E}\,\mathcal{M}\left(\left[a^{\mathrm{T}} + b^{\mathrm{T}} G_{(n)} \mid b^{\mathrm{T}}\right] v_{(n)}\right) = 0$. Hence,

$$\mathbb{E}\, e = (b^{\mathrm{T}} c - 1)\gamma.$$

To ensure an unbiased estimation, it is required that

$$b^{\mathrm{T}} c = 1. \tag{8}$$

The variance of the estimation error can be obtained after some algebraic derivations as

$$\mathrm{Var}(e) = \|(a^{\mathrm{T}} + b^{\mathrm{T}} G_{(n)}) R_{(n)}\|^2 + \|b^{\mathrm{T}} R_{(n)}^{-1}\|^2, \tag{9}$$

where $R_{(n)} = \mathrm{diag}\{e^{r_1}, \ldots, e^{r_n}\}$, and $\|\cdot\|$ is the Euclidean norm.

To enhance the estimation precision, we want to reduce the variance. However, it is easy to see that under constraint (8), the variance (9) can never achieve zero for any finite choices of parameters. Therefore, the secret can be perfectly estimated only if some parameters assume values at infinity. One choice of parameters is to let $\|c\| \to \infty$ and $\|a\|,\ \|b\| \to 0$, which is physically meaningless. Another method is to apply infinite squeezing, i.e., letting the squeezing parameters $r_j \to \infty$ and

$$a^{\mathrm{T}} + b^{\mathrm{T}} G_{(n)} = \mathbf{0}^{\mathrm{T}}. \tag{10}$$

Combining Eqs. (8) and (10) yields that

$$\left[a^{\mathrm{T}} \mid b^{\mathrm{T}}\right]\left[\begin{array}{c|c} I & \mathbf{0} \\ \hline G_{(n)} & c \end{array}\right] = \left[\mathbf{0}^{\mathrm{T}} \mid 1\right]. \tag{11}$$

Eq. (11) is a condition that guarantees n players to get the secret perfectly under infinite squeezing.

Now, consider the case when there are only k collaborating players where $k < n$. To simplify the notation, we use $A_{J,K}$ to denote a matrix obtained by taking rows with indices in J and columns in K from a matrix A, where J, K are subsets of $N = \{1, \ldots, n\}$. For the case of a vector, we can similarly define v_J. Removing the rows and columns corresponding to these players from Eq. (11), we obtain

$$\begin{bmatrix} a_J^{\mathrm{T}} & b_J^{\mathrm{T}} \end{bmatrix} \begin{bmatrix} I_{J,N} & \mathbf{0} \\ G_{J,N} & c_J \end{bmatrix} = \begin{bmatrix} 0 \cdots 0 \; 1 \end{bmatrix}, \tag{12}$$

where $J = \{j_1, \ldots, j_k\}$. Equation (12) is a sufficient and necessary condition for k players from a set of n players to recover the secret perfectly under infinite squeezing.

We show that by using weighted CVGS, any QSS threshold protocol of CPvtC scheme with (k, n), where $k \leq n < 2k$, can be implemented. This demonstrates that CVGS is a useful physical resource to QSS protocols. This result is presented in the following Theorem.

Theorem 1 *For arbitrary k, n satisfying $\frac{n}{2} < k \leq n$, a (k, n) threshold protocol of CPvtC scheme can be implemented on a weighted CVGS with infinite squeezing.*

To keep the flow of the paper, the proof is given in "Appendix 7.1".

This theorem depends on the assumption of infinite squeezing. But in practical experiments, infinitely squeezed light is inaccessible. So, we must analyze the effect of finite squeezing. We want to show that Eq. (12) is still an equivalent condition for a set of players to access the secret in the finite squeezing case. To see why, we suppose the squeezing parameters are such that $r_i = r$ for any i in $\{1, \ldots, n\}$. If Eq. (12) is true, a and b can be determined by Eq. (12). Then, the error variance is

$$\mathrm{Var}(e) = \sum_{j \in J} b_j^2 e^{-2r}, \tag{13}$$

which does not achieve the minimum, but is close to the minimum for large r. If Eq. (12) cannot be satisfied, the error variance of any unbiased estimator must include the term $(a_j + \sum_l b_l G_{lj})^2 e^{2r_j}$, where $a_j + \sum_l b_l G_{lj} \neq 0$. If $\|c\|$ is bounded, this term will be quite large, which makes the error variance big. So, if the error introduced by the finite squeezing is within the tolerance, we can take the protocol as a threshold protocol, and Eq. (12) is still an equivalent condition to decide whether a set of players can access the secret. Thus, Theorem 1 is still true for finite squeezing case.

4 Case 2: QPvtQ scheme

In this section, we discuss the QPvtQ scheme, in which the dealer has a *quantum* secret, the qumodes encoding the secret are distributed through *private* channels, and the players share their information by *quantum* communication channels. We show that any (k, n) threshold protocol of QPvtQ scheme can be implemented by a weighted

CVGS. Moreover, if a set of players can perfectly estimate the secret qumode, the remaining players cannot obtain any information about the secret qumode. The effect of finite squeezing will also be considered.

In a QPvtQ scheme, the dealer has a secret qumode (X_S, P_S). At the beginning, the dealer prepares an $(n+1)$-mode CVGS and keeps the $(n+1)$-th qumode with quadratures (X^G_{n+1}, P^G_{n+1}) for later use. The dealer distributes the other n qumodes to the n players. Now, the dealer performs a Bell measurement as follows. First, combine the $(n+1)$-th qumode with (X_S, P_S) to yield two new qumodes (X_u, P_u) and (X_v, P_v), where

$$\begin{aligned} X_u &= \frac{X^G_{n+1} + X_S}{\sqrt{2}}, \qquad P_u = \frac{P^G_{n+1} + P_S}{\sqrt{2}} \\ X_v &= \frac{X^G_{n+1} - X_S}{\sqrt{2}}, \qquad P_v = \frac{P^G_{n+1} - P_S}{\sqrt{2}}. \end{aligned} \tag{14}$$

Second, take homodyne measurements for X_u and P_v. The measurement results $\mathcal{M}(X_u)$ and $\mathcal{M}(P_v)$ are two Gaussian random variables.

The dealer publishes these two measurement results to all the players. If any set of players can construct the qumode $(-X^G_{n+1}, P^G_{n+1})$, they can perfectly estimate the secret by simply adding the position displacement $\sqrt{2}\mathcal{M}(X_u)$ and subtracting the momentum displacement $\sqrt{2}\mathcal{M}(P_v)$ [22]. This is the idea of continuous variable quantum teleportation [23].

To construct $(-X^G_{n+1}, P^G_{n+1})$, the players can take the following steps:

1. Apply a single-mode Gaussian unitary operation and a phase insensitive amplification [24] to transform a qumode (X^G_j, P^G_j) to $(\alpha_j X^G_j + \beta_j P^G_j, \alpha'_j X^G_j + \beta'_j P^G_j)$, where α_j, β_j, α'_j, and β'_j are all real numbers;
2. Pick one qumode from the players' qumodes and transform it to $(\sum_{j=1}^n \alpha_j X^G_j + \beta_j P^G_j, \sum_{j=1}^n \alpha'_j X^G_j + \beta'_j P^G_j)$ by using nonlocal operations such as a controlled-X operation [25].

From Eq. (4), the position error can be calculated as

$$\begin{aligned} e_x &= \sum_{j=1}^{n} (\alpha_j X^G_j + \beta_j P^G_j) - (-X^G_{n+1}) \\ &= \left[a^{\mathrm{T}}\ 0\ b^{\mathrm{T}}\ 0 \right] \left[\begin{array}{c|c} I & 0 \\ \hline G_{(n+1)} & I \end{array} \right] v_{(n+1)} \\ &\quad + [\mathbf{0}^{\mathrm{T}}_{(n)}\ 1\ \mathbf{0}^{\mathrm{T}}_{(n+1)}] v_{(n+1)} \\ &= \left[[a^{\mathrm{T}}\ 1] + [b^{\mathrm{T}}\ 0] G_{(n+1)} \,\middle|\, [b^{\mathrm{T}}\ 0] \right] v_{(n+1)}, \end{aligned} \tag{15}$$

where $a = [\alpha_1, \ldots, \alpha_n]^{\mathrm{T}}$, $b = [\beta_1, \cdots, \beta_n]^{\mathrm{T}}$, $v_{(n+1)} = [X_1, \ldots, X_{n+1}, P_1, \cdots, P_{n+1}]^{\mathrm{T}}$, and $G_{(n+1)}$ is an $(n+1) \times (n+1)$ adjacency matrix. Similarly, the momentum error is

$$
\begin{aligned}
e_p &= \sum_{j=1}^{n} (\alpha'_j X_j^G + \beta'_j P_j^G) - P_{n+1}^G \\
&= \left[a'^{\mathrm{T}}\ 0\ b'^{\mathrm{T}}\ 0 \right] \left[\begin{array}{c|c} I & 0 \\ \hline G_{(n+1)} & I \end{array} \right] v_{(n+1)} \\
&\quad - [g_{n+1}^{\mathrm{T}}\ \mathbf{0}_{(n)}^{\mathrm{T}}\ 1] v_{(n+1)} \\
&= \left[[a'^{\mathrm{T}}\ 0] + [b'^{\mathrm{T}}\ 0] G_{(n+1)} - g_{n+1}^{\mathrm{T}} \middle| [b'^{\mathrm{T}}\ -1] \right] v_{(n+1)},
\end{aligned} \tag{16}
$$

where $a' = [\alpha'_1, \ldots, \alpha'_n]^{\mathrm{T}}$, $b' = [\beta'_1, \ldots, \beta'_n]^{\mathrm{T}}$, and g_{n+1}^{T} is the $(n+1)$-th row of the matrix $G_{(n+1)}$.

By applying local unitary operations, the covariance matrix of the secret qumode can be diagonalized to

$$
\begin{pmatrix} \mathrm{Var}(X_S) & 0 \\ 0 & \mathrm{Var}(P_S) \end{pmatrix}.
$$

From Eq. (1) in [26], we can get the fidelity of the estimated secret qumode as

$$
F = \frac{2}{\sqrt{\delta + \epsilon} - \sqrt{\epsilon}}, \tag{17}
$$

where

$$
\begin{aligned}
\delta &= (2\,\mathrm{Var}(X_S) + V_1)(2\,\mathrm{Var}(P_S) + V_2), \\
\epsilon &= (\mathrm{Var}(X_S)\,\mathrm{Var}(P_S) - 1) \times \\
&\qquad [(\mathrm{Var}(X_S) + V_1)(\mathrm{Var}(P_S) + V_2) - 1], \\
V_1 &= \left\| \left[\left[a^{\mathrm{T}}\ 1 \right] + \left[b^{\mathrm{T}}\ 0 \right] G_{(n+1)} \right] R_{(n+1)} \right\|^2 \\
&\quad + \left\| \left[b^{\mathrm{T}}\ 0 \right] R_{(n+1)}^{-1} \right\|^2, \\
V_2 &= \left\| \left[\left[a'^{\mathrm{T}}\ 0 \right] + \left[b'^{\mathrm{T}}\ 0 \right] G_{(n+1)} - g_{n+1}^{\mathrm{T}} \right] R_{(n+1)} \right\|^2 \\
&\quad + \left\| \left[b'^{\mathrm{T}}\ -1 \right] R_{(n+1)}^{-1} \right\|^2, \\
R_{(n+1)} &= \mathrm{diag}\{e^{r_1}, \ldots, e^{r_{n+1}}\}.
\end{aligned}
$$

To maximize the fidelity, it is required that $V_1 = V_2 = 0$. Figure 2 plots the fidelity F as a function of V_1 and V_2 for the case when $\mathrm{Var}(X_S) = 3$ and $\mathrm{Var}(P_S) = \frac{1}{3}$.

Similar to the discussions of CPvtC in Sect. 3, for infinite squeezing, we need the following conditions to perfectly recover the secret:

$$
\left[\left[a^{\mathrm{T}}\ 1 \right] + \left[b^{\mathrm{T}}\ 0 \right] G_{(n+1)} \right] = \mathbf{0}^{\mathrm{T}}, \tag{18}
$$

$$
\left[\left[a'^{\mathrm{T}}\ 0 \right] + \left[b'^{\mathrm{T}}\ 0 \right] G_{(n+1)} - g_{n+1}^{\mathrm{T}} \right] = \mathbf{0}^{\mathrm{T}}. \tag{19}
$$

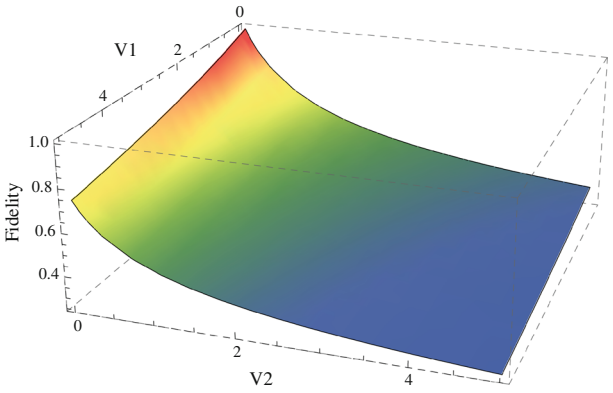


Fig. 2 Fidelity F as a function of V_1 and V_2 when $\mathrm{Var}(X_S) = 3$ and $\mathrm{Var}(P_S) = \frac{1}{3}$

Eqs. (18) and (19) can be transformed to

$$\left[a^{\mathrm{T}} \mid b^{\mathrm{T}}\right]\left[\frac{I'}{G'_{(n+1)}}\right] = \left[\mathbf{0}^{\mathrm{T}} \mid -1\right], \tag{20}$$

$$\left[a'^{\mathrm{T}} \mid b'^{\mathrm{T}}\right]\left[\frac{I'}{G'_{(n+1)}}\right] = g_{n+1}^{\mathrm{T}}, \tag{21}$$

where I', $G'_{(n+1)}$ are $n \times (n+1)$ matrices obtained by deleting the $(n+1)$-th row of the matrices I and $G_{(n+1)}$, respectively.

Our main result on general QPvtQ threshold protocols is presented in the following theorem.

Theorem 2 *Any (k, n) threshold protocol of QPvtQ scheme can be implemented with a weighted CVGS of infinite squeezing.*

The proof is given in "Appendix 7.2".

We now consider the case when n players are divided into two noncooperative groups, i.e., they do not exchange any information. It is immediate that these two groups cannot copy the secret qumode simultaneously because of the quantum no-cloning theorem. Moreover, we have the following theorem.

Theorem 3 *If one group can perfectly estimate the secret qumode, the other group cannot estimate either quadrature of the quantum secret within a finite error bound, and thus cannot obtain any information about the secret.*

The proof is provided in "Appendix 7.3".

For a $(k, 2k-1)$ threshold protocol, since any group with k or more players can perfectly estimate the secret, from Theorem 3, we know that any group with less than k players can obtain no information about the quantum secret. This holds true for any (k, n) threshold protocol, which is obtained from $(k, 2k-1)$ protocol by picking n qumodes from $2k-1$ qumodes. For these protocols, we have the following corollary.

Corollary 1 *Any player group with number less than the threshold k cannot obtain any information about the quantum secret.*

Now, consider the effect of finite squeezing. For simplicity, we assume the secret quantum state the dealer prepares is a minimum uncertainty state, i.e., $\mathrm{Var}(X_S)\,\mathrm{Var}(P_S) = 1$. We want to show the consistency of Eqs. (20) and (21) is an equivalent conditions to reconstruct the quantum secret in finite squeezing case. We still assume the squeezing parameters are all rs. If a, b, a', b' can be determined by Eqs. (20) and (21), then the fidelity of the quantum state players obtained is

$$F = \frac{2}{\sqrt{\left(2\,\mathrm{Var}(X_S) + \sum_{j\in J} b_j^2 e^{-2r}\right)\left(2\,\mathrm{Var}(P_S) + \sum_{j\in J} b_j'^2 e^{-2r}\right)}}, \tag{22}$$

which is nearly one as r is large. If Eq. (20) cannot be satisfied, V_1 in the denominator of the fidelity in Eq. (17) will include the term $(a_j + \sum_l b_l G_{lj})^2 e^{2r_j}$, which makes the fidelity nearly zero. Thus, the consistency of Eqs. (20) and (21) is the equivalent condition to reconstruct the secret qumode. Hence, Theorems 2 and 3 work well in finite squeezing case.

5 Case 3: CPubC scheme

This section is focused on the CPubC scheme, where the dealer has a *classical* secret, the qumodes encoding this secret is distributed through *public* channels, and the players collaborate to get the secret by *classical* communication channels. We will show that a (k, n) protocol of CPubC scheme exists if and only if a (k, n) protocol of QPvtQ scheme exists.

To begin with, the dealer prepares an $(n+1)$-mode graph state, keeps the $(n+1)$-th qumode, and distributes the other n qumodes to the n players. Since the qumodes are distributed through public channels, there exists risk that some eavesdroppers may get them. To ensure secure classical communications, from the method of CV quantum key distribution [27–29], the dealer takes a random homodyne measurement at the $(n+1)$-th qumode. Either the position or the momentum is measured, but which quadrature the dealer measured is unknown to the others. The measurement outcome is a random key, which the dealer will share with the players.

To get the key, the players randomly estimate either $\mathcal{M}(X_{n+1}^G)$ or $\mathcal{M}(P_{n+1}^G)$. Same as the case of CPvtC scheme in Sect. 3, the players take those three steps of Eqs. (5)–(6). Then, they exchange their results to get $\sum_{j=1}^n \mathcal{M}(\alpha_j X_j + \beta_j P_j^G)$. If the players are to estimate X_{n+1}^G, they need to consider the position estimation error

$$\begin{aligned} e_x &= \mathcal{M}\left(\left[a^{\mathrm{T}}\ 0\ b^{\mathrm{T}}\ 0\right]\left[\begin{array}{c|c} I & 0 \\ \hline G_{(n+1)} & I \end{array}\right] v_{(n+1)}\right) - \mathcal{M}\left(X_{n+1}^G\right) \\ &= \mathcal{M}\left(\left[\,[a^{\mathrm{T}}\ -1] + [b^{\mathrm{T}}\ 0]G_{(n+1)}\,\middle|\,[b^{\mathrm{T}}\ 0]\,\right] v_{(n+1)}\right). \end{aligned} \tag{23}$$

The position estimation error has zero mean, and its variance is given by

$$\begin{aligned}\mathrm{Var}(e_x) = &\left\| \left[\left[a^{\mathrm{T}} \ -1 \right] + \left[b^{\mathrm{T}} \ 0 \right] G_{(n+1)} \right] R' \right\|^2 \\ &+ \left\| \left[b^{\mathrm{T}} \ 0 \right] R'^{-1} \right\|^2 . \end{aligned} \tag{24}$$

The variance becomes 0 only when the qumodes are infinitely squeezed, and also

$$\left[a^{\mathrm{T}} \ -1 \right] + \left[b^{\mathrm{T}} \ 0 \right] G_{(n+1)} = \mathbf{0}^{\mathrm{T}}, \tag{25}$$

which leads to

$$\left[a^{\mathrm{T}} \mid b^{\mathrm{T}} \right] \left[\frac{I'}{G'_{(n+1)}} \right] = [\mathbf{0}^{\mathrm{T}} \mid 1], \tag{26}$$

If the players are to estimate P^G_{n+1}, they need to consider the momentum estimation error

$$\begin{aligned} e_p &= \mathcal{M} \left(\left[a'^{\mathrm{T}} \ 0 \ b'^{\mathrm{T}} \ 0 \right] \left[\begin{array}{c|c} I & 0 \\ \hline G_{(n+1)} & I \end{array} \right] v_{(n+1)} \right) - \mathcal{M} \left(P^G_{n+1} \right) \\ &= \mathcal{M} \left(\left[\left[a'^{\mathrm{T}} \ 0 \right] + \left[b'^{\mathrm{T}} \ 0 \right] G_{(n+1)} - g^{\mathrm{T}}_{n+1} \middle| \left[b'^{\mathrm{T}} \ -1 \right] \right] v_{(n+1)} \right), \end{aligned} \tag{27}$$

which also has zero mean with variance given by

$$\begin{aligned}\mathrm{Var}(e_p) = &\left\| \left[\left[a'^{\mathrm{T}} \ 0 \right] + \left[b'^{\mathrm{T}} \ 0 \right] G' - g^{\mathrm{T}}_{n+1} \right] R' \right\|^2 \\ &+ \left\| \left[b'^{\mathrm{T}} \ -1 \right] R'^{-1} \right\|^2 . \end{aligned} \tag{28}$$

Similar to the CPvtC scheme, to minimize the variance, we require both terms in Eq. (28) to be zero, i.e.,

$$\left[b'^{\mathrm{T}} - 1 \right] R'^{-1} = 0,$$

which implies the qumodes are infinitely squeezed; and

$$\left[\left[a'^{\mathrm{T}} \ 0 \right] + \left[b'^{\mathrm{T}} \ 0 \right] G' - g^{\mathrm{T}}_{n+1} \right] = \mathbf{0}^{\mathrm{T}}, \tag{29}$$

which can be further simplified to Eq. (30).

$$\left[a'^{\mathrm{T}} \mid b'^{\mathrm{T}} \right] \left[\frac{I'}{G''} \right] = g^{\mathrm{T}}_{n+1}. \tag{30}$$

To construct a shared key between the dealer and the players, they need to do the following:

1. The collaborative players announce the quadrature they estimated.
2. The dealer publishes the quadrature actually measured.
3. If the players' estimation quadrature matches the dealer's measurement quadrature, they keep the estimation result as the shared key; if not, they discard it and try again.

Step 3 is necessary because if the estimation quadrature matches the measurement quadrature, the players obtain an unbiased estimation of the measurement outcome $\mathcal{M}(X^G_{n+1})$ with variance Eq. (24), or $\mathcal{M}(P^G_{n+1})$ with variance Eq. (28). Otherwise, the players get something completely useless. The error in this case will be unbounded, as a homodyne measurement for the position (or momentum) will collapse the momentum (or position) into a maximally uncertain state.

The eavesdroppers cannot get any information without changing the qumodes in the quantum channels, and any disturbance to the qumodes can be detected by comparing part of the shared keys held by the dealer and the players.

What is worth mentioning is the duality between QPvtQ and CPubC schemes. We now show that a (k, n) threshold protocol can be implemented on CPubC if and only if it can be implemented on QPvtQ. We proved that in CPubC scheme, the existence of a set of players who can perfectly estimate the secret is equivalent to the consistency of Eqs. (26) and (30), and in QPvtQ scheme, that existence is equivalent to the consistency of Eqs. (20) and (21). It is clear that Eqs. (21) and (30) are the same, and Eq. (20) differs from Eq. (26) only by a sign. Thus, the existence of a (k, n) threshold protocol on CPubC is equivalent to that on QPvtQ. Similar results for the discrete variable were given in [30]. Furthermore, from Theorem 2, it is clear that a (k, n) threshold CPubC protocol exists if and only if $\frac{n}{2} < k \leq n$, and all these CPubC protocols can be implemented using CV weighted graph states. The effect of finite squeezing in the CPubC scheme is similar to the previous analysis in the Sects. 3 and 4.

6 Conclusion

This paper investigated three QSS schemes with CVGS in details, namely, CPvtC, QPvtQ, and CPubC. We designed implementation protocols for each scheme and derived analytic formula for the estimation error. This makes it possible to minimize the error variance by varying protocol parameters. We showed that a (k, n) threshold QSS protocol of the three schemes satisfying $\frac{n}{2} < k \leq n$ can be implemented by using a weighted CVGS. These protocols cover all the physically feasible threshold protocols for QPvtQ and CPubC. Specifically, the perfect estimation for two noncooperative groups on QPvtQ is exclusive. Finally, the duality between QPvtQ and CPubC schemes is discussed.

In practical experiments, we have to use finitely squeezed lights to prepare CVGSs. We have found that in a (k, n) threshold protocol, finite squeezing will bring in the existence of small error variance in the estimation of k or more players, and the access of little information about the secret for fewer than k players. Since generally, the error is small for physically realistic squeezing and the condition to access the secret remains the same as in the infinite squeezing case, finite squeezing will not repudiate any of our results. Thus, all the results are physically realistic by utilizing finitely squeezed lights in experiments.

Acknowledgments JZ thanks the financial support from the Innovation Program of Shanghai Municipal Education Commission under Grant No. 11ZZ20, Shanghai Pujiang Program under Grant No. 11PJ1405800, NSFC under Grant No. 61174086, State Key Laboratory of Precision Spectroscopy, ECNU, China, and project-sponsored by SRF for ROCS SEM. GQH thanks the financial support from NSFC under Grant No. 61102053, Project-sponsored by SRF for ROCS SEM, and SMC Excellent Young Faculty Award.

7 Appendix

7.1 Proof of Theorem 1

To guarantee all the (k, n) threshold protocols with $k \leq n < 2k$ can be implemented, the dealer only need to make sure that they can implement the case when $n = 2k - 1$. In $(k, 2k-1)$ threshold protocols, any k players can cooperatively get the secret. Even if less than k of the $2k - 1$ qumodes are removed, any k players holding the reserved qumodes can still obtain the secret. Hence, by choosing arbitrary n players from the total $2k - 1$ players, a $(k, 2k - 1)$ threshold protocol can be transformed into a (k, n) protocol. Thus, to prove Theorem 1, we only need to show that any $(k, 2k-1)$ protocol can be implemented using a weighted CVGS of infinite squeezing.

Suppose that in a communication system with one dealer and $2k - 1$ players, a set of k players collaborate to reveal the secret. Since Eq. (12) is a sufficient and necessary condition for the k players to perfectly estimate the secret, to guarantee they can get the secret, it is required that Eq. (12) with $n = 2k - 1$ has solutions. In Eq. (12), the $2k \times 2k$ matrix

$$\begin{bmatrix} I_{J,N} & \mathbf{0} \\ G_{J,N} & c_J \end{bmatrix}$$

maps a $2k$-dimensional vector $[a_J^{\mathrm{T}} \ b_J^{\mathrm{T}}]^{\mathrm{T}}$ to a $2k$-dimensional nonzero vector $[0 \ldots 0\, 1]^{\mathrm{T}}$, where $J = \{j_1, \ldots, j_k\}$ and $N = \{1, \ldots, 2k - 1\}$. If this matrix is full rank, there exists exactly one solution $[a_J^{\mathrm{T}} \, b_J^{\mathrm{T}}]$. Since the submatrix $I_{J,N}$ is always full rank, we only need to guarantee the submatrix $[G_{J,K} \ c_J]$ is full rank, where $K = N \setminus J$. This condition can be satisfied by designing the adjacency matrix G and the vector c. Here, the backslash denotes the set difference.

To show that it is a $(k, 2k - 1)$ threshold protocol, we also need to prove that any subset with fewer than k players cannot estimate the secret within a finite error bound. Indeed, we only need to prove there is no solution to Eq. (12) if k is replaced by $k - 1$. In this case, Eq. (12) becomes

$$\begin{bmatrix} a_{J'}^{\mathrm{T}} & b_{J'}^{\mathrm{T}} \end{bmatrix} \begin{bmatrix} I_{J',N} & \mathbf{0} \\ G_{J',N} & c_{J'} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & 1, \end{bmatrix} \tag{31}$$

where $J = \{j'_1, \ldots, j'_{k-1}\}$. Consider the first $2k-1$ columns of the matrix in Eq. (31). The submatrix

$$\begin{bmatrix} I_{J',N} \\ G_{J',N} \end{bmatrix}$$

maps $[a_{J'}^{\mathrm{T}}\ b_{J'}^{\mathrm{T}}]$ to a $(2k-1)$-dimensional zero vector. Since the submatrix is full rank, $[a_{J'}^{\mathrm{T}}\ b_{J'}^{\mathrm{T}}]$ can only be a zero vector, which contradicts the fact that $b_{J'}^{\mathrm{T}} c_{J'} = 1$. So, Eq. (31) has no solutions. Hence, the theorem is proved.

7.2 Proof of Theorem 2

From quantum no-cloning theorem, we know that a (k, n) threshold QPvtQ protocol must satisfy $k \leq n < 2k$. The largest possible value of n is $2k-1$. In this case, $\left[I'^{\mathrm{T}} \mid G'^{\mathrm{T}}\right]^{\mathrm{T}}$ is a $2n \times (n+1)$ matrix. Since there are $2(n-k)$ zeros in $[a^{\mathrm{T}} \mid b^{\mathrm{T}}]$, only a $2k \times 2k$ submatrix $[(I_J)^{\mathrm{T}}\ (G_{J,N})^{\mathrm{T}}]^{\mathrm{T}}$ needs to be considered in Eqs. (20) and (21). If this matrix is full rank, both Eqs. (20) and (21) have a unique solution. The matrix I_J is always full rank; thus, to make $[(I_J)^{\mathrm{T}}\ (G_{J,N})^{\mathrm{T}}]^{\mathrm{T}}$ full rank, we need to the $k \times k$ submatrix $G_{J,K}$ to be full rank as well, where $K = N \setminus J$.

If for any k players, the corresponding $G_{J,K}$ is full rank; this CVGS can be used to implement a $(k, 2k-1)$ threshold QPvtQ protocol. We can always find a proper weighted CVGS satisfying this condition. If $(k, 2k-1)$ protocols are obtained, the dealer can implement any (k, n) protocol by picking n qumodes from a $(2k-1)$-mode CVGS and distributing to n players.

7.3 Proof of Theorem 3

Divide n players into two groups: One has k players and the other $n-k$ players. We need to show that if one group can perfectly estimate the secret qumode (X_S, P_S), the other group cannot estimate either X_S or P_S within a finite error bound. If we can prove it is impossible that one group perfectly estimates X_S when the other group perfectly estimates P_S, the theorem is proved because any nonzero estimation error must be unbounded under infinite squeezing.

If the group with k players can collaborate to estimate the position distribution of the secret qumode perfectly, we have

$$\left[a_J^{\mathrm{T}}\ \ b_J^{\mathrm{T}}\right]\begin{bmatrix} I_{J,M} \\ G_{J,M} \end{bmatrix} = \left[\mathbf{0}_n^{\mathrm{T}}\ \ -1\right], \tag{32}$$

where $M = \{1, \ldots, n+1\}$, and J is a $k-$subset of $N = \{1, \ldots, n\}$. From Eq. (32), we obtain

$$b_J^{\mathrm{T}} G_{J,M\setminus J} = \left[\mathbf{0}_{n-k}^{\mathrm{T}}\ \ -1\right]. \tag{33}$$

Denote the last column of $G_{J,M\setminus J}$ as v_1.

For the other group, if they can collaborate to estimate the momentum distribution of the secret mode, we get

$$\left[a_K^{\mathrm{T}}\ \ b_K^{\mathrm{T}}\right]\begin{bmatrix} I_{K,M} \\ G_{K,M} \end{bmatrix} = g_{n+1}^{\mathrm{T}}, \tag{34}$$

where $K = N \setminus J$. We then have

$$b_K^{\mathrm{T}} G_{K,P} = v_2^{\mathrm{T}}, \tag{35}$$

where $P = M \setminus K$ and $v_2 = (g_{n+1})_P$ (recall that g_{n+1} is the last column of $G_{(n+1)}$). Hence, $v_2^{\mathrm{T}} = [v_1^{\mathrm{T}}\ 0]$. Since $G_{J,N} = \left[G_{J,K}\ v_1\right]$, we can rewrite Eqs. (33) and (35) as

$$b_J^{\mathrm{T}} \begin{bmatrix} G_{J,K} & v_1 \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{n-k}^{\mathrm{T}} & -1 \end{bmatrix}, \tag{36}$$

$$b_K^{\mathrm{T}} \begin{bmatrix} G_{K,J} & v_3 \end{bmatrix} = \begin{bmatrix} v_1^{\mathrm{T}} & 0 \end{bmatrix}, \tag{37}$$

where v_3 is the last column of $G_{K,P}$. From Eq. (37), we have $v_1^{\mathrm{T}} = b_K^{\mathrm{T}} G_{K,J}$. Substituting it into Eq. (36), we get

$$b_J^{\mathrm{T}} G_{J,K} [I \mid b_K] = [\mathbf{0}_{n-k}^{\mathrm{T}} \ -1],$$

which is a contradiction. Thus, it is impossible for one group of players to perfectly estimate the position distribution, and the other to estimate the momentum distribution, if these two groups do not have any quantum communication.

References

1. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–195 (2002)
2. Hillery, M.: Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A. **59**(3), 1829–1834 (1999)
3. Cleve, R., Gottesman, D., Lo, H.-K.: How to share a quantum secret. Phys. Rev. Lett. **83**(3), 648–651 (1999)
4. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A. **61**(4), 042311 (2000)
5. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A. **78**(4), 042309 (2008)
6. Keet, A., Fortescue, B., Markham, D., Sanders, B.C.: Quantum secret sharing with qudit graph states. Phys. Rev. A. **82**(6), 062315 (2010)
7. Sarvepalli, P.: Nonthreshold quantum secret-sharing schemes in the graph-state formalism. Phys. Rev. A. **86**(4), 042303 (2012)
8. Hein, M., Eisert, J., Briegel, H.J.: Multiparty entanglement in graph states. Phys. Rev. A. **69**(6), 062311 (2004)
9. Yu, S., Chen, Q., Lai, C.H., Oh, C.H.: Nonadditive quantum error-correcting code. Phys. Rev. Lett. **101**(9), 090501 (2008)
10. Dür, W., Aschauer, H., Briegel, H.J.: Multiparticle entanglement purification for graph states. Phys. Rev. Lett. **91**(10), 107903 (2003)
11. Gühne, O., Tóth, G., Hyllus, P., Briegel, H.J., et al.: Bell inequalities for graph states. Phys. Rev. Lett. **95**(12), 120405 (2005)
12. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Tyc, T., Ralph, T.C., Lam, P.K.: Continuous-variable quantum-state sharing via quantum disentanglement. Phys. Rev. A. **71**(3), 033814 (2005)
13. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Tripartite quantum state sharing. Phys. Rev. Lett. **92**(17), 177903 (2004)
14. Zhang, J., Braunstein, S.L.: Continuous-variable Gaussian analog of cluster states. Phys. Rev. A. **73**(3), 032318 (2006)
15. Zhang, J.: Graphical description of local Gaussian operations for continuous-variable weighted graph states. Phys. Rev. A. **78**(5), 052307 (2008)

16. Menicucci, N.C., van Loock, P., Gu, M., Weedbrook, C., Ralph, T.C., Nielsen, M.A.: Universal quantum computation with continuous-variable cluster states. Phys. Rev. Lett. **97**(11), 110501 (2006)
17. Gu, M., Weedbrook, C., Menicucci, N.C., Ralph, T.C., van Loock, P.: Quantum computing with continuous-variable clusters. Phys. Rev. A. **79**(6), 062318 (2009)
18. Morimae, T.: Continuous-variable blind quantum computation. Phys. Rev. Lett. **109**(23), 230502 (2012)
19. Ren, L., He, G., Zeng, G.: Universal teleportation via continuous-variable graph states. Phys. Rev. A. **78**(4), 042302 (2008)
20. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. Phys. Rev. Lett. **69**(20), 2881–2884 (1992)
21. DiVincenzo, D.P., Leung, D.W., Terhal, B.M.: Quantum data hiding. IEEE Trans. Inf. Theory **48**(3), 580–598 (2002)
22. Braunstein, S.L., van Loock, P.: Quantum information with continuous variables. Rev. Mod. Phys. **77**(2), 513–577 (2005)
23. Braunstein, S.L., Kimble, H.J.: Teleportation of continuous quantum variables. Phys. Rev. Lett. **80**(4), 869–872 (1998)
24. Yoshikawa, J.-I., Miwa, Y., Filip, R., Furusawa, A.: Demonstration of a reversible phase-insensitive optical amplifier. Phys. Rev. A. **83**(5), 052307 (2011)
25. Wang, Y., Su, X., Shen, H., Tan, A., Xie, C., Peng, K.: Toward demonstrating controlled-X operation based on continuous-variable four-partite cluster states and quantum teleporters. Phys. Rev. A. **81**(2), 022311 (2010)
26. Jing-Tao, Z., Guang-Qiang, H., Li-Jie, R., Gui-Hua, Z.: The dependence of fidelity on the squeezing parameter in teleportation of the squeezed coherent states. Chin. Phys. B. **20**(5), 050311 (2011)
27. Ralph, T.C.: Continuous variable quantum cryptography. Phys. Rev. A. **61**(1), 010303 (1999)
28. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**(5), 057902 (2002)
29. Weedbrook, C., Pirandola, S., Garcn, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S., et al.: Gaussian quantum information. Rev. Mod. Phys. **84**(2), 621–669 (2012)
30. Marin, A., Markham, D.: On the equivalence between sharing quantum and classical secrets, and error correction. arXiv:1205.4182 (2012)