Quantum Secret Sharing with Continuous Variable Graph State

Yadong Wu[1], Runze Cai[1], Guangqiang He[2,*], and Jun Zhang[1,†]
[1] *Joint Institute of UM-SJTU, Shanghai Jiao Tong University,*
and Key Laboratory of System Control and Information Processing (Ministry of Education), Shanghai, 200240, China
[2] *State Key Laboratory of Advanced Optical Communication Systems and Networks,*
and Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, 200240, China

(Dated: November 3, 2018)

In this paper we study the protocol implementation and property analysis for several practical quantum secret sharing (QSS) schemes with continuous variable graph state (CVGS). For each QSS scheme, an implementation protocol is designed according to its secret and communication channel types. The estimation error is derived explicitly, which facilitates the unbiased estimation and error variance minimization. It turns out that only under infinite squeezing can the secret be perfectly reconstructed. Furthermore, we derive the condition for QSS threshold protocol on a weighted CVGS. Under certain conditions, the perfect reconstruction of the secret for two non-cooperative groups is exclusive, *i.e.* if one group gets the secret perfectly, the other group cannot get any information about the secret.

PACS numbers: 03.67.Dd, 03.67.Ac, 03.67.Hk

I. INTRODUCTION

Quantum cryptography provides a sophisticated approach to achieve the communication security by taking advantage of quantum mechanics principles [1]. Among various schemes, quantum secret sharing (QSS) is a general multi-partite information security scheme that attracts extensive research interests [2–9]. It allows one dealer to distribute a secret among a number of players in such a way that a certain set of players can reconstruct the secret by taking operations collaboratively and exchanging information. In contrast to quantum key distribution [10] that guarantees the secure communication between only two parties, QSS enables multiple parties to communicate securely at the same time.

QSS has its origin in classical information theory. An early scheme was given in [2] to share either classical or quantum secret to three or four players by using the GHZ states. Ref. [3] studied general threshold schemes to share quantum secrets and showed that the quantum no-cloning theorem is the only constraint on the existence of threshold schemes. Ref. [4] further extended the results to general access structures, including non-threshold schemes. These researches have established theoretical foundations for many ensuing investigations, *e.g.* hybrid schemes [5] and twin-threshold schemes [6].

On the other hand, graph state has been extensively studied in applications such as quantum error correction [11–14], entanglement purification [15–17], entanglement measurement [18–20], and Bell inequality [21, 22]. In recent years, the implementation of QSS with graph state was introduced in [7, 23] to treat three kinds of threshold QSS schemes in a unified graph state approach and to propose embedded protocols in large graph states. Ref. [8] generalized the results to prime dimensions, and Ref. [9] investigated non-threshold schemes. However, all these results are based on discrete variable graph states.

Here we are interested in QSS with continuous variable graph state (CVGS). CVGS was first introduced in [24] as the continuous analogue of discrete variable graph state. It has the nice property that any local Gaussian operation on a CVGS can be associated with a geometric transformation on its graph representation [25]. Refs. [26, 27] showed that CVGS can be used to generate universal quantum operations and thus is potentially a useful physical resource to implement quantum computations. In addition, CVGS also finds applications in quantum communications, *e.g.* Ref. [28] proposed a protocol to realize quantum teleportation between two parties.

This paper is focused on the implementation and property analysis of QSS schemes with CVGS. We differentiate eight QSS schemes according to the secret and communication channel types. Among all these schemes, four of them have no practical values because they are either physically infeasible or insecure. We will thus investigate in the other four schemes. These extend the works in [7, 8] into the CVGS domain.

We study two essential problems for these QSS schemes with CVGS First, for each QSS scheme, we design an implementation protocol for the dealer and players so that the players may collaborate to estimate the secret. The mean and variance of the estimation error are derived explicitly. Based on the error statistics, we can derive the parameter settings for unbiased estimation. Furthermore, the protocol parameters can be tuned to minimize the error variance. In the case of infinite squeezing, it can be shown that finding the condition that a set of players can perfectly estimate the secret can be transformed to solve a set of linear equations.

The second problem is the threshold protocol, which is crucial for many applications that need decision-making.

[*] Corresponding author. Email: gqhe@sjtu.edu.cn
[†] Corresponding author. Email: zhangjun12@sjtu.edu.cn

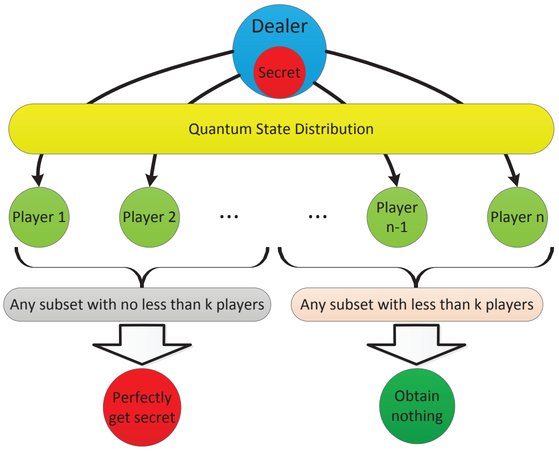
Dealer
Secret
Quantum State Distribution
Player 1
Player 2
...
...
Player n-1
Player n
Any subset with no less than k players
Any subset with less than k players
Perfectly get secret
Obtain nothing

FIG. 1: QSS (k,n) threshold protocol.

In QSS, a (k,n) threshold protocol refers to the case when k players or more can estimate the secret perfectly, and any set with less players can never get the secret within a finite error bound. We show that an arbitrary (k,n) threshold protocol with $n/2 < k \leq n$ can be implemented for three schemes using a weighted CVGS prepared with infinitely squeezed qumodes. An interesting observation is that for the scheme with quantum secret, private distribution channel, and quantum player-player channel (referred as QPrtQ), the threshold protocol for two non-cooperative 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 gurantteed. For QPrtQ and another scheme, these protocols cover all the physically feasible cases, and we also reveal the duality between them.

This paper is organized as follows. Sec. II provides a brief introduction on QSS schemes and CVGS. Three QSS schemes with CVGS are investigated in Sec. III, IV and V, respectively. We conclude the paper in Sec. VI.

II. 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 shown in Fig. 1. The dealer has a secret that is represented by either classical or quantum information. At first, the dealer encodes the secret into a prepared quantum state, and subsequently distributes it to all the players through either private or public channels. With this quantum state at hand, a group of players can either apply local operations to their own states and then exchange classical information, or take joint operations to their states. The task for these players is to reconstruct the secret based on the information circulated around.

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). Among all these eight schemes, QPubC and QPrtC are physically infeasible because it is impossible to recover unknown quantum information from classical information. Moreover, QPubQ and CPubQ are insecure because an eavesdropper can disguise identity to modify the information on public channel. Therefore, we will investigate only the four schemes in Table I.

	Secret type	Dealer-Player Channel	Player-Player Channel
CPvtC	Classical	Private	Classical
QPvtQ	Quantum	Private	Quantum
CPubC	Classical	Public	Classical
CPvtQ	Classical	Private	Quantum

TABLE I: Feasible QSS schemes.

In particular, we are interested in a (k,n) threshold protocol, which refers 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 illustrated in Fig. 1.

In this paper 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 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:

$$v_{(n)} = \begin{bmatrix} X_1 & \cdots & X_n & P_1 & \cdots & P_n \end{bmatrix}^T, \tag{2}$$

where the subscript (n) indicates the number of the qumodes. Now apply a quantum nondemolition (QND) coupling with interaction gain G_{ij} to the pair (i, j) [24]. 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 $(X_j, P_j + G_{ji}X_i)$, 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

$$v_{(n)}^G = \begin{bmatrix} X_1^G & \cdots & X_n^G & P_1^G & \cdots & P_n^G, \end{bmatrix}^T.$$

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

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

In the next three sections, we will investigate the implementations of the CPvtC, QPvtQ, and CPubC schemes in Table I. We point out that the CPvtQ scheme can be implemented by super-dense coding [35] and is indeed a quantum data hiding scheme [36, 37]. Since CPvtQ can be dealt with similarly to the others, we will focus on the first three. For simplicity, we set $\hbar = 1$ throughout this paper.

III. CASE 1: CPvtC SCHEME

In this section we study the CPvtC scheme, in which the dealer encodes a *classical* secret into a CVGS, 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 estimation error and then obtain its mean and variance. This facilitates the unbiased estimation and also the optimal tuning of protocol parameters to minimize the error variance. We will also study the condition to perfectly reconstruct the secret, and discuss the implementation of a general threshold scheme on CVGS.

We now present the implementation details of CPvtC scheme. 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 $Z(c_j\gamma) = e^{ic_j\gamma\hat{x}}$ [27] 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 $c = [c_1 \ \cdots \ c_n]^T$. 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
$$\begin{aligned} \mu_j &= \alpha_j\mathcal{M}\left(X_j + \frac{\beta_j}{\alpha_j}P_j^D\right) \\ &= \mathcal{M}(\alpha_jX_j + \beta_jP_j^D), \end{aligned} \tag{6}$$
where 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 each player can use the sum of μ_j as an estimation of the secret γ. From Eqs. (2)-(6), the estimation error e can be calculated as

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

where $a = [\alpha_1 \ \cdots \ \alpha_n]^T$, $b = [\beta_1 \ \cdots \ \beta_n]^T$, $\mathbf{0} = [0 \ \cdots \ 0]^T$, and $G_{(n)}$ is the adjacency matrix of the n-qumode graph state.

The mean of the estimation error is

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

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

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

To ensure an unbiased estimation, it is only required that

$$b^Tc = 1. \tag{8}$$

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

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

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

To enhance the estimation precision, it is desired to reduce the error variance (9). Combining with Eq. (8), it is a nonlinear constrained minimization problem with optimization variables a, b, $G_{(n)}$, and $R_{(n)}$. We can thus tune these protocol parameters to achieve a better estimation. For example, when a, b, $G_{(n)}$ are fixed, the optimal squeezing parameters that minimize the error variance can be chosen as

$$r_j = \frac{1}{2}\log\left|\frac{b_j}{(a^T + b^T G_{(n)})_j}\right|, \tag{10}$$

for $b_j \neq 0$ and $(a^T + b^T G_{(n)})_j \neq 0$.

It is also easy to observe that under constraint (8), the variance (9) can achieve 0 only if some parameters take extremal values. One choice is to apply infinite squeezing, *i.e.* letting the squeezing parameters $r_j \to \infty$ and then

$$a^T + b^T G_{(n)} = \mathbf{0}^T. \tag{11}$$

Combining Eqs. (8) and (11), we get a condition that guarantees n players to get the secret perfectly under infinite squeezing

$$\left[a^T \mid b^T\right]\left[\begin{array}{c|c} I & \mathbf{0} \\ \hline G_{(n)} & c \end{array}\right] = \left[\mathbf{0}^T \mid 1\right]. \tag{12}$$

Now let us discuss (k,n) QSS threshold protocols, which means that it requires at least k ($k \leq n$) players to estimate the secret perfectly, and any set with less than k players cannot estimate the secret within a finite error bound. Consider a set of k collaborative players with indices $j_1, \cdots, j_k$. To simplify the notation, we use $A_{J,K}$ to denote a matrix formed by taking rows with indices in J and columns in K from a matrix A, where J, K are subsets of $N = \{1, \cdots, n\}$. For the case of a vector, we can similarly define v_J. Removing the rows and columns corresponding to the remaining $n-k$ players from Eq. (12), we obtain

$$\begin{bmatrix} a_J^T & b_J^T \end{bmatrix}\begin{bmatrix} I_{J,N} & \mathbf{0} \\ G_{J,N} & c_J \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & 1 \end{bmatrix}, \tag{13}$$

where $J = \{j_1, \cdots, j_k\}$. Eq. (13) is a sufficient and necessary condition for k players from a set of n players to recover the secret perfectly under infinite squeezing.

We give a lower bound on k that ensures the physical existence of a (k,n) CPvtC threshold protocol.

Theorem 1 A (k,n) threshold protocol of CPvtC scheme satisfying $n/2 < k \leq n$ can be implemented on a weighted CVGS with infinite squeezing.

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

IV. 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 will first give the implementation protocol design, and then calculate the estimation error. We then discuss the condition of perfectly estimating the secret qumode as well as the threshold protocols under infinite squeezing.

First consider the protocol design. 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_{n+1}^G, P_{n+1}^G) 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

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

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 $(-X_{n+1}^G, P_{n+1}^G)$, they can perfectly estimate the secret by simply adding the position displacement $\sqrt{2}\mathcal{M}(X_u)$ and subtracting the momentum displacement $\sqrt{2}\mathcal{M}(P_v)$ [29]. This is the idea of continuous variable quantum teleportation [30].

To construct $(-X_{n+1}^G, P_{n+1}^G)$, the players can take the following steps:

1. Apply a single-mode Gaussian unitary operation and a phase insensitive amplification [31] to transform a qumode (X_j^G, P_j^G) to $(\alpha_j X_j^G + \beta_j P_j^G, \alpha_j' X_j^G + \beta_j' P_j^G)$, where α_j, β_j, α_j', β_j' are all real numbers;

2. Pick one qumode from the players' qumodes and transform it to $(\sum_{i=1}^n \alpha_j X_j^G + \beta_j P_j^G, \sum_{i=1}^n \alpha_j' X_j^G + \beta_j' P_j^G)$ by using nonlocal operations such as a controlled-X operation [32].

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

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

where $a = [\alpha_1, \cdots, \alpha_n]^T$, $b = [\beta_1, \cdots, \beta_n]^T$, $v_{(n+1)} = [X_1, \cdots, X_{n+1}, P_1, \cdots, P_{n+1}]^T$, and $G_{(n+1)}$ is an $(n+1)\times$

$(n+1)$ adjacency matrix. Similarly, the momentum error is

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

where $a' = [\alpha'_1, \cdots, \alpha'_n]^T$, $b' = [\beta'_1, \cdots, \beta'_n]^T$, 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 [33], we can get the fidelity of the estimated secret qumode as

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

where

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

In particular, for minimum uncertainty states, we have that $\mathrm{Var}(X_S)\,\mathrm{Var}(P_S) = 1$. Hence $\epsilon = 0$, and Eq. (17) can be simplified to

$$F = \frac{2}{\sqrt{\delta}}. \tag{18}$$

With the fidelity in Eq. (17), it is possible to optimize the protocol parameters to maximize the fidelity. To achieve perfect fidelity at 100%, it is required that $V_1 = V_2 = 0$. This amounts to the following conditions under infinite squeezing:

$$\left[[a^T\ 1] + [b^T\ 0] G_{(n+1)}\right] = \mathbf{0}^T, \tag{19}$$

$$\left[[a'^T\ 0] + [b'^T\ 0] G_{(n+1)} - g_{n+1}^T\right] = \mathbf{0}^T. \tag{20}$$

Eqs. (19) and (20) can be rewritten as

$$\left[a^T \mid b^T\right] \left[\frac{I'}{G'_{(n+1)}}\right] = \left[\mathbf{0}^T \mid -1\right], \tag{21}$$

$$\left[a'^T \mid b'^T\right] \left[\frac{I'}{G'_{(n+1)}}\right] = g_{n+1}^T, \tag{22}$$

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.

Next we study the threshold protocol for QPvtQ scheme. The following theorem can be obtained.

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 B.

Furthermore, different from CPvtC, if these k players can perfectly recover the secret, we can show that the remaining $n-k$ players cannot get any information about the secret.

Theorem 3 For two non-cooperative group with QPvtQ scheme, 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. Thus they cannot obtain any information about the secret.

The proof is provided in Appendix C.

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.

V. 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 propose an implementation protocol, and then calculate the estimation error. The threshold protocol is studied by revealing the duality between QPvtQ and CPubC and schemes.

We start from proposing the implementation protocol. First, the dealer prepares an $(n+1)$-mode CVGS, keeps the $(n+1)$-th qumode, and then 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 [10], the dealer takes a random homodyne measurement at the $(n+1)$-th qumode and obtains either $\mathcal{M}(X^G_{n+1})$ or $\mathcal{M}(P^G_{n+1})$. Here the dealer measures either the position or the momentum, but which quadrature has been measured is unknown to the others. The measurement outcome is then used as a random key that the dealer will share with the players.

Secondly, the players achieves a consensus via classical communications that they will randomly estimate either $\mathcal{M}(X^G_{n+1})$ or $\mathcal{M}(P^G_{n+1})$ in a collaborative manner. Then, they take the three steps of Eqs. (5)-(6) as in Sec. III, and exchange their results so as to use $\sum_{j=1}^n \mathcal{M}(\alpha_j X_j + \beta_j P^G_j)$ as an estimation of the secret.

Thirdly, both the dealer and the players need to make sure that the quadrature they estimated is exactly the same as the one that the dealer measured earlier. The dealer and the players will do the following:

1. The players announce the quadrature that they estimated;
2. The dealer publishes the quadrature actually measured;
3. If the quadrature estimated by the players matches the one measured by the dealer, they keep the estimation result $\sum_{j=1}^n \mathcal{M}(\alpha_j X_j + \beta_j P^G_j)$ 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. 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. This completes the protocol implementation.

Next we calculate the estimation errors for both quadratures. If the players have estimated $\mathcal{M}(X^G_{n+1})$, the position estimation error is

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

It is easy to see that the error has zero mean and we have an unbiased estimation. The error variance is given by

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

The variance achieves 0 only when the qumodes are infinitely squeezed and the following equation holds true:

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

Eq. (25) can be rewritten as

$$[a^T \mid b^T] \left[\begin{array}{c} I' \\ \hline G'_{(n+1)} \end{array}\right] = [\mathbf{0}^T \mid 1]. \tag{26}$$

If the players have estimated $\mathcal{M}(P^G_{n+1})$, the momentum estimation error is

$$e_p \tag{27}$$

$$\begin{aligned} =&\mathcal{M}\left(\left[a'^T \ 0 \ b'^T \ 0\right] \left[\begin{array}{c|c} I & 0 \\ \hline G_{(n+1)} & I \end{array}\right] v_{(n+1)} \right) - \mathcal{M}\left(P^G_{n+1}\right) \\ =&\mathcal{M}\left(\Big[\ [a'^T \ 0] + [b'^T \ 0]G_{(n+1)} - g^T_{n+1} \Big| [b'^T \ -1] \ \Big] v_{(n+1)} \right). \end{aligned} \tag{28}$$

The error e_p also has zero mean and we again have an unbiased estimation. Its variance is given by

$$\begin{aligned} \mathrm{Var}(e_p) = &\left\| \left[[a'^T \ 0] + [b'^T \ 0]G' - g^T_{n+1} \right] R' \right\|^2 \\ &+ \left\| [b'^T \ -1] R'^{-1} \right\|^2 . \end{aligned} \tag{29}$$

To make the error variance equal to 0, we need the infinite squeezing together with

$$\left[[a'^T \ 0] + [b'^T \ 0]G' - g^T_{n+1} \right] = \mathbf{0}^T, \tag{30}$$

which yields that

$$[a'^T \mid b'^T] \left[\begin{array}{c} I' \\ \hline G'' \end{array}\right] = g^T_{n+1}. \tag{31}$$

Finally, we discuss the threshold protocol of CPubC by revealing the duality between QPvtQ and CPubC schemes. We now show that under infinite squeezing, a (k,n) threshold protocol can be implemented on CPubC if and only if it can be implemented on QPvtQ. We have 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 (31), and in QPvtQ scheme that existence is equivalent to the consistency of Eqs. (21) and (22). It is clear that Eqs. (22) and (31) are the same, and Eq. (21) 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 [34]. Furthermore, from Theorem 2, a (k,n) threshold CPubC protocol exists if and only if $n/2 < k \le n$, and all these CPubC protocols can be implemented using weighted CVGSs.

VI. 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 also showed that a (k,n) threshold QSS protocol of the three schemes satisfying $n/2 < k \leq n$ can be implemented by using a weighted CVGS with infinite squeezing. These protocols cover all the physically feasible threshold protocols for QPvtQ and CPubC. Specifically, the perfect estimation for two non-cooperative groups on QPvtQ is exclusive. Finally, the duality between QPvtQ and CPubC schemes is discussed.

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, Project-sponsored by SRF for ROCS SEM, and State Key Lab of Advanced Optical Communication Systems and Networks, SJTU, China. GQH thanks the financial support from NSFC under Grant No. 61102053, Project-sponsored by SRF for ROCS SEM, and SMC Excellent Young Faculty Award.

Appendix A: Proof of Theorem 1

To guarantee all the (k,n) threshold protocols with $n/2 < k \leq n$ 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. (13) 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. (13) with $n = 2k-1$ has solutions. In Eq. (13), the $2k \times 2k$ matrix

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

maps a $2k$-dimensional vector $[a_J^T \ b_J^T]^T$ to a $2k$-dimensional nonzero vector $[0 \cdots 0\, 1]^T$, where $J = \{j_1, \cdots, j_k\}$ and $N = \{1, \cdots, 2k-1\}$. If this matrix is full rank, there exists exactly one solution $[a_J^T \ b_J^T]$. 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. (13) if k is replaced by $k-1$. In this case, Eq. (13) becomes

$$\begin{bmatrix} a_{J'}^T & b_{J'}^T \end{bmatrix} \begin{bmatrix} I_{J',N} & \mathbf{0} \\ G_{J',N} & c_{J'} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & 1 \end{bmatrix}, \tag{A1}$$

where $J = \{j'_1, \cdots, j'_{k-1}\}$. Consider the first $2k-1$ columns of the matrix in Eq. (A1). The submatrix

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

maps $[a_{J'}^T \ b_{J'}^T]$ to a $(2k-1)$-dimensional zero vector. Since the submatrix is full rank, $[a_{J'}^T \ b_{J'}^T]$ can only be a zero vector, which contradicts the fact that $b_{J'}^T c_{J'} = 1$. So Eq. (A1) has no solutions. Hence the theorem is proved.

Appendix B: Proof of Theorem 2

From quantum no-cloning theorem, we know that a (k,n) threshold QPvtQ protocol must satisfy $n/2 < k \leq n$. The largest possible value of n is $2k-1$. In this case, $\left[I'^T \mid G'^T\right]^T$ is a $2n \times (n+1)$ matrix. Since there are $2(n-k)$ zeros in $[\,a^T \mid b^T]$, only a $2k \times 2k$ submatrix $[(I_J)^T \ (G_{J,N})^T]^T$ needs to be considered in Eqs. (21) and (22). If this matrix is full rank, both Eqs. (21) and (22) have a unique solution. The matrix I_J is always full rank, thus to make $[(I_J)^T \ (G_{J,N})^T]^T$ 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.

Appendix C: 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

$$\begin{bmatrix} a_J^T & b_J^T \end{bmatrix} \begin{bmatrix} I_{J,M} \\ G_{J,M} \end{bmatrix} = \begin{bmatrix} \mathbf{0}_n^T & -1 \end{bmatrix}, \tag{C1}$$

where $M = \{1, \cdots, n+1\}$, and J is a $k-$subset of $N = \{1, \cdots, n\}$. From Eq. (C1), we obtain

$$b_J^T G_{J,M\setminus J} = \begin{bmatrix} \mathbf{0}_{n-k}^T & -1 \end{bmatrix}. \tag{C2}$$

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

$$\begin{bmatrix} a_K^T & b_K^T \end{bmatrix} \begin{bmatrix} I_{K,M} \\ G_{K,M} \end{bmatrix} = g_{n+1}^T, \tag{C3}$$

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

$$b_K^T G_{K,P} = v_2^T, \tag{C4}$$

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 $v_2^T = [v_1^T \ 0]$. Since $G_{J,N} = [G_{J,K} \ v_1]$, we can rewrite Eqs. (C2) and (C4) as

$$b_J^T \begin{bmatrix} G_{J,K} & v_1 \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{n-k}^T & -1 \end{bmatrix}, \tag{C5}$$

$$b_K^T \begin{bmatrix} G_{K,J} & v_3 \end{bmatrix} = \begin{bmatrix} v_1^T & 0 \end{bmatrix}, \tag{C6}$$

where v_3 is the last column of $G_{K,P}$. From Eq. (C6), we have $v_1^T = b_K^T G_{K,J}$. Substituting it into Eq. (C5), we get

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

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.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[3] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[4] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[5] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001).

[6] S. K. Singh and R. Srikanth, Phys. Rev. A **71**, 012328 (2005).

[7] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[8] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, Phys. Rev. A **82**, 062315 (2010).

[9] P. Sarvepalli, Phys. Rev. A **86**, 042303 (2012).

[10] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), vol. 175.

[11] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, Phys. Rev. Lett. **101**, 090501 (2008).

[12] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, Phys. Rev. A **78**, 012306 (2008).

[13] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **78**, 042303 (2008).

[14] Y. Dong, X. Deng, M. Jiang, Q. Chen, and S. Yu, Phys. Rev. A **79**, 042342 (2009).

[15] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).

[16] H. Aschauer, W. Dür, and H.-J. Briegel, Phys. Rev. A **71**, 012319 (2005).

[17] C. Kruszynska, A. Miyake, H. J. Briegel, and W. Dür, Phys. Rev. A **74**, 052316 (2006).

[18] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).

[19] D. Markham, A. Miyake, and S. Virmani, New Journal of Physics **9**, 194 (2007).

[20] M. Hajdušek and M. Murao, New Journal of Physics **15**, 013039 (2013).

[21] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, Phys. Rev. Lett. **95**, 120405 (2005).

[22] G. Tóth, O. Gühne, and H. J. Briegel, Phys. Rev. A **73**, 022303 (2006).

[23] E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix (Open Publishing Association, 2009), vol. 9 of *Electronic Proceedings in Theoretical Computer Science*, pp. 87–97.

[24] J. Zhang and S. L. Braunstein, Phys. Rev. A **73**, 032318 (2006).

[25] J. Zhang, Phys. Rev. A **78**, 052307 (2008).

[26] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Phys. Rev. Lett. **97**, 110501 (2006).

[27] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).

[28] L. Ren, G. He, and G. Zeng, Phys. Rev. A **78**, 042302 (2008).

[29] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[30] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).

[31] J.-i. Yoshikawa, Y. Miwa, R. Filip, and A. Furusawa, Phys. Rev. A **83**, 052307 (2011).

[32] Y. Wang, X. Su, H. Shen, A. Tan, C. Xie, and K. Peng, Phys. Rev. A **81**, 022311 (2010).

[33] J. Zhang, G. He, L. Ren, and G. Zeng, Chinese Physics B **20**, 050311 (2011).

[34] A. Marin and D. Markham (2012), arXiv:1205.4182.

[35] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**,

2881 (1992).

[36] D. DiVincenzo, D. Leung, and B. Terhal, Information Theory, IEEE Transactions on **48**, 580 (2002), ISSN 0018-9448.

[37] T. Eggeling and R. F. Werner, Phys. Rev. Lett. **89**, 097905 (2002).