


Article

Improving Continuous Variable Quantum Secret Sharing with Weak Coherent States

Yijun Wang ¹, Bing Jia ¹, Yun Mao ^{1,*}, Xuelin Wu ^{1,2,*} and Ying Guo ^{1,2,*} 

¹ School of Automation, Central South University, Changsha 410083, China; xxywyj@sina.com (Y.W.); jiabing20180915@163.com (B.J.)

² Jiangsu Key Construction Laboratory of IoT Application Technology, Taihu University, Wuxi 214064, China

* Correspondence: maocsu@sina.com (Y.M.); wuxuelin@gmail.com (X.W.); yingguo@csu.edu.cn (Y.G.)

Received: 9 March 2020; Accepted: 28 March 2020; Published: 1 April 2020



Abstract: Quantum secret sharing (QSS) can usually realize unconditional security with entanglement of quantum systems. While the usual security proof has been established in theoretics, how to defend against the tolerable channel loss in practices is still a challenge. The traditional (t, n) threshold schemes are equipped in situation where all participants have equal ability to handle the secret. Here we propose an improved (t, n) threshold continuous variable (CV) QSS scheme using weak coherent states transmitting in a chaining channel. In this scheme, one participant prepares for a Gaussian-modulated coherent state (GMCS) transmitted to other participants subsequently. The remaining participants insert independent GMCS prepared locally into the circulating optical modes. The dealer measures the phase and the amplitude quadratures by using double homodyne detectors, and distributes the secret to all participants respectively. Special t out of n participants could recover the original secret using the Lagrange interpolation and their encoded random numbers. Security analysis shows that it could satisfy the secret sharing constraint which requires the legal participants to recover message in a large group. This scheme is more robust against background noise due to the employment of double homodyne detection, which relies on standard apparatuses, such as amplitude and phase modulators, in favor of its potential practical implementations.

Keywords: quantum secret sharing; weak coherent state; homodyne detector

1. Introduction

Secret sharing is a branch of cryptography [1], in which the dealer distributes a secret to all participants and only legitimate participants can reconstruct the shared secret in the cooperation fashion. The dealer distributes a secret message s to n participants which at least $t \leq n$ participants combine to recover the secret. It is known as a (t, n) -threshold scheme [2–9]. Quantum secret sharing (QSS) is an extension of classical secret sharing via quantum states. Compared with the classical secret sharing, QSS protocols can achieve unconditional security based on the quantum no-cloning theorem and the Heisenberg uncertainty principle [10].

Quantum secret sharing (QSS) can be categorized into discrete variable QSS (DVQSS) [11–14] and continuous variable QSS (CVQSS) [15–22] based on the carriers used. In DVQSS, the discrete variable quantum states are used for the secret sharing, in which it carries information via weak laser pulses or the single photons. Owing to the low channel capacity and the difficulty of the preparation of single photons, it is difficult to implement in practices. In order to avoid these shortages, the continuous variable quantum states, such as coherent states and squeezed states, can be used for the information carriers, resulting in the CVQSS. Coherent states can be generated and operated by linear optical components and squeezed states can be generated from them through non-linear interactions. Furthermore, both of them increase the channel capacity.

In the traditional QSS schemes, most of them are (n, n) -threshold schemes, in which only all the n participants work together can recover the secret message from dealer, but any part of participants are impossible to restore the secret. For example, Cleve et al. proposed an initial (t, n) threshold DVQSS protocol in theoretics [11]. Correspondingly, the CVQSS was proposed with its interferometric realization that depends on infinite squeezing [23]. After that, the $(2,3)$ threshold scheme was designed using entangled system [16]. Thereafter, the (n, n) -threshold protocol was dished with weak coherent state [24]. However, most of QSS protocols are based on squeezed states which are difficult to prepare in the laboratory, compared with coherent states. Moreover, all participants have equal ability to recover the initial secret from the dealer in traditional (t, n) threshold schemes. They cannot satisfy the practical conditions which needs some specifically designated participants to share message and accomplish tasks in a large group.

Currently, the Gaussian modulated coherent state (GMCS) has been elegantly applied in continuous variable quantum cryptography [25–27]. The Gaussian modulation encodes the key information by modulating the quadratures the amplitude X and the phase P of few-photon coherent states with a centered Gaussian distribution, where X and P quadratures can be measured by a heterodyne detector or homodyne detector [28–31]. The GMCS-involved scheme has been proved to be secure against collective attacks and coherent attacks. Motivated by the elegant characteristics of the GMCS-involved system, we suggest an approach for establishing the GMCS-based CVQSS system. An improved (t, n) threshold scheme will be proposed with weak coherent states. The main feature is that, instead of all participants have equal ability to recover the secret, it requires specially designated participants for the secret sharing. Each participant imports the locally prepared GMCS into a circulating optical mode with a beam splitter, which can be implemented with current optical technologies. Compared with modulating quantum state of the passing-through photon, this can make our protocol flexible and avoid obstruction from the eavesdroppers in the quantum state preparation.

The paper is organized as follows. In Section 2, we present the GMCS-involved (t, n) scheme for the CVQSS system. In Section 3, we demonstrate the security analysis of the proposed CVQSS scheme. In Section 4, performance analysis are shown with numerical simulation results of practical parameters. Finally, the conclusions are drawn in Section 5.

2. The GMCS-Involved (t, n) Scheme for CVQSS

Enlightened by the characteristics of the GMCS-involved quantum key distribution (QKD) [19] and the topological structure of the (n, n) -threshold scheme using weak coherent states [24], we propose an improved (t, n) threshold scheme for the practical CVQSS.

As shown in Figure 1, all participants and the dealer are linked by a single fibre-based quantum channel for transmission. The first participant B_1 generates Gaussian random numbers and modulates actively the output of a local laser using phase and amplitude modulators to prepare a coherent state $|x_1 + ip_1\rangle$. Here, two variables x_1 and p_1 are independent Gaussian random numbers with zero mean and a variance of $V_1 N_0$, where N_0 is the shot-noise variance, and V_1 represents the modulation variance determined by B_1 . Then, the coherent state $|x_1 + ip_1\rangle$ is sent to the adjacent participant and passes through a highly asymmetric beam splitter of B_2 . Meanwhile, B_2 prepares the other GMCS and couples it into the spatiotemporal mode as the same as B_1 by using the second beam splitter. B_2 could realize phase-space displacements of $\{x_2, p_2\}$ by adjusting the modulation variances and the reflectivity of the asymmetric beam splitter. The remaining participants execute the similar procedure. Finally, the quantum state of dealer can be expressed as $|\sum_{j=1}^n \sqrt{T_j} x_j + i \sum_{j=1}^n \sqrt{T_j} p_j\rangle$, where T_j is the channel transmittance from the j th participant to the dealer. The dealer achieves $\{x_h, p_h\}$ by measuring the amplitude and phase quadratures of the end quantum state via double homodyne detection.

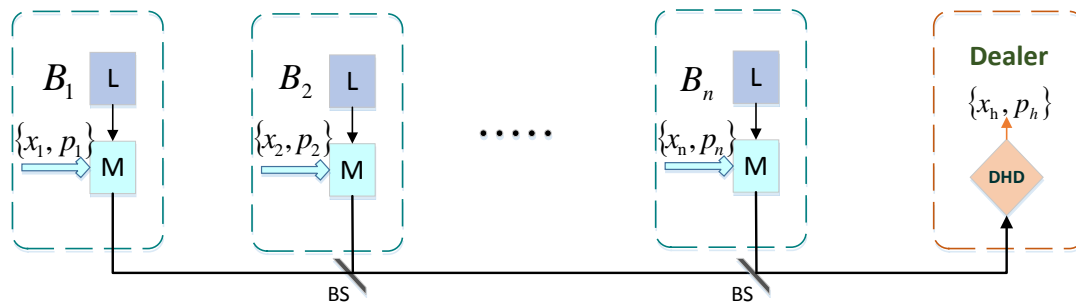


Figure 1. The state preparation of participants and the dealer. L is laser, M represents modulator, BS is beam splitter, DHD expresses double homodyne detector, and $\{x_j, p_j\}$ are independent Gaussian random numbers retained by the j^{th} participant B_j with $j \in \{1, 2, \dots, n\}$.

Stage 1. Preparation Processing :

1. The first participant B_1 generates the coherent state $|x_1 + ip_1\rangle$ based on its Gaussian random numbers $\{x_1, p_1\}$, laser and modulator, and sends it to the next participant B_2 .
2. Each of the remained participants couples the locally prepared GMCS into the spatiotemporal mode at the same time as B_1 by using the highly asymmetric beam splitter.
3. The dealer obtains $\{x_h, p_h\}$ by measuring the amplitude and phase quadratures of the received quantum state via double homodyne detection. The resulting $\{x_h, p_h\}$ is saved as raw data.
4. Repeat above steps until the dealer gets enough raw data.
5. A subset of the raw data is randomly chose and the dealer demands all the participants to publish the corresponding Gaussian random numbers. Combined with the corresponding measurement results, the transmittance $\{T_1, T_2, \dots, T_n\}$ can be achieved [32]. All participants abandon the disclosed data.
6. The dealer randomly chooses a subset of remaining raw data after step 5. The dealer presumes each participant except B_m is dishonest and demands them to publish their corresponding Gaussian random numbers.
7. The dealer replaces the measurement result by $x_F = x_h - \sum_{j=1, j \neq m}^n \sqrt{T_j} x_j$ and $p_F = p_h - \sum_{j=1, j \neq m}^n \sqrt{T_j} p_j$. In this case, $\{x_F, p_F\}$ and the raw data of B_m are same subsets. Therefore, the dealer and B_m can gain a lower bound of secure key rate R_m of the GMCS-based quantum cryptography.
8. Repeat the step 7 for n times. Finally, the dealer gets secure key rates $\{R_1, R_2, \dots, R_n\}$ [18].

Stage 2. Implementation Processing :

1. Legitimate t participants are sorted by an agreed rule using C_{lj} for $l \in \{1, 2, \dots, t\}$ and $j \in \{1, 2, \dots, n\}$.
2. Supposing that the sequence of t participants is shown in Figure 2, the dealer randomly chooses a subset of the remained raw data and demands all participants except C_{12} to publish the corresponding Gaussian random numbers. The dealer obtains $\{x_{12_1}, p_{12_1}\}$ with $x_{12_1} = x_h - \sum_{j=1, j \neq 2}^n \sqrt{T_j} x_j$ and $p_{12_1} = p_h - \sum_{j=1, j \neq 2}^n \sqrt{T_j} p_j$.
3. Repeat the step 2 for t times. Each of subset $\{x_{l_{j_l}}, p_{l_{j_l}}\}$ of the dealer is the same as $\{x_j, p_j\}$ of B_j , for $l \in \{1, 2, \dots, t\}$ and $j \in \{1, 2, \dots, n\}$.

- The dealer emerges the secure key S from raw data. Distribution of the secure key S can be described as follows

$$\begin{aligned} Z_1 &= S \pmod{x_{1j_1}}, \\ Z_2 &= S \pmod{x_{2j_2}}, \\ &\dots \\ Z_{t-1} &= S \pmod{x_{t-1j_{t-1}}}, \\ Z_t &= S \pmod{x_{tj_t}}. \end{aligned} \tag{1}$$

- The polynomial prepared by the dealer can be expressed as

$$f(x) = S + Z_1x + Z_2x^2 + \dots + Z_{t-2}x^{t-2} + Z_{t-1}x^{t-1}. \tag{2}$$

The dealer calculates $f(x)$ and obtains $\{f(x_{1j_1}), f(x_{2j_2}), \dots, f(x_{tj_t})\}$.

- The dealer recodes the $f(x_{l_j})$ by Pauli operation. Simultaneously, it prepares some decoy particles and randomly inserts them to the coding sequence. The dealer remembers the initial state and position of each decoy particles. The dealer selects the secure key rate R of the proposed protocol as the minimum of $\{R_{1j_1}, R_{2j_2}, \dots, R_{tj_t}\}$, $R_{l_j} = R_j$ [18] and sends them to all the participants according to the sequence of C_{l_j} . After affirming C_{l_j} has received the coding sequence, the dealer announces the initially inserted state and position of each decoy particles to C_{l_j} . Then $\{x_j, f(x_{l_j})\}$ becomes the private key of C_{l_j} .
- Legitimate participants restore the secret S by the Lagrange interpolation.

$$\begin{aligned} f(x) &= f(x_{1j_1})\psi_1 + f(x_{2j_2})\psi_2 + \dots + f(x_{tj_t})\psi_t \\ &= S + Z_1x + Z_2x^2 + \dots + Z_{t-1}x^{t-1}, \end{aligned} \tag{3}$$

where

$$\psi_k = \prod_{l=1, l \neq k}^t \frac{x - x_{lj_l}}{x_{kj_k} - x_{lj_l}}, \tag{4}$$

with x_{lj_l} equal to x_j for $k, l \in \{1, 2, \dots, t\}$ and $j \in \{1, 2, \dots, n\}$.

Here, procedures of the GMCS-involved CVQSS is introduced in detail. Legitimate participants can share message from the dealer based on it. Furthermore, the security is a critical factor for a QSS scheme. The security analysis of QSS is typically more involved than that of QKD. The general security proof against eavesdroppers in the channels and dishonest participants who have only appeared recently. However, dishonest participants have more superiorities to undermine the secret sharing than eavesdroppers from outside. Consequently, the following security analysis primarily focuses on both eavesdroppers and dishonest participants.

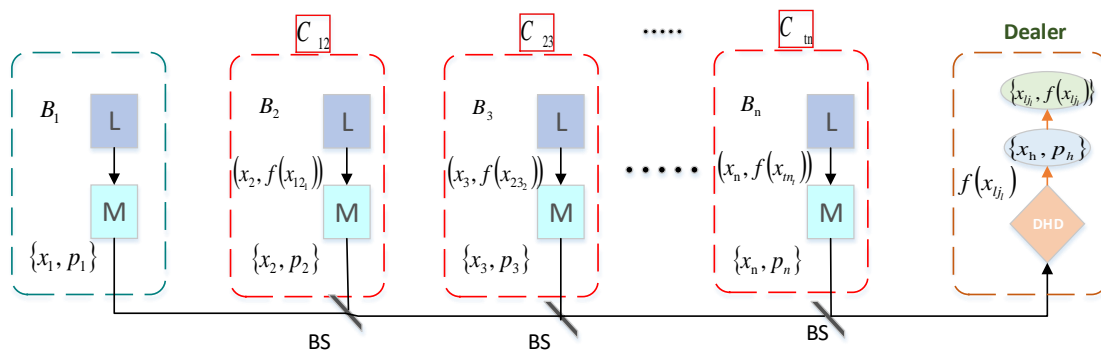


Figure 2. The data-processing of legitimate t participants and the dealer. L is laser, M represents modulator, BS is beam splitter, DHD expresses double homodyne detector, $\{x_j, p_j\}$ are independent Gaussian random numbers retained by participant B_j , $\{x_j, f(x_{ji})\}$ is the private key of C_{ij} , $l \in \{1, 2, \dots, t\}, j \in \{1, 2, 3, \dots, n\}$.

3. Security Analysis

In the following, we consider the security of the GMC-involved CVQSS against intercept-and-resend attack, collective attack, dishonest participants attack and entangle attack.

3.1. Intercept-and-Resend Attack

Intercept-and-resend attack has two situations. One is that an eavesdropper, Eve, intercepts quantum information from the dealer and copied it. Then she sends the copied quantum information to legitimate participants. Because of quantum no-cloning theorem, the copied quantum information can not happen for the GMCS-involved CVQSS system. The other is that eavesdroppers intercept quantum information from the dealer and send false quantum information to the legitimate participants rather than copy it. In this case, the GMCS-based (t, n) -threshold scheme protects quantum states by randomly inserting some decoy particles to the coding sequence. Every decoy particle is selected randomly from CV quantum states. Eavesdroppers can not determine the initial state and position of each decoy particles. We assume that the coding sequence has Ω decoy particles. The attack is found with the probability $1 - (\frac{3}{4})^\Omega$. For $\Omega \rightarrow \infty$, the probability will converge to 1 [33].

3.2. Collective Attack

Based on the polynomial and Lagrange interpolation, we find that restoring the secret requires t legitimate participants. We assume that the dealer and one of legitimate participants are honest. The rest of participants are illegal user in this secret sharing in the large group. However, $t - 1$ dishonest legitimate participants can not obtain the secret S by using collective attack, since they cannot carry out collective attack. The above-mentioned situation is similar to GMCS-based quantum cryptography. Suppose that the dealer demands $t - 1$ legitimate participants to publish their private key while the last participant holds its Gaussian random numbers and $f(x)$ from the dealer. Therefore, the last participant owns all data of legitimate participants to recover the secret key. Since the dealer is honest and attempts to generate a secret key against all the other $t - 1$ participants. In this case, it is the same as the GMCS-based quantum key distribution (QKD) and the secure key rate of the GMCS-involved CVQSS protocol can be evaluated by standard security proofs of QKD [25–27]. Because the secure key of CVQSS ought to secure against any group of $t - 1$ participants, the dealer needs to select the smallest one among secure key rates of legitimate participants and the dealer. The secure key rate of the GMCS-based QKD can be calculated between the dealer and a selected participant while other $t - 1$ legitimate participants are dishonest [24,34]. In order to show the performance of the CVQSS protocol, we execute simulations using concrete parameters and analyze the results in the next section.

3.3. Dishonest Participants Attack

When dishonest participants try to intercept other legitimate participants information to restore the secret by themselves, they can be seen as eavesdroppers. Because participants except legitimate t participants are illegal user in the large group, it has no effect even through they are dishonest. Next we discuss how to analyze security of the proposed protocol when dishonest participants appear in legitimate t participants and put error private key into the process of recover secret key. Under the circumstances, it occurs two probability, i.e., the polynomial can be restored and the polynomial can not be restored. For the first case, we assume a dishonest participant C_{l_j} make $\{x'_j, f(x_{l_{j_1}})'\}$ as its private key, where $f(x_{l_{j_1}})' \neq S + Z_1x'_j + Z_2(x'_j)^2 + \dots + Z_{t-2}(x'_j)^{t-2} + Z_{t-1}(x'_j)^{t-1}$. Using the Lagrange interpolation, the polynomial can be expressed as

$$\begin{aligned} f(x)' &= f(x_{1j_1})\psi_1 + f(x_{2j_2})\psi_2 + \dots + f(x_{l_{j_1}})'\psi_l + \dots + f(x_{tj_t})\psi_t \\ &= S' + Z'_1x + Z'_2x^2 + \dots + Z'_lx^l + \dots + Z'_{t-1}x^{t-1}, \end{aligned} \tag{5}$$

where S' is the recovered secret key. After testing and verifying, S' and Z'_τ do not satisfy the constraint in Equation (1) for $\tau \in \{1, 2, \dots, t\}$. It seems that the dishonest participant can be found by the legal participants. For the second case, supposing that a dishonest participant substitutes $\{x_j, f(x_{l_{j_1}})\}$ with $\{x_j^*, f(x_{l_{j_1}})^*\}$, where $f(x_{l_{j_1}})^* = S + Z_1x_j^* + Z_2(x_j^*)^2 + \dots + Z_{t-2}(x_j^*)^{t-2} + Z_{t-1}(x_j^*)^{t-1}$. The polynomial can be represented as

$$\begin{aligned} f(x)^* &= f(x_{1j_1})\psi_1 + f(x_{2j_2})\psi_2 + \dots + f(x_{l_{j_1}})^*\psi_l^* + \dots + f(x_{tj_t})\psi_t \\ &= S + Z_1x + Z_2x^2 + \dots + Z_lx^l + \dots + Z_{t-1}x^{t-1}. \end{aligned} \tag{6}$$

Obviously, the restored polynomial is equal to the primitive polynomial, and S is the secret key from the dealer. However, it does not satisfy the constraint $Z_l = S \pmod{x_j^*}$. By the above-mentioned measurements, we can detect the dishonest participant. If the number of dishonest participant is more than one, they can be detected with more possibility [35–38].

3.4. Entanglement Attack

In this kind of attack, Eve does not change quantum information, but disturbs the channel with entanglement attack. In the preparation stage, the dealer sends $f(x_{l_{j_1}})$ to legitimate participants based on the sequence of C_{l_j} . When Eve does not know it, she can not deal with $f(x_{l_{j_1}})$ corresponding to C_{l_j} . So it is significant to get x_j from each legitimate participant for eavesdropping. In the implementation stage, the dealer randomly chooses a subset of the remained raw data and demands all participants except C_{l_j} to publish the corresponding Gaussian random numbers. C_{l_j} keeps its Gaussian random numbers and gets x_j as the private key of C_{l_j} . In this case, x_j does not need to be transmitted in the fiber channel. Therefore, Eve can not obtain it by attacking the entangled channel.

4. Numerical Simulation

In numerical simulations of practical implementations, groups of t legitimate participants from all participants are designated with different values and geographical positions. We assume that the distance of the dealer and the farthest legitimate participant is \hbar and all the other $t - 1$ participants are randomly distributed. The minimum secure key rate is seen as the secure key rate of the proposed CVQSS system.

Because there exists the excess noise ε for every participant, the farthest legitimate participant is the one that achieves the minimum secure key rate of the dealer. The secret rate can be derived as [31]

$$K = \kappa I_{AB} - \chi_{BE}, \tag{7}$$

where κ is the reconciliation efficiency, I_{AB} expresses the Shannon mutual information shared between Alice and Bob, and χ_{BE} represents upper bound information accessible to Eve (including the other $t - 1$ participants and eavesdropper) on Bob's secret key.

The channel transmittance of the l^{th} participant can be defined as

$$T_l = 10^{-\frac{\gamma \rho_l h}{10}}, \tag{8}$$

where γ is the attenuation coefficient of the quantum channel, ρ_l represents the fiber length ratio of the l^{th} participant and the farthest participant to the dealer. In addition, the excess noise of all legitimate t participants is given by [29,39]

$$\varepsilon_t = \sum_{l=1}^t \frac{T_l}{T_h} \varepsilon, \tag{9}$$

with $T_h = 10^{-\frac{\gamma h}{10}}$. Using the channel input from Alice as reference, $\frac{T_l}{T_h} \varepsilon$ represents the l^{th} participant's excess noise. In this case, the excess noise is connected with the channel transmittance. The channel-added noise can be described as

$$\chi_f = \frac{1}{T_h} - 1 + \varepsilon_t. \tag{10}$$

Consequently, the total noise referred to the channel input between Alice and Bob can be given by

$$\chi_{tot} = \chi_f + \frac{\chi_h}{T_h}, \tag{11}$$

with $\chi_h = [1 + (1 - \eta) + 2v_{el}]/\eta$, where η is an efficiency and v denotes the noise owing to detector electronics. Moreover, the mutual information of Alice and Bob is given by

$$I_{AB} = \log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}}, \tag{12}$$

where $V = V_A + 1$ and V_A is the modulation variance of Alice.

The maximum information accessible to Eve on Bob's secret key is the Holevo quantity, which can be derived as

$$\chi_{BE} = \sum_{i=2}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right), \tag{13}$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2(x)$. The symplectic eigenvalues $\lambda_{1,2}$ can be calculated as

$$\lambda_{1,2} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4D}}{2}}, \tag{14}$$

where $\Delta = V^2(1 - 2T_h) + 2T_h + T_h^2(V + \chi_f)^2$ and $D = T_h^2(V\chi_f + 1)^2$. Furthermore, the symplectic eigenvalues $\lambda_{3,4}$ can be calculated as

$$\lambda_{3,4} = \sqrt{\frac{A \pm \sqrt{A^2 - 4B}}{2}}, \tag{15}$$

with the notations

$$A = \{\Delta\chi_h^2 + D + 1 + 2\chi_h[V\sqrt{D} + T_h(V + \chi_f)] + 2T_h(V^2 - 1)\}/[T_h(V + \chi_{tot})]^2, \tag{16}$$

$$B = \left(\frac{V + \sqrt{D}\chi_h}{T_h(V + \chi_{tot})}\right)^2.$$

The last symplectic eigenvalue λ_5 is equal to 1.

As mentioned above, the channel transmittance of the l^{th} legitimate participant changes with different fiber length to the dealer. Since the secret key rate is relevant to distance between each legitimate participant and the dealer, different kinds of distribution have a great effect on calculating the secure key rate. Because ρ_l represents the fiber length ratio of the l^{th} participant and the farthest participant to the dealer, different kinds of distribution can be described by different kinds of ρ_l . As shown in Figure 3, we achieve the relation of the secure key rate and the fiber length at different kinds of distribution and identical number of legitimate participants $t = 20$. In Figure 3, the secret key rates of different kinds distribution of legitimate participants are the same when the fiber length is short. The longer of the fiber length means more influence of different kinds distribution of legitimate participants. Different of secure key rates increases for the same fiber length.

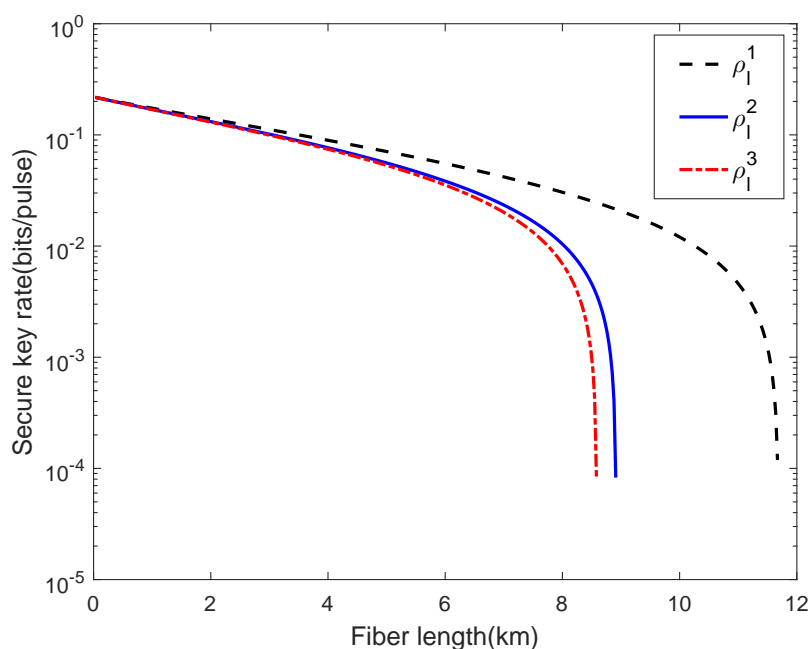


Figure 3. The secure rates of different kinds distribution of legitimate participants for $\rho_l^1 = 1 - e^{-0.2l}$, $\rho_l^2 = \frac{l}{t}$, $\rho_l^3 = \sqrt{\frac{2}{\pi}} e^{-\frac{l^2}{200}}$, $l \in \{1, 2, \dots, t\}$ and $t = 20$. The parameters are given by $V_A = 6$, $\gamma = 0.2$ dB/km, $\varepsilon = 0.01$, $\kappa = 0.98$, $\eta = 0.6$, and $v_{el} = 0.01$.

In practical implementations, various tasks need different number of legitimate participants to accomplish for the secret sharing. The number of legitimate participants of one task is determined by the dealer, and the possibility of each participant to participate the task is equal. In this case, the relation of the secure key rate and the fiber length at different number of legitimate participants t out of identical all participants $n = 25$ is shown in Figure 4. For $t = 5$, the secret key rate decreases with the fiber length increasing. With the number of legitimate participants increasing at the same for $n = 25$, the secret key rate reduces gradually at the same fiber length. When the number of legitimate participants reaches the upper limit for $t = n = 25$, the secret key rate is the smallest at the same fiber length. In this case, it becomes the (n, n) -threshold CVQSS scheme. This scheme can be conducted at 4 km with 25 legitimate participants for $\varepsilon = 0.01$. Figure 5 shows the relations of the secret key rate and the fiber length for different numbers of legitimate participants $t = 5, 50, 100$ and 200 out of identical all participants $n = 200$. For $\varepsilon = 0.001$, the number of legitimate participants can be determined randomly between 2 and 200. We find that this scheme can be conducted at 10 km with 200 legitimate participants.

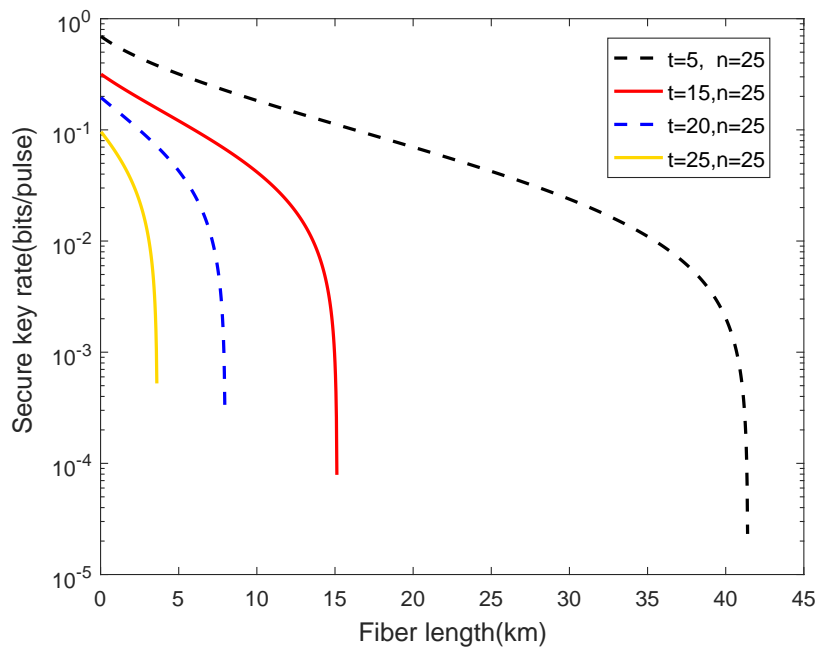


Figure 4. The secure rates of different number of legitimate participants for $n = 25$. The parameters are given by $V_A = 6$, $\gamma = 0.2$ dB/km, $\varepsilon = 0.01$, $\kappa = 0.98$, $\eta = 0.6$, and $v_{el} = 0.01$.

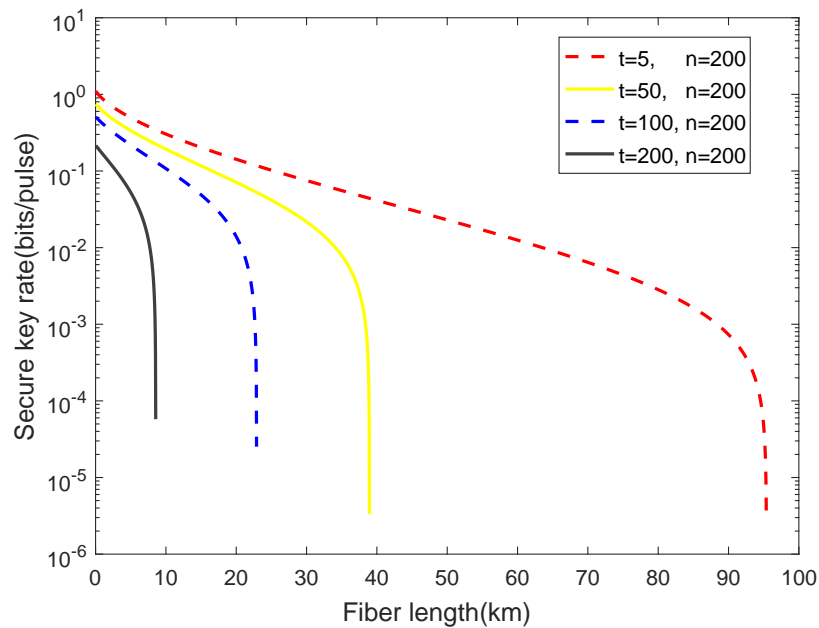


Figure 5. The secret rates of different numbers of legitimate participants for $n = 200$. The parameters are given by $V_A = 6$, $\gamma = 0.2$ dB/km, $\varepsilon = 0.001$, $\kappa = 0.98$, $\eta = 0.6$, and $v_{el} = 0.01$.

The reconciliation efficiency ranges from 0 when no information was extracted to 1 for a perfect reconciliation scheme. It is connected with the Shannon mutual information shared between Alice and Bob. The relation of the secure key rate and the fiber length at different number of legitimate participants t and reconciliation efficiency out of identical all participants $n = 50$ is shown in Figure 6. Here, we choose $t = \{15, 30, 45\}$, and values of κ are 0.98 and 0.9. The numeral relation can be displayed in Figure 6. It is obviously that by using the higher reconciliation efficiency the secure key rate under the same number of legitimate participants t is increased in comparison to the lower.

The attenuation coefficient has influence on the channel transmittance of all participants. We use a similar analytical approach to illustrate the effect of the attenuation coefficient γ on the secure key rate with different number of legitimate participants t . Figure 7 shows that the higher secure key rate and longer maximum transmission distance can be achieved by tuning the value of parameter γ to be smaller.

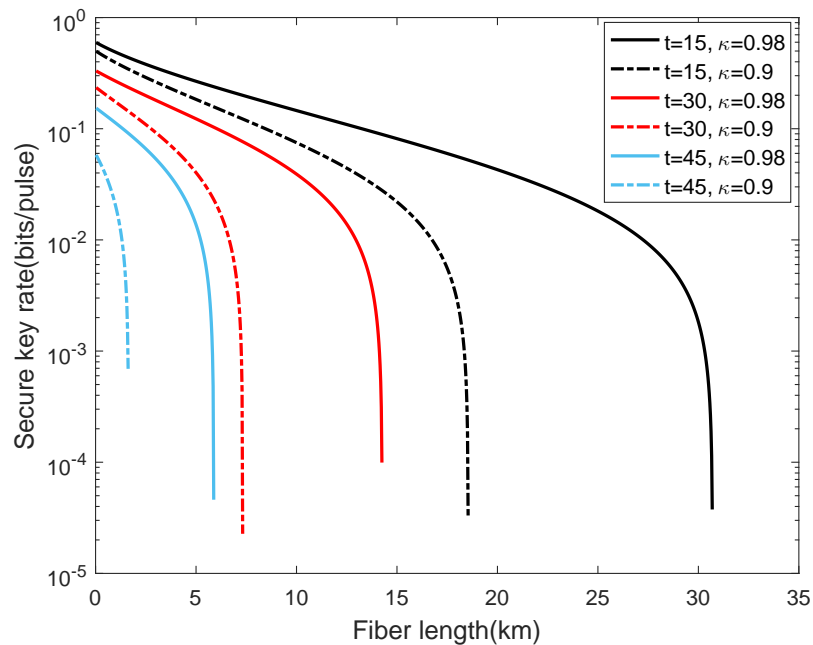


Figure 6. The secret rates of different numbers of legitimate participants and reconciliation efficiency for $n = 50$. The parameters are given by $V_A = 6$, $\gamma = 0.2$ dB/km, $\epsilon = 0.005$, $\eta = 0.6$, and $v_{el} = 0.01$.

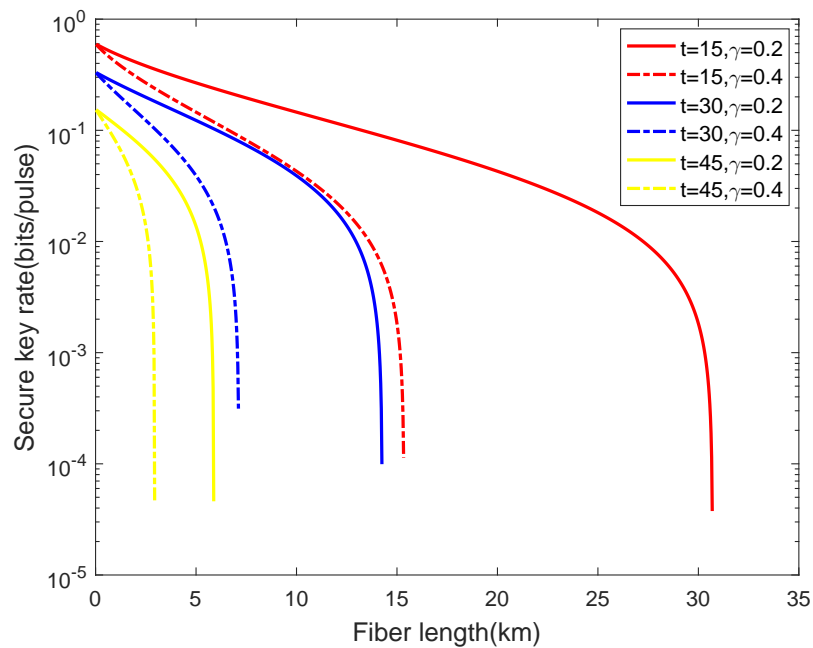


Figure 7. The secret rates of different numbers of legitimate participants and attenuation coefficient for $n = 50$. The parameters are given by $V_A = 6$, $\epsilon = 0.005$, $\kappa = 0.98$, $\eta = 0.6$, and $v_{el} = 0.01$.

5. Conclusions

We have suggested an improved approach for the GMCS-involved (t, n) threshold CVQSS. The secret sharing scheme combines weak coherent states with double homodyne detectors, making it available for practical implementations due to the fact that the GMCS can be prepared and modulated with current technologies. Compared with the traditional (t, n) threshold QSS protocols, only the designated participants could recover the original secret using the Lagrange interpolation with their encoded random variables instead of all participants dealing with equal ability. Since each participant imports a locally prepared quantum state into a circulating optical mode, it improves the security of the CVQSS system in practices. We consider the security of the proposed protocol against intercept-and-resend attack, collective attack, dishonest participants attack and entanglement attack. In addition, the proposed protocol could fit particular condition in which it needs some special participants for the secret sharing in a large group.

Author Contributions: Methodology, Y.W., B.J.; validation and data curation, Y.M., X.W.; writing—original draft preparation, Y.W., B.J.; writing—review and editing, Y.W.; visualization, Y.G.; supervision, Y.W.; project administration, Y.G.; funding acquisition, Y.W., Y.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China grant number 61871407.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612. [[CrossRef](#)]
2. Nascimento, A.C.A.; Mueller-Quade, J.; Imai, H. Improving quantum secret sharing schemes. *Phys. Rev. A* **2001**, *64*, 042311. [[CrossRef](#)]
3. Bai, C.M.; Li, Z.H.; Xu, T.T.; Li, Y.M. A generalized information theoretical model for quantum secret sharing. *Int. J. Theor. Phys.* **2016**, *55*, 4972–4986. [[CrossRef](#)]
4. Dehkordi, M.H.; Fattahi, E.T. Threshold quantum secret sharing between multiparty and multiparty using Greenberger-Horne-zeilinger state. *Quantum. Inf. Process.* **2013**, *12*, 1299–1306. [[CrossRef](#)]
5. Guo, C.; Yuan, Q.Q.; Lu, K. (t, n) Threshold secret image sharing scheme with adversary structure. *Multimed. Tools Appl.* **2017**, *7*, 21193–21210. [[CrossRef](#)]
6. Maitra, A.; Paul, G. A Resilient Quantum Secret Sharing Scheme. *Int. J. Theor. Phys.* **2015**, *54*, 398–408. [[CrossRef](#)]
7. Lu, C.B.; Miao, F.Y.; Hou, J.P. Verifiable threshold quantum secret sharing with sequential communication. *Quantum. Inf. Process.* **2018**, *17*, 310. [[CrossRef](#)]
8. Chen, Y.H.; Zhang, N.; Tian, H. A Novel Connection Correlation Scheme Based on Threshold Secret Sharing. *IEEE Commun. Lett.* **2016**, *20*, 2414–2417. [[CrossRef](#)]
9. Qin, H.W.; Dai, Y.W.; Wang, Z.Q. A secret sharing scheme based on (t, n) threshold and adversary structure. *Int. J. Inf. Secur.* **2009**, *8*, 379–385. [[CrossRef](#)]
10. Hillery, M.; Buzek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1993**, *59*, 1829–1834. [[CrossRef](#)]
11. Cleve, R.; Gottesman, D.; Lo, H.K. How to share a quantum secret. *Phys. Rev. Lett.* **1999**, *83*, 648. [[CrossRef](#)]
12. Zhang, Z. Controlled teleportation of an arbitrary n-qubit quantum information using quantum secret sharing of classical message. *Phys. Lett. A* **2006**, *352*, 55–58. [[CrossRef](#)]
13. Qin, H.; Tso, R. Efficient quantum secret sharing based on special multi-dimensional GHZ state. *Opt. Quant. Electron.* **2018**, *50*, 167. [[CrossRef](#)]
14. Khakbiz, P.; Asoudeh, M. Sequential quantum secret sharing in noisy environments. *Quantum. Inf. Process.* **2019**, *18*, 11. [[CrossRef](#)]
15. Zhao, Y.Q.; Guo, Y. High-efficient quantum secret sharing based on the Chinese remainder theorem via the orbital angular momentum entanglement analysis. *Quantum. Inf. Process.* **2013**, *12*, 1125–1139.
16. Lance, A.M.; Symul, T.; Bowen, W.P. Continuous variable $(2, 3)$ threshold quantum secret sharing schemes. *New J. Phys.* **2003**, *5*, 4. [[CrossRef](#)]

17. Yang, Y.G.; Wen, Q.Y. Threshold quantum secret sharing between multi-party and multi-party. *Sci. China Ser. G* **2008**, *51*, 1308–1315. [[CrossRef](#)]
18. Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **2015**, *17*, 6072–6092. [[CrossRef](#)]
19. Grosshans, F.; Assche, G.V.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature (London)* **2003**, *421*, 238. [[CrossRef](#)]
20. Li, J.J.; Wang, N.; Wang, Z.H. New Secret Sharing Scheme Based on Faster R-CNNs Image Retrieval. *IEEE Access* **2018**, *6*, 49348–49357. [[CrossRef](#)]
21. Wu, X.D.; Wang, Y.J.; Huang, D. Passive continuous-variable quantum secret sharing using a thermal source. *Phys. Rev. A* **2020**, *101*, 022301. [[CrossRef](#)]
22. Kogias, I.; Xiang, Y.; He, Q.Y.; Adesso, G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys. Rev. A* **2017**, *95*, 012315. [[CrossRef](#)]
23. Tyc, T.; Sanders, B.C. How to share a continuous-variable quantum secret by optical interferometry. *Phys. Rev. A* **2002**, *65*, 042310. [[CrossRef](#)]
24. Grice, W.P.; Qi, B. Quantum secret sharing using weak coherent states. *Phys. Rev. A* **2019**, *100*, 022339. [[CrossRef](#)]
25. Wang, Y.J.; Fu, J.; Guo, Y. Photon-monitoring attack on continuous-variable quantum key distribution with source in middle. *Quantum. Inf. Process.* **2014**, *13*, 2745–2757. [[CrossRef](#)]
26. Wang, Y.J.; Wang, X.D.; Li, J.W.; Guo, Y. Self-referenced continuous-variable measurement-device-independent quantum key distribution. *Phys. Lett. A* **2018**, *382*, 1149–1156. [[CrossRef](#)]
27. Wang, Y.J.; Mao, Y.Y.; Huang, W.T.; Guo, Y. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution. *Opt. Express* **2019**, *27*, 25314–25329. [[CrossRef](#)]
28. Liu, W.Q.; Peng, G.Y.; Huang, P.; Wang, S.Y.; Wang, T.; Zeng, G.H. Continuous-variable quantum key distribution based on continuous random basis choice. *Chin. Phys. B* **2018**, *27*, 070305. [[CrossRef](#)]
29. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; McLaughlin, S.W.; et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305. [[CrossRef](#)]
30. Wang, Y.J.; Wu, X.D.; Zhang, L.; Guo, Y. Performance improvement of free-space continuous-variable quantum key distribution with an adaptive optics unit. *Quantum. Inf. Process.* **2019**, *18*, UNSP 251. [[CrossRef](#)]
31. Guo, Y.; Liao, Q.; Wang, Y.; Huang D.; Huang P.; Zeng, G. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *95*, 032304. [[CrossRef](#)]
32. Guo, Y.; Ye, W.; Zhong, H.; Liao, Q. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis. *Phys. Rev. A* **2019**, *99*, 032327. [[CrossRef](#)]
33. Qin, H.W.; Zhu, X.H.; Dai, Y.W. (t, n) Threshold quantum secret sharing using the phase shift operation. *Quantum. Inf. Process.* **2015**, *14*, 2997–3004. [[CrossRef](#)]
34. Yang, Y.G.; Gao, S.; Li, D.; Zhou, Y.H.; Shi, W.M. Three-party quantum secret sharing against collective noise. *Quantum. Inf. Process.* **2019**, *18*, 215. [[CrossRef](#)]
35. Binu, V.P.; Sree Kumar, A. Secure and Efficient Secret Sharing Scheme with General Access Structures Based on Elliptic Curve and Pairing. *Wirel. Pers Commun.* **2017**, *92*, 1531–1543. [[CrossRef](#)]
36. Guo, Y.; Xie, C.; Huang, P.; Li, J.; Zhang, L.; Huang, D.; Zeng, G. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *97*, 052326. [[CrossRef](#)]
37. Chen, D.; Lu, W.; Xing, W.W. An Efficient Verifiable Threshold Multi-Secret Sharing Scheme with Different Stages. *IEEE Access* **2019**, *7*, 107104–107110. [[CrossRef](#)]
38. Cai, X.Q.; Wang, T.Y.; Zhang, R.L. Security of Verifiable Threshold Quantum Secret Sharing with Sequential Communication. *IEEE Access* **2019**, *7*, 134854–134861. [[CrossRef](#)]
39. Rfifi, S. Exploiting a Fock Cavity Field to Enhance Quantum Secret Sharing Through a Phase-Damping Noisy Channel. *Int. J. Theor. Phys.* **2016**, *55*, 4553–4563. [[CrossRef](#)]

