Continuous-variable measurement-device-independent quantum secret sharing without entanglement

Yunwu Zheng[1], Xiangyu Wang[1,*] and Song Yu[1], Ziyang Chen[2]

[1]State Key Laboratory of Information Photonics and Optical Communications Beijing University of Posts and Telecommunications Beijing, China
[2]State Key Laboratory of Advanced Optical Communication, Systems and Networks Department of Electronics, and Center for Quantum Information Technology, Peking University Beijing, China

[*]Corresponding author: xywang@bupt.edu.cn

Keywords: quantum cryptography, quantum secret sharing, measurement-device-independent.

Abstract: Quantum secret sharing is an important technique in the field of quantum cryptography. However, the existence of imperfect detector is a serious threat in practical. Here we propose a continuous-variable measurement-device-independent quantum secret sharing protocol to remove the attacks carried out on imperfect detectors. We analyze the performance of the proposed protocol under different conditions, and show that it can be extendable to a large number of participants, which is of great help to its practical implementation.

1. Introduction

Quantum secret sharing (QSS) is a protocol where a secret message is distributed and reconstructed with unconditional security. The first QSS protocol is proposed in 1999 [1], in which the dealer distributes a secret to the players by entangled states, and the players have to collaborate to reconstruct the secret. After that, several QSS protocols based on entanglement have been proposed [2,3]. More recently, in order to ease the implementation difficulties and improve the performance, sequential QSS protocols that requires no entanglement have been proposed both in discrete-variable (DV) [4] and continuous-variable (CV) [5]. The latter has the advantage of being compatible with standard telecommunication technology as well as resilient to Trojan horse attacks.

In the above CV-QSS protocol, it is implicitly assumed that the detector of the dealer is trusted. However, this assumption seems unjustified and over-optimistic in the practical system, which seriously threats the security of practical CV-QSS system. In the field of quantum key distribution (QKD), a similar problem has been solved with the proposal of continuous-variable measurement-device-independent (CV-MDI) QKD [6,7], and then the MDI method has also been applied to CV-QSS [8-10]. It is remarkable that the existing CV-MDI QSS protocols are basically based on entanglement, so the complexity of system implementation increases with a larger number of participants. Therefore, a CV-MDI QSS protocol without entanglement is needed, which is extendable to a large number of participants.

In this paper, we propose a CV-MDI QSS protocol that is secure in the presence of imperfect detectors. In our protocol, Gaussian modulated coherent states are prepared locally by each player in the secure station and injected into a circulating optical mode with the help of highly asymmetric beam splitters (HABSs), which helps the protocol extendable to a large number of players with a reasonable performance. Then the dealer also prepares a coherent state, and the quantum states from the players and the dealer are finally measured by an untrusted third party through two homodyne detectors, making our protocol secure against all detector side attacks.

DOI: 10.25236/cseem.2020.173

2. The Protocol

As shown in Fig. 1, in our CV-MDI QSS scheme, n different players are connected by a single communication channel such as a telecom fiber. The quantum states from the players and the dealer interfere at a 50:50 BS at Charlie's side, who is an untrusted third party.

There are two stages in our CV-MDI QSS protocol: the quantum stage and the classical stage. All operations conducted by each participant in the two stages are carried out in his secure station, in which the quantum module (which contains the laser, modulators and other classical/quantum components) is used to generate Gaussian-modulated coherent state in the quantum stage and the classical unit is used to post-process the raw data and generate the secret key in the classical stage.

2.1 Quantum Stage

Step 1. Each player prepares a coherent state locally using the quantum module in his secure station. For the k-th (k=1, 2, …, n) player, his coherent state is denoted by $|x_k + ip_k\rangle$, where x_k and p_k are independent Gaussian random numbers chosen by P_k.

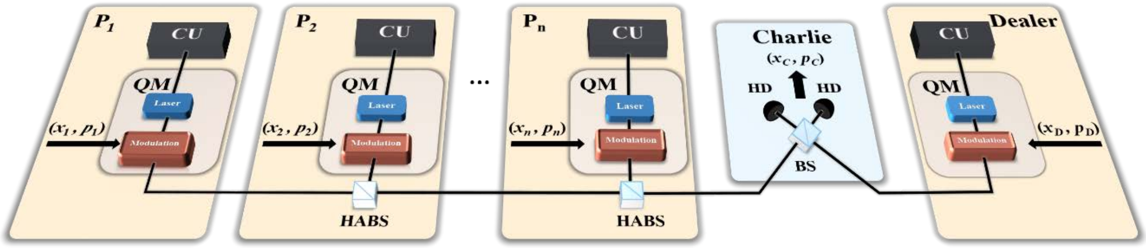

Fig 1. Schematic setup of the CV-MDI QSS protocol. QM: quantum module; CU: classical unit; HABS: highly asymmetric beam splitter; BS: 50:50 beam splitter; HD: homodyne detector. Quantum modules are used in each secure station to prepare Gaussian-modulated coherent states, then each player generates an independent secret key with the dealer using their classical units.

Step 2. Each player other than P_1 couples his quantum state into the same spatiotemporal mode as the state from P_1 via the HABS located in his secure station. At the end, the states from the players' side enter one input port of the 50:50 BS on Charlie's side, which can be described by

$$\left|\sum_{k=1}^{n}\sqrt{T_k}\,x_k + i\sum_{k=1}^{n}\sqrt{T_k}\,p_k\right\rangle \tag{1}$$

where T_k is the total transmittance (including losses due to the channel and the HABSs) experienced by the state from P_k.

Step 3. In the meantime, the dealer prepares his coherent state $|x_D + ip_D\rangle$ locally and sends it to another input port of Charlie's BS through the quantum channel.

Step 4. The untrusted third party Charlie makes a Bell measurement on the two output modes of the BS and broadcasts his measurement results, which can be described by

$$\begin{aligned} x_C &= \frac{1}{\sqrt{2}}\left(\sum_{k=1}^{n}\sqrt{T_k}\,x_k - \sqrt{T_D}x_D\right), \\ p_C &= \frac{1}{\sqrt{2}}\left(\sum_{k=1}^{n}\sqrt{T_k}\,p_k + \sqrt{T_D}p_D\right). \end{aligned} \tag{2}$$

2.2 Classical Stage

Step 1. The dealer randomly chooses a subset of the raw data, and all of the players as well as the dealer announce the corresponding Gaussian random numbers. Then the total transmittance of each player and the dealer can be calculated using the measurement results broadcast by Charlie.

Step 2. The dealer assumes that P_1 is an honest player and all the others dishonest. Then the dealer randomly chooses a subset of the remaining raw data, and requests all the other players to disclose their Gaussian random numbers. In the meantime, Charlie broadcasts the corresponding measurement results of the raw data.

Step 3. The dealer displaces the measurement results broadcast by Charlie using

$$x_N = x_C - \frac{1}{\sqrt{2}}(\sum_{k=2}^{n} \sqrt{T_k}\, x_k),$$
$$p_N = p_C - \frac{1}{\sqrt{2}}(\sum_{k=1}^{n} \sqrt{T_k}\, p_k). \tag{3}$$

After that, following the post-processing procedure of two-party CV-MDI QKD, the dealer and P_1 can derive a lower bound of the secret key rate R_1 based on $\{x_N, p_N\}$ and their own raw data. Then they generate a secret key K_1 using the reverse reconciliation scheme.

Step 4. Note that in the above steps P_1 is taken as an example, so steps 2-3 need to be repeated *n* times and in each run a different player is chosen as the honest player. Finally, the dealer selects the minimum of *n* secret key rates as the final secure rate, that is, $R = \min\{R_1, R_2, \dots, R_n\}$, and then obtains *n* independent keys $\{K_1, K_2, \dots, K_n\}$ with the players.

Finally, The dealer construct the final key K using $K = K_1 \oplus K_1 \oplus \cdots \oplus K_n$, where $\oplus$ represents modular 2 addition, and *n* players have to cooperate with each other to reconstruct it.

3. Numerical simulation

In order to calculate the secret key rate of CV-MDI QSS, we should first find the minimum of the n secret key rates. We assume that P_1 is the farthest player from Charlie with the distance L. The other *n* - 1 players are distributed at equal intervals between P_1 and Charlie. Therefore, the smallest secret key rate under normal operation will be the one between P_1 and the dealer.

For the quantum channels on the players' side and the dealer's side, both channel losses are α. Then the channel transmittance of P_k can be expressed as $T_k = 10^{-\frac{\alpha L_k}{10}}$, where L_k is the distance between P_k and Charlie. Similarly, the channel transmittance of the dealer can be calculated by $T_D = 10^{-\frac{\alpha L_D}{10}}$, where L_D is the distance between the dealer and Charlie. Besides, we assume the modulation variances of each player and the dealer are the same, denoted by *V*, and the reconciliation efficiency is β.

Here, we assume, without loss of generality, that the excess noise from each player as well as the dealer is ε_0. Since the secret key rate is usually calculated using noises referred to the channel input (at Alice), we can then calculate the excess noise introduced by P_k using

$$\varepsilon_k = \frac{T_k}{T_1} \varepsilon_0 \tag{4}$$

Then we can apply the standard security proof method of CV-MDI QKD [6] to calculate the secret key rate of our protocol. Note that in practical implementation, the dealer should evaluate the secret key rate with each player by parameter estimation using the experimental data, and then determine the secret key rate of CV-MDI QSS.

To begin with the simulation, the modulation variance *V* will undoubtedly affect the performance of the proposed protocol. For the sake of optimizing the performance of the protocol, we need to consider the optimal modulation variance of the protocol under different numbers of players and transmission distances given the distance between Charlie and the dealer $L_D = 0$ km, which is shown in Fig. 2. In the following discussion, for simplicity, we assume all the players use the same modulation variance *V* = 20, as all secret key rates are relatively large at this value. There is no doubt that if we optimize the modulation variances at different numbers of players and distances, the performance will be further improved.

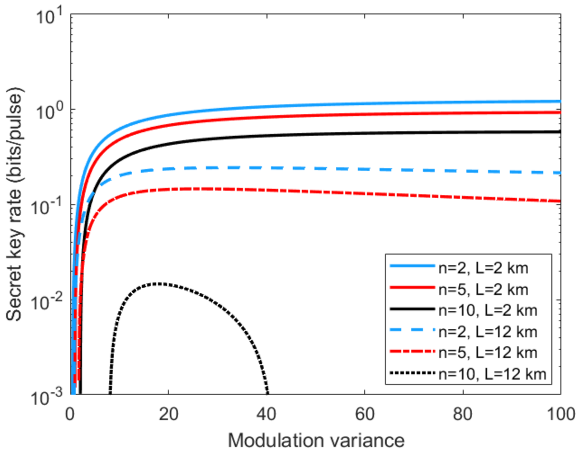

Fig 2. The relationship between secret key rates and the modulation variance V with different numbers of players n and transmission distances L. Simulation parameters are $\alpha = 0.2$ dB/km, $\varepsilon_0 = 0.01$, $\beta = 0.95$ and $L_D = 0$ km.

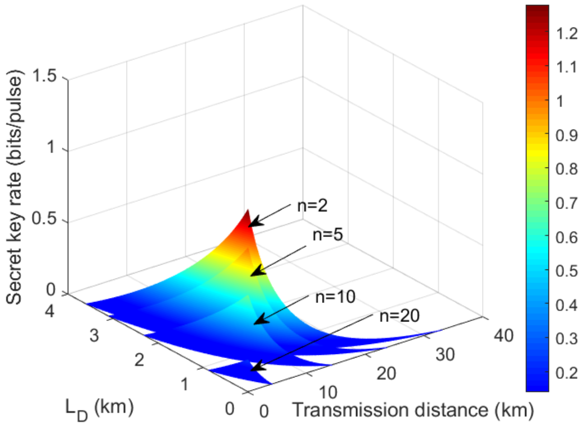

Fig 3. Secret key rate vs. the transmission distance L and L_D with different numbers of players n. Simulation parameters are $\alpha = 0.2$ dB/km, $\varepsilon_0 = 0.01$, $\beta = 0.95$, V = 20 and $\beta = 0.95$.

In our CV-MDI QSS protocol, the distance between Charlie and the dealer has a great influence on the transmission distance (the distance L between P_1 and Charlie). In Fig. 3, we take the secret key rate as a function of L and L_D, and we set the numbers of players as n = 2, 5, 10, and 20. From Fig. 3, we can observe that for the fixed n, the smaller L and L_D, the higher the secret key rate. Therefore, in order to get better performance, we need to make the dealer and Charlie as close as possible. The following simulation and discussion are also carried out in the extreme asymmetric case, that is, $L_D = 0$ km.

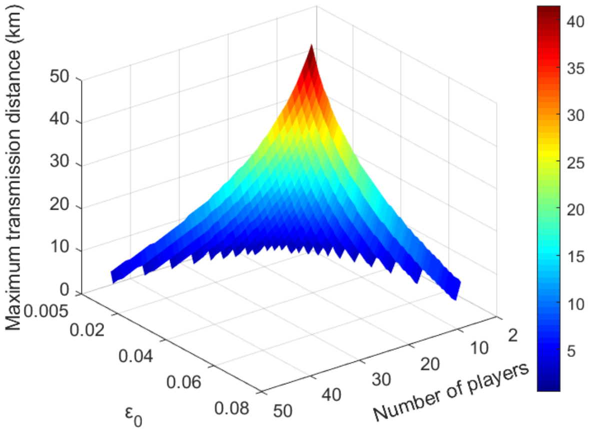

Fig 4. The maximum transmission distance vs. numbers of players n and excess noise ε_0. Simulation parameters are $\alpha = 0.2$ dB/km, V = 20, $\beta = 0.95$ and $L_D = 0$ km.

The excess noise ε_0 introduced by each player also has a great impact on the performance of the protocol. In Fig. 4, we take the maximum transmission distance as a function of the number of players and the excess noise ε_0. Obviously, when the number of players is fixed, the maximum transmission distance of the protocol will decrease sharply with the increase of the excess noise. Therefore, in practical implementation, in order to allow for more participants, we need to control the excess noise at a relatively low level.

4. Conclusions

In this paper, we introduce a CV-MDI QSS protocol where coherent states are prepared by each player and the dealer, and then measured by an untrusted third party, which can help to remove all detector side attacks against imperfect detectors. Numerical simulation results indicate that our protocol can be extended to a large number of players in the extreme asymmetric case, which makes up for the shortcoming of the existing entanglement-based CV-MDI multipartite quantum communication. Our work confirms that high performance QSS protocol is possible in the presence of imperfect detectors, which is of great help to the practical implementation of QSS.

Acknowledgment

This work was supported by the Key Program of National Natural Science Foundation of China under Grant No. 61531003, National Natural Science Foundation of China under Grant No. 62001041, China Postdoctoral Science Foundation under Grant No. 2020TQ0016, and the Fund of State Key Laboratory of Information Photonics and Optical Communications.

References

[1] M. Hillery, V. Bužek and A. Berthiaume, “Quantum secret sharing”, Phys. Rev. A. 59(1999) 1829.

[2] Z. Zhang and Z. Man, “Multiparty quantum secret sharing of classical messages based on entanglement swapping”, Phys. Rev. A. 72(2015) 022303.

[3] H. Lau and C. Weedbrook, “Quantum secret sharing with continuous-variable cluster states”, Phys. Rev. A. 88(2013) 042313.

[4] C. Schmid, P. Trojek, M. Bourennane, et al, “Experimental single qubit quantum secret sharing”, Phys. Rev. Lett. 95(2017) 012315.

[5] W. P. Grice and B. Qi, “Quantum secret sharing using weak coherent states”, Phys. Rev. A. 100(2019) 022339.

[6] Z. Li, Y. Zhang, F. Xu, X. Peng and H. Guo, “Continuous-variable measurement-device-independent quantum key distribution”, Phys. Rev. A. 89(2014) 052301.

[7] X. Ma, S. Sun, M. Jiang, M. Gui and L. Liang, “Gaussian-modulated coherent-state measurement-device-independent quantum key distribution”, Phys. Rev. A. 89(2014), 042335.

[8] Y. Wu, J. Zhou, X. Gong, et al, “Continuous-variable measurement-device-independent multipartite quantum communication”, Phys. Rev. A. 93(2016) 022325.

[9] Y. Guo, W. Zhao, F. Li, et al, “Improving continuous-variable measurement-device-independent multipartite quantum communication with optical amplifiers”, Commun. Theor. Phys. 68(2017) 191.

[10] Y. Wang, C. Tian, Q. Su, M. Wang and X. Su, “Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state”, Sci. China Inf. Sci. 62(2019) 72501.