Parameter Optimization in a Three-party Measurement-Device-Independent Quantum Key Distribution System

Yucheng Qiao, Zhengyu Li, Gan Wang, Xiang Peng and Hong Guo*

State Key Laboratory of Advanced Optical Communication System and Network, School of Electronics Engineering and Computer Science, and Center for Quantum Information Technology, Peking University, Beijing 100871, China.

* *Corresponding author: hongguo@pku.edu.cn*

Abstract

We discuss the problem of parameter optimization in a three-party measurement-device-independent quantum key distribution network and propose a new optimization method which will improve the performance of the whole system comparing to the method normally used in the two-party system.

1. Introduction

Quantum key distribution (QKD) allows communication parties to share secret keys through an unsecure quantum channel in theory, however, the practical security of QKD protocols is still critical issue due to the imperfections of the devices. The measurement-device-independent (MDI) QKD [1] is proposed to remove all the loopholes in detectors, which enhances the security of a practical system. Nevertheless, most of the researches on MDI QKD are about only two communication parties, while the real practical MDI QKD system should be applied in a multi-party QKD network, for instance, a three parties MDI network [3].

In this work, we discuss the parameter optimization problem of the three-party MDI network. When the location of each party is fixed, the parameters, including the average photon numbers (APN) of the signal states and the decoy states of each party, and the location of the detection part, should be optimized to increase the performance. However, the optimization method proposed for the two-party condition, which uses the relation $\mu_i/\mu_j = \nu_i/\nu_j = t_i/t_j$ (where t_i means the channel transmittance of i-th party) to enhances the Hong-Ou-Mandel effect [2], is not effective in the three-party condition. Here we propose a new optimization method about the APNs using the relation $\mu_i/\mu_j = \nu_i/\nu_j$, which is independent of t. The optimization result using the new relation will provide a higher total key rate for the multi-party MDI QKD system.

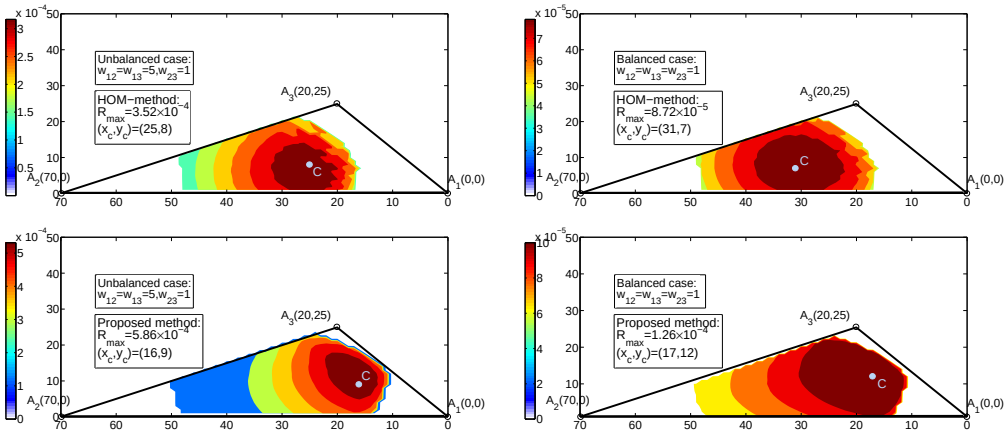
A total key rate of a multi-party MDI system is defined as

$$R = \sum_{i,j} w_{ij} R_{ij} \tag{1}$$

to evaluate the performance of the whole network, where R_{ij} means the key rate between the i-th party and the j-th party, and w_{ij} means the weight between i and j. Besides the total key rate, we require the system between each two parties to meet a threshold condition $R_{ij} > R_{th}$, in order to guarantee a minimum applicable key for each two nodes. The goal is to find the optimal APNs of i-th party's signal and decoy states μ_i, ν_i, and the optimal location of the detection part (x_c, y_c). By using the new relation, the optimization procedure is simplified by three parameters comparing to the fully optimization method which traverse all the adjustable parameters.

2. Simulation results

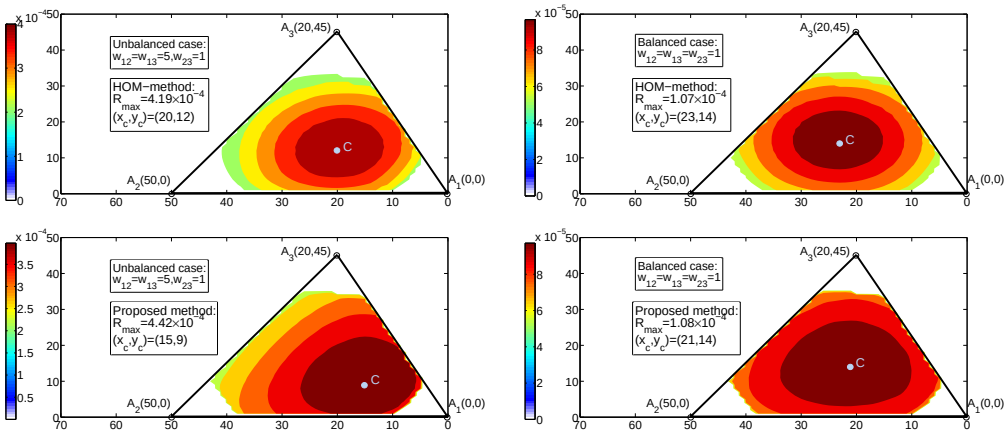
We discuss about the three-party system in both cases $w_{ij} = 1$ (balanced case) and $w_{12} = w_{13} = 5, w_{23} = 1$ which means that the 1-st party is a more important user in the network (unbalanced case). The threshold key rate R_{th} is set to be 10^{-5}. The location of the 3 parties are fixed, and we also consider two different structures, one is an acute triangle with three approaching edges, i.e., the distance between the i-th party and the j-th party $|A_iA_j|$ are nearly equal (symmetric case), the other is an obtuse triangle with one edge much shorter than others (asymmetric case). The total key rates of the above cases are optimized by using the relation $\mu_i/\mu_j = \nu_i/\nu_j$ for different locations of the detection part (here we only consider the locations inside the triangle formed by the three parties since it can be proved that for any outside location an inside location can be found with a higher total key rate). We compare our results with the results of using the HOM-method (short for the previous method with the relation $\mu_i/\mu_j = \nu_i/\nu_j = t_i/t_j$), which is shown in Fig. 1 (asymmetric case) and Fig. 2 (symmetric case).



(a) (b)

Fig. 1. The total key rate with two different optimal methods for the asymmetric case. The locations of 3 parties are fixed at $(0,0)$, $(70,0)$ and $(20,25)$ (Unit: km). The weights are set to be $w_{ij}=1$ for the balanced case and $w_{12}=w_{13}=5, w_{23}=1$ for the unbalanced case. Other simulation parameters are set as $e_d=0.01$, $Y_0=1\times10^{-6}$,$\eta_d=0.15$, $f=1.16$ (the definition of the above parameters are the same as [2]). The areas marked by different colors correspond to different levels of R, and the brown, red, orange, yellow, green, blue area refers to the level of 90% , 80% , 70% , 60% , 50% and less than 50% of the highest total key rate $R_{\max}$. The point C refers to the optimal location of the detection part. In each figure, the top one is the result of the HOM-method and the bottom is of the proposed method. (a) The unbalanced case; (b) The balanced case.

As a result, the performance of our method is better than the HOM-method. For the asymmetric case, the total secret key rate of our method is about 60% (40%) higher than the HOM-method's for the unbalanced (balanced) case, which shows the advantage of our method.



(a) (b)

Fig. 2. The total key rate with two different optimal methods for the symmetric case. The locations of 3 parties are fixed at $(0,0)$, $(50,0)$ and $(20,45)$ (Unit: km). Other parameters are set the same as in Fig. 1. The color correspond to the same key rate level as Fig. 1 as well. (a) The unbalanced case; (b) The balanced case.

For the symmetric case, although the optimal total key rate of our method is nearly the same as the HOM-method's, the total key rates for most of other locations are higher than the HOM-method's, and the areas marked by brown (the level is 90% of $R_{\max}$) in our method are also larger, which means that our method provides more optional locations of the detection part when a total key rate close to $R_{\max}$ is acceptable, i.e., $R>90\%$ of the $R_{\max}$.

3. Summary

The optimization method we proposed here is more effective for a three-party MDI QKD system, it can provide a higher optimal total key rate and more options for the location of the detection part.

Acknowledgement

This work is supported by the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), the State Key Project of National Natural Science Foundation of China (Grant No. 61531003).

References

1. H. K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. 108, 130503 (2012).
2. F. Xu, M. Curty, B. Qi, et al, "Practical aspects of measurement-device-independent quantum key distribution," New J. Phys. 15, 113007 (2013).
3. Y. Tang, H. Yin, Q. Zhao, et al, "Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network," Phys. Rev. X. 6, 011024 (2016).