Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution

Xiangyu Wang[1,2], **Yichen Zhang**[1], **Zhengyu Li**[3], **Bingjie Xu**[2], **Song Yu**[1,*], **Hong Guo**[3]

[1] *State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2] *Science and Technology on Communication Security Laboratory, Chengdu 610041, China*

[3] *State Key Laboratory of Advanced Optical Communication Systems and Networks, Peking University, Beijing 100871, China*

e-mail: yusong@bupt.edu.cn

Reconciliation is one of the most important information post-processing steps in continuous-variable quantum key distribution (CV-QKD) [1], which is used to make the legitimate parities extract the same keys from their related variables. The reconciliation step is divided into two parts. First, using some reconciliation methods to convert continuous variables into discrete variables. And then using certain error correction codes to correct all the errors on these discrete variables. In CV-QKD protocol, there are two mainly applied reconciliation methods, which are slice reconciliation [2] and multidimensional reconciliation [3]. Slice reconciliation is used in the short distance CV-QKD, while multidimensional reconciliation is used in the long distance CV-QKD. Multi-edge type low density parity check (MET-LDPC) code is a kind of liner error correction codes, whose performance is close to the Shannon's limit. Currently, for the signal-to-noise ratio (SNR) around 0.029, the reconciliation efficiency could reach 96.9% [4] when using multidimensional reconciliation and MET-LDPC codes with a rate of 0.02.

However, the code mentioned above just applicable to the single SNR. When the practical SNR is less than 0.029, the code will fail to correct errors. When the practical SNR is higher than 0.029, the efficiency will be reduced. Both of the cases will reduce the key rates of the CV-QKD protocol. Practically, quantum channel is a time-varying channel whose SNR may vary from 0.028 to 0.03, or even greater deviation. Thus, only one code can not support the full practical application.

To solve this problem, we propose an efficient rate-adaptive reconciliation protocol which changes the code rate to adapt the SNR of time-varying channel. The protocol is implemented by adding punctured bits and shortened bits into the code, where punctured bits increase the original code rate and shortened bits decrease the original code rate. For the problems mentioned above, we use the rate-adaptive reconciliation protocol to change the original code rate according to the practical SNR. The results are shown in table 1, in which for the reconciliation by using the original code, when the practical SNR is less than 0.029, the original code will fail to correct errors. When the practical SNR is higher than 0.029, the reconciliation efficiency of the original code will decrease. However, regardless of the SNR higher than 0.029 or less than 0.029, the performance of the rate-adaptive reconciliation is almost not decreased (close to 96.9%). In conclusion, the rate-adaptive reconciliation protocol can be applied to a wider range of SNR with only slight deviation of reconciliation efficiency, which will improve the robustness of practical CV-QKD systems.

SNR less than 0.029				SNR higher than 0.029			
SNR	R	β	β^o	SNR	R	β	β^o
0.0277	0.0190	96.40%	0%	0.0299	0.0205	96.46%	94.11%
0.0280	0.0192	96.38%	0%	0.0306	0.0210	96.59%	91.99%
0.0286	0.0196	96.36%	0%	0.0314	0.0215	96.40%	89.68%

Table 1: Performance comparison of the rate-adaptive reconciliation and the reconciliation by using the original code. SNR: practical signal-to-noise ratio. R: the code rate after rate-adaptive. β: reconciliation efficiency of the rate-adaptive code. β^o: reconciliation efficiency of the original code.

This work is supported in part by the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), in part by the the State Key Project of National Natural Science Foundation of China (Grant No. 61531003), and in part by the National Natural Science Foundation of China (Grant No. 61501414).

References

[1] F. Grosshans, et al., Phys. Rev. Lett. 88, 057902 (2002).

[2] J. Lodewyck, et al., Phys. Rev. A 76, 42305 (2007).

[3] A. Leverrier, et al., Phys. Rev. A 77, 42325 (2008).

[4] P. Jouguet, et al., Phys. Rev. A 84, 062317 (2011).