Composable security analysis for continuous variable measurement-device-independent quantum key distribution

Yichen Zhang[1], Zhengyu Li[2], Song Yu[1], Hong Guo[2]

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

[2] *State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Center for Quantum Information Technology, Peking University, Beijing 100871, China*

e-mail: yusong@bupt.edu.cn

Continuous-variable quantum key distribution (CV-QKD) [1] is a very attractive key distribution method as it takes the advantage of being compatible with standard telecommunication technology, especially no request of single photon detector. Despite a lot of effort invested in the theoretical analysis of CV-QKD protocols, composable security has been established for only two CV-QKD protocols, which are one-way squeezed-state protocol and no-switching protocol. The composable security proof for one-way squeezed-state protocol was obtained from an entropic uncertainty principle [2]. While the composable security proof for no-switching protocol was obtained by a composable security proof valid against collective attacks [3] followed by an additional argument to obtain security against general attacks [4, 5]. Here we give the composable security analysis of a new proposed CV-QKD protocol, continuous variable measurement-device-independent quantum key distribution (CV-MDI QKD), in which detection is conducted by an untrusted third party and naturally defend all detector side channels. Security analysis shows that the secret key rate of CV-MDI QKD protocol converges to the usual value computed from the Holevo bound in the limit of large blocks. As shown in Ref. [3], combining our security analysis here with either the de Finetti theorem or the postselection technique then shows the security of the CV-MDI QKD protocol against general attacks.

This work was 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 BUPT Excellent Ph.D. Students Foundation (CX2015205).

References

[1] C. Weedbrook *et al.*, "Gaussian quantum information", Rev. Mod. Phys. **84**, 621-669 (2012).

[2] F. Furrer *et al.*, "Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks", Phys. Rev. Lett. **109**, 100502 (2012).

[3] A. Leverrier, "Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States", Phys. Rev. Lett. **114**, 070501 (2015).

[4] A. Leverrier *et al.*, "Security of Continuous-Variable Quantum Key Distribution Against General Attacks", Phys. Rev. Lett. **110**, 030502 (2013).

[5] R. Renner *et al.*, "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography", Phys. Rev. Lett. **102**, 110504 (2009).