Enhancing the measurement-device-independent quantum key distribution using heralded single-photon sources

Qin Wang

Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Email: qinw@njupt.edu.cn

At present, most of the measurement-device-independent quantum key distributions (MDI-QKD) are based on weak coherent sources and are limited in the transmission distance under realistic experimental conditions, e.g., considering the finite-size-key effects. Here we propose a new biased decoy-state scheme using heralded single-photon sources for the three-intensity MDI-QKD, where we prepare the decoy pulses only in X basis and adopt both the collective constraints and joint parameter estimation techniques. Compared with former schemes with weak coherent sources or heralded single-photon sources, after implementing full parameter optimizations, our scheme gives distinct reduced quantum bit error rate in the X basis and thus show excellent performance, especially when the data size is relatively small.

We compare our proposed three-intensity decoy-state MDI-QKD with other three existing methods, i.e., Xu *et al*'s method [1], Zhou *et al*'s method [2] and Wang *et al*'s method [3], as shown in Fig. 1. The data size is reasonably set as $N=10^9$. Clearly, our scheme exhibits dramatic improvements than the other three. For example, it shows more than 25 km longer transmission distance than Zhou *et al*'s work, and presents more than 5 times enhancement in the key generation rate than Wang *et al*'s method at 70 km transmission distance.

In addition, our present scheme can be easily realized with current technology, and thus looks more promising in the implementation of the quantum communication.

References:

[1]. F. Xu, H. Xu, and H. K. Lo, "Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution", Phys. Rev. A 89, 052333 (2014).

[2]. Y. H. Zhou, Z. W. Yu, and X. B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful", Phys. Rev. A 93, 042324 (2016).

[3]. X. Y. Zhou, C. M. Zhang, and Q. Wang, "Implementing full parameter optimization on decoy-state measurement-device-independent quantum-key-distributions under realistic experimental conditions", Journal of the Optical Society of America B 34, 1518 (2017).

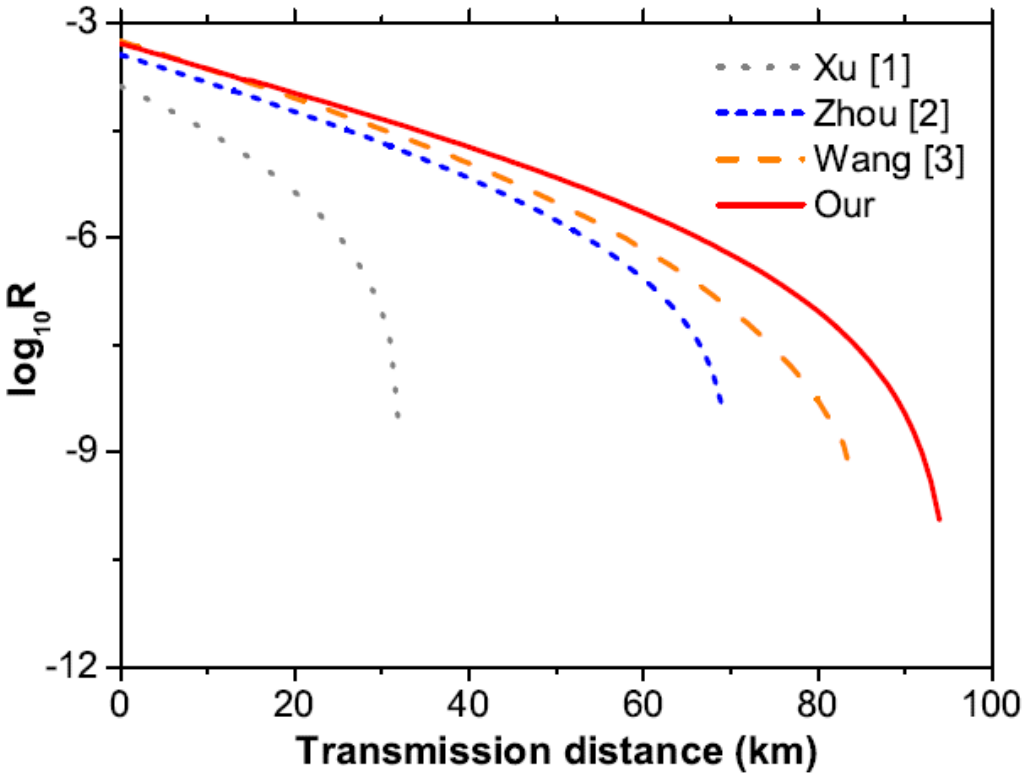


Fig.1 Comparison of the key generation rates among four different methods, i.e., Xu *et al*'s method [1], Zhou *et al*'s method [2], Wang *et al*'s method [3], and our present work. The data size is reasonably set as $N = 10^9$.