Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution

Xuyang Wang[1,2*], Wenyuan Liu[1], Pu Wang[1], and Yongmin Li[1,2*]

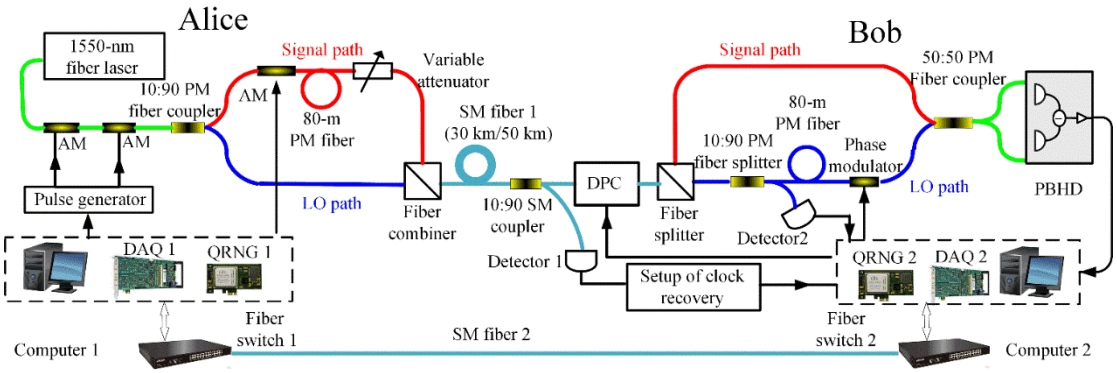
[1]State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China

[2]Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China

*wangxuyang@sxu.edu.cn

*yongmin@sxu.edu.cn

We experimentally demonstrated an all-fiber-based unidimensional continuous-variable quantum key distribution (CV QKD) protocol and analyzed its security under collective attack in realistic conditions. A pulsed balanced homodyne detector, which could not be accessed by eavesdroppers, with phase-insensitive efficiency and electronic noise, was considered. Furthermore, a new modulation method and an improved relative phase-locking technique with one amplitude modulator and one phase modulator were designed. The relative phase could be locked precisely with a standard deviation of 0.5° and a mean of almost zero. Secret key bit rates of 5.4 kbps and 700 bps were achieved for transmission fiber lengths of 30 and 50 km, respectively.



Experimental setup. AM: amplitude modulator, SM: single mode, PM fiber: polarization maintaining fiber, DAQ: data acquisition card, QRNG: quantum random number generator, DPC: dynamic polarization controller, PBHD: Pulsed balanced homodyne detector

The UD protocol simplifies the CVQKD system and reduces the cost. Although the protocol is more sensitive to the excess noise, it displays a comparable performance to the symmetrical counterpart under realistic conditions. It is expected that the presented system can find potential applications in various scenarios, such as in QKD local area networks, where the transmission distance between users is usually short and cost is a key concern. Higher secret key rates and longer distances can be expected following reduction of the excess noise and an increase of the reconciliation efficiency. Further theoretical analysis of the protocol will include finite-size effects and composable security.