Light Source Monitoring in Quantum Key Distribution with Photon Number Resolving Detector at Room Temperature

Gan Wang, Zhengyu Li, Ziyang Chen, Yucheng Qiao and Hong Guo*

State Key Laboratory of Advanced Optical Communication Systems and Networks, 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 propose a light source monitoring scheme in practical quantum key distribution systems based on photon number resolving method with a single photon detector working at room temperature. We analyze in what situations can this scheme work regardless of the high dark count rate of the SPD. Furthermore, discussions are made on the influences on QKD systems caused by the fluctuations of dark count rate and detection efficiency of the monitoring detector. Measuring of these parameter fluctuations is also done on real room-temperature detectors.

1. Introduction

Quantum key distribution (QKD) is a theoretically secure method to distribute secret keys between the information transmitter and receiver. However, in real QKD systems, the loopholes in optical components may cause practical security problems. Among them the loopholes in laser sources, especially in the widely-used weak coherent sources, are negligible. Therefore, light source monitoring (LSM) is necessary for practical security of QKD systems.

Photon number resolving (PNR) scheme, especially the passive PNR scheme [1], is a practical monitoring scheme with high performance, which requires a single photon detector (SPD). Normally, an InGaAs avalanche photon diode (APD) detector is used for monitoring. Its working temperature is lower than -30°C to suppress the dark count rate (DCR), thus demands an additional cooling module. We propose a PNR monitoring scheme with a detector working at room temperature to simplify the structure of monitor.

2. PNR monitoring with SPD in room temperature

In BB84 protocol, a QKD system's secret key rate is $R=\frac{1}{2}Q\{\Delta_1[1-H_2(e_1)]-H_2(E)\}$, where Q and E indicate the count rate and quantum bit error rate (QBER) in the QKD system, while Δ_1 and e_1 indicate the probability and bit error rate of single-photon pulses. When double decoy state protocol is adopted, it has been proved that [2]

$$\Delta_1 \geq \frac{a_1^L(a_2^L Q_d - a_2'^U Q_s - a_2^L a_0'^U Y_0 + a_2'^U a_0^L Y_0)}{Q_s(a_1'^U a_2^L - a_1^L a_2^U)}, \tag{1}$$

where a_n^U (a_n^L) is the upper (lower) bound of n photons' probability ($n=0,1,2$) of signal state, and $a_n'^U$ ($a_n'^L$) is the same value in decoy state. In our PNR scheme, when the attenuator in front of the monitoring SPD has a transmittance of η, the possibility of the SPD's not detecting a photon is $P(\eta)$. If we choose η from $\{\eta_0,\eta_1,\eta_2\}$ ($\eta_0=1$) randomly, we have proved that

$$\begin{aligned}
P_0(\eta) &= \frac{P(\eta)}{(1-\lambda)},\\
a_0^U &= a_0^L = P_0(\eta_0),\\
a_1^U &= \frac{P_0(\eta_1)-P_0(\eta_0)}{1-\eta_1},\\
a_1^L &= \frac{P_0(\eta_1)-P_0(\eta_0)[1-(1-\eta_1)^2]-(1-\eta_1)^2}{(1-\eta_1)-(1-\eta_1)^2},\\
a_2^U &= \frac{P_0(\eta_2)-P_0(\eta_0)-(1-\eta_2)a_1^L}{(1-\eta_2)^2},\\
a_2^L &= \frac{P_0(\eta_2)-P_0(\eta_0)[1-(1-\eta_2)^3]-[1-\eta_2-(1-\eta_2)^3]a_1^U-(1-\eta_2)^3}{(1-\eta_2)^2-(1-\eta_2)^3}.
\end{aligned} \tag{2}$$

λ is the DCR of the SPD. The InGaAs APD detectors with cooling used in QKD systems usually have a DCR of around 10^{-7} to 10^{-5}/pulse at the wavelength of 1550nm and the efficiency of 10%, but the DCR may rise up to a very high level when the SPDs are not cooled down [3]. However, in our calculation, when λ is known and stable, $a_n^{U(L)}$ can be got no matter what λ is, and the same conclusion is valid to $a_n'^{U(L)}$. Thus, a room-temperature SPD with high DCR can still be used for PNR monitoring.

3. Influences Caused by Parameter Fluctuations of SPD

At room temperature, the DCR and detection efficiency may fluctuate. In our experiment, the detector's origin DCR λ is 5×10^{-4}/pulse and the efficiency is η_D is 10% at room temperature [1]. Fig. 1 shows how the transmission distance of a QKD system changes when the SPD's parameters change.

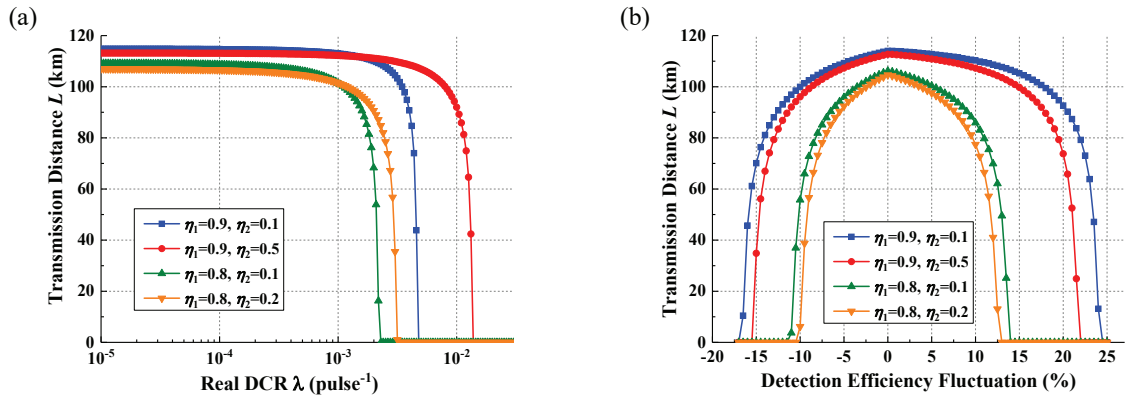

Fig. 1. The change of transmission distance when DCR (a) and detection efficiency (b) fluctuate. The mean photon number of signal state and decoy state is 0.6 and 0.1 respectively.

In experiment, our detector's DCR is not higher than 7×10^{-4}/pulse at room temperature, while its efficiency fluctuates within 2%. As a result, the transmission distance decreases less than 7km when considering the parameter fluctuations, which means the monitoring is practical and only needs slight modification in real utilization.

4. Summary

We propose a PNR LSM scheme, achieving with an SPD working at room temperature. We prove that this scheme can work when the detector's DCR is known and stable, and analyzed the influences caused by the its parameter fluctuations. The results show the feasibility of our monitoring scheme.

5. Acknowledgement

This work is supported by the State Key Project of National Natural Science Foundation of China (Grant No. 61531003), the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003) and the Foundation of Science and Technology on Security Communication Laboratory (Grant No. 9140C110101150C11048).

References

1. B. J. Xu, et al, "Passive scheme with a photon-number-resolving detector for monitoring the untrusted source in a plug-and-play quantum-keydistribution system," Phys. Rev. A 82, 042301 (2010).
2. X. B. Wang, et al, "General theory of decoy-state quantum cryptography with source errors," Phys. Rev. A 77, 042311 (2008).
3. L. C. Comandar, et al, "Room temperature single-photon detectors for high bit rate quantum key distribution," Applied Physics Letters 104.2 021101 (2014).

[1] While the detector's DCR at $-30°$C is 5×10^{-6}/pulse.