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

Gan Wang\(^1\), Zhengyu Li\(^1\), Yucheng Qiao\(^1\), Ziyang Chen\(^1\), Xiang Peng\(^1\), and Hong Guo\(^1\)*

\(^1\)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

Photon number resolving monitoring is a practical light source monitoring scheme in QKD systems, which reduces the impacts from untrusted sources effectively. This scheme requires a single photon detector, normally working at low temperature to suppress its dark count rate. In this paper, we use a room-temperature detector and show that the dark count rate is irrelevant to the monitoring performance in our scheme, which can sufficiently relax requirements on the detector’s working conditions as well as integration complexity, and this would be highly demanded for practical systems. Furthermore, influences of parameter drifts at room temperature are analyzed, and the monitoring scheme is testified in a real QKD system.

I. INTRODUCTION

Quantum key distribution (QKD) is a theoretically secure method to distribute secret keys between the information transmitter (Alice) and the receiver (Bob). After more than three decades’ development, QKD is coming to the edge of commercial applications. However, in real QKD systems, loopholes in optical components may cause practical security issues, among which the loopholes in quantum sources and detectors are the most vulnerable ones \([1–8]\). Recently-proposed measurement-device-independent protocol has removed the loopholes in detectors with practical techniques \([3–12]\), while those in sources still remain. Normally, weak coherent sources, rather than ideal single photon sources, are used in practical systems, and decoy state protocol is adopted to reduce multi-photon imperfections \([14–15]\). Under these conditions, the practical security of QKD systems is guaranteed by trusted sources, whose photon number distribution is known to Alice. In practice, trusted sources are not always available especially under the attack of eavesdroppers, thus light source monitoring (LSM) is indispensable \([16–19]\).

Commonly, there are three kinds of LSM methods, including average photon number monitoring \([8–17]\), ‘Untagged bits’ monitoring \([19–21]\), and photon number resolving (PNR) monitoring \([22–23]\), among which PNR is the most precise. Ideal PNR monitoring requires a photon number resolving detector, which can be replaced by a single photon detector (SPD) with a variable attenuator in practical scheme. The SPD used in a QKD system is normally an InGaAs avalanche photon diode detector, being cooled down by a thermo-electric cooler and working below \(-30^\circ\text{C} \sim -50^\circ\text{C}\) to suppress its dark count rate (DCR) \([24–27]\). However, when working at room temperature, an InGaAs SPD will have a high DCR \([27,28]\), which is not suitable for the receiver of QKD system but has potential of application in LSM.

In this paper, we propose and realize PNR LSM based on a room-temperature SPD. This scheme reduces the requirements of the SPD’s working conditions as well as its size and power consumptions significantly by removing cooler from the module, which makes it much easier to integrate the monitoring module in a QKD system. We prove that high DCR at room temperature leads to no degradation of the performance of monitoring, thus guarantees high security for practical QKD systems. Influences of parameter drifts as well as modifications on the mathematical model are also presented. Furthermore, our scheme is testified with a real QKD system.

This paper is organized as follows: In Sec. II A we discuss the mechanisms of why the performance of our LSM scheme is immune to high DCR at room temperature. In Sec. II B effects of parameter drifts and the corresponding modifications on the mathematical model are presented. In Sec. III we measure the ranges of the parameter drifts in real detectors and realize PNR LSM with a room temperature SPD in a practical QKD system.

II. LSM WITH A PNR DETECTOR AT ROOM TEMPERATURE

In this section, we start from a review of the basic theory of PNR LSM and then extend the discussion to the case where a room-temperature SPD is used, and also analyze the potential influences due to the parameter drifts of SPD.

A. LSM with a PNR Detector

In BB84 protocol, according to the GLLP theory, the secure key rate \(R\) of a QKD system is \([29]\)

\[
R = \frac{1}{2}Q\left\{\Delta_1[1-H_2(e_1)]-H_2(E)\right\}, \tag{1}
\]

where \(Q\) and \(E\) indicate the count rate and quantum bit error rate (QBER) in a QKD system, \(\Delta_1\) and \(e_1\) indicate

* Corresponding author: hongguo@pku.edu.cn.
the probability and bit error rate of single-photon pulses.

Decoy state protocol was introduced to estimate $\Delta_1$ and $e_1$ more precisely, offering an effective way to deal with the multi-photon problem caused by weak coherent sources \cite{14 15 30}. In double decoy states protocol, the transmitter Alice modulates the intensity of light pulses randomly into three states: signal, decoy, and vacuum state, whose light fields are

$$\rho_{\text{signal}} = \sum_{n=0}^{\infty} a_n |n\rangle \langle n|,$$

$$\rho_{\text{decoy}} = \sum_{n=0}^{\infty} a'_n |n\rangle \langle n|,$$

$$\rho_{\text{vacuum}} = |0\rangle \langle 0|,$$

where $a_n$ and $a'_n$ are the coefficients of Fock state $|n\rangle$, assumed to be known and controlled by Alice. However, in practical QKD systems, the untrusted source problem still remains, and a lower bound of $\Delta_1$ is given by \cite{18}

$$\Delta_1 \geq \frac{(a^U_2 Q_d - a^U_2 Q_a - a^L_2 a^H_4 Y_0 + a^U_2 a^H_4 Y_0)}{Q_a(a^U_2 a^L_2 - a^L_2 a^H_2)}, \quad (3)$$

where $a^U_n$ ($a^L_n$) is the upper (lower) bound of $n$ photons’ probability in signal state and $a^H_n$ ($a^L_n$) is the corresponding bound in decoy state, which needs to be monitored in real regime by LSM.

The ideal PNR LSM theory requires a photon number resolving detector, but a practical SPD is used in real situations to estimate $\{a^U_n, a^L_n, a^H_n, a^L_n\}$. Among the practical PNR LSM schemes, the passive scheme is a more practical one, as shown in Fig. 1 \cite{22}.

In signal state, when the light beam passes the VOA, a photon detector or controlled by the eavesdropper (Eve). After being emitted from the source, a light pulse passes through an optical filter (Fil), a phase randomizer (PR), and an attenuator (Att). The pulse will be encoded and a beam splitter (BS) with a transmittance $\eta_{BS}$ separates it into two beams. One goes through a variable optical attenuator (VOA) with a transmittance $\eta$ to the monitoring SPD, and the other is sent through the quantum channel to the receiver (Bob).

In this scheme, the practical SPD is equivalent to an ‘ideal’ one with an attenuator with transmittance $\eta_D$ in front of it (Fig. 2). An ‘Ideal’ detector here is defined to have a quantum detection efficiency of 100% with nonzero DCR. $\eta_{BS}$ is the transmittance of BS and we set

$$\eta_{BS} = (1 - \eta_{BS}) \eta_D, \quad (4)$$

so that the photon number distribution of the light field before entering the quantum channel and that of $\rho'$ in Fig. 2 are the same. Thus, the light field $\rho'$ in signal state reads

$$\rho'_{\text{signal}} = \sum_{n=0}^{\infty} a_n |n\rangle \langle n|, \quad (5)$$

while $\rho'$ in decoy state reads

$$\rho'_{\text{decoy}} = \sum_{n=0}^{\infty} a'_n |n\rangle \langle n|, \quad (6)$$

In signal state, when the light beam passes the VOA with transmittance of $\eta$, the probability of detecting zero photon with the detector is

$$P(\eta) = (1 - \lambda) \sum_{n=0}^{\infty} (1 - \eta)^n a_n = (1 - \lambda) P_0(\eta), \quad (7)$$

where $\lambda$ is the DCR of SPD. $P_0(\eta)$ is the probability of detecting zero photon with the ‘ideal’ detector, being irrelevant to $\lambda$.

If Alice chooses different $\eta \in \{\eta_0, \eta_1, \eta_2\} (\eta_0 > \eta_1 > \eta_2)$ randomly, $\{a^U_n, a^L_n, a^H_n, a^L_n\}$ can be calculated with $P(\eta)$ under different situations, and $P(\eta)$ is measured with the count rates of the monitoring detector. We set $\eta_0 = 1$, thus $\{a^U_n, a^L_n\}$ are given by (more detailed calculations...
are shown in Appendix A.)

\[
P_0(\eta_0) = \frac{P(\eta_0)}{1 - \lambda},
\]
\[
a_0^U = a_0^L = P_0(\eta_0),
\]
\[
a_1^U = \frac{P_0(\eta_1) - P_0(\eta_0)}{1 - \eta_1},
\]
\[
a_1^L = \frac{P_0(\eta_1) - P_0(\eta_0) - (1 - \eta_1)^2}{(1 - \eta_1) - (1 - \eta_1)^2},
\]
\[
a_2^L = \frac{P_0(\eta_2) - P_0(\eta_0) - (1 - \eta_2) a_1^L}{(1 - \eta_2)^2 - (1 - \eta_2)^3},
\]
\[
\begin{align*}
\text{Similarly, we can get } & \{a_0^{U}, a_0^{L}\} \text{ in decoy state. The above equations prove that when } \\
& \lambda \text{ is known and stable to Alice, } \{a_0^{U}, a_0^{L}\} \text{ and } \{a_0^{U}, a_0^{L}\} \text{ can be computed even though } \\
& \lambda \text{ is much higher than its value in low-temperature regime.}
\end{align*}
\]

Typically, an InGaAs avalanche photon diode detector works under \(-30^\circ C \sim -50^\circ C\) to suppress its DCR \([24, 27]\). When working at 1550 nm and having a detection efficiency of 10\%, the DCR of the SPD is \(10^{-7} \sim 10^{-5}\) per pulse at low temperature, but it will rise to a relatively high level at room temperature \([27, 31-35]\). In our experiment, the SPD has a DCR around \(5.4 \times 10^{-6}\) per pulse at low temperature, while \(5.8 \times 10^{-4}\) at room temperature. A high DCR will increase the time of calculating monitoring results, but as \(\lambda \ll 1\) still holds at room temperature, the increase of time is negligible. Meanwhile, working at room temperature not only reduces the requirements of working conditions of the SPD, but also decreases its size and power consumptions by simplifying (even removing) its temperature control, thus makes the monitoring detector much easier to be integrated in QKD systems as an important complement enhancing its practical security.

In the following part, modifications of \(\{a_n^{U(L)}, a_n^{U(L)}\}\) are discussed when considering the parameter drifts of practical SPD. According to current QKD experiments \(30-33\), in the simulation and experiment below, we set \(\mu = 0.6, \nu = 0.1\). \(\eta_1, \eta_2\) are chosen from these pairs of values: \(\{\eta_1 = 0.9, \eta_2 = 0.1; \eta_1 = 0.9, \eta_2 = 0.5; \eta_1 = 0.8, \eta_2 = 0.1; \eta_1 = 0.8, \eta_2 = 0.2\} \) (the discussion of the values of \(\eta_1\) and \(\eta_2\) can be found in Appendix A).

### B. Fluctuation of Dark Count Rate and Detection Efficiency

In our LSM scheme, the DCR of the room-temperature SPD is required to be known and stable, but it inevitably fluctuates in actual environments. Other parameters, especially the detection efficiency of SPD, may also drift. If the parameters drifts are ignored, the final secret key rate could be overestimated. To solve this problem, one method is to monitor all the parameters of the detector in real-time and calculate secret key rate with actual values. This will increase the system complexity obviously, and moreover, it is difficult to monitor all the parameters continuously. A more simple solution is to measure the range of parameter drifts and to modify \(\{a_n^{U(L)}, a_n^{U(L)}\}\) with the worst cases within the fluctuation range, which gives a reasonable estimation of the lower bound of secret key rate \(R\). In the following part, the derivation of modified mathematical model with parameter drifts as well as their valid range are presented. The modification results when using a real room-temperature SPD will be discussed in the experiment section.

Considering the drift of the DCR of SPD, we denote the original DCR as \(\lambda\), while \(\lambda'\) is the actual DCR with drifting, and \(\lambda' = (1 + \delta)\lambda\), where \(|\delta| \ll 1\). \(\{a_n^{U(L)}, a_n^{U(L)}\}\) are the bounds calculated with \(\lambda\) and \(\{a_n^{U(L)}, a_n^{U(L)}\}\) are the bounds with \(\lambda'\). \(\{a_n^{U(DCR)}, a_n^{U(DCR)}\}\) \(\{n = 0, 1, 2\}\) are given by (more detailed derivations are shown in Appendix B)

\[
\begin{align*}
& a_0^{U, DCR} = a_0^{U, DCR} \approx a_0^{U} (1 + \delta), \\
& a_1^{U, DCR} \approx a_1^{U} (1 + \delta), \\
& a_2^{U, DCR} \approx a_2^{U} (1 + \delta), \\
& a_2^{U, DCR} \approx a_2^{U} (1 + \delta) - \delta \frac{1 - \eta_1}{\eta_1},
\end{align*}
\]

Using Eq. \(9\) we calculate the system’s secret key rate \(R\) and the maximum transmission distance \(L\) when DCR drifts, as in Fig. \(3\).
while decreases when $\lambda$ increases and falls to zero when $\lambda$ is high enough. However, even when $\lambda = 10^{-3}$, $L$ only decreases by 1 km as for $\{n_1 = 0.9, n_2 = 0.1\}$, and decreases by approximately 10 km when $\lambda$ rises to $3 \times 10^{-3}$. As for the worst case $\{n_1 = 0.8, n_2 = 0.1\}$, $L$ decreases by 6 km when $\lambda = 10^{-3}$, while descends rapidly with the further increase of $\lambda$ and the system cannot generate keys when $\lambda > 2.2 \times 10^{-3}$. In practice, the DCR of the SPD with a detection efficiency 10% never reaches $10^{-3}$ at room temperature, so the decline of $L$ is within 10 km, an acceptable range in practical implementation. We also observe that when $n_1$ is fixed, the larger $n_2$ is, the larger tolerance the system has for the drift of DCR.

When the detection efficiency of the SPD varies with time, the modification method should be discussed under different conditions of both the increasing and the decreasing efficiency. Let $\eta_D$ represent the original detection efficiency and $\eta'_D$ be the actual efficiency with varying. When $\eta_D$ rises to $\eta'_D$, we have $\eta_D = (1 + \delta)\eta_D$, where $|\delta\eta_D| < 1$. $\{n_U, n_L\}$ still represent the bounds calculated with $\eta_D$, and $\{n_U, n_L\}$ are the actual bounds when $\eta_D$ rises to $\eta'_D$. Thus, $\{n_U, n_L\}$ read as

\[
\begin{align*}
  a_{n_U}^U &\approx a_0^U + a_1^U \delta + a_2^U \cdot \frac{\delta^2}{1 - \delta}, \\
  a_{n_L}^U &\approx a_0^U + a_1^U \delta + a_2^U \cdot \delta^2, \\
  a_{n_U}^L &\approx (1 - \delta)[a_1^U + a_2^U \cdot \frac{2\delta - \delta^2}{(1 - \delta)^2}], \\
  a_{n_L}^L &\approx (1 - \delta)[a_1^L + a_2^L \cdot \frac{2\delta - \delta^2}{(1 - \delta)^2}], \\
  a_{n_U}^U &\approx a_0^U + a_1^U \delta + a_2^U \cdot \frac{2\delta}{1 - \delta}, \\
  a_{n_L}^U &\approx a_0^L - a_1^L \delta - a_2^L \frac{\delta^2}{1 - \delta}. 
\end{align*}
\]

When $\eta_D$ falls to $\eta'_D$, we have $\eta_D = (1 - \delta)\eta'_D$, which is equivalent to $\eta_D = (1 + \delta)\eta'_D$, where $1 + \delta = \frac{\delta}{1 - \delta}$, $|\delta\eta_D| < 1$. Then, $\{n_U, n_L\}$, the actual bounds when $\eta_D$ decreases, read as

\[
\begin{align*}
  a_{n_U}^U &\approx a_0^U + a_1^U \delta - a_2^U \delta^2, \\
  a_{n_L}^U &\approx a_0^L - a_1^L \delta - a_2^L \delta^2, \\
  a_{n_U}^L &\approx a_0^L - a_1^L \delta - a_2^L \delta^2, \\
  a_{n_L}^L &\approx a_0^L - a_1^L \delta - a_2^L \delta^2. 
\end{align*}
\]

In conclusion, the bounds of $\{n_U, n_L\}$ under the variation of detection efficiency $\eta_D$ are given by (the detailed derivation of $\{a_{n_U}^L, a_{n_L}^L\}$ is shown in Appendix B)

\[
\begin{align*}
  a_{n_U}^U &= \max\{a_{n_U}^U, a_{n_U}^L\}, \\
  a_{n_L}^U &= \min\{a_{n_L}^U, a_{n_L}^L\}. 
\end{align*}
\]

Using Eq. 12 we simulate $R$ and $L$ when the detection efficiency drifts, as in Fig. 4.

**FIG. 4.** Transmission distance $L$ of a QKD system when the monitoring SPD’s detection efficiency $\eta_D$ drifts. The original efficiency $\eta_D = 10\%$ at room temperature.

The original efficiency $\eta_D$ is $10\%$ and for either cases when it increases or decreases, the maximum transmission distance $L$ will decline. As for $\{n_1 = 0.9, n_2 = 0.1\}$, $L$ declines by 5 km when $\eta_D$ increases by over 11.5% or decreases by over 5%, and it declines by 20 km when $\eta_D$ increases by over 19% or decreases by over 12%. As for the worst case $\{n_1 = 0.8, n_2 = 0.2\}$, $L$ declines by 5 km when $\eta_D$ increases by over 4% or decreases by over 2.5%, and declines by 20 km when $\eta_D$ increases by over 9% or decreases by over 7%. The detection efficiency fluctuation here is the relative fluctuation of original detection efficiency, which is $10\%$ in both simulation and experiment.

**III. EXPERIMENT RESULTS**

In the experiment, we use an InGaAs SPD with its thermo-electric cooler removed to make it work at room temperature. Meanwhile, we use another detector working at low temperature (below $-30^\circ$C) for comparison [34]. Each detector’s DCR is measured continuously over 60 minutes, and the results are shown in Fig. 5. At low temperature, the DCR of SPD is stable, drifting from $4.6 \times 10^{-6}$ to $6.1 \times 10^{-6}$, while the DCR of room-temperature SPD drifts from $5.3 \times 10^{-4}$ to $6.2 \times 10^{-4}$, over two orders of magnitude larger than the low-temperature case.
FIG. 5. Drifts of DCR of the detectors at low temperature and room temperature over 60 minutes.

Each detector’s detection efficiency is also measured over 60 minutes, and the results are shown in Fig. 6. The original detection efficiency of the two detectors are both 10%, and the efficiency of the low temperature SPD drifts within 1% of it in most occasions, while the efficiency drifts within 2% of itself at room temperature.

FIG. 6. Drifts of detection efficiency of the detectors at low temperature and room temperature over 60 minutes.

Next, we compare the key rates when implementing PNR LSM with a low-temperature SPD and a room-temperature SPD in a practical QKD system, and we also study the key rates with modification when considering the parameter drifts, as shown in Fig. 7. According to the discussion in Appendix A, we set \( \{ \mu = 0.6, \nu = 0.1 \} \) and get secret key rates under two conditions, \( \{ \eta_1 = 0.9, \eta_2 = 0.1 \} \) and \( \{ \eta_1 = 0.8, \eta_2 = 0.2 \} \).

For the case of \( \{ \eta_1 = 0.9, \eta_2 = 0.1 \} \), the transmission distances \( L \) are 117.1 km with a low-temperature SPD and 111.0 km with a room-temperature SPD, and 116.8 km and 108.4 km respectively after being modified. As for \( \{ \eta_1 = 0.8, \eta_2 = 0.2 \} \), the transmission distances are 103.7 km with a low-temperature SPD and 98.9 km with a room-temperature SPD, and 95.0 km and 92.0 km for the cases with modification. The secret key rates under different situations at a distance of 50 km, a typical distance in QKD networks, are also listed in Table I.

TABLE I. Secret key rates of the QKD system at a distance of 50 km under different situations. (Unit: per pulse)

| \( \mu = 0.9, \nu = 0.1 \) | \( \mu = 0.8, \nu = 0.2 \) |
|--------------------------|--------------------------|
| Room Temperature         | 3.35 \times 10^{-4}      | 1.89 \times 10^{-4} |
| Room Temperature+modification | 2.97 \times 10^{-4} | 1.34 \times 10^{-4} |
| Low Temperature          | 4.43 \times 10^{-4}      | 2.37 \times 10^{-4} |
| Low Temperature+modification | 4.38 \times 10^{-4} | 1.54 \times 10^{-4} |

It can be deduced that the PNR LSM scheme has comparable monitoring performances with such two detectors for practical applications, and the difference in transmission distances is less than 7 km, which may result from the statistical fluctuations of count rates. When
parameter drifts are taken into consideration, the transmission distances only decrease slightly after being modified, which are 2.6 km and 6.9 km in the two situations at room temperature, respectively. This proves that our monitoring scheme as well as the modification method are applicable in real QKD systems.

Compared with the low-temperature case, the secret key rates at room temperature have a noticeable decline almost reaching 25% before being modified. However, the modification itself varies with $\eta_1$ and $\eta_2$ greatly. For instance, at room temperature, $R$ decreases by less than 12% when $\{\eta_1 = 0.9, \eta_2 = 0.1\}$, and decreases by nearly 30% when $\{\eta_1 = 0.8, \eta_2 = 0.2\}$. So values of $\eta_1$ and $\eta_2$ which insure long transmission distances and high secret key rates also insure better performances under parameter drifts of the SPD, which can be used as the criteria for choosing appropriate values of $\eta_1$ and $\eta_2$. Still, at 50 km, the secret key rate can be higher than 100 kbps in a 1 GHz QKD system with a monitoring SPD at room temperature, totally comparable with current commercial systems.

IV. CONCLUSION

In summary, we propose and realize PNR LSM method by using an SPD working at room temperature, and prove that when the dark count rate of SPD is known and stable, the high DCR has no influence on monitoring performance. This can reduce the requirements of the SPD’s working conditions, making it much easier to integrate the monitor module in practical QKD systems. Furthermore, the influences from the drifts of the DCR and detection efficiency of SPD are analyzed, together with a discussion of the related modification methods. We also measure such two kind of drifts at both low temperature and room temperature in real detectors, and realize the scheme in a real QKD system. The experimental results are in good agreement with the theoretical predictions and thus verify favorable prospect of using our scheme in a practical system with the analysis of parameter drifts in real circumstances.

V. ACKNOWLEDGEMENT

We acknowledge Heping Zeng (ECNU) and Shengxiang Zhang (ROI Optoelectronics Tech.) for their supports on experiment. 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).

Appendix A: Passive PNR LSM

In PNR LSM, Alice chooses different $\eta \in \{\eta_0, \eta_1, \eta_2\}$ ($\eta_0 > \eta_1 > \eta_2$) randomly, so $\{a_{\eta_0}^U, a_{\eta_0}^L\} (n = 0, 1, 2)$ can be calculated with $P(\eta)$ of the PNR detector under different situations. When $\eta_0 = 1$,

$$P(\eta_0 = 1) = (1 - \lambda)a_0 + (1 - \lambda)P_0(\eta_0). \quad (A1)$$

In this situation, the upper bound $a_0^U$ and lower bound $a_0^L$ of $a_0$ are equal,

$$a_0 = \frac{P(\eta_0)}{1 - \lambda} = P_0(\eta_0) = a_0^U = a_0^L. \quad (A2)$$

And it can be derived that

$$\frac{P(\eta_1)}{1 - \eta_1} \geq a_0 + (1 - \eta_1)a_1, \quad (A3)$$

$$\frac{P(\eta_1)}{1 - \eta_1} \leq a_0 + (1 - \eta_1)a_1 + (1 - \eta_1)^2(1 - a_0 - a_1), \quad (A4)$$

so $a_0^U$ and $a_0^L$, the upper and lower bound of $a_1$, read

$$a_1 \leq \frac{P(\eta_1) - P(\eta_0)}{(1 - \lambda)(1 - \eta_1)} = \frac{P_0(\eta_1) - P_0(\eta_0)}{1 - \eta_1} = a_1^U, \quad (A5)$$

$$a_1 \geq \frac{P(\eta_1) - P(\eta_0)[1 - (1 - \eta_1)^2(1 - \lambda)(1 - \eta_1)^2]}{(1 - \lambda)[(1 - \eta_1) - (1 - \eta_1)^2]} = \frac{P_0(\eta_1) - P_0(\eta_0)[1 - (1 - \eta_1)^2(1 - \lambda)](1 - \eta_1)^2}{(1 - \eta_1) - (1 - \eta_1)^2} = a_1^L. \quad (A6)$$

Similarly,

$$\frac{P(\eta_2)}{1 - \lambda} \geq a_0 + (1 - \eta_2)a_1 + (1 - \eta_2)^2a_2 \geq a_0 + (1 - \eta_2)a_1^U + (1 - \eta_2)^2a_2, \quad (A7)$$

$$\frac{P(\eta_2)}{1 - \lambda} \leq a_0 + (1 - \eta_2)a_1 + (1 - \eta_2)^2a_2 + (1 - \eta_2)^3(a_3 + a_4 + a_5 + \cdots) \leq [1 - (1 - \eta_2)^3]a_0 + [1 - \eta_2 - (1 - \eta_2)^3]a_1^U + [(1 - \eta_2)^2 - (1 - \eta_2)^3]a_2 + (1 - \eta_2)^3, \quad (A8)$$
so \( a_2^U \) and \( a_2^L \) read

\[
a_2^U \leq \frac{P(\eta_2) - P(\eta_0) - (1 - \lambda)(1 - \eta_2)a_2^U}{(1 - \lambda)(1 - \eta_2)^2} = \frac{P_0(\eta_2) - P_0(\eta_0) - (1 - \eta_2)a_2^U}{(1 - \eta_2)^2} = a_2^U, \tag{A9}
\]

\[
a_2^L \geq \frac{P(\eta_2) - P(\eta_0)[1 - (1 - \eta_2)^3] - (1 - \lambda)[1 - \eta_2 - (1 - \eta_2)^3]a_2^L - (1 - \lambda)(1 - \eta_2)^3}{(1 - \eta_2)^2 - (1 - \eta_2)^3} = a_2^L. \tag{A10}
\]

\( \{a_2^U, a_2^L\} \) can be calculated from the similar equations in decoy state [22].

We set \( \eta_2 < \eta_1 < \eta_0 = 1 \), and the choosing of different \( \eta_1 \) and \( \eta_2 \) has great influence on the performance of this monitoring scheme. Fig. 8 shows the maximum transmission distance \( L \) of a QKD system corresponding to different \( \eta_1 \) and \( \eta_2 \). The closer \( \eta_1 \) is to 1 and \( \eta_2 \) is to 0, the longer \( L \) this system has. In this paper, we set \( \eta_1 \) and \( \eta_2 \) from these typical pairs of values according to Fig. 8:

\[
\eta_1 = 0.9, \eta_2 = 0.1; \eta_1 = 0.9, \eta_2 = 0.5; \\
\eta_1 = 0.8, \eta_2 = 0.1; \eta_1 = 0.8, \eta_2 = 0.2.
\]

We can find that when \( \eta_0 = 1 \), the closer \( \eta_1 \) is to 1 and \( \eta_2 \) to 0, the better the performance of PNR LSM scheme is.

\[
\text{FIG. 8. Transmission distance } L \text{ of QKD systems with PNR LSM when choosing different } \eta_1 \text{ and } \eta_2 (\eta_0 = 1).
\]

\[
\begin{align*}
& \eta_1 = 0.8, \eta_2 = 0.1, L = 106.3 \text{ km} \\
& \eta_1 = 0.8, \eta_2 = 0.2, L = 104.4 \text{ km} \\
& \eta_1 = 0.9, \eta_2 = 0.5, L = 112.7 \text{ km}
\end{align*}
\]

Appendix B: Calculation on the Fluctuation of DCR and Detection Efficiency

When the DCR \( \lambda \) changes into \( \lambda' \), let \( \lambda' = (1 + \delta \lambda, |\delta \lambda| \ll 1 \). As for \( a_{0, DCR}^{U,L} \) and \( a_{0, DCR}^{U,L} \):

\[
a_{0, DCR}^U = a_{0, DCR}^L = \frac{P(\eta_0)}{1 - \lambda'} = a_0^U \frac{1 - \lambda}{1 - \lambda'} \approx a_0^U (1 + \delta \lambda), \tag{B1}
\]

And for \( a_{1, DCR}^{U,L} \) and \( a_{2, DCR}^{U,L} \):

\[
a_{1, DCR}^U = \frac{P(\eta_1) - P(\eta_0)}{(1 - \lambda')(1 - \eta_1)} = a_1^U (1 + \delta \lambda), \\
a_{1, DCR}^L = \frac{P(\eta_1) - P(\eta_0)[1 - (1 - \eta_1)^2] - (1 - \lambda')(1 - \eta_1)^2}{(1 - \lambda')(1 - \eta_1)^2} \\
= \frac{P(\eta_1) - P(\eta_0)[1 - (1 - \eta_1)^2] - (1 - \lambda)(1 - \eta_1)^2}{(1 - \lambda)(1 - \eta_1)^2}
\]

\[
\approx a_1^L (1 + \delta \lambda) - \delta \lambda \frac{1 - \eta_2}{\eta_2}. \tag{B2}
\]

By using similar approximation, we can get \( a_{2, DCR}^U \) and \( a_{2, DCR}^L \) as

\[
a_{2, DCR}^U \approx a_2^U (1 + \delta \lambda), \\
a_{2, DCR}^L \approx a_2^L (1 + \delta \lambda) - \delta \lambda \frac{1 - \eta_2}{\eta_2}. \tag{B3}
\]

When the detector’s efficiency \( \eta_D \) increases to \( \eta_D' = (1 + \delta \eta_D) \eta_D > \eta_{BS} \). Let \( \delta \eta_D = (1 + \delta) \eta_D, |\delta \eta_D| \ll 1 \), we have

\[
a_{n, \eta_D} \uparrow \approx \sum_{m=0}^{\infty} a_m C_m^n (1 - \delta)^n \delta^{m-n}. \tag{B4}
\]

As a result,

\[
a_{0, \eta_D} \uparrow = \sum_{m=0}^{\infty} a_m \delta^m = a_0 + a_1 \delta + a_2 \delta^2 + \ldots, \tag{B5}
\]

so

\[
a_0 + a_1 \delta + a_2 \delta^2 < a_{0, \eta_D} \uparrow < a_0 + a_1 \delta + a_2 (\delta^2 + \delta^3 + \ldots) \tag{B6}
\]

And

\[
a_{1, \eta_D} \uparrow = \sum_{m=1}^{\infty} a_m (1 - \delta) \delta^{m-1}, \tag{B7}
\]
Similarly, so upper bounds \((\eta^2 = 0.61)\) are estimated by A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Optic. 48, 73 (2001).

\[ N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A 73, 022320 (2006). \]

\[ F. Xu, B. Qi, and H.-K. Lo, New J. Phys. 12, 113026 (2010). \]

\[ V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A 74, 022306 (2006). \]

\[ Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A 78, 042333 (2008). \]

\[ L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics 4, 686 (2010). \]

\[ I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. 2, 349 (2010). \]

\[ H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012). \]

\[ T. F. da Silva, D. Vitoreti, G. Xavier, G. do Amaral, G. Temporão, and J. von der Weid, Phys. Rev. A 88, 052303 (2013). \]

\[ A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. 111, 130501 (2013). \]

\[ Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, et al., Phys. Rev. Lett. 111, 130502 (2013). \]

\[ Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. 112, 190503 (2014). \]

\[ H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005). \]

\[ X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005). \]

\[ X.-B. Wang, C.-Z. Peng, and J.-W. Pan, Appl. Phys. Lett. 90, 031110 (2007). \]

\[ X. Peng, H. Jiang, B. Xu, X. Ma, and H. Guo, Opt. Lett. 33, 2077 (2008). \]
[18] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A 77, 052327 (2008).
[19] X. Peng, B. Xu, and H. Guo, Phys. Rev. A 81, 042320 (2010).
[20] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, New J. Phys. 12, 023024 (2010).
[21] B. Xu, X. Peng, and H. Guo, Phys. Rev. A 82, 042301 (2010).
[22] B. Xu, X. Peng, and H. Guo, Quantum Inf. Comput. 12, 2012.
[23] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, New J. Phys. 12, 063027 (2010).
[24] A. R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, Appl. Phys. Lett. 96, 161102 (2010).
[25] M. Lucamarini, K. Patel, J. Dynes, B. Frööhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, Opt. Express 21, 24550 (2013).
[26] L. Comandar, B. Frööhlich, M. Lucamarini, K. Patel, A. Sharpe, J. Dynes, Z. Yuan, R. Penty, and A. Shields, Appl. Phys. Lett. 104, 021101 (2014).
[27] S. Pellegrini, R. E. Warburton, L. J. Tan, J. S. Ng, A. B. Krysa, K. Groom, J. P. David, S. Cova, M. J. Robertson, and G. S. Buller, IEEE J. Quantum Elect. 42, 397 (2006).
[28] D. Gottesman, H. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).
[29] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A 72, 012326 (2005).
[30] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. 98, 010505 (2007).
[31] Z. Yuan, A. Dixon, J. Dynes, A. Sharpe, and A. Shields, New J. Phys. 11, 045019 (2009).
[32] K. Takemoto, Y. Nambu, T. Miyazawa, K. Waku, S. Hirose, T. Usuki, M. Takatsu, N. Yokoyama, K. Yoshino, A. Tomita, et al., Appl. Phys. Express 3, 092802 (2010).
[33] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Waku, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., Opt. Express 19, 10387 (2011).
[34] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, et al., Opt. Express 22, 21739 (2014).
[35] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. 96, 070502 (2006).
[36] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Opt. Express 16, 18790 (2008).
[37] Z.-Q. Yin, Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu, and G.-C. Guo, Chinese Phys. Lett. 25, 3547 (2008).
[38] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express 18, 8587 (2010).
[39] We assume the photon number distribution of the light source follows Possion distribution in simulation.
[40] The SPDs are SPD4V5MINI from ROI Optoelectronics Tech.