

Phase-matching quantum key distribution with light source monitoring

Wen-Ting Li(李文婷), Le Wang(王乐), Wei Li(李威), and Sheng-Mei Zhao(赵生妹)
Citation: Chin. Phys. B, 2022, 31 (**5**): 050310. DOI: 10.1088/1674-1056/ac4101
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

A rational quantum state sharing protocol with semi-off-line dealer

Hua-Li Zhang(张花丽), Bi-Chen Che(车碧琛), Zhao Dou(窦钊), Yu Yang(杨榆), and Xiu-Bo Chen(陈秀波)
Chin. Phys. B, 2022, 31 (**5**): 050309. DOI: 10.1088/1674-1056/ac4e02

Efficient quantum private comparison protocol based on one direction discrete quantum walks on the circle

Jv-Jie Wang(王莒杰), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)
Chin. Phys. B, 2022, 31 (**5**): 050308. DOI: 10.1088/1674-1056/ac5a3f

Analysis and improvement of verifiable blind quantum computation

Min Xiao(肖敏) and Yannan Zhang(张艳南)
Chin. Phys. B, 2022, 31 (**5**): 050305. DOI: 10.1088/1674-1056/ac2f34

Self-error-rejecting multipartite entanglement purification for electron systems assisted by quantum-dot spins in optical microcavities

Yong-Ting Liu(刘永婷), Yi-Ming Wu(吴一鸣), and Fang-Fang Du(杜芳芳)
Chin. Phys. B, 2022, 31 (**5**): 050303. DOI: 10.1088/1674-1056/ac4489

Quantum private comparison of arbitrary single qubit states based on swap test

Xi Huang(黄曦), Yan Chang(昌燕), Wen Cheng(程稳), Min Hou(侯敏), and Shi-Bin Zhang(张仕斌)
Chin. Phys. B, 2022, 31 (**4**): 040303. DOI: 10.1088/1674-1056/ac4103

Phase-matching quantum key distribution with light source monitoring

Wen-Ting Li(李文婷)[1], Le Wang(王乐)[1,2], Wei Li(李威)[1,2], and Sheng-Mei Zhao(赵生妹)[1,2,†]

[1] *Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing* 210003, *China*

(Received 10 August 2021; revised manuscript received 12 November 2021; accepted manuscript online 8 December 2021)

The transmission loss of photons during quantum key distribution (QKD) process leads to the linear key rate bound for practical QKD systems without quantum repeaters. Phase matching quantum key distribution (PM-QKD) protocol, an novel QKD protocol, can overcome the constraint with a measurement-device-independent structure, while it still requires the light source to be ideal. This assumption is not guaranteed in practice, leading to practical secure issues. In this paper, we propose a modified PM-QKD protocol with a light source monitoring, named PM-QKD-LSM protocol, which can guarantee the security of the system under the non-ideal source condition. The results show that our proposed protocol performs almost the same as the ideal PM-QKD protocol even considering the imperfect factors in practical systems. PM-QKD-LSM protocol has a better performance with source fluctuation, and it is robust in symmetric or asymmetric cases.

Keywords: phase-matching quantum key distribution, source fluctuation, light source monitoring

PACS: 03.67.Dd, 05.30.Rt, 05.40.–a, 06.30.–k **DOI:** 10.1088/1674-1056/ac4101

1. Introduction

Quantum key distribution (QKD) is the most successful application in quantum information science, and its security has been proved at the end of the last century.[1–3] It enables distant parties to achieve the secure key by harnessing the laws of quantum mechanics.[4,5] After the first QKD protocol was proposed in 1984,[4] QKD has made great progress in theory and practice, such as decoy-state QKD protocol,[6,7] measurement-device-independent (MDI) protocol,[8,9] and round-robin differential-phase-shift (RRDPS) protocol.[10,11] Usually, photons are used as information carriers in QKD's implementations. However, the transmission loss of photons has become a major obstacle in practical applications, resulting in the linear key-rate bound (PLOB bound) for QKD system.[12] In fiber-based networks, the transmission rate (η) decreases exponentially with the communication distance, which limits the transmission distance of the practical QKD system.

Marvelously, a quantum key distribution protocol, named twin field quantum key distribution (TF-QKD) protocol, was proposed in 2018[13] to surpass the PLOB bound[12] and make a quadratic improvement over phase-encoding MDI-QKD protocol.[14] It has attracted much attention recently.[15–21] For TF-QKD protocol, the security problem caused by phase randomization was its main disadvantage. And phase matching quantum key distribution (PM-QKD) protocol[22] was then proposed to resolve the security loophole by adding an extra test mode. PM-QKD protocol could not only exceed the linear key rate limit, but also resist all probe attacks due to the independence of the measurement device. Recently, Ma *et al.*[23] have proposed the reference-frame-independent design for PM-QKD protocol, which can well solve the performance degradation of reference system caused by offset. However, the quantum state prepared at the source was assumed to be an ideal coherent state in the original PM-QKD protocol. Actually, this assumption is not guaranteed in practice, leading to practical secure issues.[24] In addition, there also exists a non-ideal source problem causing the photon number distribution (PND) of the light source to be unknown and the prepared state to no longer be an ideal coherent state.

On the other hand, light source monitoring (LSM) was proposed to solve the non-ideal source problem by monitoring the photon number distribution (PND) of the non-ideal light source.[25] The monitored statistical parameters can then be used to recalibrate the PND of the light source to estimate the final secret key rate, resulting that the assumption of ideal source is not necessary in QKD process. LSM was successfully applied to MDI-QKD protocol to solve the non-ideal source problem theoretically based on the "untagged bits" concept,[26] and then based on a photon number resolving (PNR).[27] LSM was also used for the sending-or-not-sending (SNS) protocol to demonstrate that the security of SNS protocol is still valid under a source with unknown PND.[28]

In the paper, we propose a PM-QKD with light source monitoring protocol, named PM-QKD-LSM protocol. In the protocol, the non-ideal light source is used to generate the light beam by Alice and Bob independently. After phase and intensity modulation, the light beam is then split to two paths by a beam splitter (BS), where one is input to the LSM module

†Corresponding author. E-mail: zhaosm@njupt.edu

© 2022 Chinese Physical Society and IOP Publishing Ltd

to estimate the probabilities that the light pulse signals contain zero photon, one photon, or two photons, and the other is emitted to the measurement site, Charlie, for detection. By matching phases with each other during post-selection, the key information is encoded into the common phase, and then the key can be obtained through the success detection results.

The advantages of the proposed PM-QKD-LSM protocol are: (1) it overcomes the problem of non-ideal light source and improves the security of the PM-QKD protocol; (2) its performance under the unknown PND condition (UPC) can almost keep the same as that of PM-QKD protocol under ideal source condition without source fluctuation; (3) it is more independent of the source fluctuation than the PM-QKD protocol; and (4) the performance is almost unchanged as that of PM-QKD protocol under asymmetric channel.

The contribution of this paper is that we investigate the ability of LSM in solving the non-ideal light source problem in PM-QKD protocol, and discuss the performance of PM-QKD-LSM protocol under different source fluctuation. Furthermore, we enrich the work on the performance of PM-QKD-LSM protocol with symmetrical or asymmetrical channel. The results are helpful for the design of the practical PM-QKD system. In addition, the results in the paper show that the protocol we proposed not only solves the problem of non-ideal light source at the light source side, which relaxes the requirements on the light source, but also improves the security of the PM-QKD protocol. The improvement can be addressed from the following two aspects. One is that the LSM module itself has the function of monitoring the probability of the number of photons in our proposed protocol, which can detect the PNS attack. The other one is that the LSM module can also be regarded as a monitoring unit to monitoring the arrival time of the pulses so as to resist the phase-remapping attack.

The paper is organized as follows. In Section 2, we first present the PM-QKD-LSM protocol, then we use the LSM method to obtain the tight bounds of the parameters for the secret key rate, and discuss the performance of the proposed protocol under the source fluctuation. In Section 3, we present some numerical analysis results. Finally, we draw the conclusions in Section 4.

2. PM-QKD-LSM protocol

2.1. The protocol

The schematic diagram of PM-QKD-LSM protocol is shown in Fig. 1, where the two communication parties, Alice and Bob, generate her (his) coherent state pulses, independently at first. Before sending their coherent state pulses to an untrusted measurement site, Charlie, Alice and Bob use a LSM module individually to estimate the tight bound of the photon number probabilities $(P_{n\mathrm{L}}(\mu_k), P_{n\mathrm{U}}(\mu_k))$ on her(his) PND of the light source. Here, the subscribe L (U) and n denote the lower (upper) bound and the photon number $(n = 0,1,2)$, respectively. Then, Charlie is expected to perform the interference detection. This interference measurement would match the phases of Alice and Bob's signals. Conditioned on Charlie's announcement, there is a correlation between the key information of Alice and Bob.

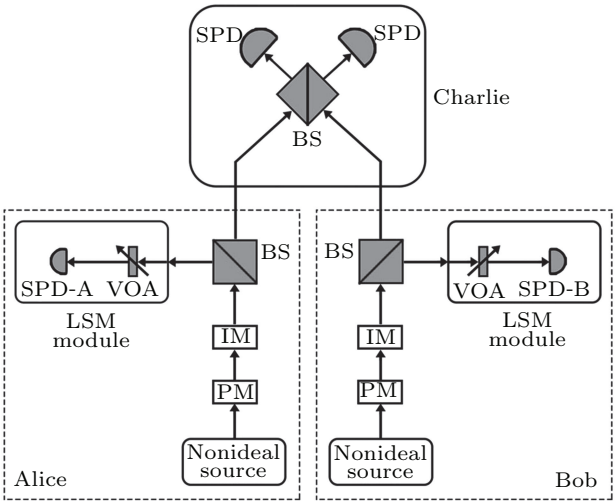


Fig. 1. The schematic diagram of PM-QKD-LSM protocol. SPD, a single photon detector; VOA, a variable optical attenuator; BS, the beam splitter; IM, intensity modulator; PM, phase modulator. The LSM module consists of a variable optical attenuator and a single photon detector(SPD-A/SPD-B).

The proposed protocol can be described in detail as follows.

(i) **State preparation** The two communication parties, Alice and Bob, randomly generate the coherent states $|\sqrt{\mu_A}\exp^{\mathrm{i}(\pi k_a+\phi_a)}\rangle_A$ and $|\sqrt{\mu_B}\exp^{\mathrm{i}(\pi k_b+\phi_b)}\rangle_B$, where the phases $\phi_a, \phi_b \in \{j_a\frac{2\pi}{M}, j_b\frac{2\pi}{M}\}$, $j_a, j_b \in \{0,1,\ldots,M-1\}$, M is the number of phase slices, $k_a, k_b \in \{0,1\}$ are the key bits, μ_A, μ_B are the average intensities, and $\mu_A, \mu_B \in \{0, \mu/2, \nu_1/2\}$, where $\mu/2$ is the signal intensity.

(ii) **Measurement** Alice and Bob use the beam splitter (BS) to split the light beam into two paths. One is used for LSM module to estimate the photon number probabilities and the other is sent to the measurement site (Charlie) with transmittances η_a (η_b). By changing the attenuation coefficient (η_i) of the VOA in the LSM module, Alice (Bob) measures the probabilities $(P^{\mu_k}(\eta_i))$ that the SPD-A (SPD-B) not responds. Charlie is expected to perform the interference detection and record which detector (right detector or left detector) clicks. A successful detection is defined as that one and only one of the two detectors clicks, denoted by L-click and R-click.

(iii) **Announcement** After Charlie announces the detection result, Alice and Bob announce the intensity settings (μ_A, μ_B) and the random phase numbers (j_a, j_b). Note that, the raw bit is obtained in Z-basis if $\mu_A = \mu_B = \mu/2$, or X-basis if $\mu_A = \mu_B$. To avoid the effect caused by the phase difference,

we introduce the phase post-compensation method, where Alice and Bob can estimate the the phase difference (ϕ_δ) by strong light pulses, then figure out the closest discrete phase $\phi_j \equiv (\frac{2\pi}{M})j$ to ϕ_δ and denote the index of the closest discrete phase as the phase slice number j_δ.

(iv) **Sifting** After Charlie announces a successful detection, Bob decides whether to flip his key bit k_b according to the result of detection. If the left detector clicks and $|j_a - j_b - j_\delta| \bmod M = 0$, the phase mismatch $\phi_{ab} = \phi_a - \phi_b - \phi_\delta \in (-\frac{\pi}{M}, \frac{\pi}{M})$, Bob does not need to flip his key bit k_b. If the right detector clicks and $|j_a - j_b - j_\delta| \bmod M = M/2$, the phase mismatch $\phi_{ab} = \phi_a - \phi_b - \phi_\delta \in (-\frac{\pi}{M} + \pi, \frac{\pi}{M} + \pi)$, Bob flips his key bit k_b. Alice and Bob group the signals by $j_s = (j_a - j_b) \bmod (M/2)$, then there are $M/2$ groups with the label of $j_s = 0, 1, \ldots, M/2-1$. Denote the group set J to be the set of remaining phase group indexes j_s. In the ideal case, the signals with $j_s = 0$ are the signals with matched phase where the phase difference $\phi_\delta = 0$. For the signals with $j_s \neq 0$, there is an intrinsic mismatched phase where the phase difference $\phi_\delta \neq 0$.

(v) **Parameter estimation** For all the raw data that they have retained, Alice and Bob record the detect number $M_{A,B}^{(j_s)}$ of different intensity combinations ($\mu_A, \mu_B \in \{0, \mu/2, \nu_1/2\}$) and phase groups j_s. According to the estimated probabilities that the source signal contains zero photon, one photon, and two photons in the LSM module, they then estimate the phase-error rate (E^{ph}) by using decoy state method.

(vi) **Key generation** Alice and Bob repeat steps (i)–(v) until they have enough sifted keys. Afterwards, they perform an error correction and privacy amplification on the sifted key bits to get a fully secret key.

2.2. The security analysis

In this section, we discuss the security of PM-QKD-LSM protocol.

As discussed above, PM-QKD-LSM protocol also includes state preparation, measurement, announcement, sifting, parameter estimation and key generation. The first difference between PM-QKD-LSM protocol and original PM-QKD protocol is the state preparation step. In original PM-QKD protocol, Alice (Bob) prepares the coherent state pulse and encodes the key information into the phases of the coherent states. It is assumed that the light source at Alice (Bob) side is a coherent state source with a average photon number which satisfies the Poisson distribution. However, the photon number distribution is unstable in the proposed PM-QKD-LSM protocol due to the non-ideal factors of the light source. Therefore, LSM module is adopted by Alice (Bob) to estimate the photon number probabilities. Obviously, the usage of LSM module does not affect the sooner measurement step, the following announcement and sifting. The second difference is the parameter estimation step, PM-QKD-LSM protocol adds the probability estimations of zero photon, one photon, and two photons precisely, which only has the relationship with the secure key rate, and is discussed in the following subsection. Hence, we only prove that the quantum state prepared in our protocol does not introduce the security problem.

First of all, in PM-QKD-LSM protocol, the quantum state prepared by Alice (Bob) is no longer an ideal coherent state under UPC, but a state with arbitrary PND. After the modulation of intensity and phase, the quantum state can be written as $|\psi_A\rangle = \sum_{k=0}^{\infty} \mathrm{e}^{\mathrm{i}k(\pi k_a + \phi_a)} \sqrt{P_k(\mu_A)} |k\rangle_A$ ($|\psi_B\rangle = \sum_{k=0}^{\infty} \mathrm{e}^{\mathrm{i}k(\pi k_b + \phi_b)} \sqrt{P_k(\mu_B)} |k\rangle_B$), where $P_k(\mu_A)$($P_k(\mu_B)$) is unknown. Because of the randomness of the phase ϕ_a, ϕ_b, $\phi_- = \phi_a - \phi_b$, the quantum density matrix of Alice and Bob can be derived as

$$
\begin{aligned}
\rho_{AB} &= \int_0^{2\pi} P(|\psi_A\rangle \otimes |\psi_B\rangle)\, \mathrm{d}\phi_- \\
&= \int_0^{2\pi} P\left[\sum_{k=0}^{\infty} \mathrm{e}^{\mathrm{i}k(\pi k_a + \phi_a)} \sqrt{P_k(\mu_A)} |k\rangle_A \otimes \sum_{m=0}^{\infty} \mathrm{e}^{\mathrm{i}m(\pi k_b + \phi_b)} \sqrt{P_m(\mu_B)} |m\rangle_B \right] \mathrm{d}\phi_- \\
&= \sum_{k=0}^{\infty} \sum_{m=0}^{\infty} \int_0^{2\pi} P[\mathrm{e}^{\mathrm{i}(k\phi_a + m\phi_b + k\pi k_a + m\pi k_b)} \sqrt{P_k(\mu_A) P_m(\mu_B)} |k\rangle_A |m\rangle_B] \mathrm{d}\phi_- \\
&= \sum_{k=0}^{\infty} \sum_{m=0}^{\infty} \int_0^{2\pi} P[\mathrm{e}^{\mathrm{i}(\frac{k+m}{2}(\phi_a + \phi_b) + \frac{k-m}{2}\phi_- + k\pi k_a + m\pi k_b)} \sqrt{P_k(\mu_A) P_m(\mu_B)} |k\rangle_A |m\rangle_B] \mathrm{d}\phi_- \\
&= \sum_{k,k',m,m'} \left[\sqrt{P_k(\mu_A) P_{k'}(\mu_A) P_m(\mu_B) P_{m'}(\mu_B)} |k\rangle_A |m\rangle_{BB} \langle m'|_A \langle k'| \right. \\
&\quad \left. \times \int_0^{2\pi} \mathrm{e}^{\mathrm{i}(\frac{k-k'+m-m'}{2}(\phi_a + \phi_b) + \frac{k-k'-m+m'}{2}\phi_- + (k-k')\pi k_a + (m-m')\pi k_b)} \mathrm{d}\phi_- \right] \\
&= \sum_{k,k',m} \sqrt{P_k(\mu_A) P_{k'}(\mu_A) P_m(\mu_B) P_{m+k'-k}(\mu_B)}\, \mathrm{e}^{\mathrm{i}(k-k')(\phi_a + \phi_b + \pi k_a + \pi k_b)} |k\rangle_A |m\rangle_{BB} \langle m + k' - k|_A \langle k'|. \qquad (1)
\end{aligned}
$$

So, ρ_{AB} can be rewritten as $\rho_{AB}=\sum_{n=0}^{\infty}P_n(\mu)|\psi_n\rangle\langle\psi_n|$, where $P_n(\mu)=\sum_{m=0}^{n}P_m(\mu_A)P_{n-m}(\mu_B)=\sum_{m=0}^{n}P_m(\mu/2)P_{n-m}(\mu/2)$. For the ideal source, $P_k(\mu_A)(P_k(\mu_B))$ is known and satisfies the Poisson distribution, and the density matrix can be written as $\rho_{AB}=\sum_{n=0}^{\infty}P_n(\mu)|n\rangle\langle n|$ when $\mu_A=\mu_B=\mu/2$. Here, $P_n(\mu)$ is obtained by the probability when m-photon pulse from Alice and $(n-m)$-photon pulse from Bob, that is,

$$\begin{aligned}&\sum_{m=0}^{n}P_m(\mu_A)P_{n-m}(\mu_B)\\&=\sum_{m=0}^{n}\frac{\mathrm{e}^{-\mu/2}(\mu/2)^m}{m!}\frac{\mathrm{e}^{-\mu/2}(\mu/2)^{n-m}}{(n-m)!}\\&=\frac{\mathrm{e}^{-\mu}\mu^n}{n!}=P_n(\mu).\end{aligned}\tag{2}$$

Hence, it is shown that the quantum state is formally consistent with that of PM-QKD protocol. Moreover, the security proof of PM-QKD protocol[22] can be fully applied to our proposed protocol.

For the actual system security, the structure of system may introduce some security vulnerabilities. We discuss the security of the proposed protocol against the security vulnerabilities, individually, as follows.

(i) **PNS attack** During the proposed protocol, the eavesdropper (Eve) has the chances to intervene and eavesdrop the signal by beam splitting attack (PNS). As PM-QKD protocol, we use the decoy state method in the proposed protocol, that is effectively against PNS attack. In addition, the LSM module used in the proposed protocol can estimate the probabilities of zero photon, single photon and two photon precisely, so that the PNS attack can be detected by Alice (Bob), and the security can be improved.

(ii) **Phase-remapping attack** Ideally, the pulses undergo a phase modulation by the phase modulator. If Eve can change the arrival time of the pulses, then the pulses will pass through the phase modulator at different time, resulting in different encoded phases. This phase remapping process allows Eve to launch an intercept-and-resend attack. However, the LSM module can also be approximately regarded as a monitoring unit to monitor the arrival time of the pulses so as to resist this attack.

(iii) **Other practical issues** A single photon detector (SPD), together with a variable attenuator, are used in our proposed protocol. The SPD may have a high dark count rate (DCR) when it works at room temperature, which may increase the time of monitoring the results. A high DCR and the increased monitoring time can introduce the overestimation of secret key rate. However, the SPD is set near the light source in our protocol and DCR $=10^{-8}\ll 1$ (in our simulations),[25] which make the increased monitoring time ignored. Of course, the DCR of SPD may fluctuate in the actual environment, and other parameters, such as the detection efficiency of SPD, may drift. One can calibrate all parameters of the monitor in real time,[25] or present a range of parameter drifts and give a reasonable estimation of the lower bound of secret key rate (R) with the worst cases within the fluctuation range.

2.3. Secret key rate of the protocol

In PM-QKD-LSM protocol, three different coefficients (η_0, η_1 and η_2) are used to concisely estimate the photon number probabilities $(P_{n\mathrm{L}}(\mu_k),P_{n\mathrm{U}}(\mu_k))$, and they are controllable. The relation[29] between $P^{\mu_k}(\eta_i)$ and $P_n(\mu_k)$ can be described as

$$P^{\mu_k}(\eta_i)=(1-P_\mathrm{d})\sum_{n=0}(1-\eta_i)P_n(\mu_k),\tag{3}$$

where $P^{\mu_k}(\eta_i)$ denotes the probability of the SPDs not responding with attenuation coefficient η_i for source μ_k. Then, according to the estimation method in Ref. [26], we can obtain those tight bounds of the photon number probabilities as

$$P_{0\mathrm{U}}(\mu_k)=P_{0\mathrm{L}}(\mu_k)=\frac{P^{\mu_k}(\eta_0)}{1-P_\mathrm{d}},\tag{4}$$

$$\begin{aligned}P_{1\mathrm{L}}(\mu_k)=&\frac{(1-\eta_2)^2P^{\mu_k}(\eta_1)-(1-\eta_1)^2P^{\mu_k}(\eta_2)}{(1-P_\mathrm{d})(1-\eta_1)(1-\eta_2)(\eta_1-\eta_2)}\\&-\left(\frac{1}{1-\eta_1}+\frac{1}{1-\eta_2}\right)P_{0\mathrm{U}}(\mu_k),\end{aligned}\tag{5}$$

$$\begin{aligned}P_{1\mathrm{U}}(\mu_k)=&\frac{(1-\eta_2)(1-\eta_1)}{[1-\eta_2-(1-\eta_1)(2-\eta_2)]}\\&\times\left\{\frac{P^{\mu_k}(\eta_1)}{(1-\eta_1)^2(1-P_\mathrm{d})}-\frac{P^{\mu_k}(\eta_2)}{(1-P_\mathrm{d})(1-\eta_2)^2\eta_2}\right.\\&+\frac{(1-\eta_2)}{\eta_2}+\frac{[1-(1-\eta_2)^3]}{(1-\eta_2)^2\eta_2}P_{0\mathrm{U}}(\mu_k)\\&\left.-\frac{P_{0\mathrm{L}}(\mu_k)}{(1-\eta_1)^2}\right\},\end{aligned}\tag{6}$$

$$\begin{aligned}P_{2\mathrm{L}}(\mu_k)=&\frac{P^{\mu_k}(\eta_2)}{(1-P_\mathrm{d})(1-\eta_2)^2\eta_2}-\frac{2-\eta_2}{1-\eta_2}P_{1\mathrm{U}}(\mu_k)\\&-\frac{1-\eta_2}{\eta_2}-\frac{[1-(1-\eta_2)^3]}{(1-\eta_2)^2\eta_2}P_{0\mathrm{U}}(\mu_k),\end{aligned}\tag{7}$$

$$P_{2\mathrm{U}}(\mu_k)=\frac{P^{\mu_k}(\eta_2)}{(1-P_\mathrm{d})(1-\eta_2)^2}-\frac{P_{0\mathrm{L}}(\mu_k)}{(1-\eta_2)^2}-\frac{P_{1\mathrm{L}}(\mu_k)}{1-\eta_2},\tag{8}$$

where $P^{\mu_k}(\eta_0)$, $P^{\mu_k}(\eta_1)$ and $P^{\mu_k}(\eta_2)$ are the probabilities of the single photon detector in Alice or Bob (SPD-A/SPD-B) not responding when the light fields pass through the variable attenuator (VOA) whose variable attenuation coefficients are η_0, η_1 and η_2, respectively, and P_d is the dark count rate of the SPD-A/SPD-B. The variable attenuation coefficients (η_1,η_2) need to meet the following condition:

$$\eta_1(2-\eta_2)>1.\tag{9}$$

To accurately bound the phase-error rate (E^{ph}) in PM-QKD-LSM protocol, we use the three-decoy-state method[30]

with intensities $\nu_0 = 0, \nu_1, \mu$ ($\mu > \nu_1 > 0$) to estimate the lower bound of Y_1 as $Y_{1\mathrm{L}}$ and the results are obtained as

$$Y_{1\mathrm{L}} = \frac{P_{2\mathrm{L}}(\mu)Q_{\nu_1} - P_{2\mathrm{L}}(\mu)P_{0\mathrm{U}}(\nu_1)Y_0}{P_{2\mathrm{U}}(\mu)P_{1\mathrm{U}}(\nu_1) - P_{2\mathrm{L}}(\nu_1)P_{1\mathrm{L}}(\mu)} + \frac{P_{2\mathrm{U}}(\nu_1)P_{0\mathrm{L}}(\mu)Y_0 - P_{2\mathrm{U}}(\nu_1)Q_\mu}{P_{2\mathrm{U}}(\mu)P_{1\mathrm{U}}(\nu_1) - P_{2\mathrm{L}}(\nu_1)P_{1\mathrm{L}}(\mu)}, \tag{10}$$

where Q_{μ_k} is the count rate of a state with intensity μ_k and Y_0 can be directly obtained by using the vacuum decoy state ($\nu_0 = 0$). The detection click probabilities are

$$\begin{aligned} P_\mu(\overline{L}) &= (1-P_\mathrm{d})\exp\left(-\frac{\eta_a\mu_a + \eta_b\mu_b}{2} - \sqrt{\eta_a\mu_a\eta_b\mu_b}\cos\phi_\delta\right), \\ P_\mu(L) &= 1 - P_\mu(\overline{L}), \\ P_\mu(\overline{R}) &= (1-P_\mathrm{d})\exp\left(-\frac{\eta_a\mu_a + \eta_b\mu_b}{2} + \sqrt{\eta_a\mu_a\eta_b\mu_b}\cos\phi_\delta\right), \\ P_\mu(R) &= 1 - P_\mu(\overline{R}), \end{aligned} \tag{11}$$

where $P_\mu(L)$ and $P_\mu(\overline{L})$ are the probabilities of the light detector clicking and no light detector clicking, respectively, and $P_\mu(R)$ and $P_\mu(\overline{R})$ are for the right detector. Considering the first order of a small ϕ_δ, we ignore $\sin^2(\frac{\phi_\delta}{2}) = 0$. Then, the total gain Q_μ can be deduced as follows:

$$\begin{aligned} Q_\mu &= P_\mu(L)P_\mu(\overline{R}) + P_\mu(\overline{L})P_\mu(R) \\ &= (1-P_\mu(\overline{L}))P_\mu(\overline{R}) + P(\mu\overline{L})(1-P_\mu(\overline{R})) \\ &= (1-P_\mathrm{d})\left(\exp\left(-\frac{1}{2}(\sqrt{\eta_a\mu_a} + \sqrt{\eta_b\mu_b})^2\right)\right. \\ &\quad \left. + \exp\left(-\frac{1}{2}(\sqrt{\eta_a\mu_a} - \sqrt{\eta_b\mu_b})^2\right)\right) \qquad (12) \\ &\quad -2(1-P_\mathrm{d})^2\left(-\frac{1}{2}(\sqrt{\eta_a\mu_a} + \sqrt{\eta_b\mu_b})^2\right. \\ &\quad \left. -\frac{1}{2}(\sqrt{\eta_a\mu_a} - \sqrt{\eta_b\mu_b})^2\right), \qquad (13) \end{aligned}$$

where μ_a and μ_b are the signal identities selected by the Alice and Bob which satisfy $\mu_a = \mu_b = \mu/2$, η_a and η_b are the transmittances between users (Bob/Alice) and the measuring site (Charlie). Normally, the η_a is obtained by the following formula:

$$\eta_a = 10^{-\alpha L_A/10}\cdot\eta_\mathrm{d}. \tag{14}$$

The η_b is the similar formula, and L_B (L_A) is distance from Bob (Alice) to Charlie and η_d is detection efficiency of detector, α is the attenuation coefficient of the corresponding channel. When PM-QKD-LSM protocol is in the case of symmetrical channel ($L_A = L_B$), the transmittance $\eta = \eta_a = \eta_b$ and the total transmission distance is denoted as $L = L_A + L_B$.

The phase-error rate $E^\mathrm{ph} = q_\mathrm{even}$, where the ratios of even components causing effective detection $q_\mathrm{even} = \sum_{k=0}^{\infty} q_{2k}$.[30] Therefore, by the above Eq. (10), we can estimate the upper bound of q_even as

$$q_{\mathrm{evenU}} = 1 - q_{1\mathrm{L}} = 1 - P_{1\mathrm{L}}(\mu)\frac{Y_{1\mathrm{L}}}{Q_\mu}, \tag{15}$$

where $q_{1\mathrm{L}}$ is the lower bound of single-photon component yield. The bit error rate $E_\mu^{(j_s)}$ is given by

$$E_\mu^{(j_s)} = \min\left(\left\{P_\mathrm{d} + \frac{\mu\eta_a + \mu\eta_b}{4} - \frac{\mu\sqrt{\eta_a\eta_b}}{2} + \mu\sqrt{\eta_a\eta_b}[e_\Delta(j_s) + e_\mathrm{d}]\right\}\frac{\mathrm{e}^{-\frac{\eta_a\mu}{2} - \frac{\eta_b\mu}{2}}}{Q_\mu}, 0.5\right), \tag{16}$$

where η is the transmittance and e_d is the misalignment error of the QKD system, the mismatch error $e_\Delta(j_s)$ which is caused by the intrinsic mismatch for different phase groups is given as

$$e_\Delta(j_s) = \begin{cases} \sin^2(\frac{\pi j_s}{M}), & 0 \le j_s \le \frac{M}{4}, \\ \sin^2(\frac{\pi}{2} - \frac{\pi j_s}{M}), & \frac{M}{4} < j_s \le \frac{M}{2} - 1, \end{cases} \tag{17}$$

which is related to the index deviation $0 \le j_s \le \frac{M}{2} - 1$. When the distance from Alice to Charlie is same as that from Bob to Charlie ($L_A = L_B$), the bit error rate $E_\mu^{(j_s)}$ can be simplified as follows:

$$E_\mu^{(j_s)} = \min\left(\{P_\mathrm{d} + \eta\mu[e_\Delta(j_s) + e_\mathrm{d}]\}\frac{\mathrm{e}^{-\eta\mu}}{Q_\mu}, 0.5\right). \tag{18}$$

According to the above analysis of PM-QKD-LSM protocol, the secret key rate of the protocol can be written as

$$R = \frac{2Q_\mu}{M}\sum_{j_s\in J}[1 - H(q_{\mathrm{evenU}}) - fH(E_\mu^{(j_s)})]. \tag{19}$$

where f is the error-correction efficiency, $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, and $E_\mu^{(j_s)}$ is the bit error rate of phase group j_s with $\mu_a = \mu_b = \frac{\mu}{2}$.

2.4. Source fluctuation

For a real-life QKD system, the PND of the light source's signal is not fixed, that is, there is a problem of the light source fluctuation. Importantly, the performance of the PM-QKD protocol is greatly degraded in this condition. Therefore, we further discuss the intensity fluctuation for PM-QKD-LSM protocol.

Specifically, the signal emitted from the light source can be considered as a fluctuated coherent state which has an average photon number with Gaussian-distribution.[27,28] In PM-QKD-LSM protocol, the signal after attenuation still has a Gaussian-distribution average photon number μ, which has a probability distribution of

$$P(\mu) = \frac{1}{\sqrt{2\pi}\sigma_{\mu_k}}\exp\left[-\frac{(\mu-\mu_0)^2}{2\sigma_{\mu_k}^2}\right], \tag{20}$$

where μ_0, σ_{μ_k} are the mean value and the standard deviation of μ_k. The probabilities $P^{\mu_k}(\eta_i)$ under the intensity fluctuation become

$$P^{\mu_k}(\eta_i) = \int P^\mu(\eta_i)P(\mu)\mathrm{d}\mu, \tag{21}$$

where $P^{\mu}(\eta_i) = (1-P_{\rm d})\,{\rm e}^{-\eta_i\mu}$.[28] Then the probabilities $P^{\mu_k}(\eta_i)$ can be simulated as

$$P^{\mu_k}(\eta_i) = (1-P_{\rm d})\exp\left[-\eta_i\mu_0 - \frac{(\eta_i\sigma_{\mu_k})^2}{2}\right], \qquad (22)$$

where $\sigma_{\mu_k} = \sigma\mu_0$, σ is the fluctuation coefficient. With Eqs. (4)–(9), the $P_n(\mu_k)$ can be estimated by $P^{\mu_k}(\eta_i)$ under considering the source fluctuation.[31,32]

3. Results with numerical simulation

In PM-QKD protocol,[30] the light source is assumed to be the ideal coherent states, thus the PND of the light source satisfies the Poisson distribution, that is, $P_n(\mu_k) = {\rm e}^{-\mu_k}\frac{\mu_k^n}{n!}$ for $\mu_k = \mu, \nu_1, \nu_0$, then the probability of $\mu_k(P_n(\mu_k))$ can be obtained exactly and we name these values as the exact values. But, in PM-QKD-LSM protocol, only the bounds of $P_n(\mu_k)$,$\{P_{n\rm L}(\mu_k), P_{n\rm U}(\mu_k)\}$, can be obtained by using the LSM module. We name the bounds as the estimation values.

We first compare the estimation values of $\{P_{n\rm L}(\mu_k), P_{n\rm U}(\mu_k)\}$ under LSM module with the exact values from $P_n(\mu_k)$. Here, we consider the ideal simulation circumstance, where the PND of the light source satisfies the Poisson distribution, thus, the probabilities $P^{\mu_k}(\eta_i)$ can be simulated as $P^{\mu_k}(\eta_i) = (1-P_{\rm d})\,{\rm e}^{-\eta_i\mu_k}$.[28] According to the Ref. [28], we also set the attenuation coefficients $\eta_0 = 1$, $\eta_1 = 0.95$, $\eta_2 = 0.9$ for the constraints in Eq. (9). The intensities $\mu_A = \mu_B = \mu/2$, $\nu_{1A} = \nu_{1B} = \nu_1/2$, $\nu_{0A} = \nu_{0B} = 0$. The values of μ, ν_1 can be randomly selected, but they should satisfy $\mu \geq \nu_1$. Table 1 shows the estimation values of the upper and lower bound of $P_n(\mu_k)$ in comparison with the exact values, where $\mu = 0.7$ and $\nu_1 = 0.07$ (μ and ν_1 can be randomly set only when $\mu \geq \nu_1$). The results show that the estimation values by using LSM module are very close to those exact values. For $P_0(\mu), P_0(\nu_1), P_1(\nu_1), P_2(\nu_1)$, the upper and lower bounds estimated by LSM module are the same as those of the exact values, while there are little differences for $P_1(\mu), P_2(\mu)$.

Table 1. Estimation result of $\{P_{n\rm L}(\mu_k), P_{n\rm U}(\mu_k)\}$ in the LSM scheme.

$\mu = 0.7$			$\nu_1 = 0.07$		
$P_0(\mu)$	$P_{0\rm U}(\mu)$	$P_{0\rm L}(\mu)$	$P_0(\nu_1)$	$P_{0\rm U}(\nu_1)$	$P_{0\rm L}(\nu_1)$
0.4966	0.4966	0.4966	0.9324	0.9324	0.9324
$P_1(\mu)$	$P_{1\rm U}(\mu)$	$P_{1\rm L}(\mu)$	$P_1(\nu_1)$	$P_{1\rm U}(\nu_1)$	$P_{1\rm L}(\nu_1)$
0.3476	0.3478	0.3475	0.0653	0.0653	0.0653
$P_2(\mu)$	$P_{2\rm U}(\mu)$	$P_{2\rm L}(\mu)$	$P_2(\nu_1)$	$P_{2\rm U}(\nu_1)$	$P_{2\rm L}(\nu_1)$
0.1217	0.1260	0.1186	0.0023	0.0023	0.0023

Then, we discuss the performance of the proposed protocol. The parameters are the same as those in Ref. [30], which are listed in Table 2.

Figure 2 shows the secret key generation rate of the proposed protocol against transmission distance, together with that of original PM-QKD protocol. The results show that PM-QKD-LSM protocol can exceed PLOB bound when the transmission distance is greater than 212 km, and the performance of PM-QKD-LSM protocol (dashed curve) is close to that of the original PM-QKD protocol (solid curve). The ratios of secret key rate between PM-QKD-LSM protocol and PM-QKD protocol are about 93.6%, 93.0%,92.4% at the distance of 100 km, 200 km, 400 km, and the maximum transmission distances of PM-QKD-LSM protocol and PM-QKD protocol are 504 km and 507 km, respectively, where the maximum transmission distance is calculated as $L = L_A + L_B$.

Table 2. The numerical simulation parameters.

Variable	Parameter	Simulation value
α	fiber loss coefficient	0.2 dB/km
$P_{\rm d}$	dark count rate of detector	1.0×10^{-8}
$\eta_{\rm d}$	detection efficiency	20%
$e_{\rm d}$	misalignment error	20%
f	error correction efficiency	1.14
M	number of phase slices	16

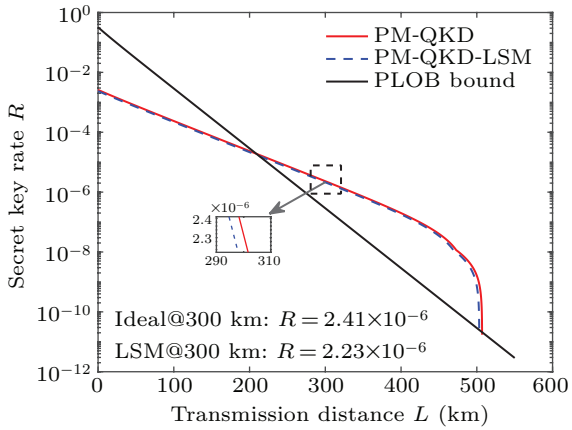


Fig. 2. The performance of PM-QKD-LSM protocol in comparison with that of PM-QKD protocol with the parameters set in Table 2. For 300 km transmission distance, the secret key rate for PM-QKD-LSM protocol is 2.23×10^{-6}, while it is 2.41×10^{-6} for PM-QKD protocol.

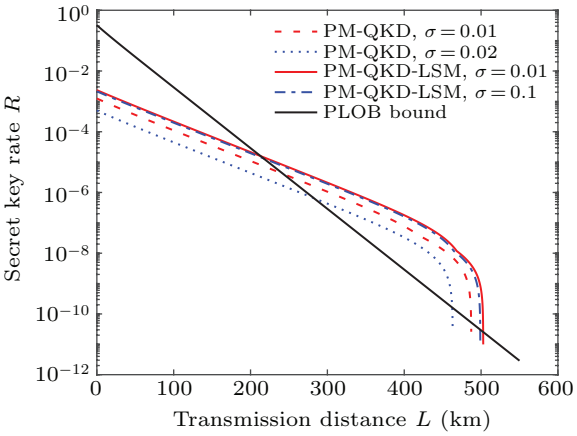


Fig. 3. The performance of the PM-QKD-LSM protocol with a non-ideal and fluctuated light source compared to the PM-QKD protocol. σ: the fluctuation coefficient. For the PM-QKD-LSM protocol, a small fluctuation $\sigma = 1\%$ (solid curve) and a large fluctuation $\sigma = 10\%$ (dash-dotted curve) are considered. For the PM-QKD protocol, a small fluctuation $\sigma = 1\%$ (dashed curve) and a relatively large fluctuation $\sigma = 2\%$ (dotted curve) are considered.

After that, we discuss the performance of both PM-QKD protocol and PM-QKD-LSM protocol under the different fluctuation coefficient $\sigma = \sigma_{\mu_k}/\mu_0$ in Fig. 3. The values of intensities for the PM-QKD-LSM protocol and the PM-QKD protocol are optimized, and other simulation parameters are set the same as Table 2. It is shown that the PM-QKD-LSM protocol performs well in the practical systems. For the different fluctuation coefficient σ, the PM-QKD protocol has a obviously weaker performance, as its maximum transmission distance decreases to about 480 km for a small fluctuated light source ($\sigma = 1\%$), then decreases to about 460 km when σ up to 2%. However, for the PM-QKD-LSM protocol, its performances are almost unchanged under the fluctuated condition from $\sigma = 1\%$ to $\sigma = 10\%$.

Then, we use the recently proposed average intensity method[33] on PM-QKD protocol to compare with PM-QKD-LSM protocol under the different fluctuation coefficient. In Ref. [33], the intensity range is $\mu^{\pm} = \overline{\mu}(1+\sigma^{\pm})$ where $\sigma^{+} = \max : \sigma_i$ and $\sigma^{-} = \min : \sigma_i$. By defining $f_n(\sigma,\overline{\mu}) = \frac{\overline{\mu}^n \exp(-\overline{\mu})}{n!}[\exp(-\sigma\overline{\mu})(1+\sigma)^n - (n-\overline{\mu})\sigma]$, the upper and lower bounds of $P_n(\mu)$ can be written as $P_{n\mathrm{U}}(\mu) = \max : f_n(\sigma,\overline{\mu})$ and $P_{n\mathrm{L}}(\mu) = \min : f_n(\sigma,\overline{\mu})$, where $\sigma \in [\sigma^{-},\sigma^{+}]$ and $\overline{\mu} \in [\overline{\mu}_{-},\overline{\mu}_{+}]$. Using the optimization algorithms, one can get the upper and lower bounds of $f_n(\sigma,\overline{\mu})$. Figure 4 shows the performance of the PM-QKD-LSM protocol and that of PM-QKD with average intensity method under different source fluctuation. Here, the finite size effects are not considered in both protocols. The simulation results show that the performance of PM-QKD-LSM protocol is better than those of PM-QKD protocol with average intensity whether the intensity fluctuation is small or large, when the transmission distance is less than 470 km. And the large intensity fluctuation has limited influence on both PM-QKD-LSM protocol and PM-QKD protocol with average intensity. But the maximum transmission distance of PM-QKD protocol with average intensity ($\sigma = 1\%$) is 508 km while the maximum transmission distance of PM-QKD-LSM protocol ($\sigma = 1\%$) is 503 km. For the large fluctuation ($\sigma = 10\%$), the maximum transmission distance of both protocols is 499 km.

The above discussions are under the symmetric condition which satisfy $L_A = L_B$. Later, we discuss the performance of PM-QKD-LSM protocol under the asymmetric channel. Hence, we set the transmission distance to satisfy $L_B - L_A = 30$ km and $\mu_A, \mu_B \in \{0, \mu/2, \nu_1/2\}$, where $\mu/2$ is the signal intensity. Other simulation parameters are set the same as those in Table 2. Figure 5 shows the performance of the PM-QKD-LSM protocol and the PM-QKD protocol under the asymmetric channel without source fluctuation, where the transmission distance $L = L_B + L_A$. The results show that PM-QKD-LSM protocol can exceed PLOB bound when the transmission distance is greater than 275 km. The performance of PM-QKD-LSM protocol (dashed curve) is almost same to that of PM-QKD protocol (solid curve) for all the transmission distance. For 300 km transmission distance, the secret key rate for PM-QKD-LSM protocol is 5.13×10^{-7}, while it is 5.70×10^{-7} for PM-QKD protocol, they are smaller than those under symmetric channel.

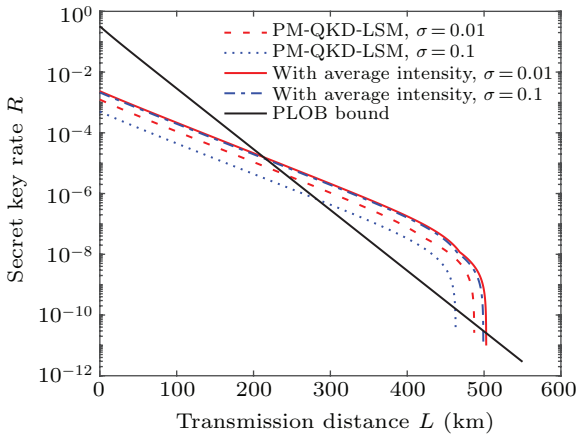


Fig. 4. The performance of the PM-QKD-LSM protocol and that of PM-QKD with average intensity method under different source fluctuation. For two different methods, a small fluctuation $\sigma = 1\%$ (red curve) and a large fluctuation $\sigma = 10\%$ (blue curve) are considered. The solid curves denote the PM-QKD-LSM protocol and dash-dotted curves denote the PM-QKD protocol with average intensity.

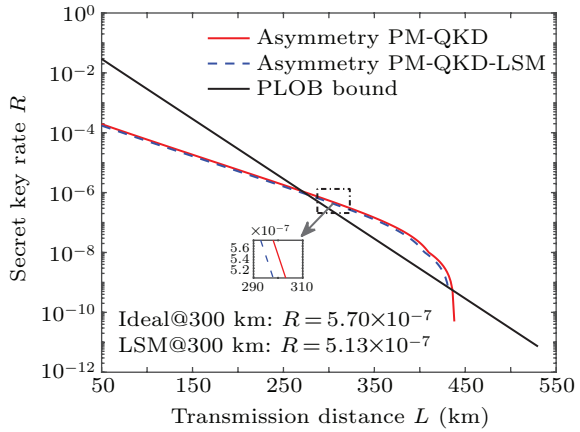


Fig. 5. The performance of the asymmetric PM-QKD-LSM protocol and the PM-QKD protocol without source fluctuate. The transmission distance is set to satisfy $L_B - L_A = 30$ km, and the abscissa represents the total transmission distance ($L = L_B + L_A$).

We further consider the effect of the light source fluctuation on the asymmetric channel. The fluctuation coefficients are set up to $\sigma = 1\%$ and $\sigma = 5\%$, respectively, and the other simulation parameters are the same as those in symmetric case. The results in Fig. 6 indicate that the PM-QKD-LSM protocol has a better performance in the case of source fluctuation, even the source fluctuation is 10 times greater than that of asymmetry PM-QKD protocol.

In addition, we show the performance of the asymmetric PM-QKD-LSM protocol under different fluctuation coefficient versus the different Alice to Charlie transmission distance in Fig. 7. The total transmission distance is set to 50 km, and the distance from Alice to Charlie is set from 5 km to

25 km. It can be seen from Fig. 7 that the performance of the asymmetric PM-QKD-LSM protocol with different source fluctuations are almost the same, which indicates the asymmetric PM-QKD-LSM protocol is also robust to the source fluctuation.

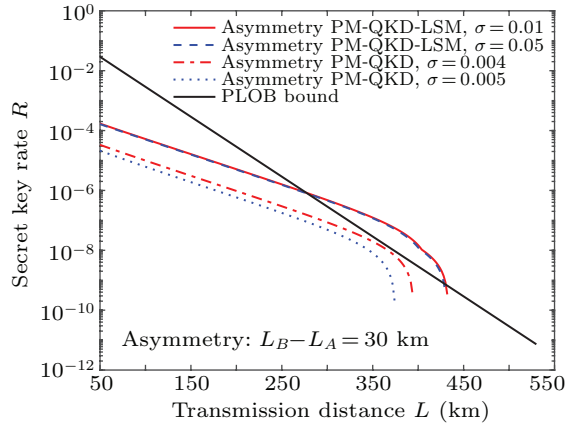


Fig. 6. The performance of the asymmetric PM-QKD-LSM protocol for different Alice to Charlie transmission distance under source fluctuation. The transmission distance is set to satisfy $L_B - L_A = 30$ km, and the abscissa represents the total transmission distance ($L = L_B + L_A$). The fluctuation coefficient $\sigma = 1\%$ (solid curve) and $\sigma = 5\%$ (dashed curve) in the asymmetric PM-QKD-LSM protocol are set, respectively. The fluctuation coefficient $\sigma = 0.4\%$ (dash-dotted curve) and $\sigma = 0.5\%$ (dotted curve) in the asymmetric PM-QKD protocol are studied, respectively.

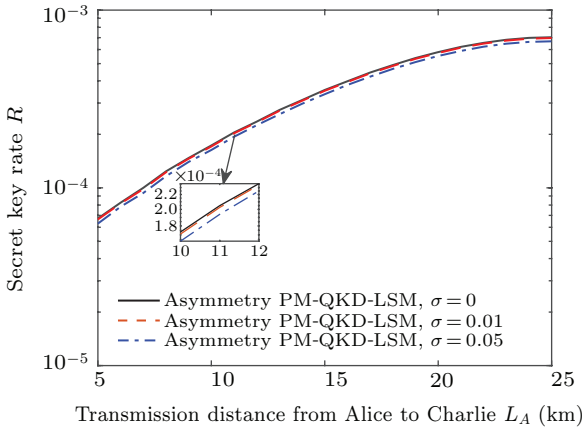


Fig. 7. The performance of the asymmetric PM-QKD-LSM protocol under different fluctuation coefficient of light source. For the asymmetric channel, the fluctuation coefficient $\sigma = 0$ (solid curve), a small fluctuation $\sigma = 1\%$ (dashed curve) and a large fluctuation $\sigma = 5\%$ (dash-dotted curve) are considered.

4. Conclusion

In this paper, we apply the LSM module to the PM-QKD protocol to solve the non-ideal source problem in practical QKD systems, where the LSM module is used to estimate the probabilities of zero photon, single photon and two photon precisely. We derive the more rigorous secret key rate under different source fluctuations. The results show that, whether in symmetric or asymmetric cases, the performance of the PM-QKD-LSM protocol under UPC is almost the same as those of the PM-QKD protocol without source fluctuation. Moreover, PM-QKD-LSM protocol has a better performance than that of PM-QKD protocol with source fluctuation. The symmetric and asymmetric PM-QKD-LSM protocol are robust to the source fluctuation. It is indicated that the PM-QKD-LSM protocol can still have a long transmission distance with the fluctuated source in practical QKD systems.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 61871234 and 62001249) and Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics, Tsinghua University (Grant No. KF201909).

References

[1] Mayers D 2001 *J. ACM* **48** 351
[2] Lo H K and Chau H F 1999 *Science* **283** 2050
[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[4] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 175
[5] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[6] Wang X B 2005 *Phys. Rev. A* **72** 012322
[7] Wang X B, Yang L, Peng C Z and Pan J W 2009 *New J. Phys.* **11** 075006
[8] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[9] Wang L, Zhao S M, Gong L Y and Cheng W W 2015 *Chin. Phys. B* **24** 120307
[10] Guan J Y, Cao Z, Liu Y, Shen-Tu G L, Pelc J S, Fejer M M, Peng C H, Ma X F, Zhang Q and Pan J W 2015 *Phys. Rev. Lett.* **114** 180502
[11] Wang L and Zhao S M 2017 *Quantum Inform. Process.* **16** 100
[12] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 1
[13] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[14] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307
[15] Chen G, Wang L, Li W, Zhao Y, Zhao S M and Gruska J 2020 *Quantum Inform. Process.* **19** 416
[16] Teng J, Yin Z Q, Yuan Fan G J, L u F Y, Wang R, Wang S, Chen W, Huang W, Xu B J, Guo G C and Han Z F 2021 *Phys. Rev. A* **104** 062441
[17] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[18] Xu H, Yu Z W, Jiang C, Hu X L and Wang X B 2020 *Phys. Rev. A* **101** 042330
[19] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053
[20] Xue K, Zhao S M, Mao Q P and Xu R 2021 *Quantum Inform. Process.* **20** 320
[21] Chen J P, Zhang C, Liu Y, Jiang C, Zhang W J, Han Z Y, Ma S Z, Hu X L, Li Y H, Liu H, Zhou F, Jiang H F, Chen T Y, Li H, You L X, Wang Z, Wang X B, Zhang Q and Pan J W 2021 *Nat. Photonics* **15** 570
[22] Ma X, Zeng P and Zhou H 2018 *Phys. Rev. X* **8** 031043
[23] Jin A, Zeng P, Penty R V and Ma X F 2021 *Phys. Rev. Appl.* **16** 034017
[24] Wang X B 2007 *Phys. Rev. A* **75** 052301
[25] Peng X, Jiang H, Xu B J, Ma X F and Guo H 2008 *Opt. Lett.* **33** 2077
[26] Xu F 2015 *Phys. Rev. A* **92** 012333
[27] Qiao Y C, Wang G, Li Z Y, Xu B J and Guo H 2019 *Phys. Rev. A* **99** 052302
[28] Qiao Y C, Chen Z Y, Zhang Y C, Xu B J and Guo H 2020 *Entropy* **22** 36
[29] Wang G, Li Z, Q iao Y, Chen Z, Peng X and Guo H 2018 *IEEE J. Quantum Electron.* **54** 9300110
[30] Zeng P, Wu W J and Ma X F 2020 *Phys. Rev. Appl.* **13** 064013
[31] Yu Y, Wang L, Zhao S M and Mao Q P 2021 *Opt. Express* **29** 2227
[32] Zhang X X, Wang Y, Jiang M S, Zhou C, Lu Y F and Bao W S 2021 *JOSA B* **38** 724
[33] Lu F Y, Yin Z Q, Wang R, Yuan-Fan G J, Wang S, He D Y, Chen W, Huang W, Xu B J, Guo G C and Han Z F 2019 *New J. Phys.* **21** 123030