# Passive decoy-state quantum key distribution using weak coherent pulses with modulator attenuation*

Li Yuan(李 源)[a)b)], Bao Wan-Su(鲍皖苏)[a)b)†], Li Hong-Wei(李宏伟)[b)], Zhou Chun(周 淳)[a)b)], and Wang Yang(汪 洋)[a)b)]

[a)] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450004, *China*
[b)] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 17 March 2015; revised manuscript received 7 August 2015; published online 10 October 2015)

Passive decoy-state quantum key distribution is more desirable than the active one in some scenarios. It is also affected by the imperfections of the devices. In this paper, the influence of modulator attenuation on the passive decoy-state method is considered. We introduce and analyze the unbalanced Mach–Zehnder interferometer, briefly, and combining with the virtual source and imaginary unitary transformation, we characterize the passive decoy-state method using a weak coherent photon source with modulator attenuation. According to the attenuation parameter $\delta$, the pass efficiencies are given. Then, the key generation rate can be acquired. From numerical simulations, it can be seen that modulator attenuation has a non-negligible influence on the performance of passive-state QKD protocol. Based on the research, the analysis method of virtual source and imaginary unitary transformation are preferred in analyzing passive decoy state protocol, and the passive decoy-state method is better than the active one and is close to the active vacuum + weak decoy state under the condition of having the same modulator attenuation.

**Keywords:** quantum key distribution, passive decoy state, modulator attenuation, weak coherent pulses

**PACS:** 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/24/11/110307

## 1. Introduction

Quantum key distribution (QKD)[1,2] allows two legal communication parties, Alice and Bob, to establish a common and secret key when the channel is accessible to an eavesdropper, Eve. It is an important part of quantum cryptography. Compared with the classical cryptography, the biggest advantage of quantum cryptography is the unconditional security which is based on the fundamental laws of physics: no-cloning theorem and uncertainty principle.[3]

Since Bennett and Brassard proposed the best-known protocol—BB84 protocol,[1] quantum cryptography has developed well both theoretically and experimentally.[4–11] The unconditional security of QKD protocol was given by Lo H K and Chau H F,[12] first. It was based on the situation that Alice and Bob both have the quantum computers, which is still commercially unavailable with current technology. Hence, people wanted to find some other ways to prove the unconditional security. Shor P and Preskill J[5] gave the proof that the security of QKD protocol based on state preparation and state measurement is equal to that of QKD protocol based on entanglement purification. Combined with the CSS (Calderbank–Shor–Steane) codes and entanglement purification, the unconditional security can be proven by current correction technology. Renner *et al.*[13] used the information theory to prove the unconditional security which gives the upper bound of the amount of information that Eve can get. In 2008, Horodecki *et al.*[14] first proved that QKD protocol can generate a security key when there is no entanglement purification.

The proofs of the unconditional security of QKD protocol are based on the ideal condition.[15] This means the single-photon source, the perfect detector, the safe and credible channel, and so on. However, in the real situation, the conditions mentioned before are not easy to satisfy. There are many unavoidable imperfections in a practical QKD system like multi-photon pulse, attenuation of detector, non-authenticated channel, and finite resources. They undoubtedly threaten the security of QKD. Therefore, researching the impact of the factors in real conditions on the security of QKD system is important.

To analyze the influencing factors as mentioned, some researchers improved the original protocols or presented new protocols such as decoy-state protocol[16–20] and device-independent QKD (DI-QKD).[21–31] Some other researchers used the mathematical and information knowledge to characterize the impact of the imperfect factors on the security of QKD by a security proof.

In this paper, we analyze the security of the passive decoy-state method[32,33] based on the phase-coding protocol[34] under the condition of modulator attenuation. The phase-coding protocol where the unbalanced Mach–Zehnder interferometer (UMZI)[35,36] is commonly used is more stable than the polarization one. The UMZI is composed of two parts: a long arm and a short arm. In the ideal station, we con-

*Project supported by the National Natural Science Foundation of China (Grant No. 11304397).
†Corresponding author. E-mail: 2010thzz@sina.com
© 2015 Chinese Physical Society and IOP Publishing Ltd 

sider that the attenuation of the short arm is equal to that of the long arm. However, due to the imperfect phase modulator (PM) in the long arm, it will introduce more loss than the short arm. The security of QKD system is affected.

Currently, the method for analyzing modulator attenuation is mainly to establish a new model to replace the original actual phase modulator. The new model is more easy to analyze. In 2010, Li *et al.*[37] presented imaginary unitary transformation and virtual source to analyze the security of BB84 protocol. Ferenczi *et al.*[38] provided a qubit-based security proof on unbalance BB84 protocol. In this paper, the imaginary unitary transformation and virtual source model are introduced to the passive decoy-state method, and the security of passive decoy-state method with modulator attenuation is also analyzed.

The rest of this paper is organized as follows: In Section 2 and Section 3, we introduce the decoy-state protocol and the WCP source that can be used in the passive decoy-state method, respectively. In Section 4, we recall the UMZI model and analyze it with the method that using a perfect PM and an unbalanced attenuator replace the imperfect PM. We consider the passive decoy-state method with imaginary unitary transformation and virtual source under the modulator attenuation condition in Section 5. Finally, Section 6 gives a summary of this paper.

## 2. Decoy state protocol

It has been noted that the necessary assumptions that the ideal QKD system needs are not easy to satisfy. In the original proposal of the BB84 protocol, a single-photon source is necessary. However, the single-photon source is still unavailable with the current technology. A weak coherent pulse (WCP) source was used instead and many WCP-based experiments have been done since the first QKD experiment.[39] However, due to the multiphoton pulses sent by WCP source, the QKD system will suffer from photon-number splitting (PNS) attack.[40,41] To protect QKD system from PNS attack, one can use the decoy-state method which could closely reach the performance of single-photon sources. Actually, the initial decoy-state method can be called active decoy-state method in which Alice prepares the decoy states actively. However, due to the "active" process, it may bring some side channel information that Eve can make use of to have an attack. For the real active (regular) decoy-state experiments, it is more difficult to verify the assumption that Eve cannot distinguish decoy and signal states.[42]

To solve this problem, the passive decoy-state method was presented. It can reduce the side channel information in the decoy-state preparation procedure. Different from the active decoy-state method which actively changes the intensity of the laser pulses randomly, the passive decoy-state method only has one intensity pulse. The key point to distinguish in the passive decoy-state method is clicking or no clicking for Alice's detector.

The common point between the passive decoy state and the active decoy state is that the counting rates and the error rates of the pulse of the same photon-number states from the signal states and the decoy states shall be equal to each other,[17]

$$Y_m = Y'_m, \quad e_m = e'_m, \tag{1}$$

where $Y_m$ and $Y'_m$ denote the counting rates of $m$ photons from signal states and decoy states, respectively, and $e_m$ and $e'_m$ denote the error rates of $m$ photons from signal states and decoy states, respectively.

In 2005, Lo *et al.*[17] combined the decoy state method with the results provided by the Gottesman–Lo–Lütkenhaus–Preskill (GLLP)[6] analysis and gave the exact formula for secure key generation rate as follows:

$$R \geq \sum_l \max\left\{R^l, 0\right\}, \tag{2}$$

where $R^l$ satisfies

$$R^l \geq q\left\{p_0^l Y_0 + p_1^l Y_1 \left[1 - H_2\left(e_1\right)\right] - Q^l f\left(E^l\right) H_2\left(E^l\right)\right\}. \tag{3}$$

The parameter $q$ is the efficiency of the protocol. For the standard BB84 protocol,[1] $q = 1/2$, $f\left(E^l\right)$ denotes the efficiency of the error correction protocol as a function of the error rate $E^l$,[43] typically $f\left(E^l\right) \geq 1$ with Shannon limit $f\left(E^l\right) = 1$ (usually, we set 1.22 as its approximate value), $e_1$ denotes the single photon error rate, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

In this paper, we define that $c$ denotes "click" of the detector while $\bar{c}$ denotes "no click". We denote the signals that cause a click of Alice's detector as signal states. The ones that cause no click of Alice's detector are decoy states.

## 3. Transformed WCP source that is used for the passive decoy-state method

Due to the characters of the WCP source itself, it cannot be used for the passive decoy-state method directly. Curty *et al.*[42,45] have adjusted the WCP source to make it output two Fock diagonal states, so that it can be used for the passive decoy-state method. The fundamental setups are shown as follows.

In Fig. 1, $\rho$ and $\sigma$ denote the coherent states of two phase-randomized WCP source states, respectively,

$$\rho = \mathrm{e}^{-\mu_1} \sum_{n=0}^{\infty} \frac{\mu_1^n}{n!} |n\rangle\langle n|, \tag{4}$$

$$\sigma = \mathrm{e}^{-\mu_2} \sum_{n=0}^{\infty} \frac{\mu_2^n}{n!} |n\rangle\langle n|, \tag{5}$$

with $\mu_1$ and $\mu_2$ denoting the mean photon numbers of the two signals, respectively. It should be noted that the WCP source that Curty *et al.* have changed is phase-randomized WCP. Without additional explanations, the WCP source mentioned throughout this paper is the source which is shown in Fig. 1. We consider the threshold detector as the photon-detector in Fig. 1. In this scenario, the joint probability of having $n$ photons in output mode $a$ and $m$ photons in output mode $b$ can be written as[45]

$$p_{n,m} = \frac{\upsilon^{n+m}\mathrm{e}^{-\upsilon}}{n!m!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n(1-\gamma)^m\mathrm{d}\theta, \tag{6}$$

where the parameters $\upsilon$, $\gamma$, and $\xi$ are given by

$$\begin{aligned}\upsilon &= \mu_1+\mu_2,\\ \gamma &= \frac{\mu_1 t+\mu_2(1-t)+\xi\cos\theta}{\upsilon},\\ \xi &= 2\sqrt{\mu_1\mu_2(1-t)t},\end{aligned} \tag{7}$$

and $t$ denotes the transmittance of a beam splitter.

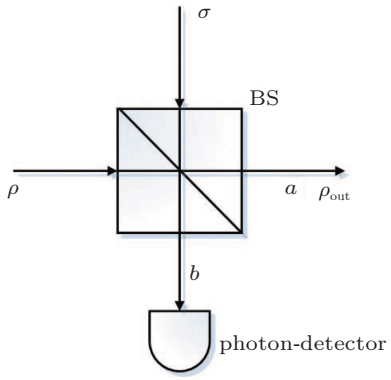



**Fig. 1.** The WCP sources[42,45] that are used for passive decoy-state method.

Whenever the sender, Alice, does not protect the result of the measurement in mode $b$, the probability of having $n$ photons in mode $a$ can be written as

$$p_n^t = \sum_{m=0}^{\infty} p_{n,m} = \frac{\upsilon^n}{n!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n\mathrm{e}^{-\upsilon\gamma}\mathrm{d}\theta. \tag{8}$$

For Alice's detector, the joint probability of having $n$ photons in mode $a$ and no click in the threshold detector now has the form

$$\begin{aligned}p_n^{\bar{c}} &= (1-\varepsilon)\sum_{m=0}^{\infty}(1-\eta_{\mathrm{d}})^m p_{n,m}\\ &= (1-\varepsilon)\frac{\upsilon^n\mathrm{e}^{-\eta_{\mathrm{d}}\upsilon}}{n!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n\mathrm{e}^{-(1-\eta_{\mathrm{d}})\upsilon\gamma}\mathrm{d}\theta,\end{aligned} \tag{9}$$

where the parameter $\varepsilon$ denotes dark count and $\eta_{\mathrm{d}}$ denotes the detection efficiency of the detector.

Then, the probability of having $n$ photons in mode $a$ and producing a click in Alice's threshold detector is

$$p_n^c = p_n^t - p_n^{\bar{c}}. \tag{10}$$

## 4. Unbalanced Mach–Zehnder interferometer and simple analysis

Currently, the practical QKD systems can be divided into phase-coding protocol[34] and polarization protocol. For comparison, the phase-coding protocol is more stable than the polarization one. Unbalanced Mach–Zehnder interferometer[35,36] (UMZI) is commonly used. The fundamental setups are shown in Fig. 2.

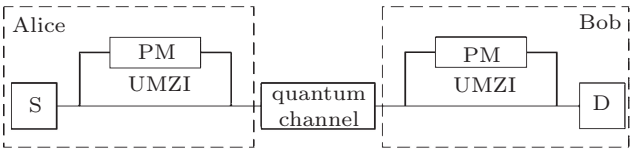



**Fig. 2.** The quantum part of the QKD setup with unbalanced Mach–Zehnder interferometer.

UMZI is composed of a long arm and a short arm, where the long arm has a phase modulator (PM). In the proof of QKD's security, it is assumed that the attenuation of the long arm is equal to the one of the short arm, and Alice's attenuation has no effect on the security of QKD system. Bob's attenuation can belong to the attenuation of the channel. Theoretically, they do not affect the secure key generation of QKD. However, the practical PM in the long arm will introduce more loss, so that the attenuations are not equal. Under this condition, the photon states emitted from Alice are imperfect BB84 states. In this case, the key generation rate and security of QKD will be affected.

From Fig. 2, we can see that the photon states entering the quantum channel can be divided into photon states from the short arm and long arm, respectively. After the phase modulation of Bob's side, the two photon states are divided into four photon states. In this paper, we consider that the phase of the photon from the long arm is randomly modulated by 0, $0.5\pi$, $\pi$ or $1.5\pi$ in Alice's side. Because only the single photon state transmitted in the quantum channel can be used, the practical single photon state is

$$\begin{aligned}&\frac{1}{\sqrt{\mu_{\mathrm{s}}+\nu_{\mathrm{l}}}}\left(\sqrt{\mu_{\mathrm{s}}}|1\rangle_{\mathrm{s}}+\sqrt{\nu_{\mathrm{l}}}|1\rangle_{\mathrm{l}}\right),\\ &\frac{1}{\sqrt{\mu_{\mathrm{s}}+\nu_{\mathrm{l}}}}\left(\sqrt{\mu_{\mathrm{s}}}|1\rangle_{\mathrm{s}}+\mathrm{i}\sqrt{\nu_{\mathrm{l}}}|1\rangle_{\mathrm{l}}\right),\\ &\frac{1}{\sqrt{\mu_{\mathrm{s}}+\nu_{\mathrm{l}}}}\left(\sqrt{\mu_{\mathrm{s}}}|1\rangle_{\mathrm{s}}-\sqrt{\nu_{\mathrm{l}}}|1\rangle_{\mathrm{l}}\right),\\ &\frac{1}{\sqrt{\mu_{\mathrm{s}}+\nu_{\mathrm{l}}}}\left(\sqrt{\mu_{\mathrm{s}}}|1\rangle_{\mathrm{s}}-\mathrm{i}\sqrt{\nu_{\mathrm{l}}}|1\rangle_{\mathrm{l}}\right),\end{aligned} \tag{11}$$

where $|1\rangle_{\mathrm{s}}$ denotes the single-photon state in the short arm. $|1\rangle_{\mathrm{l}}$ denotes the single-photon state in the long arm after PM,

and $\mu_s$ is the average source intensity of the short arm, and $\nu_l$ is the average source intensity of the long arm after PM.

As mentioned, the attenuation of the long arm is equal to the one of the short arm in the proof of QKD's security, i.e. $\mu_s = \nu_l$. Due to the imperfection of the devices, the attenuation of the long arm is larger than that of the short arm. Therefore, $\mu_s > \nu_l$. We call the photon states emitted from Alice unbalanced states.

A simple analytical model is replacing the practical PM in the long arm by a perfect PM and an unbalanced attenuator.[37]

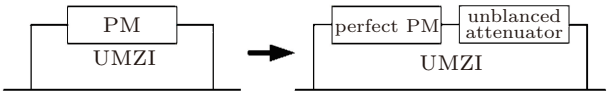



**Fig. 3.** A perfect PM and an unbalanced attenuator.

The loss from the practical PM can belong to the unbalanced attenuator. Based on this, two hypotheses are: (i) The unbalanced attenuator can be controlled by the eavesdropper, Eve. (ii) The single-photon states emitted by Alice are ideal BB84 states. Based on the above assumptions, we can get the key generation rate

$$R \geq 10^{-\alpha d/10} S P_A P_B, \tag{12}$$

where $S$ is the probability distribution of the single-photon states when we consider that Alice's PM is perfect, $\alpha$ denotes the loss coefficient of the quantum channel, $d$ represents the transmission distance, $P_A$ and $P_B$ are the pass efficiencies of Alice and Bob, respectively. Usually, they can be written as $P_A = (\mu_s + \nu_l)/2\mu$ and $P_B = \nu_l/(\mu_s + \nu_l)$. Theoretically, we consider that only the single-photon state emitted by Alice can generate the key bit. The multi-photon state has no contributions to the key generation. Note that the single-photon states attenuated from the multi-photon states by the unbalanced attenuator also cannot be used to generate the key bit. Combining the two hypotheses, the final key generation rate is low.

## 5. Passive decoy-state method with imaginary unitary transformation and virtual source

In this section, the idea of imaginary unitary transformation and virtual source[37] is introduced. Combined with the passive decoy-state method, we consider the influence on the security of the passive decoy-state method under the condition of modulator attenuation. Firstly, we will introduce imaginary unitary transformation and virtual source briefly. The fundamental setups are shown in Fig. 4. Reference [37] has proved that the practical photon states, i.e., the states in Eq. (11), are as secure as the perfect BB84 state when considering the practical state is equal to the perfect BB84 state combining with a unitary transformation.

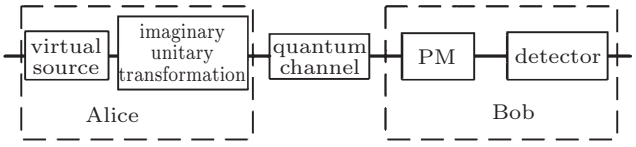



**Fig. 4.** The quantum part of the QKD setup with imaginary unitary transformation and virtual source.

Unitary transformation does not change the inner product of vectors, the eigenvalues or the eigenvectors of the matrix. An important application of unitary transformation in quantum mechanics is converted between different representations. The unitary transformation in Fig. 4 is a virtual structure, so there is no need to implement it in the practical QKD experiment. The unitary transformation is given as follows:

$$\begin{aligned}
&U|0\rangle_l|0\rangle_s|0\rangle_A = |0\rangle_l|0\rangle_s|0\rangle_A,\\
&U|0\rangle_l|1\rangle_s|0\rangle_A = |0\rangle_l|1\rangle_s|0\rangle_A,\\
&U|1\rangle_l|0\rangle_s|0\rangle_A = \frac{\sqrt{\nu_l}}{\sqrt{\mu_s}}|1\rangle_l|0\rangle_s|0\rangle_A + \frac{\sqrt{\mu_s-\nu_l}}{\sqrt{\mu_s}}|0\rangle_l|0\rangle_s|1\rangle_A,\\
&U|n\rangle_l|m\rangle_s|0\rangle_A = |n\rangle_l|m\rangle_s|0\rangle_A, m+n \geq 2,
\end{aligned} \tag{13}$$

where $|0\rangle_A$ and $|1\rangle_A$ are mutually orthogonal states in Alice's side. They are emitted randomly. Alice does not know each state, and $|n\rangle_s$ and $|n\rangle_l$ denote the $n$-photon states in the short arm and the long arm, respectively, $n$ means the number of the photon.

From Eq. (13), it can be seen that the unitary transformation does not change the vacuum state, multi-photon state, and single-photon state in the short arm. However, the single-photon state will be $|1\rangle_l|0\rangle_s|0\rangle_A$ with a probability of $\nu_l/\mu_s$ and $|0\rangle_l|0\rangle_s|1\rangle_A$ with a probability of $(\mu_s - \nu_l)/\mu_s$ after the unitary transformation.

Similar to Section 4, the average source intensity is changed from $2\mu_s$ to $\mu_s + \nu_l$ because of the imaginary unitary transformation. Therefore, the pass efficiency of the imaginary unitary transformation is $P_U = (\mu_s + \nu_l)/2\mu_s$.

In the model of imaginary unitary transformation and virtual source, the practical photon states in the quantum channel are regarded as the perfect BB84 states emitted by the virtual source and changed by unitary transformation.

After the phase randomization, the density matrix of the virtual source is

$$\begin{aligned}
&\phi_n = A_n|0\rangle_s|0\rangle_l\langle 0|_s\langle 0|{A_n}^+,\\
&A_1 = \left(\frac{1}{\sqrt{2}}a_s^+ + e^{i\varphi}\frac{1}{\sqrt{2}}a_l^+\right),\\
&A_n = \left(\frac{\sqrt{\mu_s}}{\sqrt{\mu_s+\nu_l}}a_s^+ + e^{i\varphi}\frac{\sqrt{\nu_l}}{\sqrt{\mu_s+\nu_l}}a_l^+\right)^n, \quad n \neq 1.
\end{aligned} \tag{14}$$

In this paper, the source considered is the WCP source in Section 3, so the single photon state of the virtual source emitted by Alice's side is given by

$$p_1' = \frac{p_1^t}{P_U}. \tag{15}$$

The probability distribution multi-photon state of the virtual source can be respectively expressed by

$$p_n' = p_n^t, \ \ (n \geq 2). \tag{16}$$

Next, we will analyze the key generation rate combining with passive decoy-state method.

From Eqs. (6)–(8), we can find that the joint probabilities are determined by the initial intensities $\mu_1$ and $\mu_2$, and it is difficult to obtain $\mu_1$ and $\mu_2$ from $\mu_s$ and $v_1$. To calculate the final key generation rate, we introduce a modulator attenuation parameter $\delta$. Its expression is

$$\delta = \frac{v_1}{\mu_s}. \tag{17}$$

Then, the pass efficiencies of Alice and Bob can be regarded as the function of $\delta$.

The distinction between signal state and decoy state is determined by the results of the detector in Alice's side

$$P_{\bar{c}} = \sum_{n=0}^{\infty} p_n^{\bar{c}} = (1-\varepsilon)\,\mathrm{e}^{-\eta_d[\mu_1(1-t)+\mu_2 t]} I_{0,\eta_d\xi}, \tag{18}$$

$$P_c = 1 - P_{\bar{c}}, \tag{19}$$

where $\varepsilon$ represents the dark count, $\eta_d$ denotes the detection efficiency of the detector, $t$ is the transmittance of a beam splitter. In this paper, $t = 1/2$, $I_{a,b}$ is the modified Bessel function of the first kind,[41]

$$I_{a,b} = \frac{1}{2\pi \mathrm{i}} \oint \mathrm{e}^{(b/2)(t+1/t)} t^{-a-1}\,\mathrm{d}t. \tag{20}$$

The $Q^c$ and $Q^{\bar{c}}$ are the overall gains of Alice's detector producing a click and no click, respectively, $Q^t$ denotes the overall gain that Alice ignores the result of her measurement in mode $b$. They can be expressed by

$$Q^{\mathrm{t}} = 1-(1-Y_0)\,\mathrm{e}^{-\eta_{\mathrm{sys}}\omega} I_{0,\eta_{\mathrm{sys}}\xi}, \tag{21}$$

$$Q^{\bar{c}} = P_{\bar{c}} - (1-\varepsilon)(1-Y_0)\, e^{(\eta_d-\eta_{\mathrm{sys}})\omega-\eta_d v} I_{0,(\eta_d-\eta_{\mathrm{sys}})\xi}, \tag{22}$$

$$Q^c = Q^t - Q^{\bar{c}}. \tag{23}$$

Correspondingly, the error rates can be acquired as

$$E_{\mathrm{t}} = \left(e_0 - e_d\right) Y_0/Q_{\mathrm{t}} + e_d, \tag{24}$$

$$E_{\bar{c}} = \left(e_0 - e_d\right) Y_0 P_{\bar{c}}/Q_{\bar{c}} + e_d, \tag{25}$$

$$E_c = E_{\mathrm{t}} - E_{\bar{c}}, \tag{26}$$

where $\omega = \mu_1 t + \mu_2(1-t)$, $\eta_{\mathrm{sys}}$ denotes the overall transmittance of the system. It can be written as $\eta_{\mathrm{sys}} = P_A P_B \eta_{\mathrm{channel}} \eta_{\mathrm{Bob}}$, $P_A$ and $P_B$ represent the pass efficiencies of Alice and Bob, respectively, $\eta_{\mathrm{Bob}}$ is the overall transmittance of Bob's detection apparatus, $\eta_{\mathrm{channel}}$ can be related to a transmission distance $d$ measured in km for the given QKD schemes as

$$\eta_{\mathrm{channel}} = 10^{-\alpha d/10},$$

where $\alpha$ represents the loss coefficient of the channel measured in dB/km.

In the ideal station, $P_A = 1$ and $P_B = 1/2$. However, they will change under the real condition. Here, we can see the essence of the modulator attenuation. The additional loss coming from the modulator of the long arm weakens the pulses, so that the pass efficiencies of Alice and Bob are changed. After all, the overall transmittance of the system is affected.

According to the GLLP formula, we can get the key generation rate as

$$R^c \geq q\left\{Q_{1,c}\left[1-H_2\left(e_1\right)\right] - Q_c f\left(E_c\right) H_2\left(E_c\right)\right\}. \tag{27}$$

Due to the contributions of the decoy state in the passive decoy-state method, the key generation rate of the decoy state needs to be calculated

$$R^{\bar{c}} \geq q\left\{Q_{1,\bar{c}}\left[1-H_2\left(e_{1,\bar{c}}\right)\right] - Q_{\bar{c}} f\left(E_{\bar{c}}\right) H_2\left(E_{\bar{c}}\right)\right\}. \tag{28}$$

Finally, the key generation rate of the passive decoy-state method is

$$R = \max\left\{R^c, 0\right\} + \max\left\{R^{\bar{c}}, 0\right\}. \tag{29}$$

## 6. Numerical simulations

In this section, some numerical simulations are taken to show how modulator attenuation influences the final key generation rate. In this scenario, the yield of $n$-photon state can be expressed as[17,20]

$$Y_n = 1-(1-Y_0)\left(1-\eta_{\mathrm{sys}}\right)^n. \tag{30}$$

We set $\mu_1 = 0.5$ and $\mu_2 = 0.0001$. The other experimental QKD parameters are shown in Table 1. which come from Ref. [47].

**Table 1.** Experimental QKD parameters.

| $\alpha$/dB·km$^{-1}$ | $\eta_{\mathrm{Bob}}$ | $e_d$ | $Y_0$ | $\eta_d$ | $\upsilon$ |
|---|---|---|---|---|---|
| 0.21 | 0.045 | 0.033 | $1.7\times10^{-6}$ | 0.12 | $3.2\times10^{-7}$ |

First, we will give a simulation of the passive decoy-state method in the ideal station. In this case, the PM in the long arm of UMZI will not introduce extra attenuation which means $v_1 = \mu_s$ and $\delta = 1$, so the pass efficiencies of Alice: $P_A = 1$. For the phase-coding QKD protocol, only the interfering pulses, which produce clicks in the middle time ($t_2$ in Fig. 5), are used for the key generation. The pass efficiencies of Bob: $P_B = 1/2$.

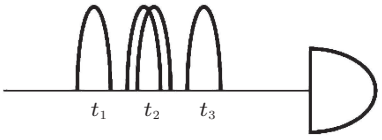



**Fig. 5.** The interfering pulses.

Then, we will simulate the method of replacing the practical PM in the long arm by a perfect PM and an unbalanced attenuator. Comparing with the virtual source, we also combine the method with the passive decoy-state method. In this case, due to the unbalanced attenuator, $P_A = (\mu_s + \nu_l)/2\mu_s$ and $P_B = \nu_l/(\nu_l + \mu_s)$. It should be noted that we assume that the unbalanced attenuator can be controlled by Eve, so when we calculate the probability distributions of $n$-photon state, $\nu_l = \mu_s$. Figure 6 gives the relationships between $R$ and $d$ of $\delta = 1/2, 1/3, 1/4$, respectively. The curve of $\delta = 1$ denotes the ideal condition.

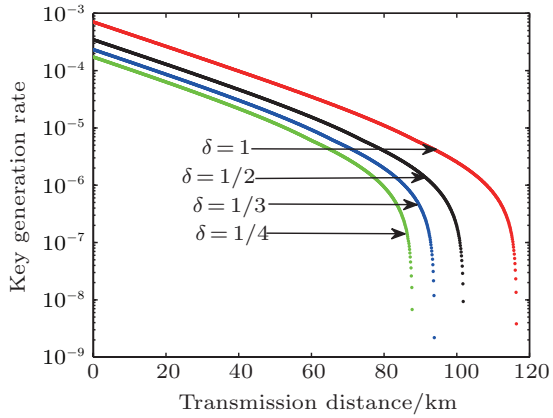



**Fig. 6.** (color online) The relationship between key generation rate ($R$) and the transmission distance ($d$) of the passive decoy-state method under the analysis of replacing the practical PM by a perfect PM and an unbalanced attenuator.

Next, we shall give the numerical simulations of the passive decoy-state method with the method of imaginary unitary transformation and virtual source. In this case, we consider the practical PM which would introduce extra attenuation to the QKD system, so $\nu_l < \mu_s$. It has been mentioned that the practical photon states in the quantum channel can been regarded as the perfect BB84 states emitted by the virtual source and changed by unitary transformation. Combined with the nature of unitary transformation, $P_A$ is equal to 1. $P_B = \nu_l/(\nu_l + \mu_s)$. Figure 7 shows the relationship between $R$ and $d$ of $\delta = 1/2, 1/3, 1/4$, respectively. Similarly, the curve of $\delta = 1$ denotes the ideal condition.

We compare the above cases when $\delta = 1/3$. To get a better result, we define $R(\delta)/R$ as the fidelity of the passive decoy-state method considering modulator attenuation, where $R(\delta)$ and $R$ are the key generation rates with and without modulator attenuation.

According to Figs. 8 and 9, we can find that no matter which analytical method is chosen, the modulator attenuation will affect the key generation rate and transmission distance of practical QKD system. Comparing with the methods of unbalanced attenuator and virtual source, it shows that the method of virtual source is better than the method of unbalanced attenuator in the key generation rate and transmission distance.

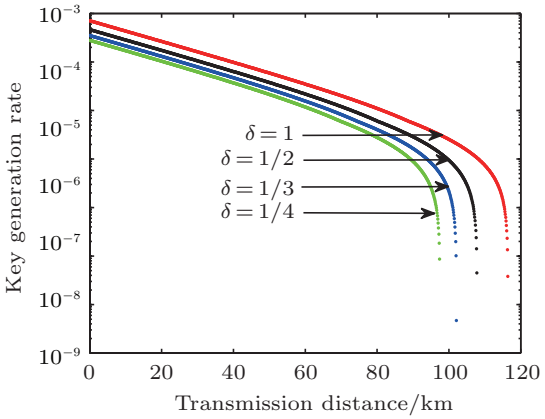



**Fig. 7.** (color online) The relationship between key generation rate ($R$) and the transmission distance ($d$) of passive decoy-state method under the analysis of imaginary unitary transformation and virtual source.

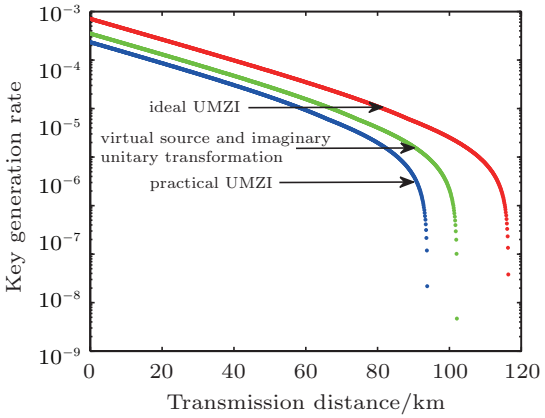



**Fig. 8.** (color online) The relationship between key generation rate ($R$) and the transmission distance ($d$) of passive decoy-state method under different conditions.

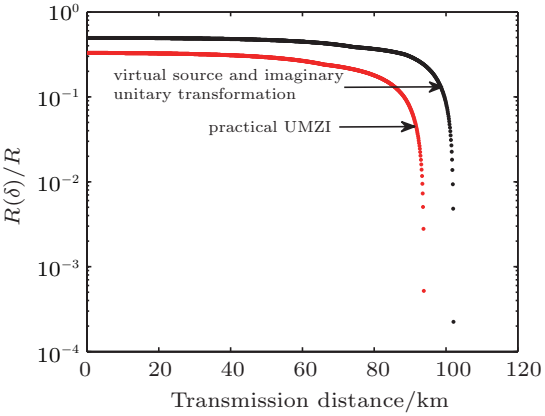



**Fig. 9.** (color online) The relationship between $R(\delta)/R$ and the transmission distance ($d$) of passive decoy-state method under different conditions.

Finally, we give the comparison of the $R(\delta)/R$ versus transmission distance among the one decoy-state, vacuum + weak decoy-state, and passive decoy-state methods when $\delta = 1/3$. Figure 10 shows the answer. Based on Fig. 10, it can be seen that the passive decoy-state method is better than the active one decoy state when the extreme transmission distance is taken into consider. The $d$ of the passive decoy-state method is a little smaller than that of the vacuum + weak decoy-state. If $d > 60$ km, the fidelity $R(\delta)/R$ of the passive decoy-state method is larger than the one of one decoy-state and is close to the $R(\delta)/R$ of vacuum + weak decoy-state. In a word, the passive decoy-state method is better than the one decoy-state and is close to the vacuum + weak decoy-state.

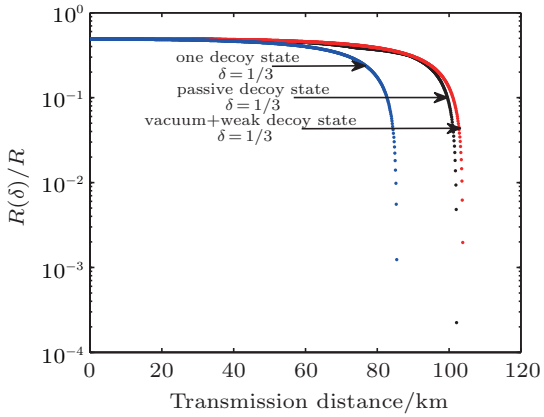



**Fig. 10.** (color online) The relationships between $R(\delta)/R$ and the transmission distance ($d$) of passive decoy-state method, one decoy-state and vacuum + weak decoy-state.

## 7. Conclusions

In summary, the passive decoy-state method with WCP source in the case of modulator attenuation is considered. Two safety equivalent models were used to analyze the attenuation of UMZI. One is replacing the practical PM in the long arm by a perfect PM and an unbalanced attenuator. The other one is an imaginary unitary transformation and virtual source. They were compared with the ideal situation and different attenuations. According to the numerical simulations, it seems that modulator attenuation has a non-negligible influence on the final key rate of the passive decoy-state QKD protocol with WCP source. The larger the attenuation is, the smaller the key generation rate and extra transmission distance are. Besides, evidence shows that the analytical method of virtual source is better than the unbalanced attenuator one both in the key generation rate and transmission distance. Moreover, comparing with the active one decoy-state and the active vacuum + weak decoy-state methods, the result shows that the passive decoy-state method is better than the active one decoy state and is close to the active vacuum + weak decoy state under the condition of having the same modulator attenuation. The conclusions can be used for the actual operation of QKD systems.

## References


[1] Bennett C H and Brassard G 1984 *IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE) pp. 175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) Chaps. 2 and 12
[4] Lo H K and Chau H F 1990 *Science* **283** 2050
[5] Shor P and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[6] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[7] Wang S, Chen W, Guo J F and Yin Z Q 2012 *Opt. Lett.* **37** 1008
[8] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photonics* **7** 378
[9] Wang J Y 2013 *Nat. Photonics* **7** 387
[10] Zhao L Y, Li H W, Yin Z Q, Chen W, You J and Han Z F 2014 *Chin. Phys. B* **23** 100304
[11] Li M, Treeviriyanupab P, Zhang C M, Yin Z Q, Chen W and Han Z F 2015 *Chin. Phys. B* **24** 010302
[12] Lo H K and Chau H F 1999 *Science* **283** 5410
[13] Renner R 2005 *Security of Quantum Key Distribution* (PhD thesis) quant-ph/0512258
[14] Horodecki K, Horodecki M, Horodecki P, Leung D and Oppenheim J 2008 *IEEE Transactions on Information Theory* **54** 2604
[15] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[16] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[17] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[18] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[19] Wang X B 2005 *Phys. Rev. A* **72** 012322
[20] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[21] Acin A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[22] Gisin N, Pironio S and Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501
[23] Pawlowski M and Brunner N 2011 *Phys. Rev. A* **84** 010302
[24] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[25] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[26] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307
[27] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319
[28] Zhou C, Bao W S, Chen W, Li H W, Yin Z Q, Wang Y and Han Z F 2013 *Phys. Rev. A* **88** 052333
[29] Li F Y, Yin Z Q, Li H W, Chen W, Wang S, Wen H, Zhao Y B and Han Z F 2014 *Chin. Phys. Lett.* **31** 070302
[30] Dong C, Zhao S H, Zhang N, Dong Y, Zhao W H and Liu Y 2014 *Acta Phys. Sin.* **63** 200304 (in Chinese)
[31] Dong C, Zhao S H, Dong Y, Zhao W H and Zhao J 2014 *Acta Phys. Sin.* **63** 170303 (in Chinese)
[32] Mauerer W and Silberhorn C 2007 *Phys. Rev. A* **75** 050305(R)
[33] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 *Phys. Rev. Lett.* **99** 180503
[34] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[35] Mo X F, Zhu B, Han Z F, Gui Y Z and Guo G C 2005 *Opt. Lett.* **30** 2632
[36] Han Z F, Mo X F, Gui Y Z and Guo G C 2005 *Appl. Phys. Lett.* **86** 221103
[37] Li H W, Yin Z Q, Han Z F, Bao W S and Guo G C 2010 *Quantum Inf. Comput.* **10** 0771
[38] Ferenczi A, Narasimhachar V and Lütkenhaus N 2012 *Phys. Rev. A* **86** 042327
[39] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J A 1992 *J. Cryptol.* **5** 3
[40] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863
[41] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[42] Curty M, Morder T, Ma X and Lutkenhaus N 2009 *Opt. Lett.* **34** 3238
[43] Brassard G and Salvail L 1993 *Proceedings of Advances in Cryptology-EUROCRYPT'93, Lofthus, Norway,* 1993, *Lecture Notes in Computer Science* (New York: Springer) p. 410
[44] Ma X and Lo H K 2008 *New J. Phys.* **10** 073018
[45] Curty M, Ma X, Qi B and Moroder T 2010 *Phys. Rev. A* **81** 022310
[46] Arfken G 1985 *Mathematical Mehthods for Physicists* (3rd edn.) (New York: Academic)
[47] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762