Practical security of wavelength-multiplexed decoy-state quantum key distribution

Liang-Yuan Zhao,[1,2,3,*] Qian-Jun Wu,[1] Hong-Kang Qiu,[1] Jian-Lin Qian,[2] and Zheng-Fu Han[3]

[1] *Jiangsu Hengtong Qasky Quantum Information Research Institute Co., Ltd., Suzhou, Jiangsu 215200, China*
[2] *Jiangsu Hengtong Optic-Electric Co., Ltd., Suzhou, Jiangsu 215200, China*
[3] *Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei, Anhui 230026, China*

(Received 23 March 2020; accepted 13 January 2021; published 26 February 2021)

Wavelength division multiplexing (WDM) of quantum key distribution (QKD) with classical optical channels has been proven to be feasible experimentally. In this paper, we will analyze the practical security of WDM-QKD theoretically. Specifically, we first establish the noise model of classical signals. Then, the influence of classical noises on the performance of decoy-state WDM-QKD is studied with a finite-key security analysis. For numerical simulations, the effect of classical noise-reduction methods for different experimental settings is given. The secret key rate and maximum transmission distance of WDM-QKD is simulated with various sent number of quantum pulses or transmitted power of classical signals. Furthermore, the performance of two kinds of decoy-state WDM-QKD is compared, which shows that the optimal decoy-state protocol for WDM-QKD is related to the sent number of quantum pulses. Since WDM-QKD is desired to reduce the cost of QKD networks and since experiments have already been carried out, our work can not only close the gap between theory and practice, but also be used to optimize the experimental parameters and improve its performance.

DOI: 10.1103/PhysRevA.103.022429

I. INTRODUCTION

Quantum key distribution (QKD) can make two legal users, e.g., Alice and Bob, share a string of common true random bits which is theoretically safe against an eavesdropper Eve with unconditional security. For QKD to work normally, quantum signals are usually transmitted in a separate fiber in practice as the power of classical signals is strong, which otherwise would generate noises to seriously reduce the signal-to-noise ratio of QKD.

The fact that quantum signals transmit separately with classical signals makes the cost and difficulty increase when a QKD network is deployed. To overcome the damage caused by classical signals to QKD in the same fiber, much effort has been made since the first demonstration of the feasibility of the coexistence of O-band (∼1310 nm) quantum signals and C-band (∼1550 nm) classical signals by Townsend in 1997 [1]. With the lower loss of the C-band optical signal in fiber communication, both signals were then merged into one fiber at the C-band simultaneously using wavelength division multiplexing (WDM) technology [2–5]. Moreover, the classical channel can be encrypted by a quantum key produced by the accompanying QKD [6,7]. Recently, field trials for the coexistence of quantum and classical signals have been conducted around the world [8–10] with the increase of classical signals power [7,11] and secure transmission distance [12], which boost the large-scale deployment of QKD in existing telecommunication networks.

In a WDM-QKD system, classical signals can cause various types of noise due to the linear or nonlinear interactions with fiber. Although the noises may have little influence on classical communication, it cannot be ignored for the implementation of QKD. Based on previous research, the classical channel crosstalk noise leaking into the quantum channel is the main source of out-band noise for QKD [2], while the spontaneous Raman scattering (SRS) and four-wave mixing (FWM) noises are the main in-band one [3,6]. Many methods that try to suppress these classical noises in WDM-QKD have been proposed and experimentally verified, such as reducing the power of classical signals [1], or spectral or temporal filtering in the QKD receiver [3,5,6,13]. However, there is lack of detailed analysis for the practical security of WDM-QKD in theory. To close the gap between theory and practice, here we give a strict secret key rate for WDM-QKD using finite-key security analysis. Moreover, the influence of classical noises on the performance of WDM-QKD is analyzed and simulated, which can be used in experiments.

In this paper, we first study the model of classical noises and their influence on decoy-state [14–16] WDM-QKD in Sec. II. Then, the finite-key security analysis of WDM-QKD is given in Sec. III. At last, in Sec. IV, we simulate and discuss the effect of classical noise-reduction methods and the performance of decoy-state WDM-QKD with different experimental settings.

II. NOISE MODEL OF THE WDM-BASED QKD

Before the evaluation of the practical security of WDM-QKD, we will model the noises caused by classical channels and show their influence. Here we consider both the out-band and in-band classical noises for WDM-QKD.

[*] zhaoly@htgd.com.cn

2469-9926/2021/103(2)/022429(10)

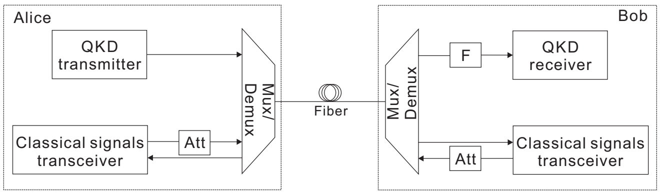


FIG. 1. Schematic of a general structure of WDM-QKD. ATT: optical attenuator; F: filter; Mux/Demux: wavelength division multiplexer or demultiplexer.

A. General structure of WDM-QKD

To model the classical noises, a general structure of the WDM-QKD setup is shown in Fig. 1. In the figure, the quantum channel and classical channel are integrated into one single fiber through the WDM technology. For reducing the strength of classical noises, the transmitted power of classical signals is adjustable so that both the QKD and classical communication systems can work normally. Furthermore, a filter with bandwidth $\Delta\lambda$ is placed before the QKD receiver which is used to isolate the classical noises. In the QKD receiver, the gate width τ_D of the single-photon detector (SPD) is adjusted to play the role of temporal filtering.

B. Classical channel crosstalk noise

As the isolation of the demultiplexer in Fig. 1 is limited, the photons of classical signals may leak into the quantum channel, which is the main source of out-band noise for QKD. The intensity of classical channel crosstalk noise at the output of the demultiplexer is given as

$$\begin{aligned} P_{\text{leak}} &= P(0)t_{\text{mux}}t_{AB}t_{\text{leak}}t_{\text{demux}} \\ &= P(0)10^{-\frac{I}{10}}10^{\frac{-\alpha_c L}{10}}10^{-\frac{\xi}{10}}10^{-\frac{I}{10}}, \end{aligned} \tag{1}$$

where $P(0)$ is the transmitted power of the classical signal at the multiplexer, I is the insertion loss of the multiplexer or demultiplexer, α_c is the fiber loss coefficient for the incident classical signals, L is the fiber length, and ξ is the isolation of the demultiplexer. Then, $t_{\text{mux}} = 10^{-\frac{I}{10}}$ and $t_{\text{demux}} = 10^{-\frac{I}{10}}$ are the transmittances of the multiplexer and demultiplexer, respectively, $t_{AB} = 10^{\frac{-\alpha_c L}{10}}$ is the fiber transmittance, and $t_{\text{leak}} = 10^{-\frac{\xi}{10}}$ is the ratio of crosstalk from the classical channel into the quantum channel.

Then, within the gate width τ_D of the SPD, the number of crosstalk noise photons that arrive at the QKD receiver after the filter is given by

$$N_{\text{leak}} = \frac{P_{\text{leak}}\tau_D t_F^c}{hf_c}, \tag{2}$$

where h is the Planck constant, f_c is the frequency of classical signals, and t_F^c is the transmittance of the filter for crosstalk noise. Therefore, the detection probability of crosstalk noise by the QKD receiver is

$$Y_{\text{leak}} = N_{\text{leak}}\eta_{\text{Bob}}^c, \tag{3}$$

where $\eta_{\text{Bob}}^c = t_{\text{Bob}}^c\eta_D^c$ is the transmittance of the QKD receiver with the internal transmittance of optical components t_{Bob}^c and SPD efficiency η_D^c for crosstalk noise.

C. Spontaneous Raman scattering noise

Based on the previous WDM-QKD experiments [3,5,6], it is known that the Raman scattering noise induced by the nonlinear interaction of classical signals with fiber is one of the main noise sources for QKD. As the transmitted power threshold for classical signals to trigger stimulated Raman scattering is usually not reached in a practical WDM system [17], we will only consider the effect of SRS in this paper. In Fig. 1, when quantum signals are transmitted in the same direction with classical signals, the power of SRS noise, i.e., forward SRS noise, at the output of the fiber is given by [6,18]

$$P_{\text{ram}}^f = \frac{10\beta P(0)t_{\text{mux}}\Delta\lambda}{(\alpha_r - \alpha_c)\ln 10}\left(10^{-\frac{\alpha_c L}{10}} - 10^{-\frac{\alpha_r L}{10}}\right), \tag{4}$$

where β and α_r are the normalized SRS cross section [6] and fiber loss coefficient at the wavelength of SRS noise, respectively. While the transmission directions of quantum signals and classical signals are opposite, the power of SRS noise, i.e., backward SRS noise, at the output of the fiber is given by [6,18]

$$P_{\text{ram}}^b = \frac{10\beta P(0)t_{\text{mux}}\Delta\lambda}{(\alpha_c + \alpha_r)\ln 10}\left(1 - 10^{-\frac{(\alpha_c+\alpha_r)L}{10}}\right). \tag{5}$$

If the frequencies of classical signals and SRS noises are near, i.e., $\alpha_c \approx \alpha_r$, the power of forward and backward SRS noises can be approximated to

$$\begin{aligned} P_{\text{ram}}^f &\approx \beta P(0)t_{\text{mux}}L\Delta\lambda 10^{-\frac{\alpha_r L}{10}}, \\ P_{\text{ram}}^b &\approx \frac{5\beta P(0)t_{\text{mux}}\Delta\lambda}{\alpha_r \ln 10}\left(1 - 10^{-\frac{\alpha_r L}{5}}\right). \end{aligned} \tag{6}$$

Note that only the photons of in-band SRS noises, which have the same frequency as quantum signals, can pass the filter in front of the QKD receiver efficiently. Therefore, within the gate width τ_D of SPD, the photon numbers of in-band forward and backward SRS noises arriving into the QKD receiver can be given by

$$N_{\text{ram}}^f = \frac{P_{\text{ram}}^f\tau_D t_{\text{demux}}t_F^r}{hf_r}, \quad N_{\text{ram}}^b = \frac{P_{\text{ram}}^b\tau_D t_{\text{demux}}t_F^r}{hf_r}, \tag{7}$$

where f_r and t_F^r are the frequency and transmittance of the filter for the in-band SRS noises. For the in-band case, there are $f_r \approx f_q, \alpha_r \approx \alpha_q$, and $t_F^r \approx t_F^q$, where f_q, α_q, and t_F^q are the frequency, fiber loss coefficient, and filter transmittance for quantum signals, respectively. Correspondingly, the detection probabilities of forward and backward in-band SRS noises are

$$Y_{\text{ram}}^f = N_{\text{ram}}^f\eta_{\text{Bob}}, \quad Y_{\text{ram}}^b = N_{\text{ram}}^b\eta_{\text{Bob}}, \tag{8}$$

where $\eta_{\text{Bob}} = t_{\text{Bob}}\eta_D$ is the transmittance of the QKD receiver with the internal transmittance of optical components t_{Bob} and SPD efficiency η_D for the in-band noise photons or quantum signals.

D. Four-wave mixing noise

When two or more classical channels are multiplexed into one fiber, the FWM effect arises due to the third-order nonlinearity of the fiber [19]. Assume the frequencies of three classical channels are f_i, f_j, and f_k, with $k \neq i, j$; the frequency of the noise generated through FWM is [19]

$$f_{ijk} = f_i + f_j - f_k, \tag{9}$$

which may fall into the quantum channel, resulting in in-band FWM noise. The peak power of the FWM noise at the output of the fiber is given by [20]

$$P_{ijk} = \frac{\eta_{ijk} D_{ijk}^2 \chi^2 P_i(0) P_j(0) P_k(0) t_{\text{mux}}^3 10^{-\frac{\alpha_c L}{10}}}{9\left(\frac{\alpha_c \ln 10}{10}\right)^2}\left(1 - 10^{-\frac{\alpha_c L}{10}}\right)^2, \tag{10}$$

where $D_{ijk} = 1, 3$, or 6 is the degeneracy factor which corresponds to three, two, or none of the involved frequencies being the same, χ is the nonlinear coefficient of the fiber, and $P_i(0)$, $P_j(0)$, and $P_k(0)$ are the transmitted powers of the classical signals. Since the impact of the FWM effect will decrease dramatically with the enlarging of channel spacing [17], we can only consider the classical signals with small channel spacing and make the fiber loss coefficients of three classical channels equal to α_c. η_{ijk} is the FWM efficiency, which is given by [20]

$$\eta_{ijk} = \frac{\left(\frac{\alpha_c \ln 10}{10}\right)^2}{\left(\frac{\alpha_c \ln 10}{10}\right)^2 + \Delta B^2}\left[1 + \frac{4\times 10^{-\frac{\alpha_c L}{10}} \sin^2(\Delta BL/2)}{\left(1 - 10^{-\frac{\alpha_c L}{10}}\right)^2}\right], \tag{11}$$

where ΔB is the difference between the propagation constants of the classical channels due to fiber dispersion, and ΔBL is the phase mismatch coefficient. ΔB is given by [21]

$$\Delta B = \frac{2\pi\lambda_k^2}{c}\Delta f_{ik}\Delta f_{jk}\left[D_c(\lambda_k) + \frac{\lambda_k^2}{2c}(\Delta f_{ik} + \Delta f_{jk})\frac{dD_c(\lambda_k)}{d\lambda}\right], \tag{12}$$

where $\lambda_k = \frac{c}{f_k}$, c is the speed of light in vacuum, $\Delta f_{ak} = |f_a - f_k|$ $(a = \{i, j\})$, and $D_c(\lambda_k)$ and $\frac{dD_c(\lambda_k)}{d\lambda}$ are the chromatic dispersion and its slope at wavelength λ_k.

For in-band FWM noise, i.e., $f_{ijk} \approx f_q$, the arriving photon number and detection probability of FWM noise at the QKD receiver within gate width τ_D of the SPD are

$$N_{fwm} = \frac{P_{ijk}\tau_D t_{\text{demux}} t_F^{ijk}}{h f_{ijk}}, \quad Y_{fwm} = N_{fwm}\eta_{\text{Bob}}, \tag{13}$$

where the filter transmittance $t_F^{ijk} \approx t_F^q$.

E. Influence on the decoy-state WDM-QKD

For the noncoexistent QKD, detector dark counts are the main source of noise. However, the background noise for WDM-QKD contains not only detector dark counts, but also the classical noises introduced by classical signals in the same fiber, which will further damage the performance of QKD. In the following, take the commonly used phase-randomized weak coherent state sources for example. Let the average photon numbers be $m = \{\mu, \nu_1, \nu_2, \dots\}$ for signal and decoy-state sources, respectively. Then, the yield of an n-photon state for decoy-state WDM-QKD is given by

$$Y_n = Y_d + Y_c + \eta_n - Y_d Y_c - Y_d\eta_n - Y_c\eta_n + Y_d Y_c \eta_n, \tag{14}$$

where Y_d is the background rate for noncoexistent QKD, and $\eta_n = 1 - (1 - \eta)^n$ is the transmittance of the n-photon state. Note that in WDM-QKD, the overall transmission and detection efficiency η of the transmitted quantum signals will become

$$\eta = t_{AB} t_{\text{demux}} t_F^q \eta_{\text{Bob}}, \tag{15}$$

where the transmittances of the demultiplexer and filter are included. Y_c is the in-band classical noise detection rate for WDM-QKD, which can be expressed by

$$Y_c = f\left(Y_{\text{leak}}, Y_{\text{ram}}^f, Y_{\text{ram}}^b, Y_{fwm}\right). \tag{16}$$

According to Sec. II, Eq. (16) can be concretized based on the configuration of WDM-QKD, such as the number and transmission direction of the classical channels. For example, Y_c can be given as

$$Y_c = \begin{cases} Y_{\text{leak}} + Y_{\text{ram}}^f & \text{(Case 1)} \\ Y_{\text{ram}}^b & \text{(Case 2)} \\ \sum_{a=1}^3 Y_{\text{leak},a} + \sum_{a=1}^3 Y_{\text{ram},a}^f + Y_{fwm} & \text{(Case 3)}, \end{cases} \tag{17}$$

where Case 1 represents one classical channel with the same direction of quantum channel, Case 2 represents one classical channel with the opposite direction of quantum channel, and Case 3 represents three classical channels with the same direction of quantum channel.

It can be seen from Eq. (14) that the detection events of in-band classical noises will make a contribution to the yield of the n-photon state directly. For example, consider the case where a classical noise photon, such as a SRS photon, arrives at Bob in the time slot in which a single photon emitted by Alice is naturally lost. It affects the yield of the one-photon state. Furthermore, the error rate of the n-photon state is affected directly as well, which can be given by

$$e_n = \frac{e_0(Y_d + Y_c - Y_d Y_c) + e_{det}\eta_n(1 - Y_d - Y_c + Y_d Y_c)}{Y_n}, \tag{18}$$

where e_{det} is the misalignment error rate of WDM-QKD. Here, assume that the error rate of in-band classical noises is the same with detector dark counts and both are equal to $e_0 = \frac{1}{2}$.

Following Eqs. (14)–(18), the overall gain and quantum bit error rate (QBER) of the signal and decoy states for WDM-QKD are given by

$$\begin{aligned} Q_m &= \sum_{n=0}^{\infty} Y_n \frac{m^n}{n!} e^{-m} \\ &= Y_d + Y_c - Y_d Y_c + [1 - (Y_d + Y_c - Y_d Y_c)](1 - e^{-\eta m}), \end{aligned} \tag{19}$$

$$\begin{aligned} E_m Q_m &= \sum_{n=0}^{\infty} e_n^b Y_n \frac{m^n}{n!} e^{-m} \\ &= e_0(Y_d + Y_c - Y_d Y_c) \\ &\quad + e_{det}(1 - e^{-\eta m})[1 - (Y_d + Y_c - Y_d Y_c)]. \end{aligned} \tag{20}$$

III. FINITE-KEY SECURITY ANALYSIS FOR DECOY-STATE WDM-QKD

For decoy-state WDM-QKD, let the probabilities that Alice uses the signal and decoy sources be q_m, and the probabilities that Alice and Bob choose the basis $\gamma = \{Z, X\}$ be q_γ. The secret key length in one basis, e.g., Z basis, can be given from [15,22]

$$K^Z \geqslant M_{1\mu}^Z\big[1 - h\big(e_{1\mu}^{pZ}\big)\big] - M_\mu^Z f\big(E_\mu^Z\big) h\big(E_\mu^Z\big), \tag{21}$$

where $M_{1\mu}^Z$ and M_μ^Z are the numbers of Z-basis sifted key from the single-photon signal state and the overall signal state, respectively, $e_{1\mu}^{pZ}$ and E_μ^Z represent the phase error rate and QBER, correspondingly, $f(E_\mu^Z)$ denotes the error-correction inefficiency, and $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Note that M_μ^Z and E_μ^Z can be measured in experiment, while the bounds of $M_{1\mu}^Z$ and $e_{1\mu}^{pZ}$ need to be estimated using the decoy-state method [23].

In the asymptotic case, the parameters of the single-photon state required by Eq. (21) can be estimated accurately from the measured values of WDM-QKD, which will converge to the underlying true values. Then, the final key length of WDM-QKD can be obtained safely. However, in practical WDM-QKD, the number of transmitted quantum states is finite, resulting in the measured values fluctuating statistically, which is known as the finite-key effect and cannot be ignored when estimating the final key length. Here, before giving a finite-key security analysis for decoy-state WDM-QKD, we will first review the improved Chernoff bound method used for fluctuation analysis in Ref. [24].

With a failure probability ε, the confidence interval of the expectation value $\mathbb{E}[\zeta]$ for an observed value $\zeta > 0$ is given as

$$\mathbb{E}^L[\zeta] = \frac{\zeta}{1+\delta^L}, \quad \mathbb{E}^U[\zeta] = \frac{\zeta}{1-\delta^U}, \tag{22}$$

where $\mathbb{E}^L[\zeta]$ and $\mathbb{E}^U[\zeta]$ denote the lower and upper bounds of $\mathbb{E}[\zeta]$, and δ^L and δ^U can be obtained from the following equations:

$$\left[\frac{e^{\delta^L}}{(1+\delta^L)^{1+\delta^L}}\right]^{\frac{\zeta}{1+\delta^L}} = \frac{\varepsilon}{2}, \quad \left[\frac{e^{-\delta^U}}{(1-\delta^U)^{1-\delta^U}}\right]^{\frac{\zeta}{1-\delta^U}} = \frac{\varepsilon}{2}. \tag{23}$$

Using the Lambert W function [25], the solutions of Eq. (23) are

$$\begin{aligned} \frac{1}{1+\delta^L} &= -W_0\big(-e^{\frac{\ln(\frac{\varepsilon}{2})-\zeta}{\zeta}}\big), \\ \frac{1}{1-\delta^U} &= -W_{-1}\big(-e^{\frac{\ln(\frac{\varepsilon}{2})-\zeta}{\zeta}}\big). \end{aligned} \tag{24}$$

If $\zeta = 0$, we simply have $\mathbb{E}^L[\zeta] = 0$ and $\mathbb{E}^U[\zeta] = -\ln(\frac{\varepsilon}{2})$.

Based on Eqs. (22)–(24), the confidence intervals of the expectation values of M_m^γ and $E_m^\gamma M_m^\gamma$ can be given as $\mathbb{E}^L[M_m^\gamma]$, $\mathbb{E}^U[M_m^\gamma]$, $\mathbb{E}^L[E_m^\gamma M_m^\gamma]$, and $\mathbb{E}^U[E_m^\gamma M_m^\gamma]$, where M_m^γ and $E_m^\gamma M_m^\gamma$ are the numbers of sifted key and quantum bit error for basis γ. Assume the total number of transmitted quantum states is N. Then, these confidence intervals can be used to calculate the lower and upper bounds of the overall gain and QBER for the signal and decoy states, which results in

$$\begin{aligned} &\mathbb{E}^L\big[Q_m^\gamma\big] = \frac{\mathbb{E}^L\big[M_m^\gamma\big]}{N_m^\gamma}, \quad \mathbb{E}^U\big[Q_m^\gamma\big] = \frac{\mathbb{E}^U\big[M_m^\gamma\big]}{N_m^\gamma}, \\ &\mathbb{E}^L\big[E_m^\gamma Q_m^\gamma\big] = \frac{\mathbb{E}^L\big[E_m^\gamma M_m^\gamma\big]}{N_m^\gamma}, \\ &\mathbb{E}^U\big[E_m^\gamma Q_m^\gamma\big] = \frac{\mathbb{E}^U\big[E_m^\gamma M_m^\gamma\big]}{N_m^\gamma}, \end{aligned} \tag{25}$$

where $N_m^\gamma = q_m q_\gamma^2 N$ represents the number of quantum states with Alice and Bob using the same basis γ with average photon number m. Furthermore, the lower bound number of the γ-basis sifted key stemming from single-photon states is

$$M_1^{\gamma L} = Y_1^{\gamma L} q_\gamma^2 N (q_\mu e^{-\mu}\mu + q_\nu e^{-\nu}\nu), \tag{26}$$

where $Y_1^{\gamma L}$ is the lower bound of Y_1^γ, which can be derived from the decoy-state method combining with Eqs. (22)–(25). Note that $M_1^{\gamma L}$ consists of the single-photon states coming from both the signal state and decoy state. Among them, the lower bound for the contribution from the single-photon signal state can be given by the reverse form of the Chernoff bound,

$$M_{1\mu}^{\gamma L} = (1-\delta) p_1^\mu M_1^{\gamma L}, \tag{27}$$

where $\delta = \frac{-\ln(\varepsilon/2) + \sqrt{[\ln(\varepsilon/2)]^2 - 8\ln(\varepsilon/2) p_1^\mu M_1^{\gamma L}}}{2 p_1^\mu M_1^{\gamma L}}$, $p_1^\mu = \frac{q_\mu e^{-\mu}\mu}{q_\mu e^{-\mu}\mu + \sum_{m\neq\mu} q_m e^{-m} m}$ is the corresponding proportion of the single-photon signal state due to the Poisson distribution of source intensity.

In the finite resource case, the relationship between the phase error rate and QBER for the single-photon state, i.e., $e_{1\mu}^{pZ} = e_1^{bX}$, is no longer correct [26], for there is a deviation θ between the two error rates due to statistical fluctuations. The upper bound of deviation θ^U can be characterized by the random sampling theorem with a failure probability ε such that [26]

$$\varepsilon = \frac{\sqrt{M_1^{XL} + M_{1\mu}^{ZL}}}{\sqrt{e_1^{bXU}\big(1 - e_1^{bXU}\big) M_1^{XL} M_{1\mu}^{ZL}}} 2^{-(M_1^{XL} + M_{1\mu}^{ZL})\xi(\theta^U)}, \tag{28}$$

where $\xi(\theta^U) = h(e_1^{bXU} + \theta^U - q^x\theta^U) - q^x h(e_1^{bXU}) - (1-q^x)$ $h(e_1^{bXU} + \theta)$ with $q^x = \frac{M_1^{XL}}{M_1^{XL} + M_{1\mu}^{ZL}}$. Then, the upper bound of the phase error rate is given by

$$e_{1\mu}^{pZU} = e_1^{bXU} + \theta^U, \tag{29}$$

where e_1^{bXU} is the upper bound of e_1^{bX}, which can be derived from the decoy-state method combining with Eqs. (22)–(25).

IV. NUMERICAL SIMULATION

In this section, we will simulate the performance of classical noises and WDM-QKD based on the above analysis. For the simulation, quantum and classical channels coexist in a standard single-mode fiber (SSMF) using the C-band dense wavelength division multiplexing (DWDM) technology.

In the following, the performances of two kinds of decoy-state WDM-QKD are evaluated for different sent number of quantum states and transmitted power of classical signals. To

TABLE I. Parameters used for the performance simulation of WDM-QKD.

Parameter	Value
α_q, α_c (loss coefficient of fiber)	0.21 dB/km
I (insertion loss of Mux/Demux)	1.5 dB
ξ (isolation of Mux/Demux)	80 dB
$\Delta\lambda$ (bandwidth of filter)	35.2367 pm
t_F^{leak} (filter transmittance for out-band noise)	0.01
t_F^q (filter transmittance for quantum signal)	0.95
t_F^r, t_F^{ijk} (filter transmittance for in-band noise)	0.95
β (coefficient of SRS)	2×10^{-9}/(km nm)
D_{ijk} (degeneracy factor)	3
χ (nonlinear coefficient of fiber)	1.2/(W km)
$D_c(\lambda_k)$ (chromatic dispersion of fiber)	18 ps/(nm km)
$\frac{dD_c(\lambda_k)}{d\lambda}$ (slope of the chromatic dispersion)	0.056 ps/(nm^2 km)
Δf_{ak} (frequency difference)	400 GHz
h (Planck constant)	6.63×10^{-34} J s
c (light speed)	299792458 m/s
λ_q (wavelength of quantum signal)	1550 nm
N (total sent number of quantum signals)	10^{10}
E_0 (QBER of vacuum state)	0.5
$f(E_\mu^Z)$ (error-correction inefficiency)	1.22
$t_{\rm Bob}$ (internal transmittance of optical components)	0.9
η_D (SPD efficiency)	0.045
Y_d (detector dark count rate)	1.7×10^{-6}
τ_D (gate width of SPD)	100 ps
e_d (misalignment error rate)	0.033
ε (failure probability)	10^{-10}

maximize the final secret key rate $R = \frac{K^Z}{N}$, the biased bases choice is considered and the choice rates are optimized. We also optimize the intensities and associated rates of signal and decoy states. The parameters used in the simulation are listed in Table I.

A. Comparison of the in-band classical noises

To reduce the intensity of classical noises, many methods have been put forward. Among them, crosstalk noise can be relieved remarkably through the high isolation band WDM [2]. Other noise-reduction techniques, such as adjusting the classical signals power, spectral, or temporal filtering, have been proposed to deal with the in-band noises. However, in previous research, FWM noise is always considered to be negligible compared with SRS noise if the above methods are used. In this section, we will compare the two in-band noises strictly with different experimental parameters. The simulation result shows that FWM noise may be larger than SRS noise in some situations, which means that it cannot always be ignored for WDM-QKD.

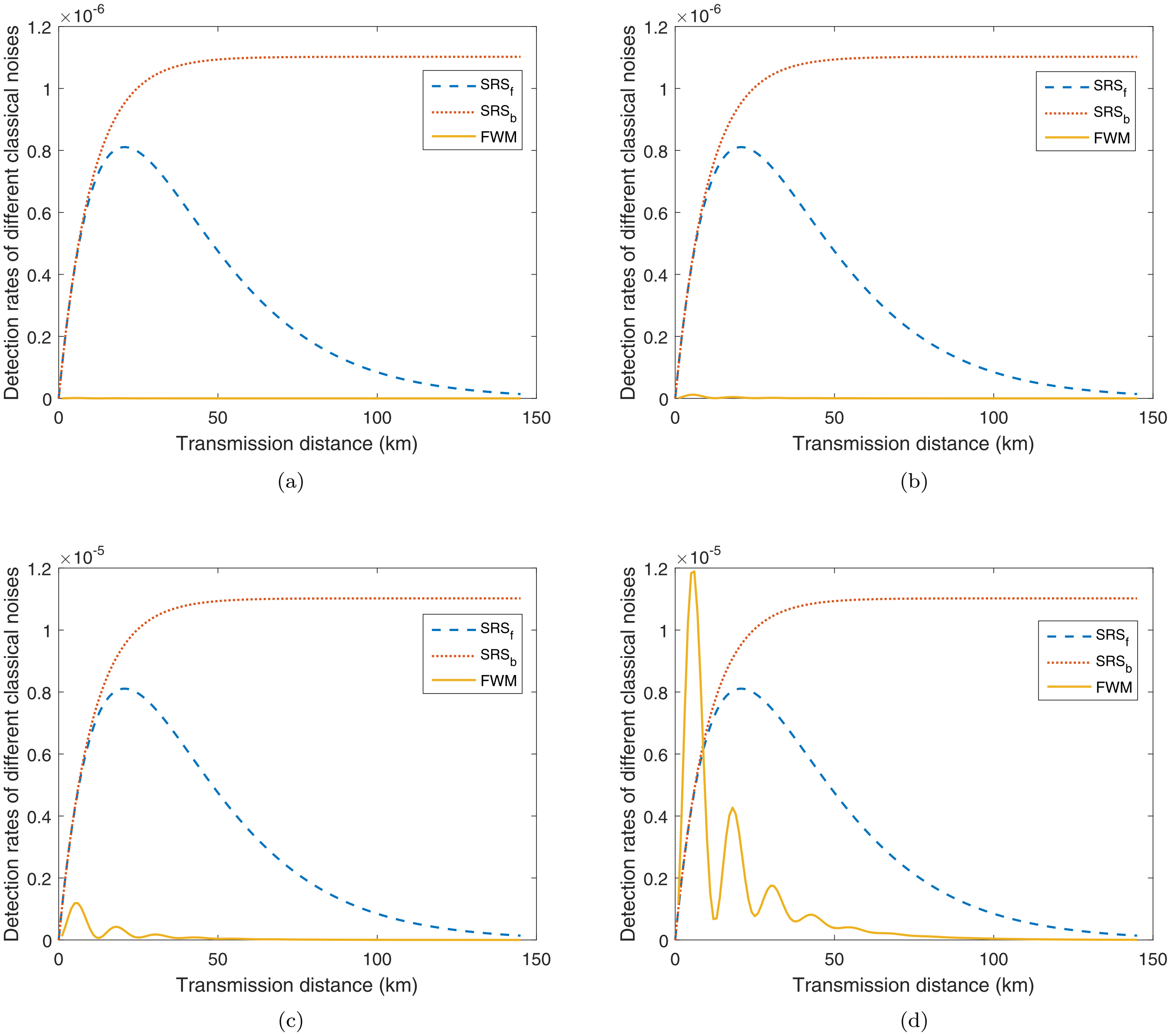
Before the comparison, note that as for the filtering of classical noises in frequency and time domains by filter F and SPD, respectively, in Fig. 1, the bandwidth $\Delta\lambda$ and gate width $\Delta\tau_D$ cannot be infinitely small simultaneously. The product of the two factors, i.e., time-bandwidth product (TBP), is limited by the following lower bound [5]:

$$\left(\frac{c}{\lambda^2}\Delta\lambda\right)\Delta\tau_D \geqslant \frac{2\ln 2}{\pi}, \tag{30}$$

where λ is the central wavelength of F. Combining with Eqs. (6), (7), and (13), it can be seen that the effect of spectral and temporal filtering for in-band classical noises is limited by the TBP bound.

In the following simulations, we will make TBP remain at the lower bound, which means that SRS noise is well suppressed. Let us first consider the case that three classical channels are existing in one fiber and the transmitted power of classical signals is low, e.g., −10 dBm. From Figs. 2(a) and 2(b), it shows that the intensity of SRS noise is far greater than FWM noise.

Then, let the emission power of classical signals increase to, e.g., 0 dBm. It can be seen from Figs. 2(c) and 2(d) that the detection rates of in-band classical noises go up. However, when the transmission distance is short, FWM noise cannot be ignored. Moreover, seeing Fig. 2(d), if the gate width $\Delta\tau_D$ is large, the intensity of FWM noise can exceed the SRS one. In Fig. 3, it more clearly shows the relationships between the detection rates of in-band classical noises and the transmitted power of classical signals with a short transmission distance, $L = 15$ km. As can be seen in the figure, when the power of the classical signals is low, FWM noise is smaller than SRS noise. With the increase of the classical signals power, the detection rate of FWM noise grows at an exponential rate and quickly exceeds the SRS one. Comparison of the results show that reducing the transmitted power of the classical signals is a straightforward way to decrease the classical noises. However, once the emission power of the classical signals cannot be changed, it is preferred to narrow the gate width of the SPD than the bandwidth of the filter F.



(a)

(b)

(c)

(d)

FIG. 2. Comparison of the detection rates of SRS noise and FWM noise. SRS_f and SRS_b denote the forward and backward SRS noises, respectively. The transmission power of the classical signals is -10 dBm for (a) and (b), while it is increased to 0 dBm for (c) and (d). (a), (c) The bandwidth of filter $\Delta\lambda = 35.23$ pm and the gate width of SPD $\Delta\tau_D = 100$ ps. (b), (d) The bandwidth of filter $\Delta\lambda = 3.523$ pm and the gate width of SPD $\Delta\tau_D = 1$ ns.

B. Performance of decoy-state WDM-QKD

In this section, we will analyze the performance of WDM-QKD with three classical channels transmitting in the same direction as the quantum channel. The vacuum+weak decoy-state method [23] is used to estimate Y_1^γ and e_1^{bX}, whose specific forms refer to Eqs. (34) and (37) in Ref. [23]. First, the secret key rates of two-decoy-state WDM-QKD with different finite resources are shown in Fig. 4. The transmitted power of the classical signals is fixed to be -10 dBm. It can be seen that with the sent number of quantum pulses going up, the secret key rates and maximum secure distances increase as well.

We also compare the performance of WDM-QKD with the noncoexistent one in terms of the asymptotic case. From Fig. 4, we can see that both the secret key rate and maximum secure distance of QKD decrease in the WDM system. An interesting phenomenon is that under the given parameters in Table I, the maximum secure distance is reduced by 9 km for WDM-QKD. However, the distance reduction due to the insertion losses of DWDM and filter F is 8.2 km. It reminds us that reducing the insertion losses of WDM and the filter is important to improve the maximum secure distance.

Furthermore, the relationships between total sent number of quantum pulses and the corresponding maximum secure distance are simulated in Fig. 5 with different transmitted power of classical signals. It can be seen that the more the transmitted number of quantum pulses, the longer the maximum secure distance. The maximum secure distance

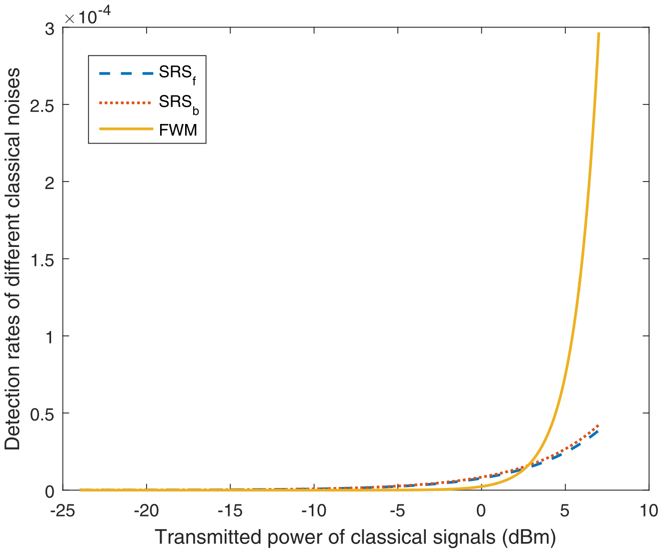


FIG. 3. The relationships between the detection rates of SRS and FWM noises and the transmitted power of the classical signals with $L = 15$ km. $\mathrm{SRS_f}$ and $\mathrm{SRS_b}$ denote the forward and backward SRS noises respectively. The bandwidth of filter $\Delta\lambda = 3.523$ pm and the gate width of SPD $\Delta\tau_D = 1$ ns.

approaches the infinite-key case if N is larger than about 10^{12} for each transmitted power of classical signals. On the other hand, to make the secure key rate positive, the minimum sent number of quantum pulses should increase as the transmitted power of classical signals becomes stronger. In Fig. 5, the range of the minimum value of N is about 10^7 to 10^8.

At last, we analyze the influence of the transmitted power of the classical signals on the performance of WDM-QKD. The relationships between the maximum secure distance and classical signals transmission power are shown in Fig. 6. It can be seen that the maximum secure distance declines with the transmitted power of the classical signals. If the power is high enough, the maximum secure distance drops to zero sharply.

C. Comparison of WDM-QKD with different decoy-state protocols

In the above simulations, the two-decoy-state protocol with vacuum+weak decoy states is considered. Next, we will compare the performance of one-decoy-state WDM-QKD with the two-decoy-state one. For consistency, the specific forms of Y_1^{γ} and e_1^{bX} refer to Eqs. (41) and (37) in Ref. [23] for the one-decoy-state WDM-QKD. First, fixing the transmitted power of the classical signals, the comparison of the secret key rates with different finite resources for the two-decoy-state WDM-QKD is shown in Fig. 4. Furthermore, the comparison of the relationships between the maximum secure distance and total sent quantum pulses number is demonstrated in Fig. 5. It can be seen from the two figures that when the total sent number of quantum pulses is small, the secret key rate and maximum secure distance of one-decoy-state WDM-QKD has an advantage over the two-decoy-state one. However, as the

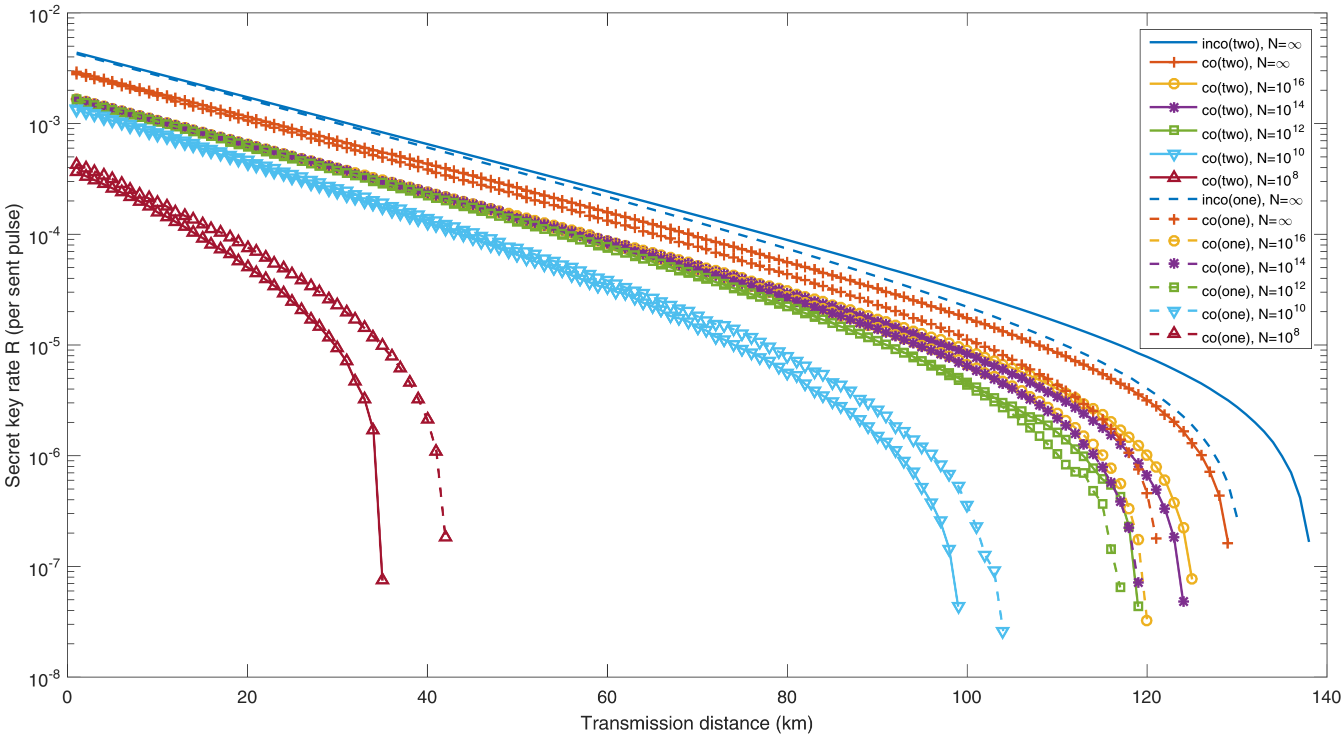


FIG. 4. The relationships between the secret key rate and transmission distance for WDM-QKD with different finite resources. The transmitted power of classical signals is fixed to be −10 dBm, and the other parameters used are listed in Table. I. Note that co(two) denotes the two-decoy-state WDM-QKD with solid lines in the figure, and co(one) denotes the one-decoy-state WDM-QKD with dashed lines. The various transmitted numbers of quantum signals are distinguished by the data point symbols. For comparison, the performances of noncoexistent QKD with symbols inco(two) and inco(one) for the two-decoy-state protocols are also shown in the same figure.

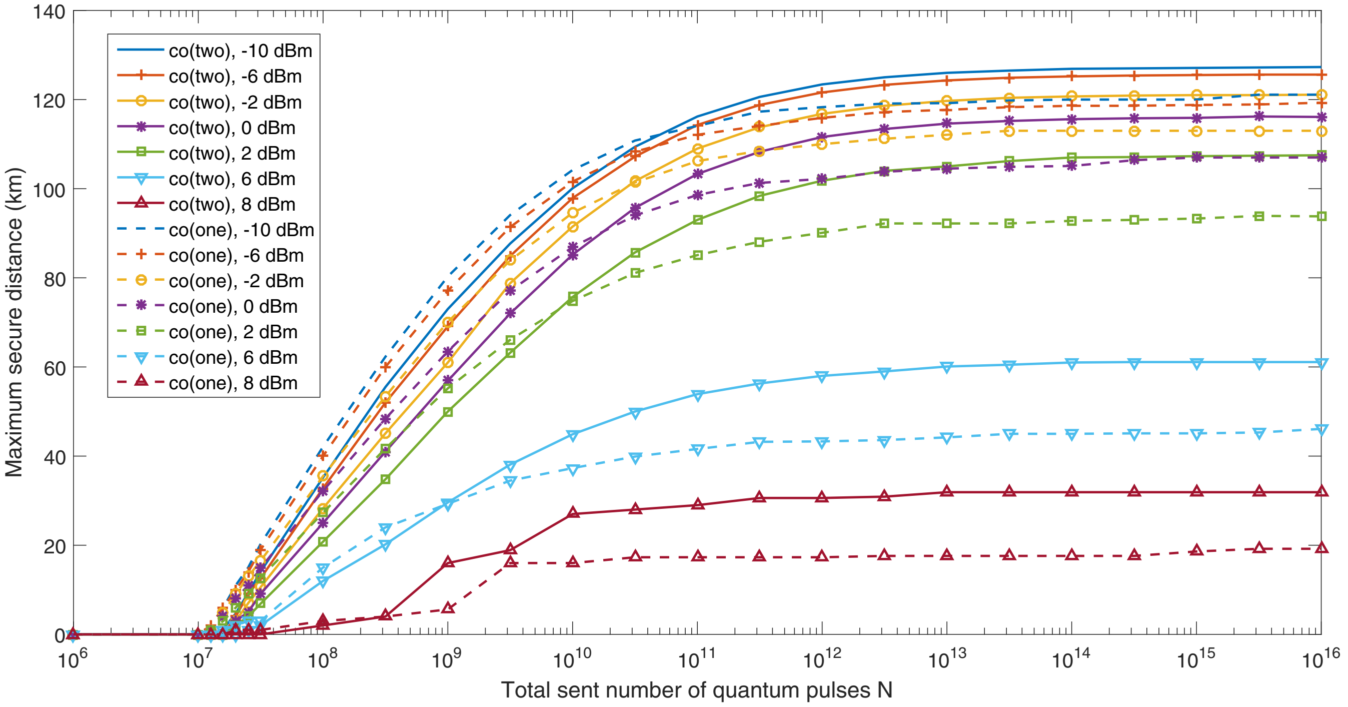


FIG. 5. The relationships between the maximum secure distance and total sent number of quantum pulses for WDM-QKD with fixed classical signals transmission power. The maximum secure distance approaches the asymptotic case if $N \geqslant 10^{12}$. The range of the minimum value of N is about 10^7 to 10^8 to make the secret key rate positive. The various transmitted powers of classical signals are distinguished by the data point symbols. The meanings of co(two) with solid lines and co(one) with dashed lines are the same as in Fig. 4.

sent number of quantum pulses increases, the performance of two-decoy-state WDM-QKD will exceed the one-decoy-state one.

At last, the performance comparison of the two WDM-QKD with different transmitted power of classical signals is depicted in Fig. 6. It shows that when $N = 10^8$, the

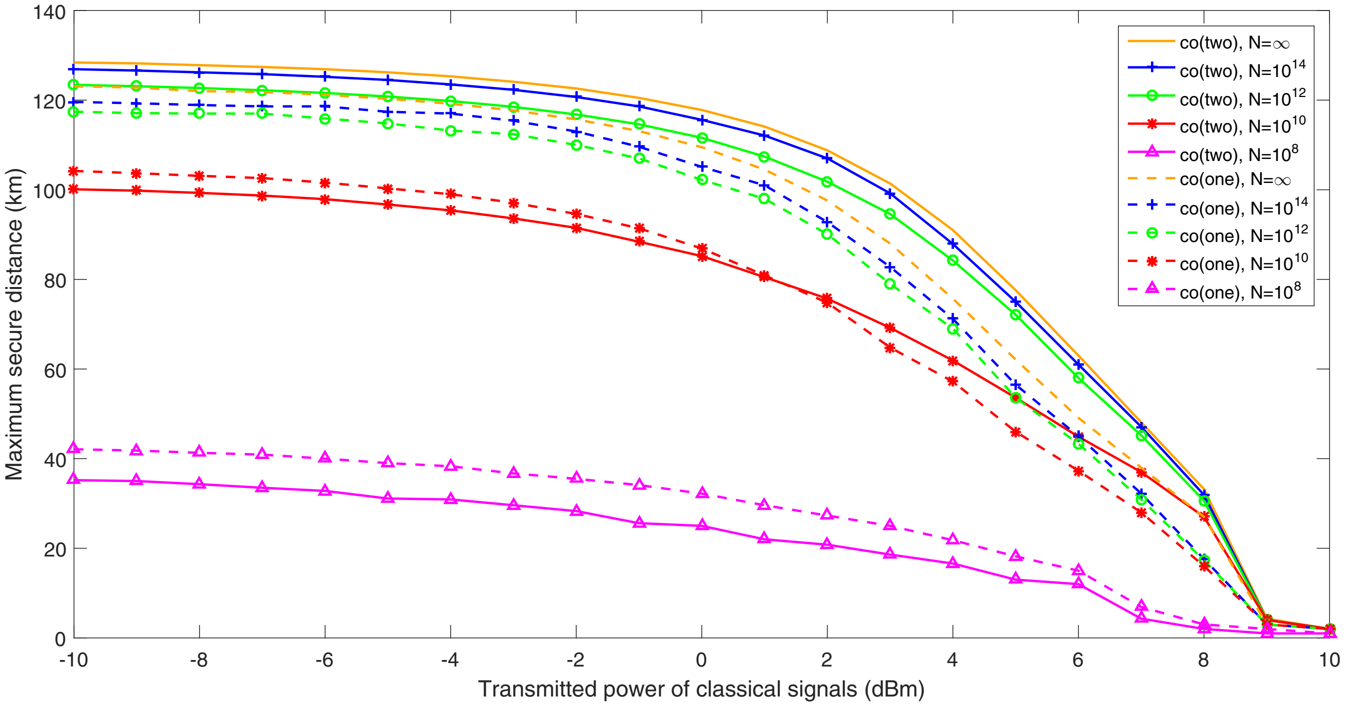


FIG. 6. The relationships between the maximum secure distance and transmitted power of classical signals for WDM-QKD with fixed sent number of quantum pulses. The various transmitted numbers of quantum signals are distinguished by the data point symbols. The meanings of co(two) with solid lines and co(one) with dashed lines are the same as in Figs. 4 and 5.

maximum secure distance of one-decoy-state WDM-QKD always outperforms the two-decoy-state one. Note that when $N = 10^{10}$, the solid and dashed red lines with asterisks in Fig. 6 cross, where the maximum secure distance of one-decoy-state WDM-QKD is first larger than and then less than that of the two-decoy-state one with the increase of the classical signals emission power. However, as the total sent number of quantum pulses continues to increase, the performance of two-decoy-state WDM-QKD always exceeds the one-decoy-state one regardless of classical signals powers.

V. CONCLUSION

In conclusion, we have systematically analyzed the practical security of decoy-state WDM-QKD in theory. First, the classical noises model of WDM-QKD is established, accompanied by the numerical simulation of the effect of three methods on reducing them. The simulation result shows that reducing the classical signals transmission power can remarkably suppress the strength of classical noises. Narrowing the gate width of SPD will reduce the intensities of the two in-band classical noises. However, due to the limitation of TBP, narrowing the bandwidth of the filter cannot always mitigate the impact of in-band classical noises for large classical signals transmission power.

Furthermore, the decoy-state model of WDM-QKD is revised with finite-key security analysis. And the performance of decoy-state WDM-QKD is simulated under various finite resources. We also display the effect of the transmitted power of the classical signals on WDM-QKD. In addition, the performance of one-decoy-state WDM-QKD is compared with the two-decoy-state one, which shows that the former has advantages with small sent number of quantum pulses.

The method and result of the paper can be directly used in the experiment for integrating BB84 QKD into the existing WDM optical communication system. It provides the theoretical basis to relieve the classical noises and optimize the experimental settings. The analysis method developed in the paper is universal, which can be utilized by a variety of practical copropagation systems. In this work, WDM-QKD with SSMF and DWDM technology is simulated, while the system with low loss and large effective area fiber and/or the coarse WDM can also be analyzed. Moreover, the method can be extended to other QKD protocols, such as the recent measurement-device-independent QKD [27,28] and twin-field QKD [29–31]. In the future, other practical security issues, such as the source flaws and detector loopholes for WDM-QKD, can be analyzed based on this work.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous referees for the many constructive comments to improve the quality of this article. This work was supported by the Natural Science Foundation of Jiangsu Province (Grant No. BK20180193) and the China Postdoctoral Science Foundation (Grant No. 2018M632226).

[1] P. D. Townsend, Electron. Lett. **33**, 188 (1997).

[2] T. J. Xia, D. Z. Chen, G. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, *Optical Fiber Communication Conference* (Optical Society of America, Anaheim, CA, 2006), p. OTuJ7.

[3] N. Peters, P. Toliver, T. Chapuran, R. Runser, S. McNown, C. Peterson, D. Rosenberg, N. Dallmann, R. Hughes, K. McCabe *et al.*, New J. Phys. **11**, 045012 (2009).

[4] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, New J. Phys. **12**, 103042 (2010).

[5] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, Appl. Phys. Lett. **104**, 051123 (2014).

[6] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, New J. Phys. **12**, 063027 (2010).

[7] J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards *et al.*, Sci. Rep. **6**, 35149 (2016).

[8] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert *et al.*, Opt. Express **22**, 23121 (2014).

[9] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao *et al.*, Opt. Express **26**, 6010 (2018).

[10] D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. Della Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe *et al.*, EPJ Quantum Technol. **6**, 5 (2019).

[11] L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen *et al.*, Phys. Rev. A **95**, 012301 (2017).

[12] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Optica **4**, 163 (2017).

[13] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Phys. Rev. X **2**, 041010 (2012).

[14] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

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

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

[17] T. Schneider, *Nonlinear Optics in Telecommunications* (Springer, Berlin, 2007).

[18] H. Kawahara, A. Medhipour, and K. Inoue, Opt. Commun. **284**, 691 (2011).

[19] F. Forghieri, R. Tkach, and A. Chraplyvy, Opt. Fiber Telecommun. IIIA **1**, 196 (1997).

[20] K. Hill, D. Johnson, B. Kawasaki, and R. MacDonald, J. Appl. Phys. **49**, 5098 (1978).

[21] N. Shibata, R. Braun, and R. Waarts, IEEE J. Quantum Electron. **23**, 1205 (1987).

[22] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[23] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[24] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Phys. Rev. A **95**, 012333 (2017).

[25] S. Bahrani, O. Elmabrok, G. C. Lorenzo, and M. Razavi, J. Opt. Soc. Am. B **36**, B99 (2019).

[26] C.-H. F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, 012318 (2010).

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

[28] X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, Phys. Rev. A **96**, 052337 (2017).

[29] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).

[30] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Phys. Rev. X **9**, 021046 (2019).

[31] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin *et al.*, Phys. Rev. Lett. **123**, 100505 (2019).