Chin. Phys. Lett. **39**, 070301 (2022)

Twin-Field Quantum Key Distribution Protocol Based on Wavelength-Division-Multiplexing Technology

Yanxin Han(韩雁鑫)[1], Zhongqi Sun(孙钟齐)[1], Tianqi Dou(窦天琦)[2], Jipeng Wang(王吉鹏)[1], Zhenhua Li(李振华)[1], Yuqing Huang(黄雨晴)[1], Pengyun Li(李鹏云)[3], and Haiqiang Ma(马海强)[1*]

[1]*School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*China Telecom Research Institute, Beijing 102209, China*
[3]*China Academy of Electronics and Information Technology, China Electronic Technology Group Corporation, Beijing 100041, China*

(Received 14 April 2022; accepted manuscript online 16 May 2022)

Quantum key distribution (QKD) generates information-theoretical secret keys between two parties based on the physical laws of quantum mechanics. Following the advancement in quantum communication networks, it becomes feasible and economical to combine QKD with classical optical communication through the same fiber using dense wavelength division multiplexing (DWDM) technology. This study proposes a detailed scheme of TF-QKD protocol with DWDM technology and analyzes its performance, considering the influence of quantum channel number and adjacent quantum crosstalk on the secret key rates. The simulation results show that the scheme further increases the secret key rate of TF-QKD and its variants. Therefore, this scheme provides a method for improving the secret key rate for practical quantum networks.

DOI: 10.1088/0256-307X/39/7/070301

Quantum key distribution (QKD) provides an information-theoretical secure method for distributing secret keys between distant parties based on the principle of quantum mechanics.[1] The first proposed QKD protocol in 1984[2] has received significant attention.[3−10] However, in applications, concerns with practical devices may result in the use of idealized models without security analysis. The proposed decoy state[11,12] protocol can handle the security issue of photon number splitting (PNS)[13] caused by the imperfect photon source, making QKD useful under weak coherent pulses. In addition, the measurement device-independent QKD (MDI-QKD) protocol was proposed in 2012,[14] having the advantage of immunity against all attacks on the detector side, which further improves the actual security of QKD. QKD has achieved a longer realizable distance[15] and higher secret key rate[16] due to the various theoretical and experimental research on it. However, the maximum possible key rate for communication between users in the absence of quantum memory is limited to the linear key rate Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound, which can be expressed as $R \leq -\log_2(1-\eta)$, where η is the transmittance of the experiment setups.[17] Fortunately, the secret key rate of the twin-filed QKD (TF-QKD) protocol proposed in 2018 is described as $R \sim O(\sqrt{\eta})$,[18] which exceeds the PLOB bound. TF-QKD has a higher final key rate than MDI-QKD because it not only retains all the advantages of MD-QKD but is also caused by single-photon interference. Inspired by the original TF-QKD, several theoretical studies and variants[19−21] that further enhance the secret key rate of QKD systems have been proposed.

Currently, the application of QKD has been extended from point-to-point communication to optical network communication. Most of the fiber-based QKD experiments use dark fiber as the quantum channel. However, the demand for dark fiber increases as the number of quantum secure communication network users increases, resulting in a sharp rise in deployment costs. Moreover, although the existing key rate has been improved, it cannot satisfy the requirements of the QKD network for information transmission. An effective solution is to carry multiple quantum and classical data signals on a single fiber for simultaneous transmission, and wavelength division multiplexing (WDM)[22] is a standard technique of this scheme. Previous research[23−32] showed that WDM technology combines the existing communication network with the QKD network to send more quantum signals in the same transmission distance, effectively improving the key transmission rate. Further, the combination of mode-pairing MDI-QKD protocol[33] and WDM technology can not only reduce the experimental difficulty but also improve the key rate, providing a new direction for developing QKD networks.

*Corresponding author. Email: hqma@bupt.edu.cn
© 2022 Chinese Physical Society and IOP Publishing Ltd

However, most of the previous QKD schemes based on WDM technology only considered the effect of classical signals on QKD performance and are yet to consider quantum signals. In this study, we present a detailed scheme for a TF-QKD protocol using dense-WDM (DWDM)[34] technology and analyze its performance. We have used numerical simulations to analyze the feasibility of considering different numbers of quantum channels and the effect of crosstalk on adjacent quantum channels. In addition, we analyze the performance of PM-QKD using the DWDM technology to verify that a TF-QKD variant combined with the DWDM technology has the same performance.

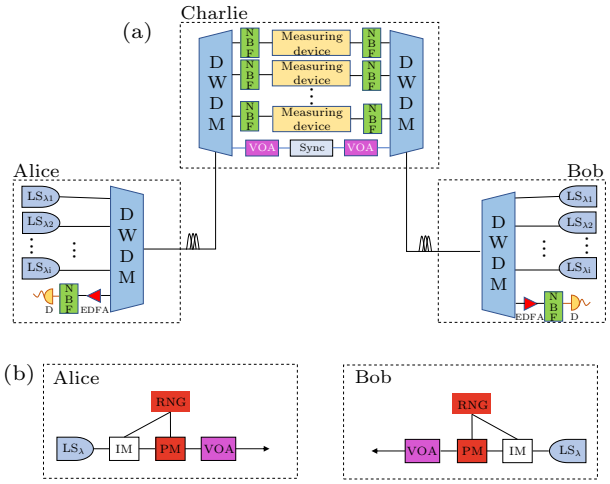

Fig. 1. (a) Schematic of TF-QKD system based on DWDM. (b) Schematic of Alice and Bob sending pulses. LS: Laser source; Sync: Synchronization clock; VOA: variable optical attenuator; DWDM: dense wavelength division multiplexer; EDFA: erbium-doped fiber amplifier; NBF: narrow-band optical filter; D: single-photon detector; IM: intensity modulator; PM: phase modulator; RNG: random number generator.

Figure 1(a) illustrates the schematic of the TF-QKD system based on DWDM. Figure 1(b) shows that Alice and Bob have the same sending setup in each channel. The goal of Charlie's classical signals is to synchronize Alice's and Bob's signals. For quantum signals, Alice and Bob use the DWDM techniques to combine independent random phase pulses through variable optical attenuators (VOAs) and then send them to Charlie. Charlie uses the DWDM to separate the quantum signals and announce the response of the detector. In this process, a dispersion compensated fiber is selected to minimize the effect of dispersion on the transmitted pulse signal, erbium-doped fiber amplifiers (EDFAs) are used to amplify and recover the Sync signal, and narrow-band optical filters (NBFs) are used to filter out spontaneous Raman noise.[35,36] The protocol's specific process is as follows:

1. An authenticated channel is set up for public statements made by legitimate users Alice and Bob. In addition, Alice and Bob emit single-photon pulses. The pulses modulated by Alice and Bob were gathered into a single optical fiber using WDM technology and sent to Charlie. Charlie receives the pulses and makes independent interferometric measurements for the same wavelength, using an optical demultiplexer to decompose the pulse. Then, Alice and Bob get the results published by Charlie.

2. Alice and Bob randomly select phases ρ_a and ρ_b in the interval $[0, 2\pi)$, respectively, which is split into $M = 16$ equal phase slices $\Delta_k = 2\pi k/M$, with $k = \{0, 1, \ldots, M-1\}$. The random phase value selected by Alice and Bob must fall into one of the phase slices, and only that phase slice, Δ_k, should be recorded.

3. Alice and Bob both send bright unmodulated optical pulses to Charlie for interference, and feedback adjustment is made to minimize the phase misalignment between Alice and Bob. These guarantee the stability of the communication channels.

4. Alice and Bob attenuate the emitted light pulses and modulate the phase and intensity of the attenuated pulses. Alice and Bob selected random values for the intensities $\mu_{a,b} \in \{\frac{u}{2}, \frac{v}{2}, \frac{w}{2}\}$, the bit phases $\partial_{a,b} \in \{0, \pi\}$, corresponding to bit values $\{0, 1\}$, respectively; the basis phases $\beta_{a,b} \in \{0, \frac{\pi}{2}\}$, corresponding to the basis $\{X, Y\}$, respectively; then, Alice and Bob modulated random phase $\rho_{a,b} \in [0, 2\pi)$ loaded on the fiber and recorded the phase slices $\Delta_{k(a)}$ or $\Delta_{k(b)}$, which the random phase ρ_a and ρ_b fell into. Further, they prepared pulses with intensities $\mu_{a,b} \in \{\frac{u}{2}, \frac{v}{2}, \frac{w}{2}\}$ and phases $\phi_{a,b} = (\alpha_{a,b} + \beta_{a,b} + \rho_{a,b}) \oplus 2\pi$ and sent them to Charlie.

5. Charlie receives the incoming pulses sent by Alice and Bob and records the interference result using detectors. Then, he publicly announces the results of the detectors. Then, he publicly announces the result of the detectors' response. Among these, the results that none or both of the detectors clicked are discarded.

6. Alice announces the intensities, μ_a, the basis phases, β_a, and the phase slices, $\Delta_{k(a)}$; then, Bob announces that his information is consistent with Alice. Alice and Bob discard any mismatched values. They only declare the value of the matched bits in the Y basis for the decoy-state parameter estimation and Eve's eavesdropping, while maintaining the value and intensity of the X basis to distill the secret key.

7. Bob deduces Alice's bit phase value, ∂_a, via the interference results. The users can then distill a key bit equal to 0(1) when $\partial_a = 0(\pi)$.

8. Finally, Alice and Bob distill the final security key using the result of parameter estimation to perform error correction and privacy amplification.

In the above process, the phase randomization of the phase slice causes the random phases loaded by Alice and Bob to be different. However, Alice and Bob discard all mismatched values in step 6, and the random phases, ρ_a and ρ_b, loaded by Alice and Bob will always differ by less than $2\pi/M$ for a pair of twin fields. In the TF-QKD system, the key bits are distilled only from the intensity class $\mu_{a,b} \in \left\{\frac{u}{2}, \frac{v}{2}, \frac{w}{2}\right\}$, with the probabilities $p_w = p_v \ll p_u = 1-p_w-p_v \leq 1$. For the overall gain, Q_u is given by[18]

$$Q_u = 1 - (1 - P_{\rm dc})^2 e^{-u\tilde{\eta}}, \tag{1}$$

with $\tilde{\eta} = \eta_{\rm det} \times \hat{\eta}$. Here $P_{\rm dc}, \eta_{\rm det}$ and $\hat{\eta}$ are the dark count, the detection efficiency of Charlie, and the transmission efficiency, respectively. In addition, the gains Q_v and Q_w are analogous to Q_μ and can be obtained by replacing u with v or w. For the error rates, E_u is given as follows:[18]

$$E_u = \left\{e^{-u\tilde{\eta}[1-(e_{\rm opt}+E_M)]} - e^{-u\tilde{\eta}(e_{\rm opt}+E_M)}\right\} \frac{1}{2Q_u}(1 - P_{\rm dc}) + \frac{1}{2}, \tag{2}$$

where $e_{\rm opt}$ is the channel optical error rate, and the error rates E_v and E_w are analogous to E_u. Further, y_1 and e_1 can be estimated using the decoy-state method:[18]

$$y_1 = \frac{u^2 Q_v e^v - u^2 Q_w e^w - (v^2 - w^2)}{u(uv - uw - v^2 + w^2)}, \tag{3}$$

$$e_1 = (E_v Q_v e^v - E_w Q_w e^w)/[y_1(v - w)], \tag{4}$$

where[18]

$$y_0 = (vQ_w e^w - wQ_v e^v)/(v - w). \tag{5}$$

Compared with the efficient BB84,[37] a distance L in TF-QKD can be regarded as the distance of $\frac{L}{2}$ in QKD, and can be expressed as[18]

$$\begin{aligned} R(\mu, L) =& \frac{1}{2}\frac{1}{M}\left[R_{\rm QKD}\left(\mu, \frac{L}{2}t\right)\right]_{\oplus E_M} \\ =& \frac{1}{2}\frac{1}{M}\{Q_1[1 - H_2(e_1)] - fQ_\mu H_2(E_\mu)\}. \end{aligned} \tag{6}$$

The notation $\oplus E_M$ represents the intrinsic quantum bit error rate (QBER) of TF-QKD because of the random phase, the coefficient $\frac{1}{M}$ represents the selection from the phase slice. The optimal $E_M \simeq 1.275\%$ can be obtained by setting $M = 16$. Here f accounts for the efficiency of error correction, H_2 is the binary Shannon entropy, and $Q_1 = p_{1/\mu} y_1$ is the lower bound for the single-photon gain.

The smaller the channel interval, the more the crosstalk photons generated between channels when using WDM technology to improve the secret key rate of information transmission. In a DWDM system, if multiple quantum signals are simultaneously transmitted to the fiber, the channel crosstalk will severely affect the performance of the QKD system, or even prevent the operation of the QKD system completely. In addition, WDM and demultiplexer with high isolation ratio can isolate the carrier and sideband photon interference of classical light to a certain extent.[38]

In TF-QKD based on the WDM system, the input excessive noise power at the Charlie receiver, $P_{\rm Charlie}$, within the quantum channel bandwidth of wavelength, $B_{\rm Q}$, produces excessive noise, $P_{\rm c}$, which is given as follows:

$$P_{\rm c} = 4\eta_{\rm det}\frac{P_{\rm Charlie}}{h\upsilon_{\rm Q} B_{\rm Q}}. \tag{7}$$

Here, h is the Planck constant, and $\upsilon_{\rm Q}$ is the optical center frequency of the quantum signal. Because both Alice and Bob transmit information to Charlie in the TF-QKD system, the noise induced by Alice's direct transmission of information to Bob is twice as much,[39] thus the coefficient of Eq. (7) is 4. We classify the noise photons generated by the crosstalk of adjacent quantum channels as part of the background noise (dark count of the detector) to quantify the effect of noise photons on the system performance.

Therefore, the overall gain $Q_u(P_{\rm c})$ for TF-QKD is expressed as follows:

$$Q_u(P_{\rm c}) = 1 - [1 - (P_{\rm dc} + P_{\rm c})]^2 e^{-u\tilde{\eta}}. \tag{8}$$

The gains Q_v and Q_w are analogous to Q_u and can be obtained by replacing u with v or w. Similarly, for the error rates, $E_u(P_{\rm c})$ is given as follows:

$$E_u(P_{\rm c}) = \{e^{-u\tilde{\eta}[1-(e_{\rm opt}+E_M)]} - e^{-u\tilde{\eta}(e_{\rm opt}+E_M)}\} \frac{1}{2Q_u(P_{\rm c})}(1 - P_{\rm dc} - P_{\rm c}) + \frac{1}{2}. \tag{9}$$

In addition, the error rates E_v and E_w are analogous to E_u.

Therefore, in this study the final secret key rate is given as follows:

$$R(P_{\rm c}) = \frac{2}{M}\{Q_1(P_{\rm c})[1 - H_2(e_1)] - fQ_\mu(P_{\rm c})H_2(E_\mu(P_{\rm c})) + Q_0(P_{\rm c})\}, \tag{10}$$

where Q_0 is the estimated number caused by zero photon pulses (dark and crosstalk counts).

As aforementioned, the TF-QKD protocol has many variants. We use the PM-QKD protocol as an

example to analyze the performance of TF-QKD protocol variants with DWDM technology.

In the PM-QKD protocol, Alice (Bob) randomly prepares weak coherent states $|\sqrt{\mu_a}e^{i(\phi_a+\pi k_a)}\rangle_A$ ($|\sqrt{\mu_b}e^{i(\phi_b+\pi k_b)}\rangle_B$), and adds a random phase $\phi_A(\phi_B)$ to the weak coherent states. Then, Charlie receives and measures them. According to the measurement results announced by Charlie, Alice and Bob can generate raw key bits after postselection of the cases satisfying $\phi_A \approx \phi_B$. Thus, the structure setting is also the same as that of TF-QKD protocol. In addition, the PM-QKD not only maintains the characteristics of single-photon interference but also ensures security based on entanglement purification, ensuring that the secret key rate beats the linear bound. In PM-QKD, when Alice and Bob select $\frac{\mu}{2}$, the overall gain and QBER, Q_μ and E_μ, are given by[19]

$$Q_\mu \approx 1-(1-2P_{\rm dc})e^{-\eta\mu}, \tag{11}$$

$$E_\mu \approx (P_{\rm dc}+\eta\mu e_\delta)\frac{e^{-\eta\mu}}{Q_\mu}. \tag{12}$$

Both Q_μ and E_μ can be directly estimated in the experiment. The secret key rate of the PM-QKD protocol can be expressed as[19]

$$R=\frac{2}{M}Q_\mu[1-fH_2(E_\mu)-H_2(E_\mu^X)], \tag{13}$$

where $\frac{2}{M}$ is the sifting factor; E_μ^X is the phase error rate reflecting the information leakage, which can be bounded by[19]

$$E_\mu^X \le {\rm e}_0^Z q_0+\sum_{k=0}^{\infty}{\rm e}_{2k+1}^Z q_{2k+1}+\Big(1-q_0-\sum_{k=0}^{\infty}q_{2k+1}\Big). \tag{14}$$

Here, q_k is the estimated ratio of the "k-photon signal" to the full detected signal:[19]

$$q_k=\frac{(e^{-\mu}\mu^k/k!)Y_k}{Q_\mu}, \tag{15}$$

where Y_k and e_k^Z are the yield and bit error rate, respectively; when Charlie's light source is a k-photon number state, we have[19]

$$Y_k \approx 1-(1-2P_{\rm dc})(1-\eta)^k, \tag{16}$$

$$e_k^Z \approx \frac{P_{\rm dc}(1-\eta)^k+e_\delta[1-(1-\eta)^k]}{Y_k}, \tag{17}$$

where $e_\delta=\frac{\pi}{M}-\frac{M^2}{\pi^2}\sin^3(\frac{\pi}{M})$ is the misalignment error rate.

The PM-QKD system using DWDM is similar to a TF-QKD system. Likewise, when DWDM technology is applied to the PM-QKD, multiple quantum signals are simultaneously transmitted to the fiber and there are crosstalk photons that can affect performance. Therefore, the overall gain and QBER, $Q_\mu(P_{\rm c})$ and $E_\mu(P_{\rm c})$, are given as follows:

$$Q_\mu(P_{\rm c}) \approx 1-[1-2(P_{dc}+P_{\rm c})]e^{-\eta\mu}, \tag{18}$$

$$E_\mu(P_{\rm c}) \approx (P_{dc}+P_{\rm c}+\eta\mu e_\delta)\frac{e^{-\eta\mu}}{Q_\mu(P_{\rm c})}. \tag{19}$$

In addition,

$$Y_k(P_{\rm c}) \approx 1-[1-2(P_{dc}+P_{\rm c})](1-\eta)^k, \tag{20}$$

$$q_k(P_{\rm c})=\frac{(e^{-\mu}\mu^k/k!)Y_k(P_{\rm c})}{Q_\mu(P_{\rm c})}, \tag{21}$$

$$e_k^Z(P_{\rm c}) \approx \frac{(P_{dc}+P_{\rm c})(1-\eta)^k+e_\delta[1-(1-\eta)^k]}{Y_k(P_{\rm c})}. \tag{22}$$

Thus, $E_\mu^X(P_{\rm c})$ are also affected by crosstalk photons.

The final secret key rate is given by

$$R(P_{\rm c})=\frac{2}{M}\{Q_\mu(P_{\rm c})[1-fH_2(E_\mu(P_{\rm c}))-H_2(E_\mu^X(P_{\rm c}))] + Q_0(P_{\rm c})\}. \tag{23}$$

We used numerical simulations to analyze the performance of TF-QKD based on the DWDM technology. First, we discuss the effect of the number of quantum channels on the key rate. Then, we simulate the secret key rate of TF-QKD, and Table 1 lists the values of parameters. Figure 2 shows the simulation results of the secret key rate in TF-QKD with the different numbers of WDM channels. The results show that the secret key rate of TF-QKD with the multi-channel simultaneous transmission is higher than the single-channel transmission under the same distance, and the trend of increasing security key rate is not linear.

Table 1. Values of parameters in simulation.

Parameters	M	f	u	v	w	$e_{\rm opt}$	$\eta_{\rm det}$	$P_{\rm dc}$ (per pulse)
Values	16	1.15	0.4	10^{-2}	10^{-4}	3%	30%	1×10^{-8}

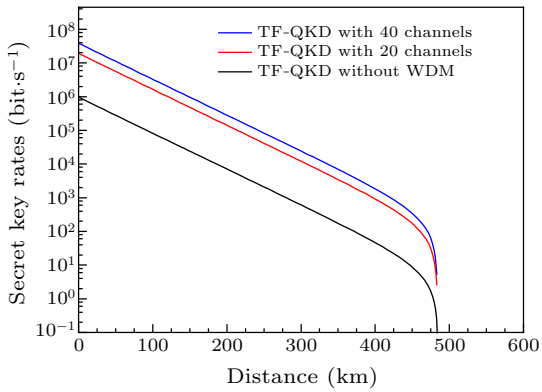

Fig. 2. Secret key rate of TF-QKD based on DWDM. The lines from top to bottom are the secret key rates for different numbers ($N=40$, 20, and 1).

The numerical simulation parameters for the PM-QKD protocol are listed in Table 2, and the result of

the numerical simulation is shown in Fig. 3. Compared with the application without DWDM technology, the secret key rate of PM-QKD based on DWDM is higher and increases as the number of channels increases, like the purple and green lines. Because the TF-QKD variants are derived from the original TF-QKD, DWDM technology can be applied to the TF-QKD and to its variants by simultaneously transmitting multiple wavelengths carrying information.

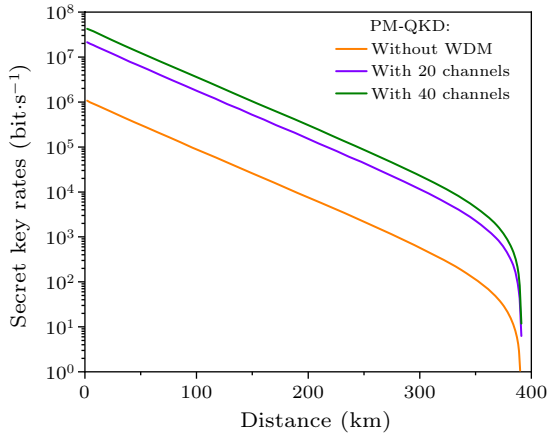

Fig. 3. Secret key rate of PM-QKD based on DWDM. The lines from top to bottom are the secret key rates for different numbers ($N = 40$, 20, and 1).

Table 2. Values of parameters in simulation of PM-QKD.

Parameters	M	f	μ	$\eta_{\rm det}$	$P_{\rm dc}$ (per pulse)	e_δ
Values	16	1.15	0.3	14.5%	8×10^{-8}	1.5%

Then, we discuss the effect of quantum channel noise-induced crosstalk on the secret key rate. As an example, we compare and analyze the secret key rate of a single channel with and without DWDM at 1550 nm wavelength. Figures 4 and 5 show the simulation results of the key rate of TF-QKD and PM-QKD with different crosstalk photons. The key rate and transmission distance of TF-QKD and PM-QKD decrease as the DWDM crosstalk noise increase. We will use TF-QKD as an example (Fig. 4). The blue line represents the secret key rate without the DWDM technology. The red line represents the secret key rate with crosstalk only affected by one channel, and the value of $P_{\rm c}$ is the same as the value of the detector's dark count, corresponding to the first and last channels. The yellow line represents the secret key rate with crosstalk affected by two channels, corresponding to the middle channels, with the value of $P_{\rm c}$ equal to two times the dark count. If the quantum signal is multiplexed with the classical signal, the crosstalk between the channels will increase significantly and the corresponding secret key generation rate will drop rapidly, as depicted by the purple line. However, the total secret key rate increases for all channels. The analysis and results for PM-QKD are the same for TF-QKD (Fig. 5). Therefore, the TF-QKD and its variants based on DWDM technology can simultaneously send information from multiple wavelengths and increase the total secret key rate, providing a solution to satisfy the requirements of future large-scale networks.

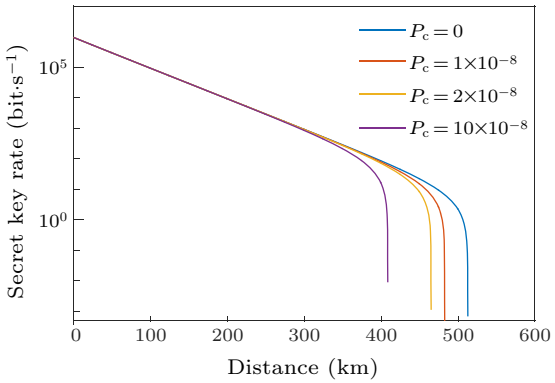

Fig. 4. Secret key rate of TF-QKD for a single channel at different crosstalk photon counts. The lines from left to right are the secret key rate for different numbers of crosstalk photons ($P_{\rm c} = 10 \times 10^{-8}$, 2×10^{-8}, 1×10^{-8} and 0).

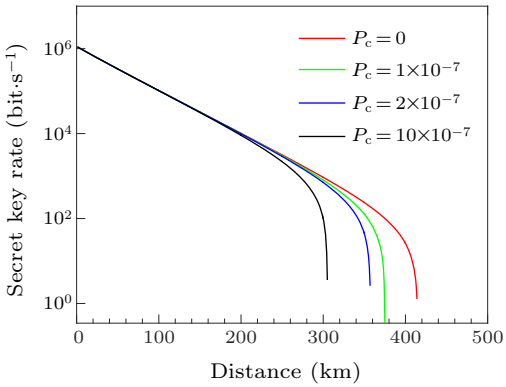

Fig. 5. Secret key rate of PM-QKD for a single channel at different crosstalk photon counts. The lines from left to right are the secret key rate for different numbers of crosstalk photons ($P_{\rm c} = 10 \times 10^{-7}$, 2×10^{-7}, 1×10^{-7} and 0).

In summary, we have proposed a detailed scheme of TF-QKD protocol based on DWDM technology and analyze its performance, transmitting multiple pulse signals using the same fiber. In our analysis, we consider two main factors affecting the performance: the number of quantum channels and the crosstalk photons between adjacent quantum channels. The simulation results show that the overall secret key rate of the TF-QKD system can be significantly improved, though the key rate per channel is reduced. The behavior of this system can be effectively improved by increasing the number of quantum channels and reducing the crosstalk of adjacent quantum channels. Moreover, we use the PM-QKD protocol as an example to ensure that the variant form of the TF-QKD protocol combined with DWDM has the same charac-

teristics. Notably, we propose a method to increase the key rate, which provides a reference for realizing multiuser quantum communication in the future.

Acknowledgment. This work was supported by the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications (Grant No. IPOC2021ZT10), the National Natural Science Foundation of China (Grant No. 11904333), the Fundamental Research Funds for the Central Universities (Grant No. 2019XD-A02), and BUPT Innovation and Entrepreneurship Support Program (Grant No. 2022-YC-T051).

References

[1] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 9–12 December 1999, Banglore, India, p 175
[3] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev. A* **54** 3824
[4] Diamanti E, Lo H K, Qi B and Yuan Z 2016 *npj Quantum Inf.* **2** 16025
[5] Lütkenhaus N and Shields A J 2009 *New J. Phys.* **11** 045005
[6] Dou T Q, Wang J P, Li Z H, Qu W X, Yang S Y, Sun Z Q, Zhou F, Han Y X, Huang Y Q and Ma H Q 2020 *Chin. Phys. Lett.* **37** 110301
[7] Huang L Y, Zhang Y C and Yu S 2021 *Chin. Phys. Lett.* **38** 040301
[8] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[9] Xu P, Bao S W, Li H W, Wang Y and Bao H Z 2017 *Chin. Phys. Lett.* **34** 020302
[10] Tang G Z, Sun S H and Li C Y 2019 *Chin. Phys. Lett.* **36** 070301
[11] Wang X B 2005 *Phys. Rev. A* **72** 012322
[12] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[13] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[14] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[15] Boaron A *et al.* 2018 *Phys. Rev. Lett.* **121** 190502
[16] Takeoka M, Guha S and Wilde M M 2014 *Nat. Commun.* **5** 5235
[17] Pirandola S, Laurenza R, Ottaviani C, and Banchi L 2017 *Nat. Commun.* **8** 15043
[18] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[19] Ma X, Zeng P and Zhou H 2018 *Phys. Rev. X* **8** 031043
[20] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[21] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z H 2019 *Phys. Rev. Appl.* **11** 034053
[22] Ishio H, Minowa J and Nosu K 1984 *J. Lightwave Technol.* **2** 448
[23] Townsend P D 1997 *Electron. Lett.* **33** 188
[24] Nweke N I 2005 *Appl. Phys. Lett.* **87** 174103
[25] Patel K A, Dynes J F, Lucamarini M, Choi I, Sharpe A W, Yuan Z L, Penty R V and Shields A J 2014 *Appl. Phys. Lett.* **104** 051123
[26] Sun W *et al.* 2018 *J. Appl. Phys.* **123** 043105
[27] Eriksson T *et al.* 2019 *Commun. Phys.* **2** 9
[28] Cai C, Sun Y and Ji Y 2020 *New J. Phys.* **22** 083020
[29] Lin R and Chen J 2021 *IEEE Commun. Lett.* **25** 3918
[30] Li J H, Shi L, Wang J H, Li T X and Xue Y 2021 *AOPC: Optical Sensing and Imaging Technology. SPIE* **12065** 1206530
[31] Xue R *et al.* 2022 *Phys. Rev. Appl.* **17** 024045
[32] Shi S and Xiao N 2022 *Opt. Commun.* **507** 127603
[33] Zeng P, Zhou H Y, Wu W J and Ma X F 2022 arXiv:2201.04300 [quant-ph]
[34] Patel K, Dynes J, Lucamarini M, Choi I, Sharpe A, Yuan Z, Penty R and Shields A 2014 *Appl. Phys. Lett.* **104** 051123
[35] Patel K, Dynes J, Choi I, Sharpe A, Dixon A, Yuan Z, Penty R and Shields A 2012 *Phys. Rev. X* **2** 041010
[36] Peters N *et al.* 2009 *New J. Phys.* **11** 045012
[37] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133
[38] Yoshino K I *et al.* 2012 *Opt. Lett.* **37** 223
[39] Sun Z Q *et al.* 2021 *Chin. Phys. B* **30** 110303