Performance of phase-matching quantum key distribution based on wavelength division multiplexing technology

Haiqiang Ma(马海强)[1,†,‡], Yanxin Han(韩雁鑫)[1,†,§], Tianqi Dou(窦天琦)[2], and Pengyun Li(李鹏云)[3]

[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 9 March 2022; revised manuscript received 23 April 2022; accepted manuscript online 12 May 2022)

Quantum key distribution (QKD) generates information-theoretical secure keys between two parties based on the physical laws of quantum mechanics. The phase-matching (PM) QKD protocol allows the key rate to break the quantum channel secret key capacity limit without quantum repeaters, and the security of the protocol is demonstrated by using equivalent entanglement. In this paper, the wavelength division multiplexing (WDM) technique is applied to the PM-QKD protocol considering the effect of crosstalk noise on the secret key rate. The performance of PM-QKD protocol based on WDM with the influence of adjacent classical channels and Raman scattering is analyzed by numerical simulations to maximize the total secret key rate of the QKD, providing a reference for future implementations of QKD based on WDM techniques.

Keywords: quantum key distribution, wavelength division multiplexing, secret key rate

PACS: 03.67.Dd, 03.67.Hk, 03.67.−a **DOI:** 10.1088/1674-1056/ac6ee3

1. Introduction

Quantum key distribution (QKD) guarantees the security of quantum communication based on the principle of quantum mechanics.[1] Since the first QKD protocol was proposed in 1984,[2] it has been widely concerned theories and experiment.[3–13] However, in applications, the unsatisfactory equipment may lead to some vulnerabilities that can be attacked,[14,15] mainly in the light source at the transmitter and detector at the receiver. As a countermeasure, the decoy-state protocol[16,17] settle the security issue of photon number splitting (PNS), and measurement device independent (MDI) QKD protocol is immune to all attacks against the vulnerabilities of detectors.[18] However, without quantum memory, the maximum possible key rate is limited to the linear key rate PLOB bound, which can be expressed as $R \leq -\log_2(1-\eta)$, where η is transmittance of the experiment setups.[19] Fortunately, the twin-field QKD (TF-QKD) protocol proposed in 2018 has the secret key rate described as $R \sim O(\sqrt{\eta})$,[20] which exceeds the PLOB bound. Compared with the MDI-QKD protocol, the TF-QKD protocol has a higher secret key rate because it not only retains all the advantages of the MDI-QKD protocol, but is caused by single-photon interference rather than two-photon interference. Inspired by the TF-QKD protocol, many theoretical protocols[21–23] and experiments were developed to promote the development of QKD. Among them, the phase-matching (PM) QKD protocol[21] is a scheme that uses entanglement purification to prove security and devises a phase compensation scheme instead of phase locking. Therefore, PM-QKD has the dual advantages of practicality and safety.

Currently, QKD applications have expanded from point-to-point to optical network communications.[24] Most fibre-based QKD experiments use dark fibre as the quantum channel.[25] However, as the number of users of quantum secure communication networks increases, the need for dark fibre increases, which leads to a sharp increase in deployment costs. In addition, the transmission of signals through separate channels in different fibres will not only reduce the efficiency of the fibres, but will also lead to temporal deviation between different signals, causing great inconvenience to high-speed communication and making QKD unworkable. Wavelength division multiplexer (WDM),[26] a technology that multiplexes signals and transmits them in the same fibre, can solve this problem well. It has also been shown in numerous experiments[27–31] that WDM technology can be applied to QKD systems to send more signals over the same transmission distance to effectively increase the key transmission rate. What's more, WDM technology can combine two QKD systems to improve the secret key rate. In addition, there is a growing demand for multiplexing QKD with conventional optical communication in a single fiber due to the high cost of leasing and maintaining fiber resources.

WDM can be generally divided into coarse (C) WDM[32] dense (D) WDM[33] according to the size of the wavelength in-

†These authors contributed equally.
‡Corresponding author. E-mail: hqma@bupt.edu.cn
§Corresponding author. E-mail: hyxin@bupt.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

terval for multiplexing. DWDM is considered as one of the approaches to further expand information transmission capacity at smaller wavelength intervals which in C-band is generally 0.8 mn or 0.4 mn. As for the fiber link, there are two transmission modes based on DWDM technology,[34] full-duplex with a single fibre and bidirectional with two fibres, the difference between them being whether the classical signal can be transmitted in both directions in an optical fiber. However, the power of the classical channel is much stronger than that of the quantum signal, making the coexistence of these two signals not straightforward.[35] When applying DWDM techniques to transmit different signals in a fibre, the quantum channel inevitably is invaded by crosstalk noise photons due to the incomplete isolation of the channel, the non-linear effects of the fibre, etc., which destroy the performance of the QKD.[36]

In this paper, the DWMD technique based on full-duplex with a single fiber transmission is applied to the PM-QKD protocol, and the influencing factors of limiting QKD distance and secret key rate with different power and wavelength ranges are analyzed for the case where channel noise exists.

2. PM-QKD protocol based on DWDM technology

As shown in Fig. 1, classical channels could offer bidirectional communications. Each end-user, Alice and Bob, sends multiple signals of different wavelengths, which are combined by optical multiplexer and transmitted in optical fiber for a long distance. After arriving at an intermediate station, Charlie who could even be a malicious party, the optical signals are separated by optical de-multiplexer and then measured independently after passing through a narrow-band filter (NBF) to exclude noise. And, the single-photon detector (D) is in the method of gate-mode.

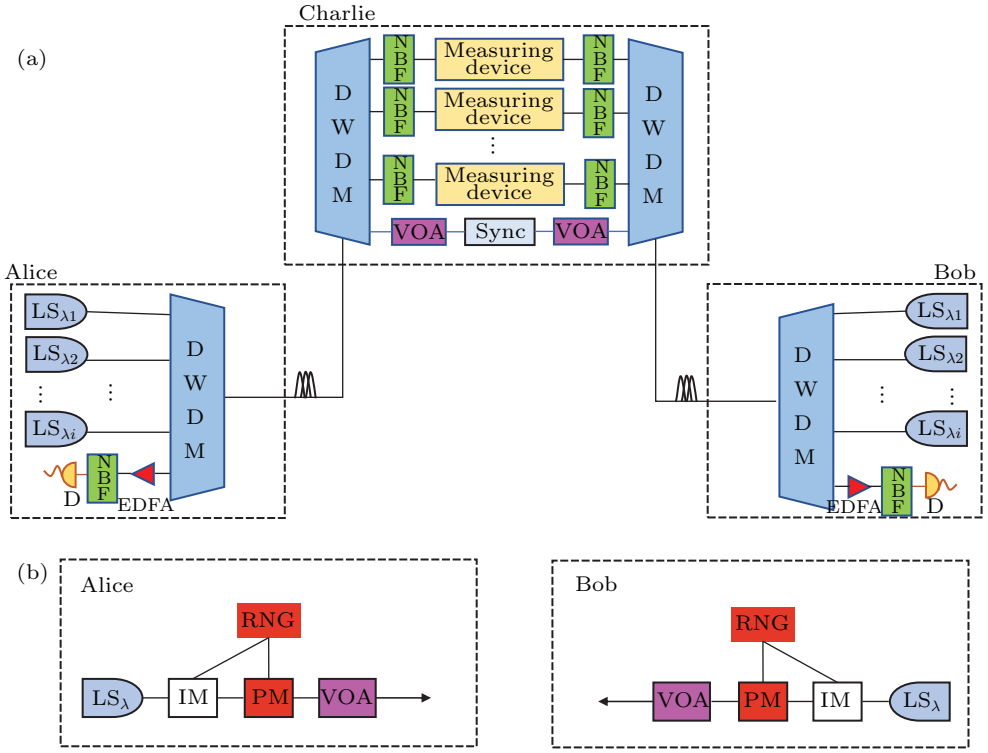


Fig. 1. (a) Schematic for PM-QKD system based on DWDM. (b) Schematic diagram of Alice and Bob sending pulses at (a). LS: laser source; Sync: synchronization clock; VOA: variable optical attenuator; DWDM: dense wavelength division multiplexer; EDFA: erbium doped fiber amplifier; NBF: narrow-band optical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

For the PM-QKD protocol based on DWDM technique, we take single channel of quantum signal as an example. First, Alice (Bob) prepares weak coherent states $\left|\sqrt{\mu_a}\,e^{i(\phi_a+\pi k_a)}\right\rangle_A$ $\left(\left|\sqrt{\mu_b}\,e^{i(\phi_b+\pi k_b)}\right\rangle_B\right)$, where k_a (k_b) is the key information, and ϕ_A (ϕ_B) is the random phase. The users send them to Charlie for independent measurement. Besides, for each independent signal, Alice and Bob pronounce random phases based on the Charlie detector response and choose the case that satisfies $\phi_A \approx \phi_B$ to generate the raw key bits. Then, Alice and Bob perform error correction and privacy amplification on the sifted key bits to generate a secret key. In PM-QKD, when Alice and Bob select $\mu/2$, the secret key rate of PM-QKD protocol can be expressed as[21]

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

where $2/M$ is the sifting factor; E_μ^X is the phase error rate reflecting the information leakage, f stands for the efficiency of error correction code; H_2 is the binary Shannon entropy func-

tion; and Q_μ and E_μ are the overall gain and the error rates, respectively.

When DWDM technology is applied to PM-QKD, it inevitably brings some noise affecting the secret key rate, the most notable of which is the background noise arriving at the receiver. The phase mismatch and linear loss of the fibre can effectively suppress the generation of four-way mixed noise over long fibre distances (50 km and above).[37] So this noise is mainly caused by adjacent channel crosstalk and spontaneous Raman scattering (SRS).[36] The effect of these two types of noise on the performance of the QKD is analyzed respectively as following.

Adjacent channel crosstalk noise

In the application of DWDM technology, the influence brought by the imperfection of the device should be considered. Because the isolation of the multiplexer cannot resist all the classical signals, the classical signals leaked into the quantum channel will produce cross talk to reduce the bit rate of QKD. In general, the probability of leakage from classical channels to two adjacent quantum channels is much higher than that of non-adjacent channels. In addition, NBF we use at the receiving end can effectively suppress non-adjacent channel crosstalk noise. In this paper, we only analyze the crosstalk effect of adjacent channels. We denote the DWDM neighbor channel isolation by γ_α. Then in the transmission fiber, the power, P^{ile}, generated by a single classical channel can be obtained by

$$P^{\text{ile}} = P\mathrm{e}^{(-\alpha L)}10^{(-\gamma_\alpha/10)}, \tag{2}$$

where P is the transmit power of the classical channel, represents the average fiber loss coefficients of both the classical and quantum channels, and L represents the fiber channel length. Then, the corresponding number rate of crosstalk photons generated is

$$P_{\text{c}}^{\text{ile}} = \frac{P^{\text{ile}}\lambda_{\text{q}}T_{\text{d}}\eta_{\text{d}}10^{(-0.1t_{\text{ins}})}}{hc}hc, \tag{3}$$

where λ_{q} and λ_{d} are the wavelengths of the quantum and classical channels, respectively. T_{d} and η_{d} denote the gate width and detection efficiency of the detector, and t_{ins} represents the total insertion loss of the DWDM and the filter.

Spontaneous Raman scattering noise

Inelastic scattering SRS at the same wavelength as the quantum channel is immune to high-isolation DWDM devices and filters, and the SRS noise has a wide spectrum that can easily leak into the quantum channel.[32] SRS noise can be divided into two ways, quantum signal and classical signal transmission direction is the same as forward SRS noise, conversely, backward SRS noise.

For a laser of power P input in the fiber, the SRS noise scattered onto the quantum channel at the output port of the fiber can be expressed as

$$P^{\text{F}} = P\mathrm{e}^{-\alpha L}L\beta\left(\lambda_{\text{d}},\lambda_{\text{q}}\right)\Delta\lambda, \tag{4}$$

$$P^{\text{B}} = P\frac{1-\mathrm{e}^{-2\alpha L}}{2\alpha}\beta\left(\lambda_{\text{d}},\lambda_{\text{q}}\right)\Delta\lambda. \tag{5}$$

Here, $\beta\left(\lambda_{\text{d}},\lambda_{\text{q}}\right)$ is the effective SRS coefficient, P^{F} and P^{B} are the forward and backward SRS noise powers generated in the quantum channel as classical light and quantum signals co-propagate and counter-propagate along the fibre, respectively. $\Delta\lambda$ is the bandwidth of NBF. Correspondingly, the photon number rates of forward and backward SRS noise are

$$P_{\text{c}}^{\text{F}} = \frac{P^{\text{F}}\lambda_{\text{q}}T_{\text{d}}\eta_{\text{d}}10^{(-0.1t_{\text{ins}})}}{hc} = C^{\text{F}}\lambda_{\text{q}}\beta\left(\lambda_{\text{d}},\lambda_{\text{q}}\right), \tag{6}$$

$$C^{\text{F}} = \frac{P\mathrm{e}^{-\alpha L}L\Delta\lambda T_{\text{d}}\eta_{\text{d}}10^{(-0.1t_{\text{ins}})}}{hc}, \tag{7}$$

$$P_{\text{c}}^{\text{B}} = \frac{P^{\text{B}}\lambda_{\text{q}}T_{\text{d}}\eta_{\text{d}}10^{(-0.1t_{\text{ins}})}}{hc} = C^{\text{B}}\lambda_{\text{q}}\beta\left(\lambda_{\text{d}},\lambda_{\text{q}}\right), \tag{8}$$

$$C^{\text{B}} = \frac{P\frac{1-\mathrm{e}^{-2\alpha L}}{2\alpha}\Delta\lambda T_{\text{d}}\eta_{\text{d}}10^{(-0.1t_{\text{ins}})}}{hc}, \tag{9}$$

where h is Planck's constant, c is the speed of light, the coefficients C^{F} and C^{B} are independent of the specific wavelength.

For duplex DWDM systems, the main noise affecting the PM-QKD secret key rate is the noise generated by the joint action of adjacent channel crosstalk noise and SRS noise. For both classical and quantum signals of a single channel, the crosstalk photon number rate affecting the PM-QKD performance is

$$P_{\text{c}}^{\text{C}} = P_{\text{c}}^{\text{ile}} + P_{\text{c}}^{\text{R}} = P_{\text{c}}^{\text{ile}} + P_{\text{c}}^{\text{F}} + P_{\text{c}}^{\text{B}}. \tag{10}$$

For the transmission mode in which a single classical signal is multiplexed with N quantum signals, since the crosstalk noise of non-adjacent channels can be effectively suppressed by DWDM and NBF, the number of crosstalk photons affecting the secret key rate of QKD is

$$P_{\text{c}}^{\text{C}} = P_{\text{c}}^{\text{ile}} + \sum_{n=1}^{N} P_{\text{c}}^{\text{C}}N. \tag{11}$$

3. The numerical simulation

We use numerical simulations to analyze the performance of PM-QKD based on DWDM technology. In order to be of practical application, we set the wavelength of the classical channel to be larger than that of the quantum channel to take advantage of the lower Raman noise of the anti-Stokes. In addition, we place the channel in the C-band. We need to track the input power of the classical channel in order to deal with the quantum channel impairment caused by the classical channel. To facilitate the performance comparison with the original PM-QKD protocol, we used the parameters set in the Ref. [21] for numerical simulations. The specific parameter values used for the numerical simulation are shown in Table 1.

Table 1. Values of parameter in simulation.

Parameter	M	f	μ	$\eta_{\rm det}$	$P_{\rm dc}$ (per pulse)	e_δ	$\lambda_{\rm q}$ (nm)	$\lambda_{\rm d}$ (nm)	$\eta_{\rm d}$	$T_{\rm d}$ (ps)	$t_{\rm ins}$ (dB)	$\Delta\lambda$ (nm)
Values	16	1.15	0.3	14.5%	8×10^{-8}	1.5%	1551.72	1552.52	0.15	500	5.5	0.12

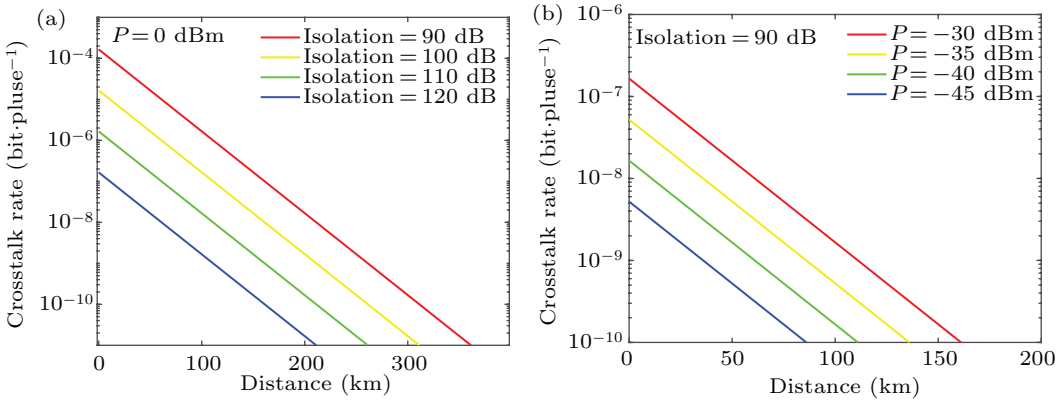


Fig. 2. Crosstalk noise rate for different influencing factors. (a) At different isolation. (b) At different input power of the classical channel.

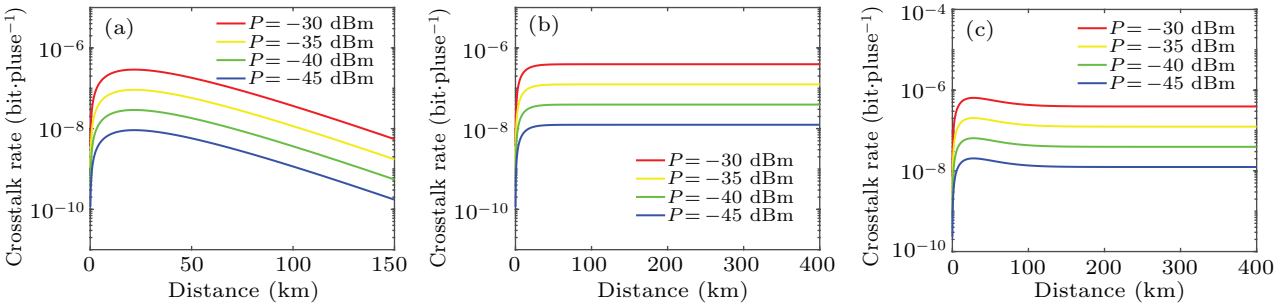


Fig. 3. Crosstalk noise rates for different types of Raman scattering at different input powers of the classical channel. (a) Forward Raman scattering. (b) Backward Raman scattering. (c) Total Raman scattering.

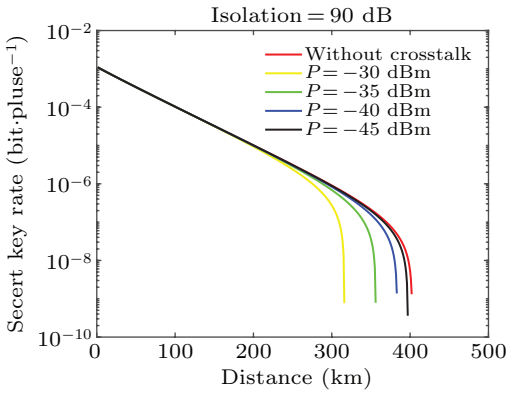


Fig. 4. Secret key rate for PM-QKD protocol with different input power of the classical channel.

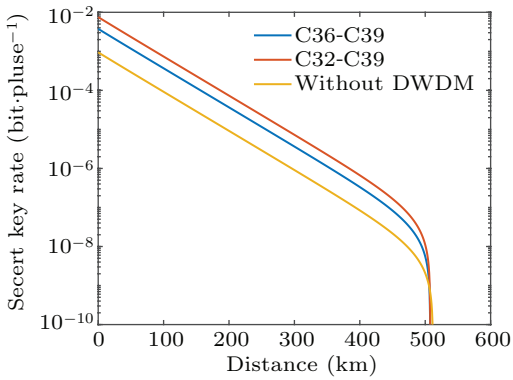


Fig. 5. Secret key rate of PM-QKD protocol with different number of quantum channel multiplexes.

The following cases are performed numerical simulations and theoretical analyses: (1) When only crosstalk of adjacent classical channels is considered, the crosstalk photon nosie rates for different isolation and input power are shown in Figs. 2(a) and 2(b). (2) When only SRS noise is considered, the relationship between crosstalk photon noise rates and input power are shown in Fig. 3. It can be seen from Fig. 3(c) that with the increase of transmission distance, the influence of crosstalk photon noise rate of backward SRS is significantly stronger than that of forward SRS. Classical signal back propagation ensures the limitation of QKD performance. Moreover, when the input power is −45 dBm, the decreasing trend of the crosstalk photon nosie rate of the total SRS noise becomes larger obviously. (3) In the case of cooperative propagation of adjacent channels based on a single optical fiber, the relationship between secret key rate and input power is shown in Fig. 4. It can be seen that the application of DWDM technology affects the secret key rate with single wavelength channel, to the extent that it is related to the input power. (4) Based on the above results, using the ITU-TG.692 standard with an

interval of 100 GHz, Fig. 5 shows the effect of different quantum channel numbers on the PM-QKD secret key rate. This suggests that the rates can be further increased with greater numbers of WDM channels when the rates are saturated. It is worth noting that in multiplexed channels, the noise produced by adjacent channel crosstalk is more limiting to PM-QKD performance than that produced by SRS, because the photons accumulated along the fiber are eventually lost as fiber attenuation increases, resulting in a reduction of SRS noise.

4. Conclusions

In this paper, we discuss the factors that affect the performance of PM-QKD based on DWDM technology. The main elements are the quantitative analysis of the variation of channel noise rate at different input powers and the secret key rate of the PM-QKD under the influence of different noises. In addition, the secret key rate of PM-QKD with different number of quantum channels is also simulated. The simulation results show that as the input power of the classical channel decreases, the isolation of DWDM becomes wider and the channel crosstalk noise has less impact on the performance of the PM-QKD. For different channel parameters, the optimal values of the PM-QKD performance are given separately according to the full duplex DWDM scheme based on a single fibre. In this paper, the application of DWDM technology to PM-QKD is extended to provide a reference for realizing a quantum communication network with both secret and high speed.

Acknowledgements

Project 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] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595
[2] Bennett C H and Brassard G 1984 *Processings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1999, Banglore, India (IEEE, New York, 1984) p. 175
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys* **74** 145
[4] Lütkenhaus N and Shields A J 2009 *New J. Phys.* **11** 045005
[5] Grünenfelder F, Boaron A, Rusca D, Martin A and Zbinden H 2018 *Appl. Phys. Lett.* **112** 051108
[6] Gan Y H, Wang Y, Bao W S, He R S, Zhou C and Jiang M S 2019 *Chin. Phys. Lett.* **36** 040301
[7] Liao S K, Lin J, Ren J G, Liu W Y, *et al.* 2017 *Chin. Phys. Lett.* **34** 090302
[8] Tang G Z, Sun S H and Li C Y 2019 *Chin. Phys. Lett.* **36** 070301
[9] Mao Y, Liu Q, Guo Y, Zhang H and Zhou J 2019 *Chin. Phys. Lett.* **36** 100302
[10] Zhao Y B, Zhang W L, Wang D, Song X T, Zhou L J and Ding C B 2019 *Chin. Phys. B* **28** 104203
[11] Li J J, Wang Y, Li H W and Bao S W 2020 *Chin. Phys. B* **29** 030303
[12] Li X, Yuan H W, Zhang C M and Wang Q 2020 *Chin. Phys. B* **29** 070303
[13] Tang G Z, Sun S H, Chen H, Li C Y and Liang L M 2016 *Chin. Phys. Lett.* **33** 120301
[14] Zhang C M, Zhu J R and Wang Q 2018 *Commun. Theor. Phys.* **70** 379
[15] Tang Z, Wei K, Bedroya O, Qian L and Lo H K 2016 *Phys. Rev. A* **93** 042308
[16] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[17] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[18] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[19] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[20] Lucamarini M, Yuan Z, Dynes J and Shields A 2018 *Nature* **557** 400
[21] Ma X, Zeng P and Zhou H 2018 *Phys. Rev. X* **8** 031043
[22] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[23] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053
[24] Fernandez V, Collins R J, Gordon K J, Townsend P D and Buller G S 2009 *IEEE J. Quantum Electron.* **43** 130
[25] Qi B, Zhu W, Qian L and Lo H K 2010 *New J. Phys.* **12** 103042
[26] He R S, Jiang M S, Wang Y, Gan Y H, Zhou C and Bao W S 2019 *Chin. Phys. B* **28** 040303
[27] Townsend P 1997 *Electron. Lett.* **33** 188
[28] Nweke N I 2005 *Appl. Phys. Lett.* **87** 174103
[29] Patel K A, Dynes J F, Lucamarini M and Choi I, Sharpe A W, Yuan Z L, Penty R V and Shields A J 2014 *Appl. Phys. Lett.* **104** 051123
[30] Sun W, Wang L J, Sun X X, Mao Y Q, Yin H L, Wang B X, Chen T Y and Pan K W 2018 *J. Appl. Phys.* **123** 043105
[31] Sun Z Q, Han Y X, Dou T Q, Wang J P, Li Z H, Zhou F, Huang Y Q and Ma H Q 2021 *Chin. Phys. B* **30** 110303
[32] Patel K A, Dynes J F, Choi I, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2012 *Phys. Rev. X* **2** 041010
[33] Huang D, Lin D, Wang C, Liu W Q, Fang S H, Peng J Y and Zeng G H 2015 *Opt. Express* **23** 17511
[34] Bahrani S, Razavi M and Salehi J A 2018 *Sci. Rep.* **8** 3456
[35] Bahrani S, Razavi M and Salehi J A 2016 *24th European Signal Processing Conference (EUSIPCO) AUG 28-SEP 02*, 2016, Budapest, Hungary, pp. 483–487
[36] Eraerds P, Walenta N, Legré M, Gisin N and Zbinden H 2010 *New J. Phys.* **12** 063027
[37] Du S, Tian Y and Li Y 2020 *Phys. Rev. Appl.* **14** 024013