Phase-matching quantum key distribution with advantage distillation

Rui-Qiang Wang\textsuperscript{1,2,3}, Chun-Mei Zhang\textsuperscript{4,5}, Zhen-Qiang Yin\textsuperscript{1,2,3,*}, Hong-Wei Li\textsuperscript{5}, Shuang Wang\textsuperscript{1,2,3}, Wei Chen\textsuperscript{1,2,3}, Guang-Can Guo\textsuperscript{1,2,3} and Zheng-Fu Han\textsuperscript{1,2,3}

\textsuperscript{1} CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, People’s Republic of China
\textsuperscript{2} Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People’s Republic of China
\textsuperscript{3} State Key Laboratory of Cryptology, PO Box 5159, Beijing 100878, People’s Republic of China
\textsuperscript{4} Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing, 210003, People’s Republic of China
\textsuperscript{5} Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450000, People’s Republic of China

* Authors to whom any correspondence should be addressed.
E-mail: cmz@njupt.edu.cn and yinzq@ustc.edu.cn

Keywords: quantum key distribution, quantum cryptography, quantum information, phase-matching QKD, advantage distillation

Abstract
Phase-matching quantum key distribution (PM-QKD) provides a promising solution to surpass the fundamental rate–distance bound without quantum repeaters. In this paper, we insert an additional advantage distillation (AD) step after quantum communication to improve the performance of PM-QKD. Simulation results show that, by splitting the raw key into blocks of only a few bits so as to identify highly correlated bit pairs, the AD method can tolerate high system misalignment errors and improve the secret key rate and transmission distance significantly, which is very promising in current PM-QKD systems.

1. Introduction
Quantum key distribution (QKD) \cite{1,2} can distribute information-theoretic secret keys between two legitimate peers Alice and Bob, even in the presence of an eavesdropper Eve. Owing to the advantage of the theoretic security, lots of QKD demonstrations with high rate and long distance have been reported \cite{3–7}. However, the fundamental rate–distance bound \cite{8,9} limits the performance of these demonstrations, which was widely believed to hold for practical QKD systems without relays.

Fortunately, twin-field QKD (TF-QKD) \cite{10} opens the possibility of overcoming the rate–distance bound without quantum repeaters. Inspired by the original TF-QKD protocol, many variants \cite{11–19} have been proposed to rigorously improve the security, and some of them have been demonstrated experimentally \cite{20–26}. One of the variants, named phase-matching QKD (PM-QKD) \cite{11,19}, adopts only one basis for key generation and parameter estimation, which can overcome the rate–distance bound under large system misalignment errors. However, it is unknown whether the performance of PM-QKD can be further improved.

In this paper, we propose to improve the performance of PM-QKD with the advantage distillation (AD) method. Note that the AD method has already been adopted in various QKD protocols \cite{27–33}. By splitting the raw key into blocks of only a few bits, we can separate highly correlated bit pair from weakly correlated information. Simulation results show that, PM-QKD with AD can tolerate high system misalignment errors, and improve both the secret key rate and transmission distance significantly.

The rest of this paper is organized as follows. In section 2, we briefly review the security of QKD with AD. In section 3, we introduce PM-QKD with AD. In section 4, we illustrate the numerical results of PM-QKD with AD. We conclude the paper in section 5.
2. Security of QKD with AD

In an entanglement-based scheme, Alice prepares the quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends the second qubit to Bob through the quantum channel. Then Alice and Bob take inputs from four dimensional Hilbert spaces $H_A \otimes H_B$ to apply the measurements of the $Z$ and $X$ bases, where the $Z$ basis consists of $|0\rangle$ and $|1\rangle$, and the $X$ basis consists of $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Since the quantum channel is controlled by Eve, the final state shared between Alice and Bob can be given as

$$\sigma_{AB} = \lambda_0 |\Phi_0\rangle \langle \Phi_0 | + \lambda_1 |\Phi_1\rangle \langle \Phi_1 | + \lambda_2 |\Phi_2\rangle \langle \Phi_2 | + \lambda_3 |\Phi_3\rangle \langle \Phi_3 |,$$

where $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $|\Phi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, and $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1$. Obviously, the single photon error rates in the $Z$ and $X$ bases are constrained by $\lambda_2 + \lambda_3 = e_x$ and $\lambda_1 + \lambda_3 = e_s$, respectively. The secret key rate shared between Alice and Bob can be given by

$$R \geq \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} \left\{ S(A|E) - H(A|B) \right\}$$

$$= \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} \left\{ 1 - (\lambda_0 + \lambda_1)H\left( \frac{\lambda_0}{\lambda_0 + \lambda_1} \right) - (\lambda_2 + \lambda_3)H\left( \frac{\lambda_2}{\lambda_2 + \lambda_3} \right) - H(\lambda_0 + \lambda_1) \right\},$$

where $E$ is Eve’s ancillary state, $S(A|E) = S(A,E) - S(E)$, $H(A|B) = H(A,B) - H(B)$, $H(x) = -x \log(x) - (1-x) \log(1-x)$ and $S(\rho) = -\text{tr}(\rho \log \rho)$ are entropy functions. Note that Eve is free to choose optimal $\lambda_i$ to eavesdrop as long as $\lambda_i$ is constrained by the error rates in different bases.

To improve the performance of QKD, the AD method was proposed [27], which can increase the secret key rate shared between Alice and Bob. Specifically, Alice and Bob split their raw key into blocks $a_1, a_2, \ldots, a_b$ and $b_1, b_2, \ldots, b_b$ of size $b$. Depending on a randomly chosen bit $c \in \{0, 1\}$, Alice sends the message $m = \{m_1, m_2, \ldots, m_b\} = \{a_1 \oplus c, a_2 \oplus c, \ldots, a_b \oplus c\}$ to Bob through an authenticated classical channel. They accept the block if and only if Bob announces the result of $\{m_1 \oplus y_1, m_2 \oplus y_2, \ldots, m_b \oplus y_b\}$ is $\{0, 0, \ldots, 0\}$ or $\{1, 1, \ldots, 1\}$. Then, they keep the first bit of their initial block as raw key. Obviously, the successful probability of AD on a certain block of size $b$ is

$$p_{\text{succ}} = (\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b,$$

and the quantum state shared between Alice and Bob can be given by

$$\tilde{\sigma}_{AB} = \tilde{\lambda}_0 |\Phi_0\rangle \langle \Phi_0 | + \tilde{\lambda}_1 |\Phi_1\rangle \langle \Phi_1 | + \tilde{\lambda}_2 |\Phi_2\rangle \langle \Phi_2 | + \tilde{\lambda}_3 |\Phi_3\rangle \langle \Phi_3 |,$$

where

$$\tilde{\lambda}_0 = \frac{(\lambda_0 + \lambda_1)^b + (\lambda_0 - \lambda_1)^b}{2p_{\text{succ}}},$$

$$\tilde{\lambda}_1 = \frac{(\lambda_0 + \lambda_1)^b - (\lambda_0 - \lambda_1)^b}{2p_{\text{succ}}},$$

$$\tilde{\lambda}_2 = \frac{(\lambda_2 + \lambda_3)^b + (\lambda_2 - \lambda_3)^b}{2p_{\text{succ}}},$$

$$\tilde{\lambda}_3 = \frac{(\lambda_2 + \lambda_3)^b - (\lambda_2 - \lambda_3)^b}{2p_{\text{succ}}}.$$  

Consequently, the secret key rate of QKD enhanced with AD can be modified as

$$\tilde{R} \geq \max_b \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} \frac{1}{b p_{\text{succ}}} \left[ 1 - \left( \tilde{\lambda}_0 + \tilde{\lambda}_1 \right) H\left( \frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1} \right) - \left( \tilde{\lambda}_2 + \tilde{\lambda}_3 \right) H\left( \frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3} \right) - H\left( \tilde{\lambda}_0 + \tilde{\lambda}_1 \right) \right].$$  

3. PM-QKD with AD

Based on the original PM-QKD proposed in [11, 19], we give the procedure of PM-QKD with AD as follows:

(a) **State preparation.** Alice chooses a random key bit $k_d \in \{0, 1\}$, an intensity $\mu_d \in \{\mu, \mu_1, \mu_2, \ldots\}$, and a random phase $\phi_{d\prime}$ from the set $\{2\pi \mu_d\}^{M-1}$ to prepare the coherent state $\sqrt{\mu_d} e^{i(\phi_{d\prime} + \pi k_d)}$. Similarly, Bob chooses $k_{d\prime}, \mu_{d\prime}$ and $\phi_{d\prime}$ to prepare the coherent state $\sqrt{\mu_{d\prime}} e^{i(\phi_{d\prime} + \pi k_d)}$. 


(b) **Measurement.** Alice and Bob transmit their quantum states to a third party Eve. If Eve is cooperative, she interferes the states on a 50:50 beam splitter, directs the two output pulses to two threshold detectors $L$ and $R$, and records her measurement results.

(c) **Announcement.** Eve announces her measurement results. Then, Alice and Bob announce their random phases and intensities $j_{d'}$, $\mu_{d'}$ and $j_{d''}$, $\mu_{d''}$ respectively, and keep those events with $\mu_{d'} = \mu_{d''} = \mu$, and $j_{d'} = j_{d''} = j_0' = j_0''$. Sifting.

(d) **Sifting.** Alice and Bob repeat the above steps sufficient times. When Eve announces a successful detection (either $L$ clicks or $R$ clicks), Alice and Bob keep $k_d$ and $k_{d''}$ as their raw key bits. Bob flips his key bit $k_d$ if Eve announces detector $R$ clicks. If $j_{d'} = j_{d''} = j_0' = j_0''$, Bob flips his key bit $k_d$.

(e) **Parameter estimation.** For all the raw data they have obtained, Alice and Bob can estimate the gains $Q_{\mu}$, and quantum bit error rates $E_{\mu}$, for different intensities. Then, they can estimate the information leakage $E_{\mu}^X$.

(f) **AD.** For the events with $\mu_{d'} = \mu_{d''} = \mu$, Alice and Bob perform AD on every block of $b$ bits in their raw key to obtain highly correlated raw key bits.

(g) **Post-processing.** Alice and Bob perform key reconciliation and privacy amplification on the raw key data to get the final secret keys.

The secret key rate of PM-QKD with AD is

$$R \geq \max_b \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} \frac{1}{bM} Q_{\mu} P_{\text{succ}} \left[ 1 - \left( \frac{\lambda_0 + \lambda_1}{\lambda_0 + \lambda_1 + \lambda_2} \right) H \left( \frac{\lambda_0}{\lambda_0 + \lambda_1 + \lambda_2} \right) - \left( \frac{\lambda_2 + \lambda_3}{\lambda_2 + \lambda_3 + \lambda_1} \right) H \left( \frac{\lambda_2}{\lambda_2 + \lambda_3 + \lambda_1} \right) - f \left( H(E_{\mu}) \right) \right], \quad (7)$$

subject to

$$E_{\mu} = \lambda_2 + \lambda_3,$$

$$E_{\mu}^X \leq \lambda_1 + \lambda_3 \leq E_{\mu}^X,$$

$$\lambda_0 + \lambda_1 = \lambda_2 + \lambda_3 = 1,$$

$$P_{\text{succ}} = (E_{\mu})^b + (1 - E_{\mu})^b,$$

$$\bar{E}_{\mu} = \frac{(E_{\mu})^b}{(E_{\mu})^b + (1 - E_{\mu})^b},$$

$$\lambda_0 = \frac{(\lambda_0 + \lambda_1)^b + (\lambda_0 - \lambda_1)^b}{2((\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b)},$$

$$\lambda_1 = \frac{(\lambda_0 + \lambda_1)^b - (\lambda_0 - \lambda_1)^b}{2((\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b)},$$

$$\lambda_2 = \frac{(\lambda_2 + \lambda_3)^b + (\lambda_2 - \lambda_3)^b}{2((\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b)},$$

$$\lambda_3 = \frac{(\lambda_2 + \lambda_3)^b - (\lambda_2 - \lambda_3)^b}{2((\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b)},$$

where $E_{\mu}^X$ and $E_{\mu}^X$ denote the low and upper bounds of $E_{\mu}^X$ [19], which can be estimated with the decoy-state method [34–36], and $f$ denotes the error correction efficiency. We emphasize that, if Alice and Bob adopt infinite number of decoy states, they can obtain the exact values of $E_{\mu}^X$, and the second inequality in equation (8) will be reduced to an equality, that is, $E_{\mu}^X = \lambda_1 + \lambda_3$.

4. **Simulation**

For a typical implementation PM-QKD [19], we assume that the detection efficiency of single-photon detectors $\eta_d$ is 20%, the dark count rate of single-photon detectors $p_d$ is $1 \times 10^{-8}$, the error correction efficiency $f$ is 1.1, the loss coefficient of the standard fiber link $\alpha$ is 0.2 dB km$^{-1}$, and the number of phase slices $D$ is 16 which is large enough to ignore the effect of discrete phase randomization [19]. For simplicity, we adopt infinite number of decoy states in our simulation, and the calculation models for $Q_{\mu}$, $E_{\mu}$ and $E_{\mu}^X$ are given by [19].
Figure 1. Results of the secret key rate with respect to the transmission distance between Alice and Bob under \( e_d = 1\% \) and 13\%. The black line denotes the PLOB bound [9], the solid PM-AD curves denote the results of PM-QKD with AD, and the dotted PM curves denote the results of original PM-QKD. The nonsmooth points in PM-AD indicate the change of optimal \( b \) (see figure 2 for details).

Figure 2. Results of the optimal \( b \) with respect to the transmission distance between Alice and Bob in PM-QKD with AD, under \( e_d = 1\% \) and 13\%.

\[
Q_\mu = 1 - (1 - 2p_d)e^{-2\mu},
E_\mu = \frac{(p_d + 2\eta\mu e_d)e^{-2\eta\mu}}{Q_\mu},
E_X = q_{even} = \frac{e^{-2p_d(\cosh(2\mu) - (1 - 2p_d)\cosh(2(1 - \eta)\mu))}}{Q_\mu}.
\]  

With equations (7)–(9), we simulate the performance of PM-QKD with AD in the asymptotic case under different system misalignment errors \( e_d \). The results of PM-QKD with AD under \( e_d = 1\% \) and 13\% are shown in figure 1, and the results of PM-QKD without AD are plotted in comparison. Note that, for fair comparison, the simulation of original PM-QKD here only considers the same and opposite phases, which is different from [19]. In figure 1, PM-AD denotes PM-QKD with AD, and PM denotes the original PM-QKD protocol. It can be seen that PM-QKD with AD is more tolerable to noises, and the corresponding optimal values of \( b \) are illustrated in figure 2. Under \( e_d = 1\% \), the secret key rates of PM-AD and PM are the same when the transmission distance is less than about 500 km, and the corresponding optimal \( b \) for PM-AD stays to be 1, which indicates that the AD procedure is actually not performed; while PM-AD begins to show its obvious advantage when the transmission distance is larger than about 500 km. Under \( e_d = 13\% \), PM-AD exhibits
performance better than that of original PM-QKD especially in the long distance range, which demonstrates the necessity of the AD procedure in PM-QKD under large system misalignment error.

To further investigate the great tolerance of noises in PM-QKD with AD, we plot the results of secret key rate under $e_d = 20\%$ in figure 3 and the corresponding optimal $b$ in figure 4. It can be seen that, under $e_d = 20\%$, PM-AD can just beat the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound, which demonstrates the necessity of the AD procedure in PM-QKD again. Moreover, as shown in figures 2 and 4, when the transmission distance is not so long, the optimal $b$ stays to be 1 under $e_d = 1\%$ or 2 under $e_d = 13\%, 20\%$; while with the increase of transmission distance which will introduce more noises, the correlation of raw key becomes weaker, hence the optimal $b$ begins to increase. We emphasize that in the PM-QKD protocol with AD, larger $b$ promises longer transmission distance and greater noise tolerance, while it also means lower secret key rate. Hence, to accelerate the computation time, we reasonably set the searching range of $b$ to be the set $[1, 7]$ in all our simulations.

5. Conclusion

In conclusion, we have proposed to insert an additional AD procedure in PM-QKD, and investigated its performance in the asymptotic case. Simulation results demonstrate that PM-QKD with AD can tolerate large system misalignment errors only by splitting the raw key of Alice and Bob into blocks of a few bits.
Particularly, the AD procedure does not change the hardware of PM-QKD, which can be conveniently applied to current systems. We expect our work can provide a valuable reference for researchers to design QKD systems.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (Grant No. 2020YFA0309802), the National Natural Science Foundation of China (Grant Nos. 62171424, 61961136004). Chun-Mei Zhang was supported by the China Postdoctoral Science Foundation (Grant Nos. 2019T120446, 2018M642281) and the Natural Science Foundation of NJUPT (Grant Nos. NY221058, 1311). Hong-Wei Li was supported by NSAF (Grant No. U2130205) and Natural Science Foundation of Henan (Grant No. 202300410532).

Data availability statement

The data generated and/or analysed during the current study are not publicly available for legal/ethical reasons but are available from the corresponding author on reasonable request.

ORCID iDs

Rui-Qiang Wang https://orcid.org/0000-0002-5296-6507
Chun-Mei Zhang https://orcid.org/0000-0002-4682-0384
Zhen-Qiang Yin https://orcid.org/0000-0002-3486-3934

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. Computers, Systems and Signal Processing pp 175–9
[2] Ekert A K 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661–3
[3] Fröhlich B, Lucamarini M, Dynes J F, Comandar L C, Tam W W-S, Plews A, Sharpe A W, Yuan Z and Shields A J 2017 Long-distance quantum key distribution secure against coherent attacks Optica 4 163–7
[4] Wang S, Chen W, Guo J-F, Yin Z-Q, Li H-W, Zhou Z, Guo G-C and Han Z-F 2012 2 GHz clock quantum key distribution over 260 km of standard telecom fiber Opt. Lett. 37 1008–10
[5] Boaron A et al 2018 Secure quantum key distribution over 421 km of optical fiber Phys. Rev. Lett. 121 190502
[6] Yin H-L et al 2016 Measurement-device-independent quantum key distribution over a 404 km optical fiber Phys. Rev. Lett. 117 190501
[7] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 High-rate measurement-device-independent quantum cryptography Nat. Photon. 9 397–402
[8] Takeoka M, Guha S and Wilde M M 2014 Fundamental rate-loss tradeoff for optical quantum key distribution Nat. Commun. 5 5235
[9] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications Nat. Commun. 8 15043
[10] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Overcoming the rate–distance limit of quantum key distribution without quantum repeaters Nature 557 400–3
[11] Ma X, Zeng P and Zhou H 2018 Phase-matching quantum key distribution Phys. Rev. X 8 031043
[12] Tamaki K, Lo H-K, Wang W and Lucamarini M 2018 Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound (arXiv:1805.05511)
[13] Wang X-B, Yu Z-L and Hu X-L 2018 Twin-field quantum key distribution with large misalignment error Phys. Rev. A 98 062323
[14] Cui C, Yin Z-Q, Wang R, Chen W, Wang S, Guo G-C and Han Z-F 2019 Twin-field quantum key distribution without phase postselection Phys. Rev. Appl. 11 034053
[15] Curty M, Azuma K and Lo H-K 2019 Simple security proof of twin-field type quantum key distribution protocol npj Quantum Inf. 5 64
[16] Lin J and Lütkenhaus N 2018 Simple security analysis of phase-matching measurement-device-independent quantum key distribution Phys. Rev. A 98 042332
[17] Yin H-L and Fu Y 2019 Measurement-device-independent twin-field quantum key distribution Sci. Rep. 9 3045
[18] Wang R et al 2020 Optimized protocol for twin-field quantum key distribution Commun. Phys. 3 149
[19] Zeng P, Wu W and Ma X 2020 Symmetry–protected privacy: beating the rate–distance linear bound over a noisy channel Phys. Rev. Appl. 13 064013
[20] Minder M, Pittaluga M, Roberts G L, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2019 Experimental quantum key distribution beyond the repeaterless secret key capacity Nat. Photon. 13 334–8
[21] Wang S, He D-Y, Yin Z-Q, Li F-Y, Cui C-H, Chen W, Zhou Z, Guo G-C and Han Z-F 2019 Beating the fundamental rate–distance limit in a proof-of-principle quantum key distribution system Phys. Rev. X 9 021046
[22] Zhong X, Hu J, Curty M, Qian L and Lo H-K 2019 Proof-of-principle experimental demonstration of twin-field type quantum key distribution Phys. Rev. Lett. 123 100506
[23] Fang X-T et al 2020 Implementation of quantum key distribution surpassing the linear rate-transmittance bound Nat. Photon. 14 422–5
[24] Liu Y et al 2019 Experimental twin-field quantum key distribution through sending or not sending Phys. Rev. Lett. 123 100505
[25] Chen J-P et al 2020 Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km Phys. Rev. Lett. 124 070501
[26] Wang S et al 2022 Twin-field quantum key distribution over 830 km fibre Nat. Photon. 16 154–61
[27] Renner R 2008 Security of quantum key distribution Int. J. Quantum Inf. 06 1–127
[28] Kraus B, Branciard C and Renner R 2007 Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses Phys. Rev. A 75 012316
[29] Bae J and Acín A 2007 Key distillation from quantum channels using two-way communication protocols Phys. Rev. A 75 012334
[30] Murta G, Rozpędek F, Ribeiro J, Elkouss D and Wehner S 2020 Key rates for quantum key distribution protocols with asymmetric noise Phys. Rev. A 101 062321
[31] Tan E Y-Z, Lim C C-W and Renner R 2020 Advantage distillation for device-independent quantum key distribution Phys. Rev. Lett. 124 020502
[32] Li H-W, Zhang C-M, Jiang M-S and Cai Q-Y 2022 Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology Commun. Phys. 5 53
[33] Li H-W, Wang R-Q, Zhang C-M and Cai Q-Y 2022 Improving the performance of twin-field quantum key distribution with advantage distillation technology (arXiv:2202.10059)
[34] Wang X-B 2005 Beating the photon-number-splitting attack in practical quantum cryptography Phys. Rev. Lett. 94 230503
[35] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution Phys. Rev. Lett. 94 230504
[36] Ma X, Qi B, Zhao Y and Lo H-K 2005 Practical decoy state for quantum key distribution Phys. Rev. A 72 012326