Discrete-phase-randomized twin-field quantum key distribution with advantage distillation

Chun-Mei Zhang,[1,2] Zhe Wang,[1,2] Yu-Da Wu,[1,2] Jian-Rong Zhu,[3] Rong Wang,[4,*] and Hong-Wei Li[5,†]

[1]*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[2]*State Key Laboratory of Cryptology, Beijing 100878, China*

[3]*School of Information Technology, Jiangsu Open University, Nanjing 210017, China*

[4]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong 999077 SAR, China*

[5]*Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450000, China*

(Received 2 January 2024; accepted 8 May 2024; published 22 May 2024)

The twin-field quantum key distribution (TF-QKD) protocol and its variants provide promising solutions to long-distance information-theoretic-secure communication, which can surpass the fundamental rate-loss bound without quantum repeaters. Different from other variants, the discrete-phase-randomized TF-QKD variant only needs to modulate weak coherent sources with random discrete phases, which avoids the necessity of modulating continuously randomized phases and can be implemented with current technology. However, the discrete-phase-randomized variant compromises the performance of TF-QKD under high channel losses and error rates. To overcome this dilemma, we propose to adopt the advantage distillation method to improve the performance of discrete-phase-randomized TF-QKD, and analyze its security in the asymptotic case. Without changing the optical hardware of TF-QKD systems, the proposed scheme can improve the secret key rate under high channel losses and error rates, and extend the tolerable channel loss as well.

DOI: 10.1103/PhysRevA.109.052432

I. INTRODUCTION

Based on the laws of quantum physics, quantum key distribution (QKD) [1] can provide two distant legitimate peers, Alice and Bob, with information-theoretic secret keys, in the presence of an eavesdropper, Eve. Due to the superiority of proven security, much effort has been devoted to promote the secret key rate and tolerable channel loss of practical QKD systems [2–7]. However, the performance of these demonstrations is upper bounded by the fundamental repeaterless rate-loss bound [8,9], more precisely, the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound $R \leqslant -\log_2(1-\eta)$ [9], where R is the secret key rate and η is the overall channel transmittance between Alice and Bob. Fortunately, twin-field QKD (TF-QKD) [10] unlocks the possibility of breaking the rate-loss bound without quantum repeaters. Inspired by the original TF-QKD protocol, a series of variants [11–26] have been proposed to rigorously improve the security and performance, and some of them have been demonstrated experimentally [27–35].

To ensure the security of TF-QKD, the weak coherent sources (WCSs) prepared by Alice and Bob should be randomly switched between the code mode and the test mode. The events in the code mode constitute the raw key, and the events in the test mode can be used to bound the channel parameters. The decoy-state method [36–38] is always adopted in the test mode to estimate the channel parameters more accurately. In the decoy-state scheme, the phases of WCSs should be continuously randomized in $[0, 2\pi)$, which can be regarded as a classical mixture of photon-number states. However, the preparation of continuous-phase-randomized WCSs is technically challenging. To bridge the gap between theory and practice in phase randomization, the discrete-phase-randomized WCSs, which modulate a finite number of phases to approach an infinite number of phases, are alternatively adopted in the decoy-state Bennett-Brassard 1984 (BB84) QKD [39], measurement-device-independent QKD [40], and TF-QKD [21–25]. Particularly, Ref. [21] modulates only two phases in the code mode, and Ref. [22] modulates M phases. The difference in the code mode leads to different implementations of TF-QKD and different formulas of phase error rate and secret key rate.

Nevertheless, the discrete-phase-randomized WCSs, which can be implemented with current technology, compromise the performance of TF-QKD under high channel losses and error rates. Fortunately, as one kind of universal methods, advantage distillation (AD) [41] can obviously enhance the secret key rate of QKD under high channel losses and error rates, which has been successfully applied to enhance the performance of some QKD protocols [42–53]. In particular, Ref. [47] assumed that TF-QKD were implemented with continuous-phase-randomized WCSs, the preparation of which, however, is technically demanding by the state of the art. Reference [48] empirically modulated many discrete phases to approach the continuous-phase-randomized WCSs, which lacks a rigorous security analysis nevertheless. Intuitively, the effect of discrete-phase-randomized modulation can be reduced by choosing an appropriate number of phases. However, there are two major issues which need to be carefully addressed: (1) how to rigorously determine the

*rwangphy@hku.hk

†lihow@ustc.edu.cn

 ©2024 American Physical Society

appropriate number of phases, and (2) the performance of some TF-QKD variations [11,18,19,22] is directly affected by the number of phases. Therefore, considering both the feasibility and performance of implementation, it is necessary to adopt the AD method to improve the performance of discrete-phase-randomized TF-QKD. Simulation results show that the AD method can improve the secret key rate of discrete-phase-randomized TF-QKD under high channel losses and error rates, and extend the tolerable channel loss as well. Furthermore, the proposed scheme only adds an extra step of dividing raw key bits into blocks of a few bits so as to extract highly correlated bits, which enjoys the same optical hardware as the previous scheme and can be efficiently integrated into the current discrete-phase-randomized TF-QKD systems.

II. DISCRETE-PHASE-RANDOMIZED TF-QKD WITH AD

The procedure of discrete-phase-randomized TF-QKD with AD runs as follows:

(1) *State preparation*. Alice (Bob) randomly chooses the code mode or test mode for each trial.

(a) If the code mode is chosen, she (he) randomly selects a key bit k_a (k_b) and a random number x (y) to prepare a coherent state $|\sqrt{\mu}e^{i(k_a\pi+2\pi x/M)}\rangle$ ($|\sqrt{\mu}e^{i(k_b\pi+2\pi y/M)}\rangle$), where $k_a, k_b \in \{0,1\}$, $x, y \in \{0,1,2,\ldots,M-1\}$, μ denotes the intensity of coherent states, and M, which is even, denotes the number of discrete phases.

(b) If the test mode is chosen, she (he) randomly selects an intensity ξ_a (ξ_b) and a random number x (y) to prepare a coherent state $|\sqrt{\xi_a}e^{i2\pi x/M}\rangle$ ($|\sqrt{\xi_b}e^{i2\pi y/M}\rangle$), where $\xi_a, \xi_b \in \{\mu, \nu, \omega\}$ denote the intensities of decoy states.

(2) *Measurement.* Alice and Bob transmit the prepared quantum states to a third party Eve. An honest Eve interferes the received states on a 50:50 beam splitter, directs the two output pulses to two threshold detectors L and R, and announces the measurement results. Only the result of detector L or R clicking is considered as a successful measurement.

(3) *Announcement.* After repeating the above steps many times, Alice and Bob announce the corresponding modes for those trials with successful measurements.

(a) For trials in the code mode, they announce their x and y. If it is the matched trial $x = y$ or opposite trial $x = y \pm M/2$, they keep k_a and k_b as a sifted key. If it is the opposite trial $x = y \pm M/2$, Bob flips his key bit k_b. Moreover, if Eve announces only detector R clicks, Bob flips his key bit k_b.

(b) For trials in the test mode, they announce ξ_a, x, ξ_b, and y, and only keep the matched trials $x = y$ or opposite trials $x = y \pm M/2$ with the same intensity $\xi_a = \xi_b$ to calculate gains.

(4) *AD*. For the sifted key bits, Alice and Bob perform AD to obtain highly correlated key bits. To be specific, Alice and Bob split their sifted key into a series of b-bit blocks $\{x_1, x_2, \ldots, x_b\}$ and $\{y_1, y_2, \ldots, y_b\}$, respectively. For each b-bit block $\{x_1, x_2, \ldots, x_b\}$, Alice chooses a random bit $c \in \{0,1\}$, performs the bitwise XOR operation, and sends the result $m = \{m_1, m_2, \ldots, m_b\} = \{x_1 \oplus c, x_2 \oplus c, \ldots, x_b \oplus c\}$ to Bob through an authenticated classical channel. Upon receiving m, Bob calculates the result of $\{m_1 \oplus y_1, m_2 \oplus y_2, \ldots, m_b \oplus y_b\}$. If and only if Bob gets the result $\{0,0,\ldots,0\}$ or $\{1,1,\ldots,1\}$, Alice and Bob keep the first bit of their initial b-bit block, x_1 and y_1, as the processed key.

(5) *Postprocessing*. They perform key reconciliation and privacy amplification to get final secret keys.

The secret key rate of discrete-phase-randomized TF-QKD with AD is given by

$$\tilde{R}_d \geqslant \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b}\frac{2}{M} Q_\mu p_s \Bigg[1 - (\tilde{\lambda}_0+\tilde{\lambda}_1)H\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0+\tilde{\lambda}_1}\right) - (\tilde{\lambda}_2+\tilde{\lambda}_3)H\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2+\tilde{\lambda}_3}\right) - fH(\tilde{E}_\mu)\Bigg], \tag{1}$$

and the details of all terms in Eq. (1) can be found in Sec. III.

III. SECURITY ANALYSIS

In this section, we first analyze the security of QKD with AD based on the ideal single-photon sources, then extend this security analysis into the scenarios of continuous-phase-randomized TF-QKD with AD. Lastly, by relating Eve's behavior with the channel parameters, we discuss the security of discrete-phase-randomized TF-QKD with AD.

The general prepare-and-measure QKD can be equivalently translated into an entanglement-based scheme. For an entanglement-based QKD scheme where Alice prepares the quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, she keeps the first qubit and sends the second qubit to Bob through the quantum channel. Then Alice and Bob take inputs from 2×2-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 can be totally controlled by Eve, the eventual state shared between Alice and Bob can be expressed as

$$\sigma_{AB} = \lambda_0|\Phi_0\rangle\langle\Phi_0| + \lambda_1|\Phi_1\rangle\langle\Phi_1| + \lambda_2|\Phi_2\rangle\langle\Phi_2| + \lambda_3|\Phi_3\rangle\langle\Phi_3|, \tag{2}$$

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 $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1$. It is obvious that the error rates in the Z and X bases, denoted as E^Z and E^X, are constrained by $\lambda_2 + \lambda_3 = E^Z$ and $\lambda_1 + \lambda_3 = E^X$, respectively. With Lemma 7.1.1 in Ref. [41], the final secret key rate shared between Alice and Bob can be concluded as

$$R \geqslant \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \Bigg[1 - (\lambda_0+\lambda_1)H\left(\frac{\lambda_0}{\lambda_0+\lambda_1}\right) - (\lambda_2+\lambda_3)H\left(\frac{\lambda_2}{\lambda_2+\lambda_3}\right) - H(\lambda_2+\lambda_3)\Bigg], \tag{3}$$

where $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ denotes the binary Shannon entropy function.

To improve the performance of QKD, Alice and Bob can perform the AD method [41] after the measurement step. The purpose of AD is to identify subsets of highly correlated bits so as to separate them from weakly correlated information. As illustrated in step 4 in Sec. II, the successful probability of AD for each b-bit block is $p_s = (\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b$, and the

quantum state shared between Alice and Bob is

$$\tilde{\sigma}_{AB} = \tilde{\lambda}_0|\Phi_0\rangle\langle\Phi_0| + \tilde{\lambda}_1|\Phi_1\rangle\langle\Phi_1| + \tilde{\lambda}_2|\Phi_2\rangle\langle\Phi_2| + \tilde{\lambda}_3|\Phi_3\rangle\langle\Phi_3|, \tag{4}$$

where

$$\begin{aligned}\tilde{\lambda}_0 &= \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]},\\ \tilde{\lambda}_1 &= \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]},\\ \tilde{\lambda}_2 &= \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]},\\ \tilde{\lambda}_3 &= \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]}.\end{aligned} \tag{5}$$

Inserting Eq. (6) into Lemma 7.1.1 in Ref. [41], the secret key rate of QKD enhanced with AD can be given by

$$\tilde{R} \geqslant \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} p_s \left[1 - (\tilde{\lambda}_0+\tilde{\lambda}_1) H\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0+\tilde{\lambda}_1}\right) - (\tilde{\lambda}_2+\tilde{\lambda}_3) H\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2+\tilde{\lambda}_3}\right) - H(\tilde{\lambda}_2+\tilde{\lambda}_3)\right]. \tag{6}$$

We emphasize that, in the case of $b = 1$, all sifted key bits can pass the AD procedure with the successful probability $p_s = 1$, and consequently Eq. (6) is the same as Eq. (3), which indicates that the AD method is not actually working. When $b \geqslant 2$, only those b-bit blocks, which are completely the same or different, can pass the AD procedure, and in this case the AD method comes into play.

Due to the shortage of ideal single-photon sources with current technology, WCSs are alternatively adopted in practical QKD systems, where the decoy-state method [36–38] is combined to defeat the potential photon-number-splitting attacks [54,55]. To adopt the decoy-state scheme, the phases of WCSs should be perfectly and continuously randomized in the $[0, 2\pi)$ range. In terms of TF-QKD, Alice and Bob modulate their WCSs with continuously randomized phases ϕ_a and ϕ_b, where $\phi_a, \phi_b \in [0, 2\pi)$. After the intensity and phase announcement, their shared state, which has either the same phase ($\phi_a = \phi_b$) or opposite phase ($\phi_a = \phi_b \pm \pi$) but with the same intensity, can be given by

$$\begin{aligned}\rho_c &= \frac{1}{2\pi}\int_0^{2\pi} d\phi_a |\sqrt{\xi}e^{i\phi_a}\rangle\langle\sqrt{\xi}e^{i\phi_a}| \otimes |\sqrt{\xi}e^{i\phi_b}\rangle\langle\sqrt{\xi}e^{i\phi_b}|\\ &= \sum_{k=0}^{\infty} P^{\xi}(k)|k,\pm\rangle_{AB}\langle k,\pm|,\end{aligned} \tag{7}$$

where $\xi \in \{\mu, \nu, \omega, \ldots\}$ denotes the mean intensity of WCSs, $P^{\xi}(k) = e^{-2\xi}(2\xi)^k/k!$ denotes the probability of obtaining the k-photon state $|k,\pm\rangle_{AB} = 1/\sqrt{2^k k!}(a^\dagger \pm b^\dagger)^k|00\rangle_{AB}$, and $|k,+\rangle_{AB}$ and $|k,-\rangle_{AB}$ denote the k-photon state with the same and opposite phases. As shown in Eq. (7), the k-photon state, which is independent of the intensity ξ, of different intensities is identical and indistinguishable for Eve. This guarantees the k-photon yields of different intensities ξ_i and ξ_j are the same, that is, $Y_k(\xi_i) = Y_k(\xi_j) = Y_k$.

Consequently, the secret key rate of continuous-phase-randomized TF-QKD with AD is

$$\tilde{R}_c \geqslant \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} Q_\mu p_s \left[1 - (\tilde{\lambda}_0+\tilde{\lambda}_1) H\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0+\tilde{\lambda}_1}\right) - (\tilde{\lambda}_2+\tilde{\lambda}_3) H\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2+\tilde{\lambda}_3}\right) - f H(\tilde{E}_\mu)\right], \tag{8}$$

which is subject to

$$\begin{aligned}&\lambda_2+\lambda_3 = E_\mu, \quad 0 \leqslant \lambda_1+\lambda_3 \leqslant \overline{E}_\mu^X,\\ &p_s = (E_\mu)^b + (1-E_\mu)^b, \quad \lambda_0+\lambda_1+\lambda_2+\lambda_3 = 1,\\ &\tilde{E}_\mu = \frac{(E_\mu)^b}{(E_\mu)^b + (1-E_\mu)^b},\\ &\tilde{\lambda}_0 = \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]},\\ &\tilde{\lambda}_1 = \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]},\\ &\tilde{\lambda}_2 = \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]},\\ &\tilde{\lambda}_3 = \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]},\end{aligned} \tag{9}$$

where Q_μ and E_μ denote the average gain and quantum bit error rate of coherent states in the code mode, $\overline{E}_\mu^X$ denotes the upper bound of the information leakage E_μ^X [19,22], f denotes the inefficiency of key reconciliation, and the successful phase sifting factor which approaches to zero in this case is temporarily omitted. We emphasize that, if Alice and Bob adopt an infinite number of decoy states, they can obtain the exact values of E_μ^X, which is $E_\mu^X = [\sum_{k=0}^{\infty} P^\mu(2k)Y_{2k}]/Q_\mu$ [19], and the inequality in Eq. (9) will be reduced to the equality $\lambda_1+\lambda_3 = E_\mu^X$; if they adopt a finite number of decoy states (e.g., the widely used signal, decoy and vacuum states [56]), $\overline{E}_\mu^X$ can be upper bounded by $1 - P^\mu(1)\underline{Y}_1/Q_\mu$, where $\underline{Y}_1$ denotes the lower bound of Y_1.

However, the preparation of continuous-phase-randomized WCSs is technically demanding by the state of the art. To address this issue, the discrete-phase-randomized source is alternatively adopted in practical QKD systems [39]. Here, we analyze the security of discrete-phase-randomized TF-QKD with AD. The state in discrete-phase-randomized WCSs after the intensity and phase announcement, which has either the same phase ($x = y$) or opposite phase ($x = y \pm M/2$) but with the same intensity, can be expressed as a combination of approximated photon number states, that is,

$$\begin{aligned}\rho_d &= \frac{1}{M}\sum_{x=0}^{M-1} \left|\sqrt{\xi}e^{i\frac{2\pi x}{M}}\right\rangle_A\left\langle\sqrt{\xi}e^{i\frac{2\pi x}{M}}\right| \otimes \left|\sqrt{\xi}e^{i\frac{2\pi y}{M}}\right\rangle_B\left\langle\sqrt{\xi}e^{i\frac{2\pi y}{M}}\right|\\ &= \sum_{k=0}^{M-1} P_M^{\xi}(k)\left|\lambda_k^{\xi},\pm\right\rangle_{AB}\left\langle\lambda_k^{\xi},\pm\right|,\end{aligned} \tag{10}$$

where M denotes the number of modulated discrete phases, $P_M^{\xi}(k) = \sum_{l=0}^{\infty}[e^{-2\xi}(2\xi)^{lM+k}/(lM+k)!]$ denotes the probability of obtaining the approximated k-photon state

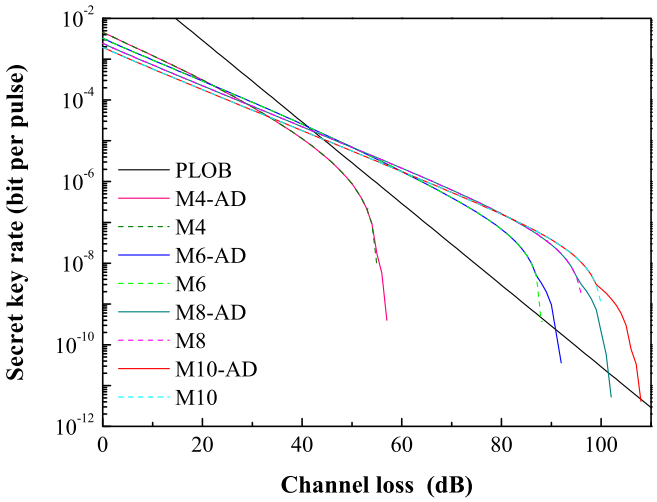

FIG. 1. Comparison of discrete-phase-randomized TF-QKD with and without AD under $e_d = 1.5\%$. The solid black line denotes the result of the PLOB bound [9], and the solid (dashed) colorful curves from left to right denote the results of TF-QKD with (without) AD when modulating 4, 6, 8, and 10 phases. The nonsmooth points in the solid colorful curves indicate the change of optimal b in AD. For details, see Fig. 2, which gives an example of optimal b when modulating 10 phases in TF-QKD with AD.

$|\lambda_k^{\xi}, \pm\rangle_{AB} = [e^{-\xi}/\sqrt{P_M^{\xi}(k)}] \sum_{l=0}^{\infty} [(\sqrt{2\xi})^{lM+k}/\sqrt{(lM+k)!}$ $|lM+k, \pm\rangle_{AB}]$, and $|\lambda_k^{\xi}, +\rangle_{AB}$ and $|\lambda_k^{\xi}, -\rangle_{AB}$ denote the approximated k-photon state with the same and opposite phases. Different from Eq. (7), the approximated k-photon state $|\lambda_k^{\xi}, \pm\rangle_{AB}\langle\lambda_k^{\xi}, \pm|$ in Eq. (10) depends on the intensity ξ, which provides some possibilities for Eve to distinguish the signal and decoy states. Therefore, the approximated k-photon yields of different intensities ξ_i and ξ_j are different, that is, $Y_k^{\xi_i} \neq Y_k^{\xi_j}$. To ensure the security of the decoy-state method with discrete-phase-randomized sources, the difference of the approximated k-photon yields of different intensities is characterized by $|Y_k^{\xi_i} - Y_k^{\xi_j}| \leqslant \sqrt{1 - F_{\xi_i\xi_j,k}^2}$, where $F_{\xi_i\xi_j,k} = |\langle\lambda_k^{\xi_i}, + \,|\, \lambda_k^{\xi_j}, +\rangle| = |\langle\lambda_k^{\xi_i}, - \,|\, \lambda_k^{\xi_j}, -\rangle|$ represents the fidelity between $|\lambda_k^{\xi_i}, \pm\rangle_{AB}$ and $|\lambda_k^{\xi_j}, \pm\rangle_{AB}$ [22,39]. Correspondingly, the upper bound of E_{μ}^{X} in the discrete-phase-randomized case should be estimated by the following routines [22],

$$\bar{E}_{\mu}^{X} = \max_{Y_k^{\xi}} \left[\sum_{k=0}^{M/2-1} P_M^{\mu}(2k) Y_{2k}^{\mu} \right] \Big/ Q_{\mu}$$

s.t.

$$Q_{\xi} = \sum_{k=0}^{M-1} P_M^{\xi}(k) Y_k^{\xi},$$

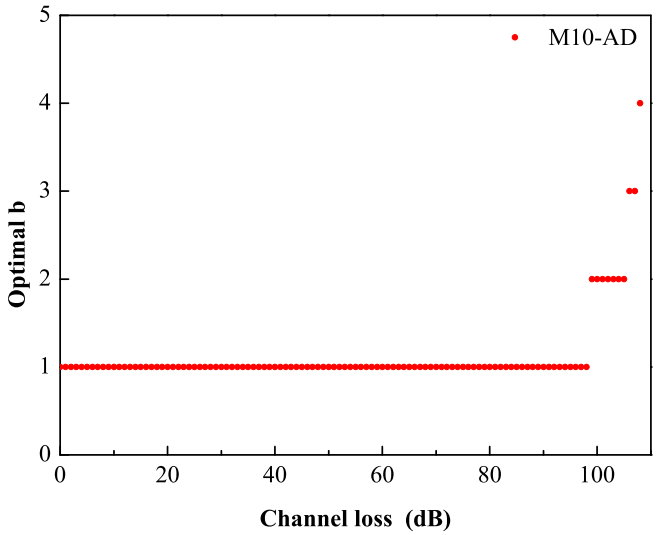

FIG. 2. Results of the optimal b when modulating 10 phases in TF-QKD with AD under $e_d = 1.5\%$.

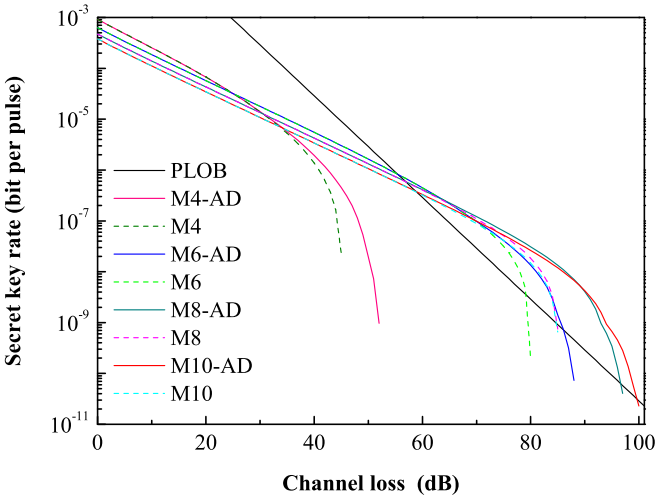

FIG. 3. Comparison of discrete-phase-randomized TF-QKD with and without AD under $e_d = 11\%$. The solid black line denotes the result of the PLOB bound [9], and the solid (dashed) colorful curves from left to right denote the results of TF-QKD with (without) AD when modulating 4, 6, 8 and 10 phases. The non-smooth points in the solid colorful curves indicate the change of optimal b in AD.

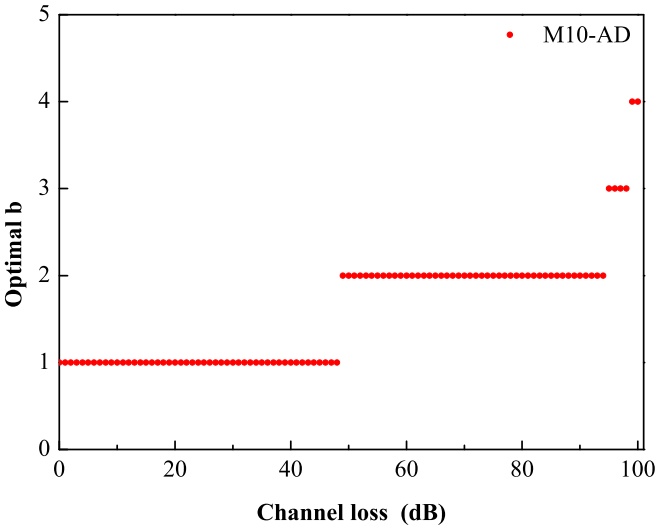

FIG. 4. Results of the optimal b when modulating 10 phases in TF-QKD with AD under $e_d = 11\%$.

TABLE I. Secret key rate of discrete-phase-randomized TF-QKD with and without AD under $e_d = 1.5\%$.

Protocols	$M = 4$	$M = 6$	$M = 8$	$M = 10$
Without AD	8.39×10^{-9} @ 55 dB	3.67×10^{-10} @ 88 dB	1.79×10^{-9} @ 96 dB	1.01×10^{-9} @ 100 dB
With AD	1.68×10^{-8} @ 55 dB	3.25×10^{-9} @ 88 dB	3.02×10^{-9} @ 96 dB	2.36×10^{-9} @ 100 dB

$$\begin{aligned}
&\sum_{k=0}^{M/2-1} P_M^{\mu}(2k) Y_{2k}^{\mu} \leqslant Q_{\mu}/2, \\
&\left|Y_k^{\xi_i} - Y_k^{\xi_j}\right| \leqslant \sqrt{1 - F_{\xi_i \xi_j, k}^2}, \\
&0 \leqslant Y_k^{\xi} \leqslant 1.
\end{aligned} \tag{11}$$

With the estimated $\overline{E}_{\mu}^{X}$, the secret key rate of discrete-phase-randomized TF-QKD with AD can be given by

$$\begin{aligned}
\tilde{R}_d \geqslant \max_b \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} \frac{1}{b} \frac{2}{M} Q_{\mu} p_s \Bigg[& 1 - (\tilde{\lambda}_0 + \tilde{\lambda}_1) H\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1}\right) \\
& - (\tilde{\lambda}_2 + \tilde{\lambda}_3) H\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3}\right) - f H(\tilde{E}_{\mu}) \Bigg],
\end{aligned} \tag{12}$$

subject to

$$\begin{aligned}
& E_{\mu} = \lambda_2 + \lambda_3, \quad 0 \leqslant \lambda_1 + \lambda_3 \leqslant \overline{E}_{\mu}^{X}, \\
& p_s = (E_{\mu})^b + (1 - E_{\mu})^b, \quad \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1, \\
& \tilde{E}_{\mu} = \frac{(E_{\mu})^b}{(E_{\mu})^b + (1 - E_{\mu})^b}, \\
& \tilde{\lambda}_0 = \frac{(\lambda_0 + \lambda_1)^b + (\lambda_0 - \lambda_1)^b}{2[(\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b]}, \\
& \tilde{\lambda}_1 = \frac{(\lambda_0 + \lambda_1)^b - (\lambda_0 - \lambda_1)^b}{2[(\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b]}, \\
& \tilde{\lambda}_2 = \frac{(\lambda_2 + \lambda_3)^b + (\lambda_2 - \lambda_3)^b}{2[(\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b]}, \\
& \tilde{\lambda}_3 = \frac{(\lambda_2 + \lambda_3)^b - (\lambda_2 - \lambda_3)^b}{2[(\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b]},
\end{aligned} \tag{13}$$

where the $2/M$ factor denotes the successful phase sifting probability, and the meanings of the rest of the variables are the same as in Eq. (8). Here, we simply consider security against collective attacks in the asymptotic scenario. To extend the analysis to security against coherent attacks in the finite-key regime, one can refer to Refs. [57–59].

IV. SIMULATIONS

To investigate the performance of discrete-phase-randomized TF-QKD with AD, we assume that the detection efficiency η_d of single-photon detectors is 20%, the dark count rate d of single-photon detectors is 10^{-8}, the inefficiency f of key reconciliation is 1.1, and the size b of every split block in AD is reasonably optimized in the [1,4] range. The calculation models for Q_{μ} and E_{μ} are

$$Q_{\mu} = (1 - d)(1 - \mathrm{e}^{-2\eta\mu} + 2d\mathrm{e}^{-2\eta\mu}), \tag{14}$$

and

$$E_{\mu} = (1 - d)(e_d - e_d \mathrm{e}^{-2\eta\mu} + d\mathrm{e}^{-2\eta\mu})/Q_{\mu}, \tag{15}$$

where e_d denotes the intrinsic misalignment error rate, and η denotes the overall transmission efficiency between Alice and Bob, which includes the optical channel loss and the detection efficiency of single-photon detectors. In the simulation, we adopt the widely used three-intensity decoy-state scheme [56], where the intensities of signal and decoy states, denoted as μ and ν, are chosen by the coarse-grained exhaustive search, and the intensity of the vacuum state, denoted as ω, is set to be 0.

When the misalignment error rate is relatively small, e.g., $e_d = 1.5\%$, we compare the performance of discrete-phase-randomized TF-QKD with and without AD when modulating different number of phases ($M = 4, 6, 8, 10$), and the corresponding results are shown in Fig. 1. It can be seen that the AD method can enhance the performance of discrete-phase-randomized TF-QKD in varying degrees, particularly expand the range of breaking the PLOB bound [9] when $M = 6, 8, 10$. On the other hand, modulating 10 phases in TF-QKD can almost achieve the maximum channel loss, and further numerical simulation demonstrates that modulating 12 and 14 phases cannot tolerate much more obvious channel loss, which indicates that there is no need to empirically modulate more phases in TF-QKD to approach the continuous-phase-randomized sources. At the same time, we plot the trend of optimal b when modulating 10 phases in TF-QKD with AD in Fig. 2. When the channel loss is less than 99 dB, the optimal b is equal to 1, which indicates that all sifted key bits between Alice and Bob can pass the AD procedure, and consequently the secret key rate of TF-QKD with AD is equal to that of without AD. When the channel loss is greater than 99 dB, the optimal b is larger than or equal to 2, which

TABLE II. Secret key rate of discrete-phase-randomized TF-QKD with and without AD under $e_d = 11\%$.

Protocols	$M = 4$	$M = 6$	$M = 8$	$M = 10$
Without AD	2.37×10^{-8} @ 45 dB	2.09×10^{-10} @ 80 dB	7.40×10^{-10} @ 85 dB	6.46×10^{-10} @ 85 dB
With AD	4.55×10^{-7} @ 45 dB	1.35×10^{-8} @ 80 dB	1.34×10^{-8} @ 85 dB	1.19×10^{-8} @ 85 dB

TABLE III. Tolerable channel loss of discrete-phase-randomized TF-QKD with and without AD under $e_d = 1.5\%$.

Protocols	$M = 4$	$M = 6$	$M = 8$	$M = 10$
Without AD	55 dB	88 dB	96 dB	100 dB
With AD	57 dB	92 dB	102 dB	108 dB

TABLE IV. Tolerable channel loss of discrete-phase-randomized TF-QKD with and without AD under $e_d = 11\%$.

Protocols	$M = 4$	$M = 6$	$M = 8$	$M = 10$
Without AD	45 dB	80 dB	85 dB	85 dB
With AD	52 dB	88 dB	97 dB	100 dB

means the AD method does play its role. Intuitively, with the increase of transmission loss which will introduce more noises to Alice and Bob's sifted key, the correlation of their sifted key becomes weaker. To identify highly correlated bits so as to separate them from weakly correlated bits, the optimal b becomes larger in the high loss regime.

To further investigate the tolerance of error rates, we compare the performance of discrete-phase-randomized TF-QKD with and without AD under $e_d = 11\%$, and the corresponding results are shown in Fig. 3. It can be seen that the AD method improves the performance of discrete TF-QKD more significantly when the misalignment error rate e_d becomes large. Specifically, when modulating 10 phases in TF-QKD, the AD method begins to show its superiority at the channel loss of 48 dB where the optimal b is equal to 2 (as exhibited in Fig. 4). Moreover, as illustrated in Figs. 1 and 3, the proper increase of M raises the tolerable channel loss, but reduces the successful sifting probability. Therefore, to achieve the optimal performance of discrete-phase-randomized TF-QKD with AD, the number of modulated phases should be adjusted dynamically according to the channel loss. Lastly, we list the secret key rate and tolerable channel loss of discrete-phase-randomized TF-QKD with and without AD in Tables I and II and Tables III and IV, respectively, which clearly demonstrate the superiority of the AD method.

V. CONCLUSION

In conclusion, we propose a protocol of discrete-phase-randomized TF-QKD with AD, and investigate its performance in the asymptotic case. Simulation results demonstrate that, by splitting the sifted key into blocks of only b bits (say, $b = 2, 3, 4$) to identify highly correlated key bits, the performance of discrete-phase-randomized TF-QKD can be greatly enhanced under high channel losses and error rates. Furthermore, our simulation results indicate that, to achieve the optimal performance of discrete-phase-randomized TF-QKD with AD, the number of modulated phases should be adjusted dynamically according to the channel loss. In future research, it would be interesting to apply the AD method to improve the performance of other TF-QKD variations [21,23–26]. We expect our work can provide a valuable reference for researchers to design practical TF-QKD systems.

ACKNOWLEDGMENTS

This work is supported by National Natural Science Foundation of China (62371244, 62301235, U2130205) and Natural Science Foundation of Henan (242300421219). R.W. is supported by the University of Hong Kong start-up grant.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] 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, Long-distance quantum key distribution secure against coherent attacks, Optica **4**, 163 (2017).

[3] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, 2 GHz clock quantum key distribution over 260 km of standard telecom fiber, Opt. Lett. **37**, 1008 (2012).

[4] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[5] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[6] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photonics **9**, 397 (2015).

[7] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, and Z.-F. Han, Robust and adaptable quantum key distribution network without trusted nodes, Optica **9**, 812 (2022).

[8] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[10] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[11] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).

[12] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound, arXiv:1805.05511.

[13] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).
[14] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 034053 (2019).
[15] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).
[16] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).
[17] H.-L. Yin and Y. Fu, Measurement-device-independent twin-field quantum key distribution, Sci. Rep. **9**, 3045 (2019).
[18] R. Wang, Z.-Q. Yin, F.-Y. Lu, S. Wang, W. Chen, C.-M. Zhang, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Optimized protocol for twin-field quantum key distribution, Commun. Phys. **3**, 149 (2020).
[19] P. Zeng, W. Wu, and X. Ma, Symmetry-protected privacy: Beating the rate-distance linear bound over a noisy channel, Phys. Rev. Appl. **13**, 064013 (2020).
[20] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate, Phys. Rev. A **101**, 042330 (2020).
[21] G. Currás-Lorenzo, L. Wooltorton, and M. Razavi, Twin-field quantum key distribution with fully discrete phase randomization, Phys. Rev. Appl. **15**, 014016 (2021).
[22] C.-M. Zhang, Y.-W. Xu, R. Wang, and Q. Wang, Twin-field quantum key distribution with discrete-phase-randomized sources, Phys. Rev. Appl. **14**, 064070 (2020).
[23] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution with discrete-phase-randomized weak coherent states, Phys. Rev. Res. **2**, 043304 (2020).
[24] X. Zhang, Y. Wang, M. Jiang, Y. Lu, H. Li, C. Zhou, and W. Bao, Phase-matching quantum key distribution with discrete phase randomization, Entropy **23**, 508 (2021).
[25] Y.-W. Xu, R. Wang, and C.-M. Zhang, Discrete-phase-randomized twin-field quantum key distribution without phase postselection in the test mode, Quantum Inf. Process. **20**, 199 (2021).
[26] X.-L. Hu, C. Jiang, Z.-W. Yu, and X.-B. Wang, Universal approach to sending-or-not-sending twin field quantum key distribution, Quantum Sci. Technol. **7**, 045031 (2022).
[27] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).
[28] 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, Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system, Phys. Rev. X **9**, 021046 (2019).
[29] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field type quantum key distribution, Phys. Rev. Lett. **123**, 100506 (2019).
[30] X. T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y. L. Tang, Y. J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M. J. Li, H. Chen, Y. A. Chen, Q. Zhang, C. Z. Peng, X. Ma, T. Y. Chen, and J. W. Pan, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).
[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, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution through sending or not sending, Phys. Rev. Lett. **123**, 100505 (2019).
[32] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830 km fibre, Nat. Photonics **16**, 154 (2022).
[33] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, Nat. Commun. **14**, 928 (2023).
[34] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution over 1000 km fiber distance, Phys. Rev. Lett. **130**, 210801 (2023).
[35] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, D. Ma, C. Zhang, W.-X. Pan, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, C.-Y. Lu, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, 1002 km twin-field quantum key distribution with finite-key analysis, Quantum Front. **2**, 16 (2023).
[36] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).
[37] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).
[38] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[39] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, New J. Phys. **17**, 053014 (2015).
[40] Z. Cao, Discrete-phase-randomized measurement-device-independent quantum key distribution, Phys. Rev. A **101**, 062325 (2020).
[41] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **06**, 1 (2008).
[42] B. Kraus, C. Branciard, and R. Renner, Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses, Phys. Rev. A **75**, 012316 (2007).
[43] J. Bae and A. Acín, Key distillation from quantum channels using two-way communication protocols, Phys. Rev. A **75**, 012334 (2007).
[44] E. Y.-Z. Tan, C. C.-W. Lim, and R. Renner, Advantage distillation for device-independent quantum key distribution, Phys. Rev. Lett. **124**, 020502 (2020).
[45] G. Murta, F. Rozpedek, J. Ribeiro, D. Elkouss, and S. Wehner, Key rates for quantum key distribution protocols with asymmetric noise, Phys. Rev. A **101**, 062321 (2020).
[46] H.-W. Li, C.-M. Zhang, M.-S. Jiang, and Q.-Y. Cai, Improving the performance of practical Decoy-state quantum key distribution with advantage distillation technology, Commun. Phys. **5**, 53 (2022).
[47] H.-W. Li, R.-Q. Wang, C.-M. Zhang, and Q.-Y. Cai, Improving the performance of twin-field quantum key distribution with advantage distillation technology, Quantum **7**, 1201 (2023).

[48] R.-Q. Wang, C.-M. Zhang, Z.-Q. Yin, H.-W. Li, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phase-matching quantum key distribution with advantage distillation, New J. Phys. **24**, 073049 (2022).

[49] J.-R. Zhu, C.-M. Zhang, R. Wang, and H.-W. Li, Reference-frame-independent quantum key distribution with advantage distillation, Opt. Lett. **48**, 542 (2023).

[50] X.-L. Jiang, Y. Wang, J.-J. Li, Y.-F. Lu, C.-P. Hao, C. Zhou, and W.-S. Bao, Improving the performance of reference-frame-independent quantum key distribution with advantage distillation technology, Opt. Express **31**, 9196 (2023).

[51] X. Liu, D. Luo, Z. Zhang, and K. Wei, Mode-pairing quantum key distribution with advantage distillation, Phys. Rev. A **107**, 062613 (2023).

[52] Y. Zhou, R.-Q. Wang, C.-M. Zhang, Z.-Q. Yin, Z.-H. Wang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Sending-or-not-sending twin-field quantum key distribution with advantage distillation, Phys. Rev. Appl. **21**, 014036 (2024).

[53] Z. Wang, C.-M. Zhang, and H.-W. Li, Improving the performance of practical phase-matching quantum key distribution with advantage distillation, Quantum Inf. Process. **23**, 128 (2024).

[54] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[55] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

[56] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[57] M. Christandl, R. König, and R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett. **102**, 020504 (2009).

[58] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).

[59] R.-Q. Wang, Z.-Q. Yin, X.-H. Jin, R. Wang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Finite-key analysis for quantum key distribution with discrete-phase randomization, Entropy **25**, 258 (2023).