

Sending-or-not-sending twin-field quantum key distribution with advantage distillation


Yao Zhou^{1,3}, Rui-Qiang Wang^{1,3}, Chun-Mei Zhang^{2,*}, Zhen-Qiang Yin^{1,3,4,†}, Ze-Hao Wang^{1,3},
Shuang Wang^{1,3,4}, Wei Chen^{1,3,4}, Guang-Can Guo^{1,3,4} and Zheng-Fu Han^{1,3,4}

¹CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China

²Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, People's Republic of China

³CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

⁴Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China

 (Received 30 May 2023; revised 2 November 2023; accepted 5 January 2024; published 19 January 2024)

A sending-or-not-sending (SNS) protocol is a very promising variant in twin-field quantum key distribution (TFQKD) for its advantages at the regime of long distance and the robustness against large optical misalignment. The actively odd-parity pairing (AOPP) method can significantly enhance the key-rate performance of the original SNS TFQKD, which forms the AOPP SNS TFQKD protocol. In this paper, we introduce the advantage distillation (AD) method to further improve the communication distance for AOPP SNS TFQKD. We also prove the composable security against coherent attacks for the AOPP SNS TFQKD with AD in the finite-key regime for bit blocks with a size of 2 in the AD process. Our AD method for AOPP SNS TFQKD protocol is expected to improve the key-rate performance in practice without changing the SNS TFQKD experimental system.

DOI: [10.1103/PhysRevApplied.21.014036](https://doi.org/10.1103/PhysRevApplied.21.014036)

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] provides a promising solution to the secure key sharing between two remote communication nodes in the presence of the eavesdropper Eve who controls the channel and has infinite computational resources. Over the past three decades, QKD has achieved great development both in theory [3–15] and experiment [16–27] and begun to be commercially available. Improving the key-rate performance and the achievable distance is a crucial task for the practical application of QKD. However, the channel transmittance η decreases exponentially with the communication distance in the optical fiber channel, and the carrier of the information, photon, also decays exponentially with the communication distance. So the key rate is naturally constrained by the transmittance η , which has been proved to be a linear key-rate bound without quantum repeaters [28,29]. Surprisingly, the twin-field quantum key distribution (TFQKD) protocol [30] proposed in 2018, can break the linear rate-distance limit without full-fledged quantum repeaters. Although the original twin-field (TF) protocol

has problems in security proofs, this idea has given rise to various variants [31–37].

In particular, the sending-or-not-sending (SNS) protocol [32] of TFQKD encodes a random bit by sending or not sending a phase-randomized weak coherent pulse, which is different from the original TFQKD and other variants encoded on the phase. When the communicating party Alice or Bob sends a phase-randomized coherent state, it can be equivalently regarded that she or he sends a classical mixture of states of different photon numbers in Fock space, i.e., $\int_0^{2\pi} |\sqrt{\mu}e^{i\theta}\rangle \langle \sqrt{\mu}e^{i\theta}| / (2\pi) d\theta = \sum_{k=0}^{\infty} e^{-\mu} \mu^k / k! |k\rangle \langle k|$. Wang *et al.* defined $|01\rangle$ and $|10\rangle$ (one party does not send, and the other party sends a single-photon state) as the coded quantum state. By constructing conjugated quantum states $(|01\rangle + e^{i\delta} |10\rangle) / \sqrt{2}$ and $(|01\rangle - e^{i\delta} |10\rangle) / \sqrt{2}$ in the decoy mode, the traditional decoy-state method [7–9] can be directly applied to solve the security proof. Subsequently, SNS TFQKD was further improved. Ref. [38] considered the four-intensity decoy state and finite small phase slices in practice. Reference [39] proposed the actively odd-parity pairing (AOPP) method to enhance the key rate and achievable distance. References [40–42] solved the finite-key problem and completed the composable security proof of the AOPP SNS TFQKD.

*cmz@njupt.edu.cn

†yinzq@ustc.edu.cn

So far, AOPP SNS TFQKD has been a well-performing mature QKD protocol for its advantages at the regime of long distance and the presence of large misalignment. It has been reported that the achievable distance of AOPP SNS TFQKD reached 1002 km in the asymptotic regime [43]. But is it possible to further improve the key-rate performance? Recently, the advantage distillation (AD) [44] has shown advantages in some QKD protocols [45–47]. The AD method is a classical operation done in postprocessing that splits the raw key string into blocks of small size and can identify the highly correlated bit pairs by two-way classical communication. Here we introduce AD for AOPP SNS TFQKD to further improve the communication distance. The simulation results in the asymptotic case confirm the effectiveness of AD. For the simplicity of finite-key analysis and the practicability of key bit rate, we set the size of the bit blocks to 2 in the AD process, and we prove the composable security against coherent attacks for the AOPP SNS TFQKD with AD in the finite-key regime. Since the AD with bit block size 2^n (n is a natural number) can be implemented by iteratively repeating the AD step on block size of 2 for n times, our finite-key analysis method also applies to the bit block size 2^n . The simulations with finite-key effect show that AD maintains the appreciable improvement and can be directly applied to practice at the regime of long distance.

The remainder of this paper is organized as follows. In Sec. II, we list the specific process of AOPP SNS TFQKD with AD. In Sec. III, we first give the security proof in the asymptotic regime. For the simplicity of finite-key analysis and the practicability of key bit rate, we next perform a finite-key analysis on the blocks of size 2 and obtain the finite-size key rate for the given failure probability. In Sec. IV, we simulate the performance of AOPP SNS TFQKD with AD and compare it with phase-matching QKD [31,47] in the asymptotic regime. Finally, the conclusion of this paper is given in Sec. V.

II. PROTOCOL

Based on the AOPP SNS TFQKD protocol, we insert an additional AD step after AOPP as follows:

(I) State preparation: Alice (Bob) chooses the code mode with probability p_Z or the decoy mode with probability $1 - p_Z$.

(1) If Alice chooses the code mode, she selects a random bit 0 or 1 with probability p_{Z0} and $1 - p_{Z0}$. Depending on the bit selection, she chooses to not send (bit 0) or send (bit 1) a phase-randomized weak coherent state $|\sqrt{\mu}e^{i\theta_A}\rangle$ with intensity μ and a random phase $\theta_A \in [0, 2\pi)$. If Bob chooses the code mode, he selects a random bit 0 or 1 with probability $1 - p_{Z0}$ and p_{Z0} . Depending on the bit selection, he chooses to send (bit 0) or not send (bit 1) a phase-randomized weak coherent state $|\sqrt{\mu}e^{i\theta_B}\rangle$.

(2) If Alice (Bob) chooses the decoy mode, she (he) decides to send a vacuum, a phase-randomized weak coherent state with intensity μ_1 or μ_2 ($\mu_1 < \mu_2$) with probability p_0, p_1 , and $1 - p_0 - p_1$.

They repeat step (I) for N_{tot} times.

(II) Measurement: The intermediate node Charlie is supposed to perform interferometric measurement on the incoming twin-field optical pulse each round with a 50:50 beam splitter, followed by two photon detectors L and R . He records and announces the detection events. Only the rounds where one and only one of the detectors L or R clicked are defined as the successful rounds. The successful rounds are kept for subsequent steps, others are discarded.

(III) Announcement: Alice and Bob announce the mode selection for each round. The round when Alice and Bob both choose the code mode is defined as the code round. The random bits in code rounds form the raw keys. For other rounds, Alice and Bob announce the intensity information they sent. When Alice and Bob both send the optical pulses with intensity μ_1 , they should also disclose the phase information θ_A and θ_B to determine whether the phase postselection condition: $|\theta_A - \theta_B| \bmod \pi \leq \Delta/2$ is satisfied. The rounds when Alice and Bob send the optical pulses with intensity μ_1 and the phases meet the postselection condition are used to estimate the phase-flip error rate.

(IV) AOPP: Alice and Bob perform the AOPP process [39] on the raw keys to form the sifted keys, i.e., Alice randomly chooses the first bit and then randomly selects a bit different from the first one from the remaining unpaired bits for pairing. So Alice can obtain as many odd-parity pairs, which are defined as the pairs containing two different bits, as she can until she runs out of bit 0 or 1. Note that Alice discards all the remaining bits once she gets all the odd-parity pairs. She announces the position information of all paired bits in the odd-parity pairs to Bob. Bob makes the same grouping of the bits in his hand according to the position information. Then he checks the pairs' parity and announces it to Alice. They only keep the bit pairs where both sides are odd-parity pairs. Finally, Alice and Bob extract the first bits from the odd-parity groups to form the sifted keys.

(V) AD: Alice and Bob perform the AD process [44] on the sifted keys as follows. Alice and Bob split the sifted keys into blocks (x_1, x_2, \dots, x_b) and (y_1, y_2, \dots, y_b) of size b . Alice sends the message $(x_1 \oplus r, x_2 \oplus r, \dots, x_b \oplus r)$ to Bob through an authenticated public channel, where r is the uniform random number generated by Alice. Bob retains only the blocks containing bits that align either entirely identical or completely opposite to the received message, i.e., the blocks (y_1, y_2, \dots, y_b) in Bob's hand equal to (x_1, x_2, \dots, x_b) or $(x_1 \oplus 1, x_2 \oplus 1, \dots, x_b \oplus 1)$ are retained to form the processed blocks. Bob announces the reserved processed block information to Alice and Alice

retains only the initial blocks at the same position as Bob. Both parties use the first bit in the corresponding processed block to form the processed keys. Note that it is equivalent to set the block size b to 1 if we do not perform the AD step.

(VI) Parameter estimation: Alice and Bob randomly choose some processed keys to estimate the bit-flip error rate. They do the decoy-state analysis from the public round information to obtain the number of the untagged bits together with the phase-flip error rate. Note that the untagged bit is defined as the bit when only one party sends the coherent state in the code round and she (he) happens to send a single-photon state.

(VII) Key distillation: Alice and Bob distill the final keys from processed keys by error correction and privacy amplification.

III. SECURITY PROOF

If we set the block size b in step (V) to 1, all the sifted keys can pass the AD process and the processed keys are just the sifted keys. Thus, we can skip step (V) and our protocol degenerates to the AOPP SNS TFQKD. After step (IV) is executed, we denote the total number of sifted keys as N_A , the bit-flip error rate as E_A , the number of untagged bits [32] as n_{A1} and the phase-flip error rate of the untagged bits as e_{A1}^{ph} . The security of AOPP SNS TFQKD in the asymptotic case has been proved in Ref. [39] and the composable security in the finite case has been proved in Ref. [42]. We directly take the various quantities after AOPP without proof to derive the key rate after AD and complete the security proof.

A. In the asymptotic case

For the rounds generating untagged bits after AOPP, we can construct an entanglement-based scheme, that is, the local auxiliary qubits AB of Alice and Bob can be written as the joint density matrix σ_{AB} [44] with only two diagonal entries for the reason that there are no bit-flip errors in the untagged bits [32]:

$$\sigma_{AB} = \lambda_0 |\Phi_0\rangle \langle \Phi_0| + \lambda_1 |\Phi_1\rangle \langle \Phi_1|, \quad (1)$$

where $\lambda_0 = 1 - e_{A1}^{\text{ph}}$, $\lambda_1 = e_{A1}^{\text{ph}}$, $|\Phi_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and $|\Phi_1\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ are two mutually orthogonal Bell bases. If all the bits in the block of size b are untagged bits when splitting the sifted keys in AD process, we name the block as an untagged block. The first untagged bits from the untagged blocks are used to generate the final secure key, which is similar to the untagged bits in the AOPP SNS TFQKD, and we define them as processed untagged bits. It is obvious that the processed untagged bits must pass the AD step and have no bit-flip errors. The local auxiliary qubits shared by Alice and Bob corresponding to

the processed untagged bits from untagged blocks in the entanglement-based scheme can be given by [44]

$$\tilde{\sigma}_{AB} = \tilde{\lambda}_0 |\tilde{\Phi}_0\rangle \langle \tilde{\Phi}_0| + \tilde{\lambda}_1 |\tilde{\Phi}_1\rangle \langle \tilde{\Phi}_1|, \quad (2)$$

where

$$\begin{aligned} \tilde{\lambda}_0 &= \frac{(\lambda_0 + \lambda_1)^b + (\lambda_0 - \lambda_1)^b}{2} = \frac{1 + (1 - 2e_{A1}^{\text{ph}})^b}{2}, \\ \tilde{\lambda}_1 &= \frac{(\lambda_0 + \lambda_1)^b - (\lambda_0 - \lambda_1)^b}{2} = \frac{1 - (1 - 2e_{A1}^{\text{ph}})^b}{2}, \end{aligned} \quad (3)$$

$|\tilde{\Phi}_0\rangle$ and $|\tilde{\Phi}_1\rangle$ are two mutually orthogonal Bell bases. So the phase-flip error rate of the processed untagged bit is $e_{\text{AD}}^{\text{ph}} = [1 - (1 - 2e_{A1}^{\text{ph}})^b]/2$. Consequently, the asymptotic key length formula of AOPP SNS TFQKD with AD is

$$N_f = n_1[1 - h(e_{\text{AD}}^{\text{ph}})] - fN_{\text{AD}}h(E_{\text{AD}}), \quad (4)$$

where n_1 is the number of processed untagged bits, $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary Shannon entropy function, f is the error-correction inefficiency, N_{AD} is the number of processed key bits and E_{AD} is the bit-flip error rate of the processed key bits. Note that Eq. (4) degenerates to Eq. (20) in Ref. [39] if we do not perform AD step.

B. In the finite-key case

For the simplicity of finite-key analysis and the practicality of key bit rate, we consider only the finite-key effect with block size 2 below. Note that our finite-key analysis method also applies to the bit block size 2^n by iteratively repeating the AD step on block size of 2 for n times.

When Alice and Bob split the N_A sifted keys into blocks of size 2, we use the white balls and black balls model in Ref. [42] to estimate the lower bound of the processed untagged bits and the upper bound of the phase-flip error rate. We assume that the lower bound on the number of the untagged blocks is n_1 , the corresponding failure probability is ϵ_{uu} . Note that (n_1, ϵ_{uu}) can be calculated from the white balls and black balls model in Ref. [42] as follows:

$$\epsilon_{uu} = 2\xi_L\left(n_1; \frac{n_{A1}^2}{N_A^2}, \frac{N_A}{2}\right), \quad (5)$$

where $\xi_L(x; p, N)$ denotes the probability of the number of successes less than x in the binomial distribution $\mathcal{B}(N, p)$.

Our goal now is to obtain the upper bound of the phase-flip error rate after AD step from the phase-flip error rate after AOPP (also before the AD) step. References [48,49] show that the processed untagged bit with a phase-flip error is from the untagged block containing only one phase-flip bit. The number of the untagged bits with phase-flip errors in n_1 untagged blocks is $M_{A1} = 2n_1e_{A1}^{\text{ph}}$ and the lower

bound of the untagged blocks containing two phase-flip errors is M_{ee} . So the upper bound of the untagged blocks causing the phase-flip errors is $M_{AD} = M_{A1} - 2M_{ee}$. Note that M_{ee} can also be estimated by the white and black balls model with a failure probability ϵ_{ee} as follows:

$$\epsilon_{ee} = 2\xi_L \left(M_{ee}; (e_{A1}^{\text{ph}})^2, n_1 \right). \quad (6)$$

The phase-flip error rate of all the processed untagged bits is

$$e_{AD}^{\text{ph}} = \frac{M_{AD}}{n_1}. \quad (7)$$

The final key length formula of AOPP SNS TFQKD with AD protocol is

$$N_f = n_1 [1 - h(e_{AD}^{\text{ph}})] - f N_{AD} h(E_{AD}) - \log_2 \frac{2}{\epsilon_{\text{sec}}} - 2 \log_2 \frac{1}{\sqrt{2} \epsilon_{\text{PA}} \hat{\epsilon}}, \quad (8)$$

where f , N_{AD} , E_{AD} , and the function $h(x)$ have the same meaning as in Eq. (4). $-\log_2(2)/\epsilon_{\text{sec}} - 2 \log_2(1)/\sqrt{2} \epsilon_{\text{PA}} \hat{\epsilon}$ is the additional cost for verification and privacy amplification. Our protocol is $2\epsilon_{\text{tot}}$ secure, where

$$\begin{aligned} \epsilon_{\text{tot}} &= \epsilon_{\text{cor}} + \epsilon_{\text{sec}}, \\ \epsilon_{\text{sec}} &= 2\hat{\epsilon} + \epsilon_{\text{PA}} + 4\sqrt{\epsilon_s + \epsilon_n}, \\ \epsilon_n &= \epsilon_n^A + \epsilon_{uu}, \\ \epsilon_s &= \epsilon_s^A + \epsilon_{ee}. \end{aligned} \quad (9)$$

Here, ϵ_{cor} describes the failure probability of error correction, ϵ_n^A is the failure probability of the lower bound of the untagged bits after AOPP [42], ϵ_s^A is the failure probability of the upper bound of the phase-flip error rate for the untagged bits after AOPP [42], ϵ_{uu} and ϵ_{ee} have been mentioned in Eqs. (5) and (6), $\hat{\epsilon}$ is the coefficient while using the chain rules of max and min entropy and ϵ_{PA} is the failure probability of privacy amplification [40].

IV. SIMULATION

In our simulations, we assume that the device parameters of both Alice and Bob, the channel between the two parties to the intermediate node Charlie and Charlie's device for interference measurement are symmetric for brevity. We take the photon detection efficiency as 30%, the dark count rate as 1×10^{-8} , the fiber loss coefficient as 0.2 dB/km, the error rate of the vacuum count as 0.5 and the error-correction inefficiency f as 1.1. We use the linear model in Ref. [40] to simulate the experimental observables. All details of our simulations are presented in the [Appendix](#).

A. The asymptotic key rate

We use infinite pulses and infinite decoy states to simply verify the effectiveness of our AD method for the AOPP SNS TFQKD protocol. According to the simulation equations of Refs. [32,39], we already know the number of untagged bits n_{A1} after AOPP step, the phase-flip error rate of the untagged bits e_{A1}^{ph} , the number of the sifted keys N_A , and the bit-flip error rate E_A of the sifted keys. When performing the AD step, the sifted key block of size b can pass the AD check only when all the sifted keys in the block have bit-flip errors or none of them has a bit-flip error. So the probability of successfully obtaining a processed key for a sifted key block of size b is $p_{\text{succ}} = E_A^b + (1 - E_A)^b$ and the bit-flip error of the processed key is $E_{AD} = E_A^b / (E_A^b + (1 - E_A)^b)$. Since all the processed untagged bits are generated from all the untagged blocks, the number of the processed untagged bits $n_1 = (n_{A1}/N_A)^b N_A / b$. Recall that the phase-flip error rate of the processed untagged bits $e_{AD}^{\text{ph}} = [1 - (1 - 2e_{A1}^{\text{ph}})^b] / 2$. Knowing these quantities, we can optimize the intensities, probabilities and other parameters in Eq. (4) to maximize the final secure key rate.

The asymptotic key rates per round of AOPP SNS TFQKD with or without AD step at different misalignment errors are shown in Fig. 1. The dashed and solid curves in the top right corner represent the key rate (bits/round) of AOPP SNS TFQKD and AOPP SNS TFQKD with AD protocols at different distances for a misalignment error of 2%. The blue solid broken line represents the

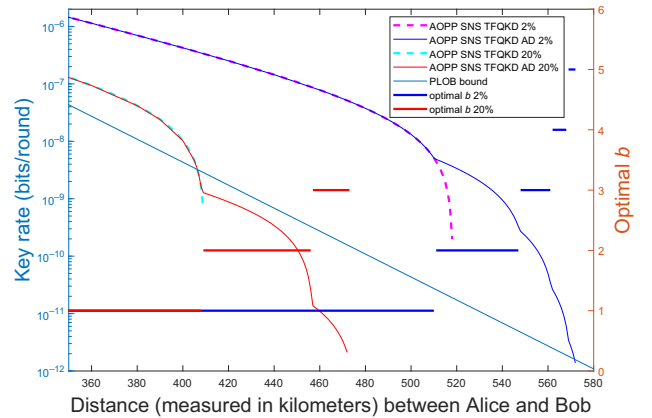


FIG. 1. The asymptotic key rates per round of AOPP SNS TFQKD with or without AD step at different misalignment errors. The dash-dotted asterisk line is the PLOB bound [28]. The dashed and solid curves in the top right corner represent the key rate (bits/round) of AOPP SNS TFQKD and AOPP SNS TFQKD with AD protocols at different distances for a misalignment error of 2%. The blue solid broken line represents the optimal block size b in AOPP SNS TFQKD with AD protocol at different distances for a misalignment error of 2%. The remaining three curves in the lower left corner of the figure denote the results for the misalignment error of 20%.

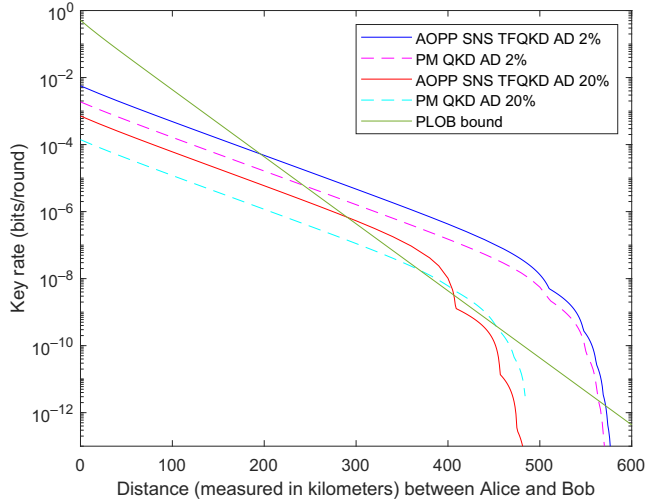


FIG. 2. The asymptotic key rates per round of AOPP SNS TFQKD with AD step and PM QKD with AD [47] at different misalignment errors. The dash-dotted asterisk line is the PLOB bound [28]. The solid curves represent the key rate (bits/round) of AOPP SNS TFQKD with AD protocol. The dashed curves represent the PM QKD with AD protocol.

optimal block size b in AOPP SNS TFQKD with AD protocol at different distances for a misalignment error of 2%. By setting the minimum key rate to 1×10^{-12} under the misalignment error of 2%, our AD method improves the achievable distance of AOPP SNS TFQKD protocol from 518 to 572 km. If we set the minimum key rate to the level that AOPP SNS TFQKD protocol can achieve, our protocol can still improve the achievable distance from 518 to 553 km. When the distance is less than 510 km, the AD block size b is 1, which means we do not need to insert an AD step. When the distance is larger than 510 km, the AD method can significantly improve the key rate at the same distance that the AOPP SNS TFQKD protocol can achieve and shows the advantages in improving communication distance. Our simulations show that the AD method brings improvement at long distances but not at short distances, which may be due to an improved signal-to-noise ratio at long distances when little signals are received. The dashed and solid curves in the lower left corner represent the key rate (bits/round) of AOPP SNS TFQKD and AOPP SNS TFQKD with AD protocols at different distances for a misalignment error of 20%. The red solid broken line represents the optimal block size b in AOPP SNS TFQKD with AD protocol at different distances for a misalignment error of 20%. From Fig. 1, it is apparent that inserting the AD step in AOPP SNS TFQKD can improve the achievable distance from 409 to 473 km under the misalignment error of 20%, which shows that the AD method can more significantly improve the maximum achievable distance under larger misalignment errors. The dash-dotted asterisk line is the PLOB bound [28]. We observe that the AD

method can also expand the distance range overcoming the linear key-rate bound under small misalignment errors for AOPP SNS TFQKD.

We conduct a comparison between the AOPP SNS TFQKD protocol and the phase-matching QKD protocol [31,47] in Fig. 2, both of which include the AD step under identical simulation parameter settings. The simulation results show that the maximum achievable distance of the two protocols are almost the same under different misalignment errors. AOPP SNS TFQKD with AD protocol generally has a higher key rate, but the PM QKD with AD protocol shows a key rate advantage at the regime of long distance under large misalignment error.

B. The finite key rate

We take 1×10^{14} pulses and four-intensity decoy states [40] to simulate the finite key rates at the misalignment errors of 2% and 20%. We set $\epsilon_{\text{cor}} = \hat{\epsilon} = \epsilon_{\text{PA}} = 10^{-10}$ and other failure probabilities to 1×10^{-20} , which is the same as Ref. [42]. We achieve $\epsilon_{\text{tot}} = 4.82 \times 10^{-9}$ secure for AOPP SNS TFQKD with AD protocol in the sense of composable security against coherent attacks.

The finite key rates per round of AOPP SNS TFQKD with or without AD step at different misalignment errors are shown in Fig. 3. The meaning of all the curves in Fig. 3 is the same as in Fig. 1, except that we calculate the finite key rates instead of the asymptotic key rates. Simulation

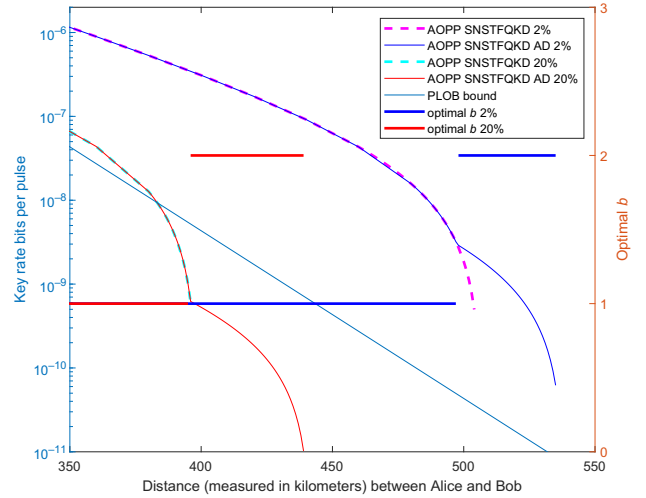


FIG. 3. The finite key rates per round of AOPP SNS TFQKD with or without AD step at different misalignment errors when sending 1×10^{14} pulses. The dashed and solid curves in the top right corner represent the key rate (bits/round) of AOPP SNS TFQKD and AOPP SNS TFQKD with AD protocols at different distances for a misalignment error of 2%. The blue solid broken line represents the optimal block size b in AOPP SNS TFQKD with AD protocol at different distances for a misalignment error of 2%. The remaining three curves in the lower left corner of the figure denote the results for the misalignment error of 20%.

results show that the AD method can improve the maximum achievable distance by 31 km under the 2% misalignment error and 43 km under the 20% misalignment error. It confirms that AD method can significantly improve the maximum achievable distance especially under the large misalignment error in practice.

V. CONCLUSION

In conclusion, we adopt the AD method to the AOPP SNS TFQKD protocol. We first prove the security in the asymptotic case. Then we prove the composable security against coherent attacks for fixed block size of 2, which can be easily generalized to the bit block size $b = 2^n$ (n is a natural number). Note that we can attempt to tackle the finite-key analysis for any bit block size $n \geq 2$ by employing the generalized black ball and white ball model. However, we encounter a mathematical challenge that demands rigorous proof. Specifically, given a fixed upper bound of the phase-flip error rate after the AD step, we want to prove that the associated failure probability does not diminish with an increase in the phase-flip error rate before the AD step, or at least make sure this holds for appropriate condition. This intriguing issue remains open for exploration in future investigations. The simulation results demonstrate that AD method can significantly improve the maximum achievable distance especially under the large misalignment error in practice. We expect our AD method can be conveniently applied to current SNS TFQKD systems without changing the experimental hardware system.

ACKNOWLEDGMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2020YFA0309802), the National Natural Science Foundation of China (Grants No. 62171424, No. 62271463, No. 62371244), the China Postdoctoral Science Foundation (Grants No. 2019T120446, No. 2018M642281), Prospect and Key Core Technology Projects of Jiangsu provincial key R & D Program (BE2022071), the Fundamental Research Funds for the Central Universities and the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701).

APPENDIX: THE SIMULATION DETAILS

We directly list the simulation formulas for AOPP SNS TFQKD with the AD method in the finite-key regime below. Note that the asymptotic key rate can be easily obtained from the finite-key regime by simply using mean values of variables.

In carrying out the AOPP SNS TFQKD protocol, Alice and Bob first choose the code and decoy mode with probability p_Z and $1 - p_Z$. In code mode, they send the vacuum state and the code intensity μ with probability p_{Z0} and

$1 - p_{Z0}$. In decoy mode, they send the vacuum state and the decoy intensity μ_1 and μ_2 with probability p_0, p_1 , and $1 - p_0 - p_1$. We denote the total pulses as N , the transmission distance as L , the phase slices in the postselection as Δ , the photon detection efficiency as η_d , the dark count rate as p_d , the fiber loss coefficient as α , the misalignment as e_d . The channel transmittance from Alice (Bob) to Charlie is $\eta = 10^{-\alpha L/20} \eta_d$.

In code mode, we divide the keys before AOPP into four categories $C0, C1, V$, and D : Alice sends the vacuum state and Bob sends the signal state, Bob sends the vacuum state and Alice sends the signal state, they both send the signal state, they both send the vacuum state. The numbers of $C0, C1, V$, and D are

$$nC0 = 2Np_Z^2 p_{Z0} (1 - p_{Z0}) ((1 - p_d) e^{-\eta\mu/2} - (1 - p_d)^2 e^{-\eta\mu}), \quad (\text{A1})$$

$$nC1 = nC0, \quad (\text{A2})$$

$$nV = 2Np_Z^2 p_{Z0}^2 p_d (1 - p_d), \quad (\text{A3})$$

$$nD = 2Np_Z^2 (1 - p_{Z0})^2 ((1 - p_d) e^{-\eta\mu} I_0(\eta\mu) - (1 - p_d)^2 e^{-2\eta\mu}), \quad (\text{A4})$$

where $I_0(x)$ is the 0-order hyperbolic Bessel function of the first kind. So the number of the keys is $n_t = nC0 + nC1 + nV + nD$ and the bit-flip error is $E_Z = (nD + nV)/n_t$. In a round of the protocol, we use “0” to indicate that Alice (Bob) sends the vacuum state, “1” to indicate that she (he) sends the decoy state intensity μ_1 and “2” to indicate that she (he) sends the decoy state intensity μ_2 , N_{ij} to indicate the total number of instances that Alice sends the state “ i ” and Bob sends the state “ j ” in the case except that both Alice and Bob choose the code mode, n_{ij} to denote the number of successful detections of instances “ N_{ij} ”. We have

$$N_{00} = ((1 - p_Z)^2 p_0^2 + 2(1 - p_Z)p_Z p_0 p_{Z0})N, \quad (\text{A5})$$

$$N_{01} = ((1 - p_Z)^2 p_0 p_1 + (1 - p_Z)p_Z p_{Z0} p_1)N, \quad (\text{A6})$$

$$N_{10} = N_{01}, \quad (\text{A7})$$

$$N_{02} = ((1 - p_Z)^2 p_0 p_2 + (1 - p_Z)p_Z p_{Z0} p_2)N, \quad (\text{A8})$$

$$N_{20} = N_{02}, \quad (\text{A9})$$

$$n_{00} = 2p_d(1 - p_d)N_{00}, \quad (\text{A10})$$

$$n_{01} = 2((1 - p_d)e^{-\eta\mu_1/2} - (1 - p_d)^2 e^{-\eta\mu_1})N_{01}, \quad (\text{A11})$$

$$n_{10} = n_{01}, \quad (\text{A12})$$

$$n_{02} = 2((1 - p_d)e^{-\eta\mu_2/2} - (1 - p_d)^2 e^{-\eta\mu_2})N_{02}, \quad (\text{A13})$$

$$n_{20} = n_{02}. \quad (\text{A14})$$

We denote the counting rate of instances “ N_{ij} ” as $S_{ij} = n_{ij}/N_{ij}$. When Alice and Bob both send the decoy intensity μ_1 , we use N_δ to denote the number of instances that

meet the phase postselection condition in all sending pulse, $n_{e\delta}$ to denote the total error counting number of these N_δ instances. We have

$$N_\delta = \frac{\Delta}{\pi}(1-p_Z)^2 p_1^2 N, \quad (\text{A15})$$

$$n_{e\delta} = \left\{ \left[\frac{1}{\Delta} \int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} (1-p_d) e^{-2\eta\mu_1 \cos^2(\frac{\delta}{2})} d\delta - (1-p_d)^2 e^{-2\eta\mu_1} \right] (1-e_d) + \left[\frac{1}{\Delta} \int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} (1-p_d) e^{-2\eta\mu_1 \sin^2(\frac{\delta}{2})} d\delta - (1-p_d)^2 e^{-2\eta\mu_1} \right] e_d \right\} N_\delta. \quad (\text{A16})$$

We denote the expected value of the observable x as $\langle x \rangle$, and $\langle \bar{x} \rangle$ and $\langle \underline{x} \rangle$ are the upper bound and lower bound of $\langle x \rangle$ when estimating the expected value from its observed value. We also denote $\varphi^U(y)$ and $\varphi^L(y)$ as the upper and lower bounds when estimating the real values according to the expected values. Note that $\langle \bar{x} \rangle$, $\langle \underline{x} \rangle$, $\varphi^U(y)$, and $\varphi^L(y)$ can be obtained by using Chernoff bound, which are described in detail in Ref. [40]. So the lower bound of the expected value of the counting rate of untagged photons before AOPP is

$$\langle \underline{s_1^Z} \rangle = \frac{1}{2\mu_1\mu_2(\mu_2 - \mu_1)} [\mu_2^2 e^{\mu_1} (\langle \underline{S_{01}} \rangle + \langle \underline{S_{10}} \rangle) - \mu_1^2 e^{\mu_2} (\langle \overline{S_{02}} \rangle + \langle \overline{S_{20}} \rangle) - 2(\mu_2^2 - \mu_1^2) \langle \overline{S_{00}} \rangle]. \quad (\text{A17})$$

The expected value of the phase-flip error rate of the untagged photon is

$$\langle \overline{e_1^{\text{ph}}} \rangle = \frac{\langle \overline{T_\Delta} \rangle - \frac{1}{2} e^{-2\mu_1} \langle \overline{S_{00}} \rangle}{2\mu_1 e^{-2\mu_1} \langle \underline{s_1^Z} \rangle}, \quad (\text{A18})$$

where $T_\Delta = n_{e\delta}/N_\delta$.

AOPP and OPER processing are equivalent in terms of security analysis [39] and we denote the equivalence coefficient as u_g :

$$u_g = \frac{n_t \min(nC_0 + nD, nC_1 + nV)}{2(nC_0 + nD)(nC_1 + nV)}. \quad (\text{A19})$$

We next consider the OPER processing on $n_o = u_g n_t$ key bits. The lower bound of untagged bits in these key bits is $n_{o1} = 2p_z^2 p_{z0}(1-p_{z0})\mu e^{-\mu} u_g N \langle \underline{s_1^Z} \rangle$. The upper bound of the number of phase errors in these untagged bits is

$M_{e_o} = n_{o1} \langle \overline{e_1^{\text{ph}}} \rangle$. We define

$$p_{C_1 C_0} = p_{C_0 C_1} = \frac{nC_0 nC_1}{n_t^2}, \quad (\text{A20})$$

$$p_{DV} = p_{VD} = \frac{nVnD}{n_t^2}. \quad (\text{A21})$$

The remaining key bits after OPER processing on the $n_o = u_g n_t$ key bits is

$$n_{n1} = \frac{n_o}{2} (p_{C_1 C_0} + p_{C_0 C_1} + p_{DV} + p_{VD}), \quad (\text{A22})$$

where the bit-flip error rate of these key bits is $E_1 = (p_{DV} + p_{VD}) / (p_{C_1 C_0} + p_{C_0 C_1} + p_{DV} + p_{VD})$. The lower bound of the untagged bit pairs is

$$\epsilon = 2\xi_L \left(\underline{n_{uu}}; \frac{n_{o1}^2}{n_o}, \frac{n_o}{2} \right), \quad (\text{A23})$$

where $\xi_L(x; p, N)$ is defined in Eq. (5). The untagged bits after OPER is

$$\epsilon = 2\xi_L \left(\underline{n_{oper}}; \frac{n_{o1}'}{n_{uu}} \left(1 - \frac{n_{o1}'}{2n_{uu}} \right), \underline{n_{uu}} \right), \quad (\text{A24})$$

where $n_{o1}' = 2n_{uu}(1/2 - \sqrt{-\log \epsilon / 2n_{uu}})$. The upper bound of phase-flip error rate of these untagged bits after OPER is $e_o^{\text{ph}} = \bar{M}_S / \underline{n_{oper}}$, where

$$\epsilon = 2\xi_L(\bar{M}_S - r; E_\tau(1 - E_\tau), \underline{n_{uu}} - r), \quad (\text{A25})$$

$$k = \varphi^L \left(n_{o1} - \frac{n_{o1}^2}{n_o} \right), \quad (\text{A26})$$

$$r = \frac{2n_{uu} + k}{k} \log \left(\frac{3k^2}{\epsilon} \right), \quad (\text{A27})$$

$$E_\tau = \frac{2n_{uu} \langle \overline{e_1^{\text{ph}}} \rangle - 2.33 \sqrt{2n_{uu} \langle \overline{e_1^{\text{ph}}} \rangle}}{2n_{uu} - r}. \quad (\text{A28})$$

So after the AOPP processing, the total number of sifted keys $N_A = 2n_{n1}$, the bit-flip error rate $E_A = E_1$, the number of untagged bits $n_{A1} = 2n_{oper}$ and the phase-flip error rate of the untagged bits $e_{A1}^{\text{ph}} = e_o^{\text{ph}}$. As an example, we just list the simulation formulas for the AD block size of 2 below for completeness.

$$p_{\text{succ}} = E_A^2 + (1 - E_A)^2, \quad (\text{A29})$$

$$E_{\text{AD}} = \frac{E_A^2}{E_A^2 + (1 - E_A)^2}, \quad (\text{A30})$$

$$N_{\text{AD}} = \frac{N_A}{2} p_{\text{succ}}, \quad (\text{A31})$$

$$\epsilon = 2\xi_L \left(n_1; \left[\frac{\varphi^L(n_{A1})}{N_A} \right]^2, \frac{N_A}{2} \right), \quad (\text{A32})$$

$$\epsilon = 2\xi_L \left(M_{ee}; (e_{A1}^{\text{ph}})^2, n_1, \right), \quad (\text{A33})$$

$$M_{\text{ph}} = n_1 e_{A1}^{\text{ph}} - M_{ee}, \quad (\text{A34})$$

$$e_{\text{AD}}^{\text{ph}} = \frac{M_{\text{ph}}}{n_1}. \quad (\text{A35})$$

All the symbols remain consistent with the previous part. Note that the simulation formulas for the block size 2^n are easily obtained from the previous part.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, 1984), p. 175.
- [2] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] D. Mayers, in *Advances in Cryptology – CRYPTO '96* (Springer Berlin Heidelberg, 1996), p. 343.
- [4] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).
- [5] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [6] B. Kraus, N. Gisin, and R. Renner, Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication, *Phys. Rev. Lett.* **95**, 080501 (2005).
- [7] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [8] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [9] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [10] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [11] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [12] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, *Nature* **509**, 475 (2014).
- [13] R. König, R. Renner, A. Bariska, and U. Maurer, Small accessible quantum information does not imply security, *Phys. Rev. Lett.* **98**, 140502 (2007).
- [14] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, *Nat. Commun.* **3**, 634 (2012).
- [15] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 3732 (2014).
- [16] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Experimental long-distance decoy-state quantum key distribution based on polarization encoding, *Phys. Rev. Lett.* **98**, 010505 (2007).
- [17] 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).
- [18] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **111**, 130502 (2013).
- [19] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Measurement-device-independent quantum key distribution over 200 km, *Phys. Rev. Lett.* **113**, 190501 (2014).
- [20] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, *Nat. Photonics* **9**, 832 (2015).
- [21] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, *Nat. Photonics* **9**, 827 (2015).
- [22] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phase-reference-free experiment of measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **115**, 160502 (2015).
- [23] 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).
- [24] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Measurement-device-independent quantum key distribution over untrusted metropolitan network, *Phys. Rev. X* **6**, 011024 (2016).
- [25] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution robust against environmental disturbances, *Optica* **4**, 1016 (2017).
- [26] S.-K. Liao *et al.*, Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [27] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussi eres, and H. Zbinden, Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, *Nat. Photonics* **17**, 422 (2023).
- [28] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).

- [29] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 5235 (2014).
- [30] 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* **557**, 400 (2018).
- [31] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, *Phys. Rev. X* **8**, 031043 (2018).
- [32] 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).
- [33] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, *Phys. Rev. A* **98**, 042332 (2018).
- [34] 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).
- [35] 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).
- [36] 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).
- [37] Y. Zhou, Z.-Q. Yin, R.-Q. Wang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution with partial phase postselection, *Phys. Rev. Appl.* **18**, 054026 (2022).
- [38] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution in practice, *Sci. Rep.* **9**, 3080 (2019).
- [39] 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).
- [40] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses, *Phys. Rev. Appl.* **12**, 024061 (2019).
- [41] C. Jiang, X.-L. Hu, H. Xu, Z.-W. Yu, and X.-B. Wang, Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects, *New J. Phys.* **22**, 053048 (2020).
- [42] C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, Composable security for practical quantum key distribution with two way classical communication, *New J. Phys.* **23**, 063038 (2021).
- [43] 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).
- [44] R. Renner, Ph.D. thesis, School Swiss Federal Institute of Technology Zurich, 2005.
- [45] 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).
- [46] 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).
- [47] 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).
- [48] H. F. Chau, Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate, *Phys. Rev. A* **66**, 060302 (2002).
- [49] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, *IEEE Trans. Inf. Theory* **49**, 457 (2003).