


## Sending-or-not-sending quantum key distribution with phase postselection

Yang-Guang Shan<sup>1,2</sup>, Yao Zhou<sup>1,2</sup>, Zhen-Qiang Yin<sup>1,2,3,\*</sup>, Shuang Wang<sup>1,2,3,†</sup>, Wei Chen<sup>1,2,3</sup>,  
De-Yong He<sup>1,2,3</sup>, Guang-Can Guo<sup>1,2,3</sup> and Zheng-Fu Han<sup>1,2,3</sup>

<sup>1</sup> CAS Key Laboratory of Quantum Information, *University of Science and Technology of China, Hefei, Anhui 230026, China*

<sup>2</sup> CAS Center for Excellence in Quantum Information and Quantum Physics, *University of Science and Technology of China, Hefei, Anhui 230026, China*

<sup>3</sup> Hefei National Laboratory, *University of Science and Technology of China, Hefei 230088, China*

 (Received 9 January 2024; revised 7 April 2024; accepted 1 August 2024; published 21 August 2024)

Quantum key distribution (QKD) could help to share a secure key between two distant peers. In recent years, twin-field (TF) QKD has been widely investigated because of its long transmission distance. One of the popular variants of TF QKD is sending-or-not-sending (SNS) QKD, which has been experimentally verified to realize 1000-km level fiber key distribution. In this article, we introduce phase postselection into the SNS protocol. With this modification, the probability of selecting “sending” can be substantially improved. The numerical simulation shows that the transmission distance can be improved both with and without the actively odd-parity pairing method. The case of discrete phase randomization is also analyzed, a similar improvement on distance can be seen.

DOI: [10.1103/PhysRevApplied.22.024056](https://doi.org/10.1103/PhysRevApplied.22.024056)

### I. INTRODUCTION

Quantum key distribution (QKD) [1] tries to establish secure communication between two distant peers, Alice and Bob, by sharing private random numbers. Guaranteed by the fundamental principles of quantum mechanics [2,3], Alice and Bob can bound the amount of information stolen by any eavesdropper (usually called Eve), thus they could extract secure keys unknown to Eve.

The basis of the security comes from the no-cloning theorem of a single photon [4]. Unluckily, because of the attenuation of the channels, a photon cannot transmit for a long distance. The PLOB bound [5,6] gives the fundamental limitation of the point-to-point QKD, in which the key rate decreases linearly with the channel transmittance ( $R \leq O(\eta)$  [6]) (see another bound in Ref. [7]). Fortunately, twin-field (TF) QKD [8] broke this limitation reaching a key rate of  $O(\sqrt{\eta})$  level. TF QKD has a unique advantage for long-distance key distribution and has been widely researched both in theory [9–13] and experiment [14–26].

Sending-or-not-sending (SNS) [10,27] QKD is a special kind of TF QKD, in which the information is encoded on the choice of sending a coherent state (sending) or a vacuum state (not sending). A distinctive advantage of SNS QKD is its high tolerance for misalignment errors, which

are the errors from the imperfect visibility of the interference caused by imperfect devices and the background disturbance from the channel [28]. Though the SNS protocol has a lot of advantages, there is a vital drawback. In SNS QKD, Alice and Bob randomly choose to send a coherent state with a probability  $p$  or a vacuum state with a probability  $1 - p$ . When they both choose to send the coherent state and a successful click occurs, they get a bit error. Since the correct clicks correspond to the case that only one of Alice and Bob chooses to send a coherent state, whose counting rate is smaller than the sending-sending case, they must choose a small sending probability  $p$  to reduce the probability of a sending-sending case ( $p^2$ ). With a small  $p$ , the total counting rate is also reduced, limiting the performance of the protocol.

To solve this problem, the actively odd-parity pairing (AOPP) postprocessing method [29–31] can be used to significantly reduce the influence of bit errors and improve the sending probability. SNS-AOPP QKD can realize both a long transmission distance and a large key rate. Recently, utilizing the advantage of SNS-AOPP QKD, the first fiber-QKD over 1000 km is reported [26].

In this article, we give another way to reduce the bit error rate by introducing phase postselection into SNS QKD. In the original SNS protocol, the phases of the coherent states are randomized. But when the phases of Alice and Bob are the same in the sending-sending cases, more left-click events (constructive interference) will happen than right-click events (destructive interference) in an interferometer. And if the phase difference between Alice and Bob is  $\pi$ ,

\*Contact author: yinzq@ustc.edu.cn

†Contact author: wshuang@ustc.edu.cn

more right-click events will happen. So before the post-processing of the keys, Alice and Bob can announce their phases of all rounds. If the phases of Alice and Bob are close, they only keep the right-click events. And if the phases are opposite, they keep only the left-click events. This sifting step may discard a part of the correct bits but almost all error bits. Thus a large sending probability  $p$  can be chosen and the total number of correct bits can be improved.

Naturally, the behavior of announcing the phases will increase the information that an eavesdropper can get. The coherent state sent by Alice or Bob cannot be treated as a mixed state of Fock states. Thus we give the security analysis of the alternative protocol in this article and compare the performance with the original SNS protocol.

We analyzed several kinds of variants of our modification. The phases of signal states can be continuously randomized or discretely randomized. We also try to apply the AOPP method to improve the transmission distance. Our numerical simulation shows that with continuous phase randomization, the transmission distance can be much longer than the original SNS protocol. With discrete phase randomization, our variant can keep this advantage. The AOPP method could drastically improve the performance of the original SNS protocol. However, the improvement is not so large if AOPP is used in our protocol. AOPP cannot help to improve the key rate of our variant, but the transmission distance is improved distinctly. Both with AOPP, our variant could have a longer distance than the SNS-AOPP protocol.

In Sec. II we introduce the procedure of our protocol. In Sec. III we give the security analysis of our protocol. In Sec. IV we conduct the numerical simulation to compare the performance of our protocol. In Sec. V we discuss some variants of our protocol. We come to a conclusion in Sec. VI.

## II. PROTOCOL DESCRIPTION

We introduce the procedure of our variant with continuous phase randomization in the following.

1. **State preparation.** For each round, Alice (Bob) randomly prepares a signal state with a probability  $q$  or a decoy state with a probability  $(1 - q)$ .

If Alice (Bob) decides to prepare a signal state, with a probability  $p$ , she (he) will prepare a weak coherent state with an intensity  $\mu$  and record a local classical bit 1 (0), otherwise (with a probability  $1 - p$ ) she (he) will prepare a vacuum state and record a local classical bit 0 (1).

If she (he) decides to prepare a decoy state, she (he) will randomly choose an intensity from  $\{\nu_1, \nu_2, \dots\}$  and prepare the corresponding weak coherent state. The number of intensities and the corresponding probabilities can

be chosen according to performance optimization or experimental convenience. A three-intensity protocol (with one decoy intensity) is analyzed in Appendix D.

When Alice (Bob) decides to send a (signal and decoy) weak coherent state, she (he) records the phase of the weak coherent state  $\theta_A$  ( $\theta_B$ ) locally.

When Alice (Bob) decides to send a vacuum state  $|0\rangle$ , she (he) produces a uniform random phase in  $[0, 2\pi)$  and records it as the phase  $\theta_A$  ( $\theta_B$ ).

Alice and Bob send the states to the third party Charlie in the middle of the channel.

In this protocol, we separate all the signal rounds (in which both Alice and Bob prepare a signal state) into two kinds. In  $\mathbb{C}$  (correct) rounds, Alice and Bob record the same classical bits, which means only one of them selects to send the vacuum state and the other chooses to send the coherent state. In  $\mathbb{E}$  (error) rounds, Alice and Bob record different classical bits, which means Alice and Bob both select to send the vacuum states or both select to send the coherent states.

2. **State measurement.** If Charlie is honest, he will perform an interferometric measurement with the two states from Alice and Bob. We assume that the left detector corresponds to the constructive interference and the right detector corresponds to the destructive interference for pulses with the same phase. Then Charlie will declare a left-click event, a right-click event, or a failed event according to the clicks of the two detectors. Left-click events and right-click events are collectively called successful events.

3. **Sifting and phase postselection.** After enough rounds of the first two steps, Alice and Bob announce their choices of preparing a signal state or a decoy state of each round. They also announce their intensity choices if they prepare the decoy states. The successful events from the case that both Alice and Bob prepare the signal states are kept as clicked signal events.

Alice and Bob announce the phases they saved in the first step publicly. For every clicked signal event with a left click, if  $|\theta_A - \theta_B - \pi| \leq \Delta$ , they keep the round as a sifted left-click event. And for every clicked signal event with a right click, if  $|\theta_A - \theta_B| \leq \Delta$  or  $|\theta_A - \theta_B - 2\pi| \leq \Delta$ , they keep the round as a sifted right-click event.

4. **Parameter estimation and postprocessing.** Alice and Bob use the decoy-state method [32–34] to estimate the phase-error rates [35–37]. We will give the phase-error analysis in Sec. III and the decoy estimation in Appendix A. And we will give the estimation of a practical three-intensity case in Appendix D.

Then Alice and Bob conduct error correction and privacy amplification to the classical bits of the remaining rounds to get the final key. They may use some two-way error-rejection methods to improve the performance of the protocol, for example, the AOPP method.

### III. SECURITY ANALYSIS

In this section, we give the security against collective attacks under asymptotic case. Thus the signal-state probability  $q$  can be set to 1.

Notice that there are two kinds of successful events, the  $\mathbb{C}$ -round events and the  $\mathbb{E}$ -round events. We cannot separate them before the error correction, thus they both contribute to the key consumption of error correction. Similar to the analysis of the original SNS protocol, we only use the  $\mathbb{C}$  rounds to generate keys.

Firstly, we give the equivalent protocol based on entanglement. In the following, we will analyze the security of right-click events, and the security of left-click events is analogous.

Because of the phase interval  $\Delta$  of the phase postselection, the phase difference between Alice and Bob is set to  $\delta \in [-\Delta, \Delta]$ . Then we can give the equivalent protocol, in which Alice and Bob prepare the state,

$$|\psi(\theta, \delta)\rangle = \left( \sqrt{1-p} |0\rangle_A |0\rangle_a + \sqrt{p} |1\rangle_A |\alpha e^{i\theta}\rangle_a \right) \otimes \left( \sqrt{1-p} |1\rangle_B |0\rangle_b + \sqrt{p} |0\rangle_B |\alpha e^{i(\theta+\delta)}\rangle_b \right), \quad (1)$$

where the subscripts  $A$  and  $B$  correspond to the local ancillas of Alice and Bob, and the subscripts  $a$  and  $b$  correspond to the states sent to Charlie. Here  $|\alpha e^{i\theta}\rangle_a$  is the weak coherent state from Alice with an intensity of  $|\alpha|^2 = \mu$  and a phase  $\theta$ . The state  $|\alpha e^{i(\theta+\delta)}\rangle_b$  is similarly defined. The state  $|0\rangle_{a(b)}$  is the vacuum state prepared by Alice (Bob). We also define  $|0\rangle_{A(B)}$  and  $|1\rangle_{A(B)}$  as two orthogonal states of the ancilla held by Alice (Bob) locally. To

get the classical bits, Alice and Bob can measure their ancillas on the  $\mathbb{Z}$  basis ( $|0\rangle$  and  $|1\rangle$ ). And the phase-error rate, which is the error rate when Alice and Bob measure their ancillas on the  $\mathbb{X}$  basis ( $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  and  $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ ), relates to the amount of information that may be leaked to eavesdroppers.  $\theta$  is the phase of Alice, which is randomized in all rounds.  $\delta$  is also randomized from  $[-\Delta, \Delta]$ .

For the  $\mathbb{C}$  rounds, only one of Alice and Bob decides to send a weak coherent state. Thus a state in a  $\mathbb{C}$  round can be written as

$$\begin{aligned} & (|00\rangle_{AB} \langle 00|_{AB} + |11\rangle_{AB} \langle 11|_{AB}) |\psi(\theta, \delta)\rangle \\ &= \sqrt{p(1-p)} (|00\rangle_{AB} |0\rangle_a |\alpha e^{i(\theta+\delta)}\rangle_b \\ &+ |11\rangle_{AB} |\alpha e^{i\theta}\rangle_a |0\rangle_b). \end{aligned} \quad (2)$$

We define that when Alice and Bob measure their ancillas on the  $\mathbb{X}$  basis,  $|+-\rangle_{AB}$  and  $|--\rangle_{AB}$  correspond to correct results, and  $|++\rangle_{AB}$  and  $|--\rangle_{AB}$  correspond to errors. Operating  $|++\rangle \langle ++|_{AB} + |--\rangle \langle --|_{AB}$  on Eq. (2), the probability of a  $\mathbb{C}$ -round right-click phase error, when a round of  $|\psi(\theta, \delta)\rangle$  is sent, can be estimated as  $P_{\text{ph}}^R(\theta, \delta) = p(1-p)P^R((|0\rangle_a |\alpha e^{i(\theta+\delta)}\rangle_b + |\alpha e^{i\theta}\rangle_a |0\rangle_b)/\sqrt{2})$ . Here  $P^R(\cdot)$  means the probability that a right-click event is declared by Charlie when a state  $|\cdot\rangle$  is sent from Alice and Bob.  $|\cdot\rangle$  can be unnormalized, and  $P^R(c|\cdot\rangle) = |c|^2 P^R(|\cdot\rangle)$ .

Realizing that the phase  $\theta$  is randomly chosen in  $[0, 2\pi)$  and  $\delta$  is also randomized, to get the average of  $P_{\text{ph}}^R$ , we calculate the integration below in Eq. (3). Here  $|j\rangle$  is the Fock state of  $j$  photons.  $\mu = |\alpha|^2$  is the intensity of the coherent state.

$$\begin{aligned} P_{\text{ph}}^R &= \frac{1}{4\pi\Delta} \int_{-\Delta}^{\Delta} d\delta \int_0^{2\pi} d\theta P_{\text{ph}}^R(\theta, \delta) \\ &= p(1-p)e^{-\mu} \left( 2P^R(|0\rangle_a |0\rangle_b) + \sum_{j=1}^{\infty} \frac{\mu^j}{j!} \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta P^R \left( \frac{e^{ij\delta} |0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right). \end{aligned} \quad (3)$$

In Eq. (3) we use the linear additivity between the measurement probability and the density matrix. In the calculation of the right-click rate, we can treat the behavior of Eve's attack and Charlie's measurement as a whole to be a POVM measurement, and we define that the corresponding POVM matrix is  $M^R$  when Charlie announces a right click. Then the probability of a right-click event can be calculated as  $P^R(|\cdot\rangle) = \text{Tr}(M^R |\cdot\rangle \langle \cdot|)$ . Then Eq. (3) can be given by Eq. (4), where  $\mathcal{P}(|\cdot\rangle) = |\cdot\rangle \langle \cdot|$ .

$$\begin{aligned} & \frac{1}{2\pi} \int_0^{2\pi} d\theta P^R \left( \frac{|0\rangle_a |\alpha e^{i(\theta+\delta)}\rangle_b + |\alpha e^{i\theta}\rangle_a |0\rangle_b}{\sqrt{2}} \right) \\ &= \frac{1}{2\pi} \int_0^{2\pi} d\theta \text{Tr} \left( M^R \mathcal{P} \left( \frac{|0\rangle_a |\alpha e^{i(\theta+\delta)}\rangle_b + |\alpha e^{i\theta}\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right) \end{aligned}$$

$$\begin{aligned}
 &= \text{Tr} \left( M^R \frac{1}{2\pi} \int_0^{2\pi} d\theta \mathcal{P} \left( \sum_{j=0}^{\infty} \sqrt{\frac{e^{-\mu} \mu^j}{j!}} e^{ij\theta} \frac{e^{ij\delta} |0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right) \\
 &= \text{Tr} \left( M^R \left( e^{-\mu} \mathcal{P}(\sqrt{2} |00\rangle_{ab}) + \sum_{j=1}^{\infty} e^{-\mu} \frac{\mu^j}{j!} \mathcal{P} \left( \frac{e^{ij\delta} |0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right) \right) \\
 &= 2e^{-\mu} \text{Tr}(M^R \mathcal{P}(|00\rangle_{ab})) + \sum_{j=1}^{\infty} e^{-\mu} \frac{\mu^j}{j!} \text{Tr} \left( M^R \mathcal{P} \left( \frac{e^{ij\delta} |0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right). \quad (4)
 \end{aligned}$$

The average right-click rate of states  $e^{ij\delta} |0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b$  can be estimated by decoy states, which is explained in detail in Appendix A.

The phase-error rate of  $\mathbb{C}$  rounds can be given by  $e_{\text{ph}}^R = P_{\text{ph}}^R / P_c^R$ , where  $P_c^R$  is the probability that a  $\mathbb{C}$ -round right-click event occurs when  $|\psi\rangle$  is sent. Then the key rate of right-click events is shown as

$$R^R = s \left( P_c^R \left( 1 - H_2 \left( \frac{P_{\text{ph}}^R}{P_c^R} \right) \right) - f P_t^R H_2(e_{\text{bit}}^R) \right), \quad (5)$$

where  $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$  is the binary entropy function, and  $f$  is the error-correction efficiency.  $s = (\Delta/\pi)$  is the phase-sifting efficiency, and  $P_t^R$  is the right-click rate of sifted rounds.  $e_{\text{bit}}^R$  is the bit-error rate of sifted right-click rounds.  $P_t^R$  is known by counting the number of sifted right-click events and  $P_c^R = P_t^R(1 - e_{\text{bit}}^R)$  is simply known after the error-correction step.

For the left-click events, the analysis is similar. The only difference is that the phase error corresponds to the left-click rate of  $(|0\rangle_a |\alpha e^{i(\theta+\delta)}\rangle_b + |-\alpha e^{i\theta}\rangle_a |0\rangle_b) / \sqrt{2}$ . The key rate is shown as

$$R^L = s \left( P_c^L \left( 1 - H_2 \left( \frac{P_{\text{ph}}^L}{P_c^L} \right) \right) - f P_t^L H_2(e_{\text{bit}}^L) \right). \quad (6)$$

And the total key rate can be shown as  $R = R^R + R^L$ .

#### IV. NUMERICAL SIMULATION

We conduct numerical simulation to show the advantage of our modification. In our simulation, infinite decoy states are assumed. Thus we can directly calculate the estimation of phase errors. The detailed calculation is shown in Appendix B. The device parameters of the simulation are

TABLE I. Parameters we used in our simulation.

$P_d$	$d$	$f$	$e_{\text{mis}}$
1	$10^{-11}$	1.1	0.04

shown in Table I, where  $P_d$  is the detecting efficiency of detectors.  $d$  is the dark counting rate of detectors.  $f$  is the error-correction efficiency.  $e_{\text{mis}}$  is the misalignment error rate.

We compare the key rates of the original SNS protocol and our variant, which is shown in Fig. 1. We can see that our variant has a longer transmission distance of about 10 dB, which corresponds to about a 50-km fiber channel.

In the original SNS protocol, the optimal sending probability is about 4%, which means that in 92% of all rounds both Alice and Bob send vacuum states. Thus at long distance, the dark counts of these rounds increase the bit errors a lot. The  $\mathbb{C}$  rounds only account for about 8%. Thus the signal-to-noise ratio is significantly influenced at long distance. And in our variant, the optimal sending probability can reach a level of 30%, which means sending-sending rounds and vacuum-vacuum rounds account for about 58%. The rest 42% rounds are  $\mathbb{C}$  rounds. Thus a longer distance is reasonable.

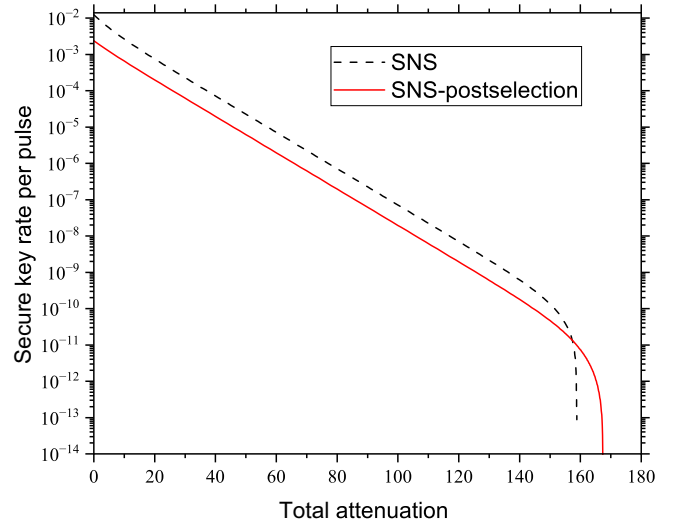


FIG. 1. The simulation result of the original SNS protocol and our modified protocol. The line SNS-postselection corresponds to the key rates of our variant, and the line SNS corresponds to the key rate of the original SNS protocol.



## V. DISCUSSION

In our numerical simulation, we have compared the performance of our modified protocol and the original SNS protocol. It seems that our protocol could reach a longer transmission distance, but the key rate is relatively lower. For the case of short transmission distance, the sifting efficiency must be the major restriction of the key rates. A small sifting interval  $\Delta$  will decrease the sifting efficiency, while a large sifting interval may increase the bit-error rate and the phase-error rate. To catch up with the performance of the SNS protocol at short distance, we give another variant of our protocol below.

In the variant protocol, Alice and Bob do not randomize the phases of weak coherent states continuously, but they randomly select from  $M$  discrete phases. In step 1 of the protocol description, when Alice (Bob) chooses to send a weak coherent state, she (he) will randomly choose a phase  $\theta_A$  ( $\theta_B$ ) from  $\{0, (2\pi/M), 2(2\pi/M), \dots, (M-1)(2\pi/M)\}$  ( $M > 0$  is an even number) and prepare a state  $|\alpha e^{i\theta_A}\rangle$  ( $|\alpha e^{i\theta_B}\rangle$ ). When she (he) chooses to send a vacuum state, she (he) also records a random phase  $\theta_A$  ( $\theta_B$ ) from  $\{0, (2\pi/M), 2(2\pi/M), \dots, (M-1)(2\pi/M)\}$ . In step 3, for left-click events, the rounds that  $|\theta_A - \theta_B| = \pi$  are kept. And for right-click events, the rounds that  $\theta_A = \theta_B$  are kept. Thus the sifting efficiency is about  $1/M$ .  $M$  is set to be an even number to keep the existence of  $|\theta_A - \theta_B| = \pi$  events. Note that  $M = 1$  is also feasible, and only one detector is needed (the right detector) to conduct the protocol. But we do not discuss it because of its low performance.

$M = 2, 4$  might be two good choices, since a big  $M$  also decreases the sifting efficiency. We give the security analysis of the  $M = 2, 4$  cases in Appendix C. We also simulated the key rates of these two cases shown in Fig. 2.

The simulation shows that with discrete phase randomization, the key rate of our variant is improved, which can approach the key rate of the original SNS protocol. The  $M = 2$  case can have a similar performance to the original SNS protocol. The  $M = 4$  case can approach the maximum distance of the continuous-phase-randomization case and have a larger key rate.

The original SNS protocol benefits a lot from the AOPP postprocessing method, which both improves the key rate and the transmission distance of the SNS protocol. The SNS-AOPP protocol has been widely used to realize long-distance QKD [23,24,26]. Realizing that the  $\mathbb{C}$  rounds of our variant have no bit errors, we can directly use the security analysis of the SNS-AOPP protocol [29] to apply AOPP on our variant. We compare the performance with AOPP in Fig. 3. The simulation shows that SNS-AOPP has an obvious advantage on key rate, but AOPP does not help to improve the key rate of our variant. However, with AOPP our variant could have a longer transmission distance overwhelming the SNS-AOPP.

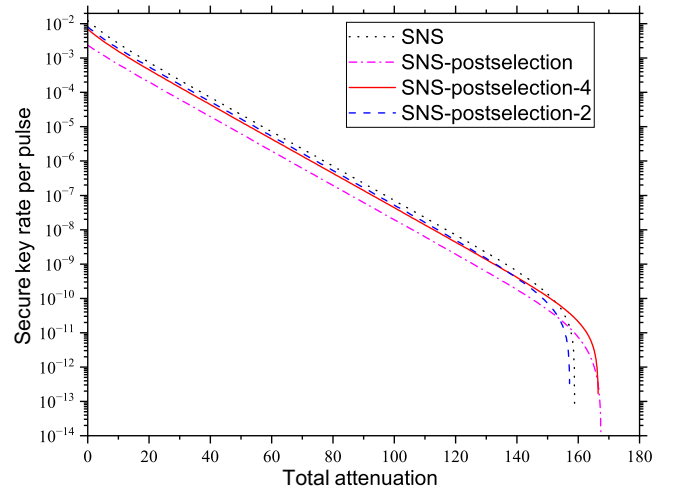


FIG. 2. The simulation result of our variants with discrete phase randomization. The line SNS-postselection-2 corresponds to the case of two random phases ( $M = 2$ ). The line SNS-postselection-4 corresponds to the case of four random phases ( $M = 4$ ).

To apply our variants in practice, we need to consider the case that Alice and Bob conduct finite rounds of the protocol. We give a simple but complete finite-key analysis for our continuous-phase-randomization case in Appendix D. In our finite-key analysis, we use only a decoy estimation of three intensities, so we estimate only the number of the phase correct events with one photon. We conduct numerical simulation to see its performance in Fig. 4. In

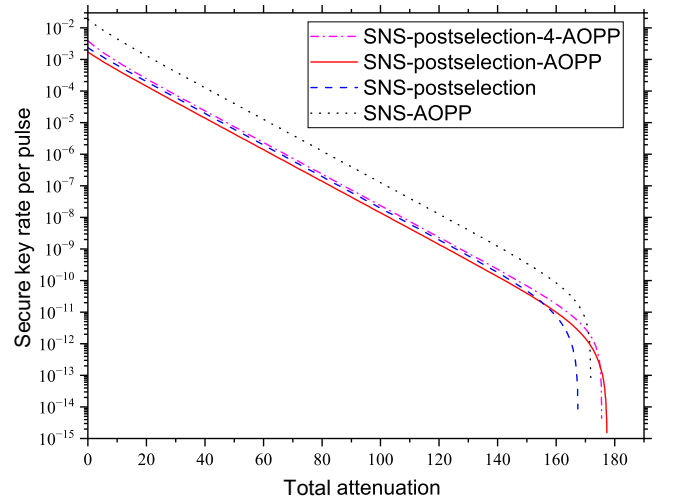


FIG. 3. The simulation result of SNS protocol and our variant with AOPP. The line SNS-AOPP corresponds to the case of the original SNS with AOPP postprocessing. The line SNS-postselection-AOPP corresponds to the case of our continuous-phase-randomization variant with AOPP. The line SNS-postselection-4-AOPP corresponds to our four-phase variant with AOPP.

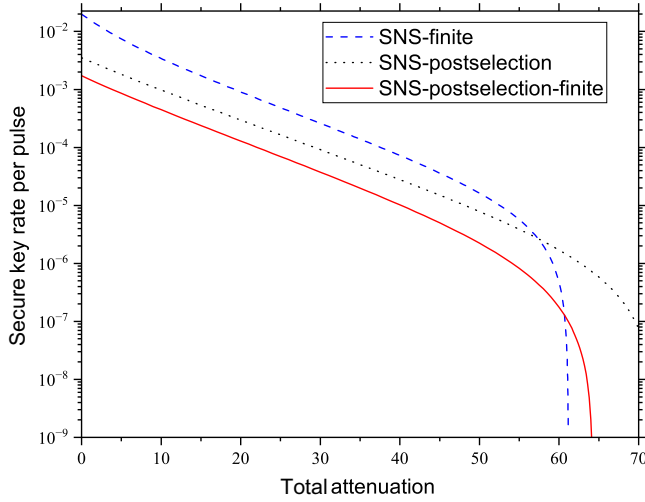


FIG. 4. The simulation result of our variant with continuous phase randomization. The line SNS-finite corresponds to the finite-key analysis of the original SNS protocol [27,38]. The line SNS-postselection corresponds to the asymptotic case of our variant. The line SNS-postselection-finite corresponds to our finite-key analysis of our variant.

the finite-key simulation, we set the dark counting rate to be  $10^{-6}$  and set  $e_{\text{mis}} = 0.02$ . The number of rounds conducted by Alice and Bob is set to  $10^{13}$  and the total security parameter is set to  $10^{-10}$ .

We can see that our variant can still have a longer distance than the original SNS protocol in the case of finite rounds. Note that the clicks of two or more photons are treated as phase errors, so the key-rate difference between the finite-key and the asymptotic cases is understandable. Thus we can also hope for a better performance if the two-photon items of the phase correct events can be estimated with a better decoy estimation, for example, a four-intensity method.

## VI. CONCLUSION

To conclude, we proposed one kind of variant of the SNS QKD by introducing phase postselection. We also analyzed the performance of our variant with discrete phase randomization and AOPP two-way postprocessing. We gave the security analysis of our variant and performed numerical simulations to compare these protocols.

Without two-way postprocessing, the continuous-phase-randomization case and the four-phase discrete-phase-randomization case of our variant can reach a much longer distance than the original SNS protocol.

With AOPP two-way postprocessing, the SNS-AOPP protocol can have a larger key rate than our variant. However, our variant still has an advantage in transmission distance.

We also give a complete finite-key analysis for our variant, a transmission distance improvement can also be

realized at the case of finite rounds. We can hope for a better performance of our variant if a more complicated decoy estimation can be applied.

The additional step of phase sifting in our variants does not increase the difficulty of experimental realization, because a similar phase announcement is needed for the decoy states in the original SNS protocol. To realize QKD at a long distance, our variant with AOPP might be a better choice than the SNS-AOPP protocol.

## 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, and No. 62301524), Prospect and Key Core Technology Projects of Jiangsu provincial key R & D Program (Grant No. BE2022071), the Fundamental Research Funds for the Central Universities, the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701), the Natural Science Foundation of Anhui (Grant No. 2308085QF216), the China Postdoctoral Science Foundation (Grant No. 2022M723064).

## APPENDIX A: FEASIBILITY OF THE DECOY-STATE ESTIMATION

The given probability of a phase error from the main text is shown as

$$P_{\text{ph}}^R = p(1-p)e^{-\mu} \left( 2P^R(|0\rangle_a |0\rangle_b) + \sum_{j=1}^{\infty} \frac{\mu^j}{j!} \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta P^R \left( \frac{e^{ij\delta} |0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right). \quad (\text{A1})$$

Similarly, the phase-error rate of left-click events is

$$P_{\text{ph}}^L = p(1-p)e^{-\mu} \left( 2P^L(|0\rangle_a |0\rangle_b) + \sum_{j=1}^{\infty} \frac{\mu^j}{j!} \times \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta P^L \left( \frac{e^{ij\delta} |0\rangle_a |j\rangle_b + (-1)^j |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right). \quad (\text{A2})$$

In practical cases, estimating the upper bounds of the phase-error rates is difficult. Luckily, we find that it is easy to estimate the lower bounds of phase-correct rates  $P_{\text{cor}}^{R/L}$  shown below. Here  $P_{\text{ph}}^{R/L}/P_c^{R/L} = 1 - P_{\text{cor}}^{R/L}/P_c^{R/L}$ .

$$P_{\text{cor}}^R = p(1-p)e^{-\mu} \left( \sum_{j=1}^{\infty} \frac{\mu^j}{j!} \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta P^R \left( \frac{e^{ij\delta} |0\rangle_a |j\rangle_b - |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right), \quad (\text{A3})$$

$$P_{\text{cor}}^L = p(1-p)e^{-\mu} \left( \sum_{j=1}^{\infty} \frac{\mu^j}{j!} \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta P^L \left( \frac{e^{ij\delta} |0\rangle_a |j\rangle_b - (-1)^j |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right). \quad (\text{A4})$$

The items with three or more photons are not needed since we need only the lower bounds and these items are too small. Thus we need only to estimate the average right-click rates of the states  $((e^{i\delta} |0\rangle_a |1\rangle_b - |1\rangle_a |0\rangle_b)/\sqrt{2})$  and  $((e^{2i\delta} |0\rangle_a |2\rangle_b - |2\rangle_a |0\rangle_b)/\sqrt{2})$  and the average left-click rates of the states  $((e^{i\delta} |0\rangle_a |1\rangle_b + |1\rangle_a |0\rangle_b)/\sqrt{2})$  and

$((e^{2i\delta} |0\rangle_a |2\rangle_b - |2\rangle_a |0\rangle_b)/\sqrt{2})$ . The decoy state method can help us to estimate these click rates.

With phase locking and phase postselection, we also keep the events that Alice and Bob send decoy states with the same intensity  $\nu$  and the phase difference is in  $[\pi - \Delta, \pi + \Delta]$ . Thus the density matrix is shown as

$$\begin{aligned} & \frac{1}{4\pi\Delta} \int_{-\Delta}^{\Delta} d\delta \int_0^{2\pi} d\theta |\sqrt{\nu}e^{i\theta}\rangle |\sqrt{\nu}e^{i(\theta+\delta)}\rangle \langle \sqrt{\nu}e^{i\theta}| \langle \sqrt{\nu}e^{i(\theta+\delta)}| = e^{-2\nu} |00\rangle \langle 00| \\ & + e^{-2\nu} 2\nu \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta \mathcal{P} \left( \frac{e^{i\delta} |01\rangle - |10\rangle}{\sqrt{2}} \right) + e^{-2\nu} \frac{(2\nu)^2}{2} \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta \mathcal{P} \left( \frac{e^{2i\delta} |02\rangle + |20\rangle - \sqrt{2}e^{i\delta} |11\rangle}{2} \right) + \dots \end{aligned} \quad (\text{A5})$$

Then the right-click rate of this state is shown as

$$e^{-2\nu} P^R(|00\rangle) + e^{-2\nu} 2\nu \left( \bar{P}^R \left( \frac{e^{i\delta} |01\rangle - |10\rangle}{\sqrt{2}} \right) \right) + e^{-2\nu} \frac{(2\nu)^2}{2} \left( \bar{P}^R \left( \frac{e^{2i\delta} |02\rangle + |20\rangle - \sqrt{2}e^{i\delta} |11\rangle}{2} \right) \right) + \dots \quad (\text{A6})$$

Here  $\bar{P}^R$  is the average right-click rate for  $\delta \in [-\Delta, \Delta]$ . The right-click rate of this state can be expressed as a linear combination of the right-click rates of states  $|00\rangle$ , the average of states  $((e^{i\delta} |01\rangle - |10\rangle)/\sqrt{2})$  and so on. Thus knowing the right-click rates of the states with different  $\nu$ , we can get the average right-click rate of states  $((e^{i\delta} |01\rangle - |10\rangle)/\sqrt{2})$  with linear programming. For the same reason, using the events that Alice and Bob have the same phases, we can get the average left-click rate of  $((e^{i\delta} |01\rangle + |10\rangle)/\sqrt{2})$ .

To estimate the click rate of the two-photon state  $((e^{2i\delta} |0\rangle_a |2\rangle_b - |2\rangle_a |0\rangle_b)/\sqrt{2})$ , we can use the relationship that

$$\begin{aligned} & \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta \left( \mathcal{P} \left( \frac{e^{2i\delta} |02\rangle - |20\rangle + \sqrt{2}ie^{i\delta} |11\rangle}{2} \right) + \mathcal{P} \left( \frac{e^{2i\delta} |02\rangle - |20\rangle - \sqrt{2}ie^{i\delta} |11\rangle}{2} \right) \right) \\ & = \mathcal{P}(|11\rangle) + \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta \mathcal{P} \left( \frac{e^{2i\delta} |02\rangle - |20\rangle}{\sqrt{2}} \right). \end{aligned} \quad (\text{A7})$$

When Alice and Bob both send decoy states with intensity  $\nu$  and their phase difference is in  $[(\pi/2) - \Delta, (\pi/2) + \Delta]$  and  $[(3\pi/2) - \Delta, (3\pi/2) + \Delta]$ , the density matrix is shown as

$$\begin{aligned} & \frac{1}{8\pi\Delta} \left( \int_{\frac{\pi}{2}-\Delta}^{\frac{\pi}{2}+\Delta} d\delta + \int_{\frac{3\pi}{2}-\Delta}^{\frac{3\pi}{2}+\Delta} d\delta \right) \int_0^{2\pi} d\theta |\sqrt{\nu}e^{i\theta}\rangle |\sqrt{\nu}e^{i(\theta+\delta)}\rangle \langle \sqrt{\nu}e^{i\theta}| \langle \sqrt{\nu}e^{i(\theta+\delta)}| \\ & = e^{-2\nu} |00\rangle \langle 00| + \frac{e^{-2\nu} 2\nu}{4\Delta} \int_{-\Delta}^{\Delta} d\delta (\mathcal{P}(|01\rangle) + \mathcal{P}(|10\rangle)) + e^{-2\nu} \frac{(2\nu)^2}{2} \frac{1}{4\Delta} \int_{-\Delta}^{\Delta} d\delta \left( \mathcal{P}(|11\rangle) + \mathcal{P} \left( \frac{e^{2i\delta} |02\rangle - |20\rangle}{\sqrt{2}} \right) \right) \\ & + \dots \end{aligned} \quad (\text{A8})$$

With linear programming, the total click rate of  $\mathcal{P}(|11\rangle) + \mathcal{P}((e^{2i\delta}|02\rangle - |20\rangle)/\sqrt{2})$  can be estimated. With the decoy states that the phases of Alice and Bob are randomized separately, Alice and Bob can estimate the click rates of states  $|11\rangle$ . Thus the click rate of  $\mathcal{P}((e^{2i\delta}|02\rangle - |20\rangle)/\sqrt{2})$  is known.

## APPENDIX B: DETAILS OF OUR SIMULATION

In this section, we will introduce the calculation of our simulation. In the simulation, it is reasonable to assume the key rates of the two detectors are the same. Thus  $R = R^R + R^L = 2R^R$ .

$P_c^R$  is the probability that a right-click  $\mathbb{C}$ -round event happens when the phases pass the sifting. It can be calculated as

$$P_c^R = 2p(1-p)(1 - e^{-\sqrt{\eta}\mu/2}(1-d)). \quad (\text{B1})$$

Here  $2p(1-p)$  is the probability of a  $\mathbb{C}$  round. Alice's coherent state  $|\alpha\rangle$  of  $|\alpha\rangle_a|0\rangle_b$  passes half of the channel with a transmittance  $\sqrt{\eta}$  and then passes a beam splitter of Charlie to reach the right detector. We do not care about the left detector here, thus the beam splitter can be treated as an attenuation with a transmittance of  $\frac{1}{2}$ .

With infinite decoy states, we directly calculate all of the items of  $P_{\text{ph}}^R$ , which are shown in Eq. (B2). For the single-photon item, with a phase difference of  $\delta$ , the probability that the photon enters the right detector becomes  $\frac{1}{2}(1 - \cos(\delta))$ . For the two-photon item of  $((e^{2i\delta}|02\rangle_{ab} - |20\rangle_{ab})/\sqrt{2})$ , we use the case of independent transmission to estimate its click rate.

$$\begin{aligned} P^R \left( \frac{e^{i\delta}|01\rangle_{ab} - |10\rangle_{ab}}{\sqrt{2}} \right) &= \sqrt{\eta} \left( 1 - (1-d) \left( \frac{1}{2}(1 - \cos(\delta))(1 - e_{\text{mis}}) + \frac{1}{2}(1 + \cos(\delta))e_{\text{mis}} \right) \right) + (1 - \sqrt{\eta})d \\ P^R \left( \frac{e^{2i\delta}|02\rangle_{ab} - |20\rangle_{ab}}{\sqrt{2}} \right) &= (1 - \sqrt{\eta}/2)^2 d + 1 - (1 - \sqrt{\eta}/2)^2 \end{aligned} \quad (\text{B2})$$

To get the  $P_t^R$ , we must use integration to get the click rate when Alice and Bob both choose to send a coherent state.  $P_t^R$  is shown in Eq. (B3), and the bit-error rate is  $e_{\text{bit}} = P_E^R/P_t^R$ .

$$\begin{aligned} P_E^R &= (1-p)^2 d + p^2 \int_{-\Delta}^{\Delta} d\delta (1 - (1-d)e^{-\sqrt{\eta}\mu(1-(1-2e_{\text{mis}})\cos(\delta))}) / (2\Delta) \\ P_t^R &= P_c^R + P_E^R \end{aligned} \quad (\text{B3})$$

With the above equations, the key rate of our continuous-phase-randomization can be calculated.

## APPENDIX C: SECURITY OF DISCRETE PHASE RANDOMIZATION

To increase the key rate by improving the sifting efficiency, we consider the case that Alice and Bob prepare only their states of two or four phases. The protocol modification has been introduced in the main body of the article in Sec. V. In the following, we give the security analysis of the cases that  $M = 2, 4$  separately.

### 1. $M = 2$

In the case of  $M = 2$ , Alice and Bob prepare only their states in two phases  $\{0, \pi\}$ . The sifting efficiency is  $1/2$ .

For right-click events, the sifting condition is  $\theta_A = \theta_B \equiv \theta$ . At the condition of a fixed common phase, the equivalent protocol and the phase-error probability is the same as the one in Sec. III with  $\delta = 0$ . The state prepared by Alice and Bob can be set to Eq. (1) with  $\delta = 0$ , and the phase error probability is  $P_{\text{ph}}^R(\theta, 0) = p(1-p)P^R(\frac{|0\rangle_a|\alpha e^{i\theta}\rangle_b + |\alpha e^{i\theta}\rangle_a|0\rangle_b}{\sqrt{2}})$ . The difference is that the average phase-error probability  $P_{\text{ph}}^{R-2}$  is for  $\theta \in \{0, \pi\}$ .

$$\begin{aligned} P_{\text{ph}}^{R-2} &= \frac{1}{2} \sum_{\theta=0,\pi} P_{\text{ph}}^R(\theta, 0) = p(1-p) \left\{ P^R \left( \sum_{j=0}^{\infty} \sqrt{\frac{e^{-\mu}\mu^{2j}}{(2j)!}} \frac{|0\rangle_a|2j\rangle_b + |2j\rangle_a|0\rangle_b}{\sqrt{2}} \right) \right. \\ &\quad \left. + P^R \left( \sum_{j=0}^{\infty} \sqrt{\frac{e^{-\mu}\mu^{2j+1}}{(2j+1)!}} \frac{|0\rangle_a|2j+1\rangle_b + |2j+1\rangle_a|0\rangle_b}{\sqrt{2}} \right) \right\}. \end{aligned} \quad (\text{C1})$$



One can verify Eq. (C1) by the summation of density matrices  $|a\rangle\langle a| + |b\rangle\langle b| = \frac{1}{2}(|a\rangle + |b\rangle)(\langle a| + \langle b|) + \frac{1}{2}(|a\rangle - |b\rangle)(\langle a| - \langle b|)$ .

The estimation of Eq. (C1) is still hard, because we know only the click rate of the states  $|0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b$  with decoy states. We can use the Cauchy-Schwarz inequality shown in Eq. (C2) to estimate the upper bound of the phase-error probability in Eq. (C3).

$$\begin{aligned} \text{Tr} \left( M^R \left( \sum_j |a_j\rangle \right) \left( \sum_j \langle a_j| \right) \right) &= \sum_j \text{Tr}(M^R |a_j\rangle\langle a_j|) + \sum_{j \neq k} \text{Tr}(M^R |a_j\rangle\langle a_k|) \\ &\leq \sum_j \text{Tr}(M^R |a_j\rangle\langle a_j|) + \sum_{j \neq k} \sqrt{\text{Tr}(M^R |a_j\rangle\langle a_j|) \text{Tr}(M^R |a_k\rangle\langle a_k|)} \end{aligned} \quad (\text{C2})$$

$$\begin{aligned} P_{\text{ph}}^{R-2} &\leq p(1-p) \left\{ \sum_{j=0}^{\infty} \frac{e^{-\mu} \mu^j}{j!} P^R \left( \frac{|0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right. \\ &+ \sum_{j \neq k} e^{-\mu} \sqrt{\frac{\mu^{2j+2k}}{2j!2k!}} \sqrt{P^R \left( \frac{|0\rangle_a |2j\rangle_b + |2j\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \sqrt{P^R \left( \frac{|0\rangle_a |2k\rangle_b + |2k\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \\ &\left. + \sum_{j \neq k} e^{-\mu} \sqrt{\frac{\mu^{2j+2k+2}}{(2j+1)!(2k+1)!}} \sqrt{P^R \left( \frac{|0\rangle_a |2j+1\rangle_b + |2j+1\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \sqrt{P^R \left( \frac{|0\rangle_a |2k+1\rangle_b + |2k+1\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \right\}. \end{aligned} \quad (\text{C3})$$

Comparing with Eq. (3), the first line of Eq. (C3) is the same when  $\delta = 0$ , but some cross terms are added. With a larger phase error, the transmission distance will be decreased.

The security key rate of this case is shown as

$$R^R = \frac{1}{2} (P_c^R \left( 1 - H_2 \left( \frac{P_{\text{ph}}^{R-2}}{P_c^R} \right) \right) - f P_{t-2}^R H_2(e_{\text{bit-2}})). \quad (\text{C4})$$

Here  $P_c^R$  is the same as the one in Eq. (5), because the click rates of  $|\alpha\rangle_a |0\rangle_b$  and  $|0\rangle_a |\alpha\rangle_b$  are not influenced by the phase.  $P_{t-2}^R$  is the right-click rate of sifted rounds and  $e_{\text{bit-2}}$  is the bit-error rate of the  $M = 2$  case.

## 2. $M = 4$

With a same method, we can give the phase error probability of  $M = 4$  case, which is shown in Eq. (C5).

$$\begin{aligned} P_{\text{ph}}^{R-4} &\leq p(1-p) \left\{ \sum_{j=0}^{\infty} \frac{e^{-\mu} \mu^j}{j!} P^R \left( \frac{|0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} \right) \right. \\ &+ \sum_{j \neq k} e^{-\mu} \sqrt{\frac{\mu^{4j+4k}}{4j!4k!}} \sqrt{P^R \left( \frac{|0\rangle_a |4j\rangle_b + |4j\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \sqrt{P^R \left( \frac{|0\rangle_a |4k\rangle_b + |4k\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \\ &\left. + \sum_{j \neq k} e^{-\mu} \sqrt{\frac{\mu^{4j+4k+2}}{(4j+1)!(4k+1)!}} \sqrt{P^R \left( \frac{|0\rangle_a |4j+1\rangle_b + |4j+1\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \sqrt{P^R \left( \frac{|0\rangle_a |4k+1\rangle_b + |4k+1\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \right\} \end{aligned}$$

$$\begin{aligned}
 & + \sum_{j \neq k} e^{-\mu} \sqrt{\frac{\mu^{4j+4k+4}}{(4j+2)!(4k+2)!}} \sqrt{P^R \left( \frac{|0\rangle_a |4j+2\rangle_b + |4j+2\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \sqrt{P^R \left( \frac{|0\rangle_a |4k+2\rangle_b + |4k+2\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \\
 & + \left. \sum_{j \neq k} e^{-\mu} \sqrt{\frac{\mu^{4j+4k+6}}{(4j+3)!(4k+3)!}} \sqrt{P^R \left( \frac{|0\rangle_a |4j+3\rangle_b + |4j+3\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \sqrt{P^R \left( \frac{|0\rangle_a |4k+3\rangle_b + |4k+3\rangle_a |0\rangle_b}{\sqrt{2}} \right)} \right\}. \quad (C5)
 \end{aligned}$$

In this case, the phase error is close to the case of continuous phase randomization when  $\delta = 0$ , because the phase errors mainly come from the items of 0, 1, and 2 photons and the cross terms of more than four photons have little influence.

The key rate of this case is shown as

$$R^R = \frac{1}{4} \left( P_c^R \left( 1 - H_2 \left( \frac{P_{\text{ph}}^{R-4}}{P_c^R} \right) \right) - f P_{t-4}^R H_2(e_{\text{bit-4}}) \right). \quad (C6)$$

$P_{t-4}^R$  is the right-click rate of sifted rounds and  $e_{\text{bit-4}}$  is the bit-error rate.

## APPENDIX D: A SIMPLE FINITE-KEY ANALYSIS

### 1. The finite-key analysis

Because the phase-error estimation of our variant seems more complicated than the one in the original SNS protocol, its practical performance under finite rounds seems to be a valuable topic. Here we give a simple but complete finite-key analysis for our variant of continuous phase randomization.

Though we require that Alice and Bob broadcast their phases of every round in the phase postselection step, we can still estimate the number of phase errors (phase correct events) by treating the states sent by Alice and Bob as mixed states with a random common phase. This is because any eavesdropper cannot change the number of phase errors after the announcement of measuring results. The phase postselection is after the announcement of all measuring results, so this step does not influence the number of phase errors. Note that this corollary has been used in the analysis of the phase-matching TF QKD [9].

We will analyze a case of three intensities  $\mu$ ,  $\nu$ , and 0. In every round, Alice and Bob independently choose to produce a signal state with a probability  $q$  or produce a decoy state with a probability  $(1 - q)$ . If she (he) decides to produce a signal state, she (he) has a probability  $p$  to produce a phase-randomized state  $|\sqrt{\mu}e^{i\theta_A}\rangle$  ( $|\sqrt{\mu}e^{i\theta_B}\rangle$ ) and saves the phase  $\theta_A$  ( $\theta_B$ ) locally, or she (he) produces a vacuum state  $|0\rangle$  and saves a random phase. If she (he) chooses to produce a decoy state, she (he) produces a phase-randomized state  $|\sqrt{\nu}e^{i\theta_A}\rangle$  ( $|\sqrt{\nu}e^{i\theta_B}\rangle$ ) and saves the phase locally.

In the rounds that both Alice and Bob choose to send a signal state and only one of them decides to send a vacuum state (the  $\mathbb{C}$  rounds), the state can be treated as the following form after the phase postselection of a same common phase.

$$\begin{aligned}
 & q^2 p (1 - p) \frac{1}{4\pi\Delta} \int_{-\Delta}^{\Delta} d\delta \int_0^{2\pi} d\theta \mathcal{P} (|00\rangle_{AB} |0\rangle_a |\sqrt{\mu}e^{i(\theta+\delta)}\rangle_b + |11\rangle_{AB} |\sqrt{\mu}e^{i\theta}\rangle_a |0\rangle_b) \\
 & = q^2 p (1 - p) \sum_{j=0}^{\infty} \frac{e^{-\mu} \mu^j}{j!} \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta \mathcal{P} (e^{ij\delta} |00\rangle_{AB} |0\rangle_a |j\rangle_b + |11\rangle_{AB} |j\rangle_a |0\rangle_b) \\
 & = q^2 p (1 - p) \sum_{j=0}^{\infty} \frac{e^{-\mu} \mu^j}{j!} \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} d\delta \\
 & \quad \mathcal{P} \left( \frac{|++\rangle_{AB} + |--\rangle_{AB}}{\sqrt{2}} \frac{e^{ij\delta} |0\rangle_a |j\rangle_b + |j\rangle_a |0\rangle_b}{\sqrt{2}} + \frac{|+-\rangle_{AB} + -+\rangle_{AB}}{\sqrt{2}} \frac{e^{ij\delta} |0\rangle_a |j\rangle_b - |j\rangle_a |0\rangle_b}{\sqrt{2}} \right). \quad (D1)
 \end{aligned}$$

In Eq. (D1), the state can be treated as a mixed state of different photons. For the one-photon item Alice and Bob send a mixed state of  $((e^{i\delta} |0\rangle_a |1\rangle_b + |1\rangle_a |0\rangle_b)/\sqrt{2})$  and  $((e^{i\delta} |0\rangle_a |1\rangle_b - |1\rangle_a |0\rangle_b)/\sqrt{2})$  from the perspective of any eavesdropper. The aim of us is to estimate the number of right clicks caused by  $((e^{i\delta} |0\rangle_a |1\rangle_b - |1\rangle_a |0\rangle_b)/\sqrt{2})$ , which corresponds to phase correct events.

Here we estimate only the phase correct events of one-photon states as the lower bound of the total phase correct events. This analysis is not tight but enough to show the advantage of our variant under finite rounds.

Because Alice and Bob only keep the rounds that passed the phase postselection, the encoding information of other rounds can be broadcast. Then they can count the number of right (left) clicks when they send intensity  $\mu$  with a phase difference in  $[\pi - \Delta, \pi + \Delta]$  ( $[-\Delta, \Delta]$ ), which is denoted as  $n_{\mu-}^R$  ( $n_{\mu+}^L$ ). For the case they both select the intensity  $\nu$ , they can also count the corresponding click numbers  $n_{\nu-}^R$  and  $n_{\nu+}^L$ . The last quantity we need to know is the count when both Alice and Bob send vacuum states. We can also use the rounds that have not passed the phase postselection when both Alice and Bob send vacuum states. The right (left) click number of these vacuum-vacuum rounds is denoted as  $n_0^R$  ( $n_0^L$ ).

The states of the  $\nu$ - $\nu$  and  $\mu$ - $\mu$  cases with opposite phases have been shown in Eq. (A5). With the three-intensity decoy-state method [32–34,39], we can estimate the number of right clicks of the state  $((e^{i\delta}|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)/\sqrt{2})$  from the sifted rounds, which is shown in the following. With the same method, the phase correct events of left clicks can also be estimated.

$$\begin{aligned} n_{\text{cor}_1}^R &= \underline{\text{cher}} \left( q^2 p (1-p) \frac{\Delta}{\pi} e^{-\mu} \mu \frac{1}{2\mu\nu(\mu-\nu)} \left( \mu^2 \frac{\underline{\text{Cher}}(n_{\nu-}^R)}{(1-q)^2 \frac{\Delta}{\pi} e^{-2\nu}} - \nu^2 \frac{\overline{\text{Cher}}(n_{\mu-}^R)}{q^2 p^2 \frac{\Delta}{\pi} e^{-2\mu}} - (\mu^2 - \nu^2) \frac{\overline{\text{Cher}}(n_0^R)}{q^2 (1-p)^2 \left(1 - \frac{2\Delta}{\pi}\right)} \right) \right) \\ n_{\text{cor}_1}^L &= \underline{\text{cher}} \left( q^2 p (1-p) \frac{\Delta}{\pi} e^{-\mu} \mu \frac{1}{2\mu\nu(\mu-\nu)} \left( \mu^2 \frac{\underline{\text{Cher}}(n_{\nu+}^L)}{(1-q)^2 \frac{\Delta}{\pi} e^{-2\nu}} - \nu^2 \frac{\overline{\text{Cher}}(n_{\mu+}^L)}{q^2 p^2 \frac{\Delta}{\pi} e^{-2\mu}} - (\mu^2 - \nu^2) \frac{\overline{\text{Cher}}(n_0^L)}{q^2 (1-p)^2 \left(1 - \frac{2\Delta}{\pi}\right)} \right) \right). \end{aligned} \quad (\text{D2})$$

Here  $\underline{\text{cher}}$ ,  $\underline{\text{Cher}}$  and  $\overline{\text{Cher}}$  are some upper bound and lower bounds estimated by Chernoff bound, which will be given in Appendix D2.

In the frame of composable security, the final key of length  $l$  is  $\epsilon_{\text{tot}}$  security if  $\epsilon_{\text{tot}} = 2\epsilon + \frac{1}{2}\sqrt{2^{l-H_{\min}^{\epsilon}(\mathbf{Z}|E')}}}$  [40]. Here  $H_{\min}^{\epsilon}$  is the  $\epsilon$ -smooth min entropy.  $\mathbf{Z}$  denotes the sifted bits of Alice.  $E'$  is the system of an eavesdropper. Defining  $l = H_{\min}^{\epsilon}(\mathbf{Z}|E') - 2\log_2(1/(2\bar{\epsilon}))$ , we have  $\epsilon_{\text{tot}} = 2\epsilon + \bar{\epsilon}$ .

Considering the information leakage and the failure probability of the error correction, the key length becomes  $l = H_{\min}^{\epsilon}(\mathbf{Z}|E) - f n_t H_2(e_{\text{bit}}) - 2\log_2(1/(2\bar{\epsilon})) - \log_2(2/(\epsilon_{\text{cor}}))$  with  $\epsilon_{\text{tot}} = 2\epsilon + \bar{\epsilon} + \epsilon_{\text{cor}}$ . Here  $n_t$  is the total number of sifted bits.

Note that our sifted bits  $\mathbf{Z}$  are separated into two parts in our analysis. We denote the correct rounds as  $\mathbf{Z}_c$  and the erroneous rounds as  $\mathbf{Z}_e$ . Using the chain rules of smooth entropy [41], we have

$$\begin{aligned} H_{\min}^{\epsilon}(\mathbf{Z}_c \mathbf{Z}_e | E) &\geq H_{\min}^{\epsilon_1}(\mathbf{Z}_e | \mathbf{Z}_c E) + H_{\min}^{\epsilon_2}(\mathbf{Z}_c | E) - \log_2 \frac{2}{\epsilon'^2} \\ &\geq H_{\min}^{\epsilon_2}(\mathbf{Z}_c | E) - \log_2 \frac{2}{\epsilon'^2} \end{aligned} \quad (\text{D3})$$

Here we have  $\epsilon = \epsilon_2 + \epsilon'$  by setting  $\epsilon_1 = 0$ .

Using the uncertainty relation [40,42], the min entropy can be get by

$$\begin{aligned} H_{\min}^{\epsilon_2}(\mathbf{Z}_c | E) &\geq n_c - n_c H_2 \left( 1 - \frac{n_{\text{cor}}}{n_c} \right) \\ &\geq n_c - n_c H_2 \left( 1 - \frac{n_{\text{cor}_1}^R + n_{\text{cor}_1}^L}{n_c} \right). \end{aligned} \quad (\text{D4})$$

$n_c$  is the number of correct sifted bits. Here, the failure probability of the phase-correct-event estimation should be less than  $\epsilon_2^2$ . The failure probability of every Chernoff bound in Eq. (D2) is  $\epsilon_2^2/8 \equiv \epsilon_x$  if it is divided equally.

Finally, the key length is shown as

$$l = n_c - n_c H_2 \left( 1 - \frac{n_{\text{cor}_1}^R + n_{\text{cor}_1}^L}{n_c} \right) - f n_t H_2(e_{\text{bit}}) - \log_2 \frac{2}{\epsilon'^2} - 2 \log_2 \frac{1}{2\bar{\epsilon}} - \log_2 \frac{2}{\epsilon_{\text{cor}}}, \quad (\text{D5})$$

$$\epsilon_{\text{tot}} = 2(\epsilon' + \sqrt{8\epsilon_x}) + \bar{\epsilon} + \epsilon_{\text{cor}}. \quad (\text{D6})$$

## 2. Chernoff bound

The Chernoff bound [43,44] is widely used in the analysis of QKD protocol. In the following, we give the content of it.

**Multiplicative Chernoff bound.** Suppose  $X_1, X_2, \dots, X_n$  are independent Bernoulli random variables and let  $X = \sum_{i=1}^n X_i$ .  $E$  is the expectation value of  $X$ . Then we have

$$\Pr(X \geq (1 + \xi_1)E) \leq e^{-\xi_1^2 E / (2 + \xi_1)} \quad (D7)$$

for  $\xi_1 \geq 0$ , and

$$\Pr(X \leq (1 - \xi_2)E) \leq e^{-\xi_2^2 E / 2} \quad (D8)$$

for  $0 < \xi_2 < 1$ .

By solving  $e^{-\xi_1^2 E / (2 + \xi_1)} = e^{-\xi_2^2 E / 2} = \epsilon_x$ , we can get the upper and lower bounds of  $X$  shown as

$$\begin{aligned} X \leq \overline{\text{cher}}(E) &= E + \frac{1}{2} \ln \frac{1}{\epsilon_x} + \frac{1}{2} \sqrt{\ln^2 \frac{1}{\epsilon_x} + 8E \ln \frac{1}{\epsilon_x}}, \\ X \geq \underline{\text{cher}}(E) &= E - \sqrt{2E \ln \frac{1}{\epsilon_x}}, \end{aligned} \quad (D9)$$

with failure probability  $\epsilon_x$  separately.

When  $X$  is known but  $E$  is unknown, we can also estimate the bound of  $E$  by solving  $E$  from Eq. (D9) in the following with a failure probability  $\epsilon_x$  separately.

$$\begin{aligned} E \leq \overline{\text{Cher}}(X) &= X + \ln \frac{1}{\epsilon_x} + \sqrt{\ln^2 \frac{1}{\epsilon_x} + 2X \ln \frac{1}{\epsilon_x}}, \\ E \geq \underline{\text{Cher}}(X) &= X + \frac{1}{2} \ln \frac{1}{\epsilon_x} - \frac{1}{2} \sqrt{\ln^2 \frac{1}{\epsilon_x} + 8X \ln \frac{1}{\epsilon_x}}. \end{aligned} \quad (D10)$$

[1] C. H. Bennett and G. Brassard, in *International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984), pp. 175–179.  
 [2] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).  
 [3] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett* **85**, 441 (2000).  
 [4] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, 802 (1982).  
 [5] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and reverse secret-key capacities of a quantum channel, *Phys. Rev. Lett.* **102**, 050503 (2009).

[6] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).  
 [7] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 5235 (2014).  
 [8] 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).  
 [9] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, *Phys. Rev. X* **8**, 031043 (2018).  
 [10] 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).  
 [11] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, *Phys. Rev. A* **98**, 042332 (2018).  
 [12] 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).  
 [13] 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).  
 [14] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, *Nat. Photonics* **13**, 334 (2019).  
 [15] 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).  
 [16] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin *et al.*, Experimental twin-field quantum key distribution through sending or not sending, *Phys. Rev. Lett.* **123**, 100505 (2019).  
 [17] 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).  
 [18] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, *Nat. Photonics* **14**, 422 (2020).  
 [19] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin *et al.*, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km, *Phys. Rev. Lett.* **124**, 070501 (2020).  
 [20] X. Zhong, W. Wang, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses, *npj Quantum Inf.* **7**, 8 (2021).  
 [21] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, *Nat. Photonics* **15**, 530 (2021).  
 [22] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields *et al.*, Coherent phase transfer for real-world twin-field quantum key distribution, *Nat. Commun.* **13**, 157 (2022).

- [23] H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen *et al.*, Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km, *Phys. Rev. Lett.* **126**, 250502 (2021).
- [24] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu *et al.*, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, *Nat. Photonics* **15**, 570 (2021).
- [25] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen *et al.*, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [26] 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 *et al.*, Experimental twin-field quantum key distribution over 1000 km fiber distance, *Phys. Rev. Lett.* **130**, 210801 (2023).
- [27] 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).
- [28] G.-J. Fan-Yuan, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, Z.-F. Han, and G.-C. Guo, Modeling alignment error in quantum key distribution based on a weak coherent source, *Phys. Rev. Appl.* **12**, 064044 (2019).
- [29] 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).
- [30] 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).
- [31] 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).
- [32] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [33] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [34] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [35] M. Hayashi, General theory for decoy-state quantum key distribution with an arbitrary number of intensities, *New J. Phys.* **9**, 284 (2007).
- [36] M. Hayashi, Upper bounds of eavesdropper's performances in finite-length code with the decoy method, *Phys. Rev. A* **76**, 012329 (2007).
- [37] M. Hayashi, Optimal decoy intensity for decoy quantum key distribution, *J. Phys. A: Math. Theor.* **49**, 165301 (2016).
- [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] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* **72**, 012326 (2005).
- [40] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, *Nat. Commun.* **3**, 634 (2012).
- [41] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, Chain rules for smooth min-and max-entropies, *IEEE Trans. Inf. Theory* **59**, 2603 (2013).
- [42] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, *Phys. Rev. Lett.* **106**, 110506 (2011).
- [43] H. Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Ann. Math. Stat.* **23**, 493 (1952).
- [44] M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis* (Cambridge University Press, Cambridge, 2017).