Unconditional Security of Sending or Not Sending Twin-Field Quantum Key Distribution with Finite Pulses

Cong Jiang,[1,2] Zong-Wen Yu,[1,3] Xiao-Long Hu,[1,2] and Xiang-Bin Wang[1,2,4,5,*,†]

[1] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China*

[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3] *Data Communication Science and Technology Research Institute, Beijing, 100191 China*

[4] *Jinan Institute of Quantum Technology, SAICT, Jinan 250101, China*

[5] *Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China*

(Received 17 April 2019; revised manuscript received 12 June 2019; published 29 August 2019)

The sending-or-not-sending protocol of the twin-field quantum key distribution (TFQKD) has its advantage of unconditional security under any coherent attack and fault tolerance to a large misalignment error. Here, we consider the complete finite-key effects for the protocol and we calculate the secure key rate with a fixed security coefficient. The numerical simulation shows that the protocol with a typical finite number of pulses in practice can produce an unconditional secure final key under general attack, including all coherent attacks. It can exceed the secure distance of 500 km in a typical finite number of pulses in practice even with a large misalignment error.

DOI: 10.1103/PhysRevApplied.12.024061

I. INTRODUCTION

Quantum key distribution (QKD) could provide unconditionally secure communication [1–8] between two parties, Alice and Bob. But security in an ideal case [5–8] does not guarantee security in practice [9–17]. Fortunately, the decoy-state method [18–21] could help us beat the photon-number-splitting (PNS) attack [9–13] and guarantee security with imperfect light sources. The decoy-state method has been widely studied in theory [22–30] and applied in experiments [31–40] such as the Micius satellite [34] and quantum networks [35–37]. Besides the decoy-state mehtod, there are other protocols such as the round-robin differential-phase-shift (RRDPS) protocol [41,42] proposed to beat the PNS attack. Measurement-device-independent QKD (MDIQKD) [43,44] can solve all possible loopholes of detection. The decoy-state MDIQKD [45–58] protocol could help us ensure the security of a protocol performed by imperfect light sources and detectors.

The 4-intensity protocol [57], together with the joint constraints [56], has greatly improved the key rate and distance of the MDIQKD. Using this protocol, a distance exceeding 400 km has been experimentally demonstrated [52] for the MDIQKD. However, the key rate of all the prior art decoy-state protocols and the MDIQKD protocols cannot be better than the linear scale of the channel transmittance. It cannot exceed the known bound of the repeaterless QKD, such as the PLOB (Pirandola, Laurenza, Ottaviani, and Banchi) bound [59] or the TGW (Takeoka, Guha, and Wilde) bound [60]. Recently, a QKD protocol named twin-field QKD (TFQKD) was proposed [61] whose key rate $R \sim O(\sqrt{\eta})$, where η is the channel transmittance, and has attracted much attention. But the later announcement of the phase information in Ref. [61] will cause security loopholes [62,63], and many variants of TFQKD have been proposed [63–70] to close the loophole. A series of experiments [71–74] have been done to demonstrate those protocols. In particular, an efficient protocol for TFQKD through the sending-or-not-sending (SNS) protocol has been given in Ref. [63]. The SNS protocol has been demonstrated in a proof-of-principle experiment in Ref. [71] and realized in real optical fiber with the effects of statistical fluctuation being taken into account [72]. The unconditional security of the SNS protocol in the asymptotic case has been proved [63] and the SNS protocol relaxes the requirement for single-photon interference accuracy. The key rate of SNS is still considerable even if the misalignment error is as large as 35%. The SNS QKD protocol with the effect of statistical fluctuation and finite decoy states has been studied in Ref. [68]. Here, we show

*xbwang@mail.tsinghua.edu.cn

†Also at Center for Atomic and Molecular Nanosciences, Tsinghua University, Beijing 100084, China.

an analysis of the complete effect of the finite-key size of the SNS QKD protocol.

The main tool we use to analyze the effect of the finite-key size is the universally composable framework [75]. A complete QKD protocol usually includes the preparation and distribution of quantum states, measurement of received quantum states, parameter estimation, error correction, and private amplification. After the error correction step, Alice gets a bit string S and Bob gets an estimate string S' of S. If the error rate is too large, the results of error correction are an empty string and the protocol aborts. A protocol is called $\varepsilon_{\rm cor}$-correct if the probability that S and S' are not the same is $\Pr(S \neq S') \leq \varepsilon_{\rm cor}$.

Also, the quantum state of Alice may be attacked by Eve in the distribution and measurement steps and some information would be leaked to Eve. To ensure the security of final secret keys, Alice and Bob apply a privacy amplification scheme based on two-universal hashing [76] to extract two shorter strings of length l from S and S'. We denote the density operator of the system of Alice and Eve as $\rho_{\rm AE}$. If

$$\min_{\rho_E} \frac{1}{2} \parallel \rho_{\rm AE} - U_A \otimes \rho_E \parallel \leq \varepsilon_{\rm sec}, \tag{1}$$

where U_A denotes the fully mixed state of Alice's system of strings of length l and ρ_E is the density operator of Eve's system, then the protocol is called $\varepsilon_{\rm sec}$-secret [54,77,78]. According to the composable framework, a protocol is called ε secure if it is both $\varepsilon_{\rm cor}$-correct and $\varepsilon_{\rm sec}$-secret, and $\varepsilon_{\rm cor} + \varepsilon_{\rm sec} \leq \varepsilon$.

This paper is arranged as follows. In Sec. II, we introduce the main results of the effect of the finite-key size. In Sec. III, we present our numerical simulation results. The article ends with some concluding remarks. The details of the calculation are shown in the appendix.

II. THE EFFECT OF FINITE-KEY SIZE OF SNS PROTOCOL

As shown in Ref. [63], there are two windows in the SNS protocol, the $\widetilde{X}$ windows and the Z windows. In a Z window, Alice (Bob) randomly decides to send a phase-radomized coherent state $|\sqrt{\mu_z}e^{i\theta_A}\rangle$ ($|\sqrt{\mu_z}e^{i\theta_B}\rangle$), with a probability p, or sends nothing (a vacuum state $|0\rangle$). In an $\widetilde{X}$ window (note that the $\widetilde{X}$ window defined here is slightly different from the definition of the X window in Ref. [63], so we use a different symbol), Alice and Bob randomly send out a phase-randomized coherent state.

The $\widetilde{X}$ windows are decoy windows and are used to estimate the counting rate s_1 and phase-flip error rate $e_1^{\rm ph}$ of the single-photon state $|01\rangle$ or $|10\rangle$ that Alice decides to send and Bob decides not to send or Alice decides not to send and Bob decides to send in the Z windows. The asymptotic case is considered in Ref. [63], and there are infinite intensities in the $\widetilde{X}$ windows and infinite pulses in the whole protocol; thus, s_1 and $e_1^{\rm ph}$ can be estimated exactly.

Alice and Bob send their prepared pulses to Charlie. Charlie is assumed to perform interferometric measurements on the received pulses and announces the measurement result to Alice and Bob. If one and only one detector clicks in the measurement process, Charlie also announces whether the left detector or right detector clicks. The effective events of Z windows and $\widetilde{X}$ windows are defined individually: it is an effective event of Z windows if one and only one detector clicks; it is an effective event of $\widetilde{X}$ windows if one and only one detector clicks and Alice and Bob send the coherent state with the same intensity, and their phases satisfy the postselection criterion, which is

$$1 - |\cos(\theta_A - \theta_B - \psi_{\rm AB})| \leq |\lambda|, \tag{2}$$

where θ_A and θ_B are the phases of coherent states prepared by Alice and Bob respectively, and $\psi_{\rm AB}$ can take an arbitrary value that can be different from time to time as Alice and Bob like, so as to obtain a satisfactory key rate for the protocol [72]. Note that $1 - |\cos[\theta_A - \theta_B - (\gamma_A - \gamma_B)]| \leq |\lambda|$ according to the security proof of Ref. [63] in the postselection criterion there [63]; both γ_A and γ_B can take arbitrary values there [63]. However, in applying the criterion, we only need the value $\gamma_A - \gamma_B$, which is actually only *one* value. Thus we could just use $\psi_{\rm AB}$ in Eq. (2) here. The value of λ is decided by the size of the phase slice, Δ, that Alice and Bob choose [61]. The Eq. (2) is equivalent to

$$|\theta_A - \theta_B - \psi_{\rm AB}| \leq \frac{\Delta}{2}, \quad |\theta_A - \theta_B - \psi_{\rm AB} - \pi| \leq \frac{\Delta}{2}. \tag{3}$$

Just as in Ref. [68], here $|x|$ means the degree of the minor angle enclosed by the two rays that enclose the rotational angle of degree x, e.g., $|-15\pi/8| = |15\pi/8| = \pi/8$, $|-\pi/10| = \pi/10$.

The phases of coherent states in Z windows are never announced in the public channel; thus, the coherent states in Z windows are phase-randomized coherent states that are equivalent to a classical mixture of different photon numbers. Only the effective events of single-photon states in those Z windows that Alice decides to send and Bob decides not to send or Alice decides not to send and Bob decides to send are untagged events; thus, we have the following formula of the final key rate:

$$R = 2p(1-p)\mu_z e^{-\mu_z} s_1[1 - h(e_1^{\rm ph})] - fS_z h(E_z), \tag{4}$$

where S_z is the counting rate of pulses in Z windows and E_z is the corresponding error rate, $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, f is the error correction inefficiency, and s_1 and $e_1^{\rm ph}$ are defined in the beginning of this section.

However, the number of pulses is finite in practice and thus there cannot be infinite intensities in $\widetilde{X}$ windows.

Here, we consider the four-intensity decoy state SNS protocol [68]. In each time, Alice and Bob randomly choose the decoy window or signal window with probabilities $1-p_z$ and p_z. If the decoy window is chosen, Alice (Bob) randomly chooses vacuum state $|0\rangle$, $|e^{i\delta_A}\sqrt{\mu_1}\rangle$, or $|e^{i\delta'_A}\sqrt{\mu_2}\rangle$ (vacuum state $|0\rangle$, $|e^{i\delta_B}\sqrt{\mu_1}\rangle$, or $|e^{i\delta'_B}\sqrt{\mu_2}\rangle$) with probabilities p_0, p_1, and $1-p_0-p_1$ respectively, where δ is random in $[0, 2\pi)$. If the signal window is chosen, Alice (Bob) randomly chooses vacuum state $|0\rangle$ or phase-randomized weak coherent state of intensity μ_z, with probabilities p_{z0} and $1-p_{z0}$. Then, Alice and Bob prepare the chosen states and send them to Charlie. Charlie is assumed to perform interferometric measurements on the received quantum signals and announces the measurement result to Alice and Bob. If one and only one detector clicks in the measurement process, Charlie also announces whether the left detector or right detector clicks. Then Alice and Bob take it as a one-detector heralded event. After Alice and Bob repeat the above steps N times, they perform the following data postprocessing steps.

1. **Sifting.** If both Alice and Bob choose the signal window, it is a Z window. If both Alice and Bob choose the decoy window, it is an $\widetilde{X}$ window. Also, we define when both Alice and Bob decide to send the phase-randomized coherent state with intensity μ_1 as the X_1 window, which is a subset of $\widetilde{X}$ windows. According to the criterion introduced in the beginning of this section, Alice and Bob decide whether a one-detector heralded event is an effective event. We define three kinds of sets, $\mathcal{Z}$, $\mathcal{X}_1$, and $\mathcal{X}_2$. The set $\mathcal{Z}$ includes all effective events in Z windows. The set $\mathcal{X}_1$ includes all effective events in X_1 windows. The set $\mathcal{X}_2$ includes all other one-detector heralded events.

2. **Parameter estimation.** For the events in the set $\mathcal{Z}$, Alice denotes it as bit 0 if she sends a vacuum state and as bit 1 if she sends a phased-randomized weak coherent state. At the same time, Bob denotes it as bit 1 if he sends a vacuum state and as bit 0 if he sends a phased-randomized weak coherent state. Finally, Alice and Bob form the n_t-bit strings Z_s and Z'_s according to the events in set $\mathcal{Z}$. Then through the decoy-state method, Alice and Bob estimate n_1 according to the events in $\mathcal{X}_2$ and estimate e_1^{ph} according the events in set $\mathcal{X}_1$, where n_1 is the lower bound of bits caused by untagged events in Z_s or Z'_s and e_1^{ph} is the upper bound of the phase-flip error rate of the untagged bits. The details of how to calculate n_1 and e_1^{ph} are shown in Appendix B.

3. **Error correction.** Alice and Bob perform an information reconciliation scheme to correct Z'_s, and Bob obtains an estimate $\hat{Z}_s$ of Z_s from Z'_s. To achieve this goal, Alice sends Bob $\mathrm{leak}_{\mathrm{EC}}$ bits of error correction data. Then Alice computes a hash of Z_s of length $\log_2(1/\varepsilon_{\mathrm{cor}})$ using a random universal hash function, and she sends the hash and hash function to Bob [76]. If the hash that Bob computes is the same as that of Alice, the probability that Z_s and $\hat{Z}_s$ are not the same, $\Pr(Z_s \neq \hat{Z}_s)$, is less than $\varepsilon_{\mathrm{cor}}$. If the hash that Bob computes is not the same as that of Alice, the protocol aborts.

4. **Private amplification.** Alice and Bob apply a privacy amplification scheme based on two-universal hashing [76] to extract two shorter strings of length l from Z_s and $\hat{Z}_s$. Alice and Bob obtain strings Z_{PA} and $\hat{Z}_{\mathrm{PA}}$, which are the final secret keys.

The protocol is $\varepsilon_{\mathrm{cor}}$-correct if the error correction step is passed. If the final length of secret keys, l, satisfies

$$l = n_1[1-h(e_1^{\mathrm{ph}})] - \mathrm{leak}_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{1}{\sqrt{2}\varepsilon_{\mathrm{PA}}\hat{\varepsilon}}, \tag{5}$$

the protocol is $\varepsilon_{\mathrm{sec}}$-secret. According to the composable framework, the security coefficient of the whole protocol is $\varepsilon_{\mathrm{tol}} = \varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}}$, where $\varepsilon_{\mathrm{sec}} = 2\hat{\varepsilon} + 4\bar{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{n_1}$. Here, $\varepsilon_{\mathrm{cor}}$ is the failure probability of error correction; $\bar{\varepsilon}$ is the failure probability for the estimation of the phase-flip error rate of those untagged bits in the Z basis, i.e., the probability that the real value of the phase-flip error rate of untagged bits is larger than e_1^{ph}; $\varepsilon_{\mathrm{PA}}$ is the failure probability of privacy amplification; and ε_{n_1} is the failure probability for the estimation of the lower bound of untagged bits in the Z basis, i.e., the probability that the real value of the number of untagged bits is smaller than n_1. The value of $\mathrm{leak}_{\mathrm{EC}}$ is related to the specific error correction schemes and, in general, $\mathrm{leak}_{\mathrm{EC}} = fn_t h(E_z)$, where E_z is the error rate of strings Z_s and Z'_s and f is the error correction inefficiency. The detailed proof is shown in Appendix A.

III. NUMERICAL SIMULATION

If an experiment of SNS protocol is done, we can first calculate the lower and upper bounds of $\langle S_{jk}\rangle$ with Eqs. (B1) and (B5)–(B9) from their observed values. Also, we can get the upper bound of $\langle T_\Delta\rangle$ in a similar way. Then, we can get the lower bound of $\langle s_1^Z\rangle$ and the upper bound of $\langle e_1^{\mathrm{ph}}\rangle$ with Eqs. (B3) and (B4). Then, we can get the lower bound of n_1 and the upper bound of e_1^{ph} with Eqs. (B10)–(B14). Finally, we can get how many bits of secret keys we can extract from this experiment with Eq. (5). The problem is that we do not have such observed values and we need to simulate what values we would observe in the experiment with the list of experimental parameters in Table I. All symbols appearing in this paragraph are defined in Appendix B.

We use the linear model to simulate the observed values of experiment with the list of experimental parameters in Table I. Without loss of generality, we assume that the distance between Alice and Charlie and the distance between

TABLE I. List of experimental parameters used in numerical simulations. Here, p_d denotes the dark count rate of Charlie's detectors; e_0 is the error rate of the vacuum count; e_d is the misalignment-error probability; η_d is the detection efficiency of Charlie's detectors; f is the error correction inefficiency; α_f is the fiber loss coefficient (dB/km); ξ is the failure probability of statistical fluctuation analysis.

p_d	e_0	e_d	η_d	f	α_f	ξ
1.0×10^{-10}	0.5	15%	80.0%	1.1	0.2	1.0×10^{-10}

Bob and Charlie are the same, and we assume that the properties of Charlie's two detectors are the same. The total transmittance of the experiment setups is $\eta = 10^{-L/100}\eta_d$, where L is the distance between Alice and Bob. The simulation of those observed values is shown in Appendix C. These values are related to η and the list of other parameters in Table I.

Here, we set $\varepsilon_{\text{cor}} = \hat{\varepsilon} = \varepsilon_{\text{PA}} = \xi$, $\bar{\varepsilon} = 3\xi$, and $\varepsilon_{n_1} = 4\xi$. Thus, the security coefficient of the whole protocol is $\varepsilon_{tol} = 20\xi = 2.0 \times 10^{-9}$. As shown in Eqs. (B3) and (B14), four parameters need to be estimated before we get n_1 [notice that we could handle $\langle \underline{S}_{01} \rangle$, $\langle \underline{S}_{10} \rangle$ and $\langle \overline{S}_{02} \rangle$, $\langle \overline{S}_{20} \rangle$ together in Eq. (B3)]. Thus, we need to use the Chernoff bound four times. Obviously, if we set the failure probability of the Chernoff bound as ξ, the probability that the real value of the number of untagged bits is smaller than n_1 is no larger than 4ξ. For the similar reason that we use the Chernoff bound three times in Eqs. (B4) and (B14) to estimate e_1^{ph}, we set $\bar{\varepsilon} = 3\xi$. In order to fairly compare the performance of generating final keys of different total pulse numbers, N, we define the key rate per sending pulse, $R = l/N$.

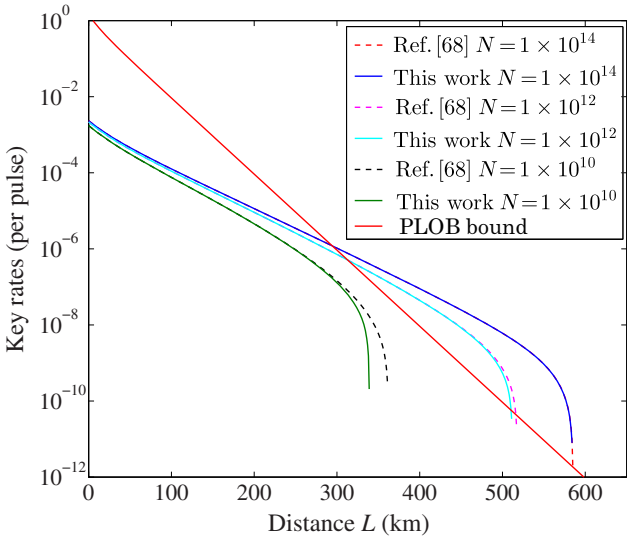

FIG. 1. The optimal key rates (per pulse) versus transmission distance (the distance between Alice and Bob) with the results of this work and Ref. [68] under the experimental parameters listed in Table I. The dashed lines are results of Ref. [68] and the solid lines are the results of this work. Here, we simulate three groups of results, where $N = 1 \times 10^{14}, 1 \times 10^{12}, 1 \times 10^{10}$. The red solid line is the PLOB bound.

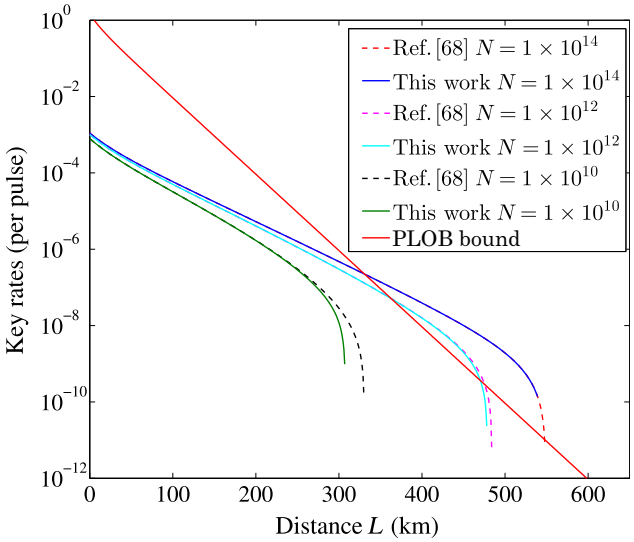

FIG. 2. The optimal key rates (per pulse) versus transmission distance (the distance between Alice and Bob) with the results of this work and Ref. [68] under the experimental parameters listed in Table I, except we set $e_d = 20\%$. The dashed lines are results of Ref. [68] and the solid lines are the results of this work. Here, we simulate three groups of results, where $N = 1 \times 10^{14}$, 1×10^{12}, 1×10^{10}. The red solid line is the PLOB bound.

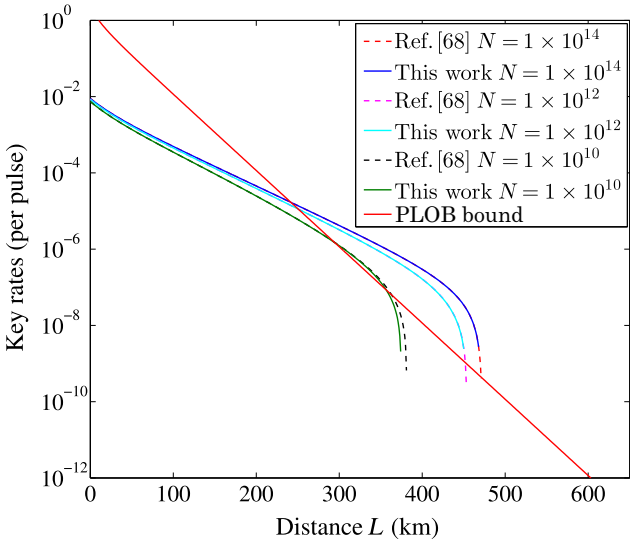

FIG. 3. The optimal key rates (per pulse) versus transmission distance (the distance between Alice and Bob) with the results of this work and Ref. [68]. We set $p_d = 1 \times 10^{-8}$ and $e_d = 5\%$; the other experimental parameters that we use are listed in Table I. The dashed lines are results of Ref. [68] and the solid lines are the results of this work. Here, we simulate three groups of results, where $N = 1 \times 10^{14}, 1 \times 10^{12}, 1 \times 10^{10}$. The red solid line is the PLOB bound.

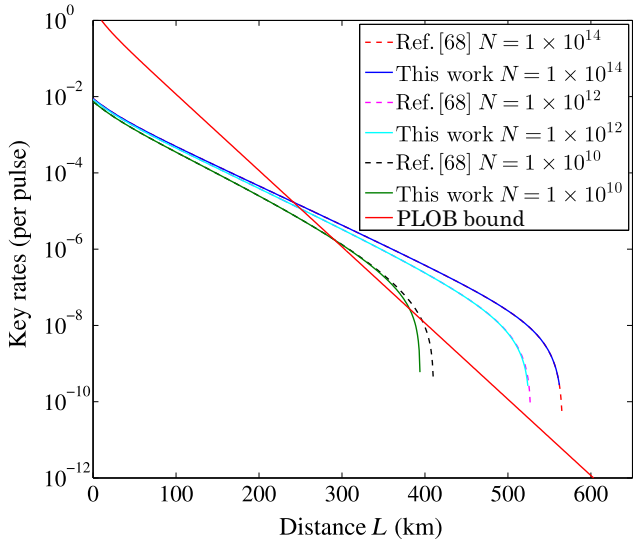

FIG. 4. The optimal key rates (per pulse) versus transmission distance (the distance between Alice and Bob) with the results of this work and Ref. [68]. We set $p_d = 1 \times 10^{-9}$ and $e_d = 5\%$; the other experimental parameters that we use are listed in Table I. The dashed lines are results of Ref. [68] and the solid lines are the results of this work. Here, we simulate three groups of results, where $N = 1 \times 10^{14}, 1 \times 10^{12}, 1 \times 10^{10}$. The red solid line is the PLOB bound.

Figures 1 and 2 are our simulation results of this work and Ref. [68] with the list of experimental parameters in Table I. The only difference between Figs. 1 and 2 is that $e_d = 15\%$ in Fig. 1 and $e_d = 20\%$ in Fig. 2. The results of this work and Ref. [68] almost overlap when we set $N = 1 \times 10^{14}$, but the difference of the results is obvious when we set $N = 1 \times 10^{10}$, especially at the end of the lines. The secure distance of the SNS protocol can still reach up to 500 km with 20% misalignment error and 1×10^{12} total pulses, even if we take all the effects of the finite-key size into consideration.

Figures 3 and 4 are our simulation results of another two groups of experimental parameters. We set $p_d = 1 \times 10^{-8}$ and $e_d = 5\%$ in Fig. 3 and $p_d = 1 \times 10^{-9}$ and $e_d = 5\%$ in Fig. 4. The other experimental parameters that we use are listed in Table I. As in Figs. 1 and 2, we simulate three groups of results, where $N = 1 \times 10^{14}, 1 \times 10^{12}, 1 \times 10^{10}$. Comparing Fig. 3 with Fig. 4, we can find that the secure distances are improved at most 100 km if the dark count is reduced by an order of magnitude. Still, the complete effect of finite size is reflected at the end of the lines, especially when the total number of pulses, N, is relatively small.

IV. CONCLUSION

In this paper, we show an analysis of the finite-key size effect of the SNS protocol and get the relation of final key length l and the security coefficient, as shown in Eq. (5). Equation (5) is derived by the method proposed in Ref. [78], and thus it can produce an unconditional secure final key under general attack, including all coherent attacks. The numerical results show that the secure distance of the SNS protocol can still reach up to 500 km with a 20% misalignment error and 1×10^{12} total pulses, even if we take all the effects of the finite-key size into consideration. This clearly shows that the SNS protocol [63] of TFQKD is on the one hand secure under general attack, i.e., as secure as the existing decoy-state MDIQKD, and on the other hand more efficient than the existing decoy-state MDIQKD by many orders of magnitude in the key rate in the long-distance domain.

ACKNOWLEDGMENTS

We thank Hai Xu for discussions. We acknowledge the financial support in part by the Ministration of Science and Technology of China through the National Key Research and Development Program of China Grant No. 2017YFA0303901 and National Natural Science Foundation of China Grants No. 11474182, No. 11774198, and No. U1738142.

APPENDIX A: THE RELATION OF THE LENGTH OF FINAL KEY AND $\varepsilon_{\mathrm{sec}}$

In this protocol, any attack on the quantum channel and detectors is allowed only if it does not break the rules of quantum mechanics, and we call the attacker Eve. We denote the system of Eve after error correction as E'. If Alice and Bob apply a privacy amplification scheme based on two-universal hashing to extract two shorter strings of length l from Z_s, the protocol is $\varepsilon_{\mathrm{sec}}$-secret [76,79]:

$$\varepsilon_{\mathrm{sec}} \leq 2\varepsilon + \frac{1}{2}\sqrt{2^{l - H_{\min}^{\varepsilon}(Z_s|E')}}, \tag{A1}$$

where $H_{\min}^{\varepsilon}(Z_s|E')$ is the ε-smooth min entropy. It measures the max probability of guessing Z_s right, giving E'. E' could be decomposed as CE, where C is the system of leakage information, while Alice and Bob perform error correction and E is the system of Eve before error correction. According to the chain rules [76], we have

$$H_{\min}^{\varepsilon}(Z_s|E') \geq H_{\min}^{\varepsilon}(Z_s|E) - |C|, \tag{A2}$$

where $|C| < \mathrm{leak}_{\mathrm{EC}} + \log_2(2/\varepsilon_{\mathrm{cor}})$. Also, we can decompose the string Z_s as $Z_1 Z_{\mathrm{rest}}$, where Z_1 is the bits caused by untagged-photon events and Z_{rest} is the other bits of Z_s [54]. Thus, according to the chain rules [80], we have

$$H_{\min}^{\varepsilon}(Z_s|E) \geq H_{\min}^{\bar{\varepsilon}}(Z_1|Z_{\mathrm{rest}}E) + H_{\min}^{\varepsilon'}(Z_{\mathrm{rest}}|E) - 2\log_2\frac{\sqrt{2}}{\hat{\varepsilon}}, \tag{A3}$$

where $\varepsilon = 2\bar{\varepsilon} + \varepsilon' + \hat{\varepsilon}$ and $H_{\min}^{\varepsilon'}(Z_{\mathrm{rest}}|E) \geq 0$.

Also, we denote the X basis as $\{\frac{1}{2}(|01\rangle + e^{i\theta}|10\rangle), \frac{1}{2}(|01\rangle - e^{i\theta}|10\rangle)\}$ and Z basis as $\{|01\rangle, |10\rangle\}$, where θ can be an arbitrary value. To get the lower bound of $H_{\min}^{\bar{\varepsilon}}(Z_1|Z_{\text{rest}}E)$, we need to use the uncertainty relation of smooth min- and max-entropy [78,81]. It says that if the untagged-photon states prepared in the X basis and Z basis are orthogonally unbiased, and if the states originally prepared and measured under the Z basis are now prepared and measured under the X basis, such that Alice and Bob obtain strings X_{s1} and X'_{s1} respectively, then we have

$$H_{\min}^{\bar{\varepsilon}}(Z_1|Z_{\text{rest}}E) \geq n_1 - H_{\max}^{\bar{\varepsilon}}(X_{s1}|X'_{s1}), \tag{A4}$$

where n_1 is the lower bound of the length of Z_1. We denote $e_X = (1/n_1)X_{s1} \oplus X'_{s1}$, which is the mismatching rate of X_{s1} and X'_{s1}. As we cannot directly observe the real value of e_X, we need to estimate e_X from the observed values of the protocol. We denote the estimated value of e_X as e_1^{ph}. As shown in Ref. [78], if the probability that $e_X \geq e_1^{\text{ph}}$ is no larger than $\bar{\varepsilon}$, then we have

$$H_{\max}^{\bar{\varepsilon}}(X_{s1}|X'_{s1}) \leq n_1 h(e_1^{\text{ph}}). \tag{A5}$$

Finally, we have

$$H_{\min}^{\varepsilon}(Z_s|E') \geq n_1[1 - h(e_1^{\text{ph}})] - \text{leak}_{\text{EC}} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2\log_2 \frac{\sqrt{2}}{\hat{\varepsilon}}. \tag{A6}$$

Combining Eqs. (5), (A1), and (A6) and setting $\varepsilon' = 0$, we have

$$\varepsilon_{\text{sec}} \leq 2\hat{\varepsilon} + 4\bar{\varepsilon} + \varepsilon_{\text{PA}}. \tag{A7}$$

Finally, containing the failure probability for the estimation of the lower bound of untagged bits in the Z basis, i.e., the probability that the real value of the number of untagged bits is smaller than n_1, ε_{n_1}, we have

$$\varepsilon_{\text{sec}} \leq 2\hat{\varepsilon} + 4\bar{\varepsilon} + \varepsilon_{\text{PA}} + \varepsilon_{n_1}. \tag{A8}$$

APPENDIX B: THE CALCULATION METHOD OF n_1 AND e_1^{ph}

The method we use here is similar to that in Ref. [68]. In an $\widetilde{X}$ window with different intensities from Alice and Bob, they do not announce any phase information in the protocol; therefore, the coherent states sent out from each side can be regarded as a classical mixture of different photon numbers. We denote $\rho = |0\rangle\langle 0|$, $\rho_1 = \sum_{k=0}(\mu_1^k e^{-\mu_1}/k!)|k\rangle\langle k|$, $\rho_2 = \sum_{k=0}(\mu_2^k e^{-\mu_2}/k!)|k\rangle\langle k|$, and $\rho_z = \sum_{k=0}(\mu_z^k/k!)|k\rangle\langle k|$, where ρ_1 and ρ_2 are the density operators of the coherent states used here in the $\widetilde{X}$ windows. This also applies to Bob's quantum state. In the whole protocol, Alice and Bob obtain $N_{jk}(jk = \{00, 01, 02, 10, 20\})$ instances when Alice sends state ρ_j and Bob sends state ρ_k. After the sifted step, Alice and Bob obtain n_{jk} one-detector heralded events. We denote the counting rate of source jk as $S_{jk} = n_{jk}/N_{jk}$. With all those definitions, we have

$$\begin{aligned} N_{00} &= [(1-p_z)^2 p_0^2 + 2(1-p_z)p_z p_0 p_{z0}]N, \\ N_{01} &= N_{10} = [(1-p_z)^2 p_0 p_1 + (1-p_z)p_z p_{z0} p_1]N, \\ N_{02} &= N_{20} = [(1-p_z)^2(1-p_0-p_1)p_0 \\ &\quad + (1-p_z)p_z p_{z0}(1-p_0-p_1)]N. \end{aligned} \tag{B1}$$

Also, we need to define two new subsets of the X_1 windows, C_{Δ^+} and C_{Δ^-}, to estimate the upper bound of e_1^{ph}. C_{Δ^+} contains all the instances in which both Alice and Bob prepare $|e^{i\delta_A}\sqrt{\mu_1}\rangle$, $|e^{i\delta_B}\sqrt{\mu_1}\rangle$, and $|\delta_A - \delta_B| \leq \Delta/2$. C_{Δ^-} contains all the instances in which both Alice and Bob prepare $|e^{i\delta_A}\sqrt{\mu_1}\rangle$, $|e^{i\delta_B}\sqrt{\mu_1}\rangle$, and $|\delta_A - \delta_B - \pi| \leq \Delta/2$. Just as in Ref. [68], here $|x|$ means the degree of the minor angle enclosed by the two rays that enclose the rotational angle of degree x, e.g., $|-15\pi/8| = |15\pi/8| = \pi/8$, $|-\pi/10| = \pi/10$. The number of instances in $C_{\Delta^\pm}$ is

$$N_{\Delta^\pm} = \frac{\Delta}{2\pi}(1-p_z)^2 p_1^2 N. \tag{B2}$$

We denote the number of effective events of right detectors responding from C_{Δ^+} as $n_{\Delta^+}^R$ and the number of effective events of left detectors responding from C_{Δ^-} as $n_{\Delta^-}^L$. We also get the counting error rate of $C_{\Delta^\pm}$, $T_\Delta = (n_{\Delta^+}^R + n_{\Delta^-}^L)/2N_{\Delta^\pm}$.

If we denote the expected value of the counting rate of untagged photons as $\langle s_1^Z\rangle$, the lower bound of $\langle s_1^Z\rangle$ is

$$\begin{aligned} \langle s_1^Z\rangle \geq \langle \underline{s}_1^Z\rangle = \frac{1}{2\mu_1\mu_2(\mu_2-\mu_1)}[\mu_2^2 e^{\mu_1}(\langle \underline{S}_{01}\rangle + \langle \underline{S}_{10}\rangle) \\ - \mu_1^2 e^{\mu_2}(\langle \overline{S}_{02}\rangle + \langle \overline{S}_{20}\rangle) - 2(\mu_2^2 - \mu_1^2)\langle \overline{S}_{00}\rangle], \end{aligned} \tag{B3}$$

where $\langle S_{jk}\rangle$ is the expected value of S_{jk}, and $\langle \overline{S}_{jk}\rangle$ and $\langle \underline{S}_{jk}\rangle$ are the upper bound and lower bound of $\langle S_{jk}\rangle$ when we estimate the expected value from its observed value.

The expected value of the phase-flip error rate of the untagged photons satisfies [68]

$$\langle e_1^{\text{ph}}\rangle \leq \langle \overline{e}_1^{\text{ph}}\rangle = \frac{\langle \overline{T}_\Delta\rangle - \frac{1}{2}e^{-2\mu_1}\langle \underline{S}_{00}\rangle}{2\mu_1 e^{-2\mu_1}\langle \underline{s}_1^Z\rangle}. \tag{B4}$$

Here we use the fact that the error rate of vacuum state is always $\frac{1}{2}$.

The formulas of $\langle \underline{s}_1^Z\rangle$ and $\langle \overline{e}_1^{\text{ph}}\rangle$ are represented by expected values, but the values that we get in experiments are observed values. To close the gap between the expected

values and observed values, we need the Chernoff bound [58,82]. Let $X_1, X_2, \ldots, X_n$ be n random samples, detected with the value 1 or 0, and let X denote their sum satisfying $X = \sum_{i=1}^{n} X_i$. ϕ is the expected value of X. We have

$$\phi^L(X) = \frac{X}{1+\delta_1(X)}, \tag{B5}$$

$$\phi^U(X) = \frac{X}{1-\delta_2(X)}, \tag{B6}$$

where we can obtain the values of $\delta_1(X)$ and $\delta_2(X)$ by solving the following equations:

$$\left(\frac{e^{\delta_1}}{(1+\delta_1)^{1+\delta_1}}\right)^{X/(1+\delta_1)} = \frac{\xi}{2}, \tag{B7}$$

$$\left(\frac{e^{-\delta_2}}{(1-\delta_2)^{1-\delta_2}}\right)^{X/(1-\delta_2)} = \frac{\xi}{2}, \tag{B8}$$

where ξ is the failure probability. Thus, we have

$$\phi^L(N_{jk}S_{jk}) = N_{jk}\langle \underline{S}_{jk}\rangle, \phi^U(N_{jk}S_{jk}) = N_{jk}\langle \overline{S}_{jk}\rangle. \tag{B9}$$

Still, Eqs. (B3) and (B4) are the lower bound of the expected values of the counting rate and the upper bound of the phase-flip error rate of single photons, respectively. The final question is what their real values are in this specific experiment, and we need the Chernoff bound to help us estimate their real values from their expected values. Similar to Eqs. (B5)–(B8), the observed value, φ, and its expected value, Y, satisfy

$$\varphi^U(Y) = [1+\delta_1'(Y)]Y, \tag{B10}$$

$$\varphi^L(Y) = [1-\delta_2'(Y)]Y, \tag{B11}$$

where we can obtain the values of $\delta_1'(Y)$ and $\delta_2'(Y)$ by solving the following equations:

$$\left(\frac{e^{\delta_1'}}{(1+\delta_1')^{1+\delta_1'}}\right)^{Y} = \frac{\xi}{2}, \tag{B12}$$

$$\left(\frac{e^{-\delta_2'}}{(1-\delta_2')^{1-\delta_2'}}\right)^{Y} = \frac{\xi}{2}. \tag{B13}$$

We define $N_1 = 2p_z^2 p_{z0}(1-p_{z0})\mu_z e^{-\mu_z} N$ and we have [68]

$$n_1 = \varphi^L(N_1\langle \underline{s}_1^Z\rangle), \quad e_1^{\mathrm{ph}} = \frac{\varphi^U(N_1\langle \underline{s}_1^Z\rangle\langle \overline{e}_1^{\mathrm{ph}}\rangle)}{N_1\langle \underline{s}_1^Z\rangle}. \tag{B14}$$

This ends the estimate of n_1 and e_1^{ph}. The estimation can also be applied to an SNS protocol with cat-state sources [83] and SNS protocol over asymmetric channel [84].

APPENDIX C: THE SIMULATION OF OBSERVED VALUES

We use the linear model to simulate the observed values of experiment with the list of experimental parameters in Table I. Without loss of generality, we assume that the distance between Alice and Charlie and the distance between Bob and Charlie are the same, and we assume that the properties of Charlie's two detectors are the same. If the total transmittance of the experiment setups is η, then we have

$$\begin{aligned}
n_{00} &= 2p_d(1-p_d)N_{00},\\
n_{01} &= n_{10} = 2[(1-p_d)e^{\eta\mu_1/2} - (1-p_d)^2 e^{-\eta\mu_1}]N_{01},\\
n_{02} &= n_{20} = 2[(1-p_d)e^{\eta\mu_2/2} - (1-p_d)^2 e^{-\eta\mu_2}]N_{02},\\
n_t &= n_{\mathrm{signal}} + n_{\mathrm{error}},\\
E_z &= \frac{n_{\mathrm{error}}}{n_t},\\
n_{\Delta+}^R &= n_{\Delta-}^L = [T_X(1-2e_d) + e_d S_X]N_{\Delta\pm},
\end{aligned}$$

where N_{00}, N_{01}, N_{10}, N_{02}, N_{20}, and $N_{\Delta\pm}$ are defined in Eqs. (B1) and (B2) and

$$\begin{aligned}
n_{\mathrm{signal}} &= 4Np_z^2 p_{z0}(1-p_{z0})[(1-p_d)e^{-\eta\mu_z/2}\\
&\quad - (1-p_d)^2 e^{-2\eta\mu_z}],\\
n_{\mathrm{error}} &= 2Np_z^2(1-p_{z0})^2[(1-p_d)e^{-\eta\mu_z} I_0(\eta\mu_z)\\
&\quad - (1-p_d)^2 e^{-2\eta\mu_z}] + 2Np_z^2 p_{z0}^2 p_d(1-p_d),\\
T_X &= \frac{1}{\Delta}\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} (1-p_d)e^{-2\eta\mu_1\cos^2\frac{\delta}{2}} d\delta\\
&\quad - (1-p_d)^2 e^{-2\eta\mu_1},\\
S_X &= \frac{1}{\Delta}\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} (1-p_d)e^{-2\eta\mu_1\sin^2\frac{\delta}{2}} d\delta\\
&\quad - (1-p_d)^2 e^{-2\eta\mu_1} + T_X,
\end{aligned}$$

where $I_0(x)$ is the 0-order hyperbolic Bessel function of the first kind.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India, 1984), p. 175.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phy. **74**, 145 (2002).

[3] N. Gisin and R. Thew, Quantum communication, Nat. Photon. **1**, 165 (2007).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phy. **81**, 1301 (2009).

[5] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, Phy. Rev. Lett. **85**, 441 (2000).

[6] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phy. **11**, 045018 (2009).

[7] K. Tamaki, M. Koashi, and N. Imoto, Unconditionally secure key distribution based on two nonorthogonal states, Phy. Rev. Lett. **90**, 167904 (2003).

[8] 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, Phy. Rev. Lett. **95**, 080501 (2005).

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

[10] H. P. Yuen, Quantum amplifiers, quantum duplicators and quantum cryptography, Quantum Semiclassical Opt: J. Eur. Opt. Soc. Part B **8**, 939 (1996).

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

[12] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, Phy. Rev. A **61**, 052304 (2000).

[13] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, New J. Phy. **4**, 44 (2002).

[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[15] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun **2**, 349 (2011).

[16] M. Hayashi, Upper bounds of eavesdropper's performances in finite-length code with the decoy method, Phy. Rev. A **76**, 012329 (2007).

[17] V. Scarani and R. Renner, Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing, Phy. Rev. Lett. **100**, 200501 (2008).

[18] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phy. Rev. Lett. **91**, 057901 (2003).

[19] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phy. Rev. Lett. **94**, 230503 (2005).

[20] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phy. Rev. Lett. **94**, 230504 (2005).

[21] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Quantum information with gaussian states, Phy. Rep. **448**, 1 (2007).

[22] X.-B. Wang, Decoy-state protocol for quantum cryptography with four different intensities of coherent light, Phy. Rev. A **72**, 012322 (2005).

[23] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Simple and efficient quantum key distribution with parametric down-conversion, Phy. Rev. Lett. **99**, 180503 (2007).

[24] X.-B. Wang, C.-Z. Peng, and J.-W. Pan, Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source, Appl. Phy. Lett. **90**, 031110 (2007).

[25] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Pan, General theory of decoy-state quantum cryptography with source errors, Phy. Rev. A **77**, 042311 (2008).

[26] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, Decoy-state quantum key distribution with both source errors and statistical fluctuations, New J. Phy. **11**, 075006 (2009).

[27] M. Peev *et al.* The secoqc quantum key distribution network in Vienna, New J. Phy. **11**, 075001 (2009).

[28] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phy. Rev. A **90**, 052314 (2014).

[29] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Reexamination of decoy-state quantum key distribution with biased bases, Phy. Rev. A **93**, 032307 (2016).

[30] H. F. Chau, Decoy-state quantum key distribution with more than three types of photon intensity pulses, Phys. Rev. A **97**, 040301 (2018).

[31] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Long-distance decoy-state quantum key distribution in optical fiber, Phy. Rev. Lett. **98**, 010503 (2007).

[32] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, Phy. Rev. Lett. **98**, 010504 (2007).

[33] 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, Phy. Rev. Lett. **98**, 010505 (2007).

[34] S.-K. Liao *et al.* Satellite-to-ground quantumkey distribution, Nature **549**, 43 (2017).

[35] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Metropolitan all-pass and inter-city quantum communication network, Opt. Exp. **18**, 27217 (2010).

[36] M. Sasaki *et al.* Field test of quantum key distribution in the tokyo qkd network, Opt. Exp. **19**, 10387 (2011).

[37] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, A quantum access network, Nature **501**, 69 (2013).

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

[39] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source, Phy. Rev. Lett. **100**, 090501 (2008).

[40] F. Xu, Y. Zhang, Z. Zhou, W. Chen, Z. Han, and G. Guo, Experimental demonstration of counteracting imperfect

sources in a practical one-way quantum-key-distribution system, Phy. Rev. A **80**, 062309 (2009).
[41] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature **509**, 475 (2014).
[42] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, Nat. Photon. **9**, 827 (2015).
[43] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phy. Rev. Lett. **108**, 130502 (2012).
[44] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantumkey distribution, Phy. Rev. Lett. **108**, 130503 (2012).
[45] X.-B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phy. Rev. A **87**, 012320 (2013).
[46] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks, Phy. Rev. Lett. **111**, 130501 (2013).
[47] 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.-F. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum key distribution, Phy. Rev. Lett. **111**, 130502 (2013).
[48] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution, Phy. Rev. Lett. **112**, 190503 (2014).
[49] 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.-F. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Measurement-device-independent quantum key distribution over 200 km, Phy. Rev. Lett. **113**, 190501 (2014).
[50] 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, Phy. Rev. Lett. **115**, 160502 (2015).
[51] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photon. **10**, 312 (2016).
[52] 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, 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, Phy. Rev. Lett. **117**, 190501 (2016).
[53] 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).
[54] 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).
[55] F. Xu, H. Xu, and H.-K. Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, Phy. Rev. A **89**, 052333 (2014).
[56] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensitydecoy-state method, Phy. Rev. A **91**, 032318 (2015).
[57] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phy. Rev. A **93**, 042324 (2016).
[58] C. Jiang, Z.-W. Yu, and X.-B. Wang, Measurement-device-independent quantum key distribution with source state errors and statistical fluctuation, Phy. Rev. A **95**, 032325 (2017).
[59] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).
[60] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).
[61] 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).
[62] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, Effective eavesdropping to twin field quantum key distribution, arXiv:1805.02272 (2018).
[63] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phy. Rev. A **98**, 062323 (2018).
[64] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound, arXiv:1805.05511 (2018).
[65] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).
[66] 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, Phy. Rev. Appl. **11**, 034053 (2019).
[67] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, arXiv:1807.07667 (2018).
[68] 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).
[69] F.-Y. Lu, Z.-Q. Yin, C.-H. Cui, G.-J. Fan-Yuan, S. Wang, D.-Y. He, W. Chen, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution with large random intensity fluctuation, arXiv:1901.04264 (2019).
[70] F. Grasselli and M. Curty, Practical decoy-state method for twin-field quantum key distribution, New J. Phy. **21**, 073001 (2019).
[71] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photon. **13**, 334 (2019).
[72] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution through sending-or-not-sending, arXiv:1902.06268 (2019).

[73] 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, Phy. Rev. X **9**, 021046 (2019).
[74] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field type quantum key distribution, arXiv:1902.10209 (2019).
[75] J. Müller-Quade and R. Renner, Composability in quantum cryptography, New J. Phy. **11**, 085006 (2009).
[76] R. Renner, Ph.D. thesis, School Swiss Federal Institute of Technology Zurich, 2005.
[77] R. König, R. Renner, A. Bariska, and U. Maurer, Small accessible quantum information does not imply security, Phy. Rev. Lett. **98**, 140502 (2007).
[78] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun **3**, 634 (2012).
[79] M. Tomamichel, R. Colbeck, and R. Renner, Duality between smooth min-and max-entropies, IEEE Trans. Inf. Theory **56**, 4674 (2010).
[80] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, Chain rules for smooth min-and max-entropies, IEEE Trans. Inf. Theory **59**, 2603 (2013).
[81] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, Phy. Rev. Lett. **106**, 110506 (2011).
[82] H. Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, Ann. Math. Stat. **23**, 493 (1952).
[83] C.-H. Zhang, C.-M. Zhang, and Q. Wang, Twin-field quantum key distribution with modified coherent states, Opt. Lett. **44**, 1468 (2019).
[84] X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, Asymmetric sending or not sending twin-filed quantum key distribution in practice, Phys. Rev. A **99**, 062316 (2019).