Concise security bounds for sending-or-not-sending twin-field quantum key distribution with finite pulses

Tingting Song,[1,2] Peiya Li,[3,*] and Jian Weng[1]
[1]College of Information Science and Technology, Jinan University, Guangzhou 510632, China
[2]Guangxi Key Laboratory of Cryptography and Information Security, Guilin 541004, China
[3]College of Cyber Security, Jinan University, Guangzhou 510632, China

(Received 30 November 2020; accepted 24 March 2021; published 7 April 2021)

Since its key rate can overcome the PLOB bound, sending-or-not-sending twin-field quantum key distribution (SNS-TF QKD) schemes attract more and more attention in the past three years. However, the inflection of statistical fluctuations on key rate was not considered quite comprehensively, which blocks the practical application of SNS-TF QKD. We take into account all the statistical fluctuations on probabilities, propose the finite-key analysis for SNS-TF QKD without any assumption on the type of attacks, and obtain the lower bound of key rates by applying an optimizing model. Then the finite-key rates are simulated under the reasonable values of some observed parameters, which shows that the key rates overcome the PLOB bound when the transmission distance is far from 350 km, if the number of pulses is fixed as $N = 10^{14}$. Compared with other SNS-TF QKD schemes, we provide concise and tight finite-key bounds since the statistical fluctuations of all parameters are considered against general attacks.

DOI: 10.1103/PhysRevA.103.042408

I. INTRODUCTION

Quantum key distribution (QKD) is the most practical protocol in quantum cryptography and is extensively applied for two-party secure communication. After Bennett and Brassard [1] proposed the first QKD protocol in 1984, unconditional security in theory attracted more and more attention [2–6]. However, there are many loopholes due to imperfect devices [7,8] in practice, and lots of attacks [9,10] on sources and detectors are found. On the highly lossy channel and non-single-photon source, photon-number-splitting (PNS) attacks [9,11] have been launched. Later, on some commercial QKD systems, quantum hackers exploited time-shift attacks [10], the phase remapping attack [12], the blinding attack [13], and wavelength-dependent attacks [14].

To resist the attacks and avoid information leakage, many researchers explored different solutions. Device-independent QKD (DI QKD) [15] moves out all the backdoors, and does not set any assumptions on settings. Its security [15–17] is based on entanglement between two communication parties, and the key rate depends on the violation of the Clauser-Horne-Shimony-Holt inequality. Unfortunately, the secure key rate of DI QKD is with the order of 10^{-10} bps, and the transmitted distance is around 5 km [18]. Thus, more effective QKD protocols should be discussed.

The decoy-state method [19,20] is mostly proposed to resist the PNS attack [9,11], and widely applied in experiments. The securities of decoy state QKD protocols are analyzed [21], especially with the finite-length pulses [22–24] under collective attack. At the same time, to eliminate all the loopholes on detectors, measurement-device-independent QKD (MDI QKD) [25] has been proposed, which removes all the assumptions on detectors. Based on the decoy-state method, MDI QKD [25,26] can resist PNS attack on non-single-photon sources and all attacks on detectors. Its secure transmission distance can reach 404 km in experiment [27], the key rate of which is with the linear order of channel transmittance η. The key rate is higher than that achievable with DI-QKD, but it is still bounded from above by the bound [28], i.e., the repeater-less bound on the private capacity of a quantum channel. Recently Lucamarini *et al.* [29] designed a twin-field QKD (TF QKD), and claim that the key rate overcomes the PLOB bound and reaches $O(\sqrt{\eta})$. Later, Wang *et al.* [30] pointed out that there is one loophole in the information postprocessing stage, and modified it to what is known as sending-or-not-sending TF QKD (SNS-TF QKD) [31]. Some other secure TF QKDs [32–34] are proposed and demonstrated in experiments [35,36]. For all TF QKD protocols, the influence of finite data size on the key rates has to be studied due to the statistical fluctuations. Up to now, the influence of statistical fluctuation on the key rates has not been taken into full consideration [33], where the deviations in source and the probabilities of k-photon pulses are neglected. Thus, the full statistical fluctuation analysis on SNS-TF QKD is necessary and crucial in the practical applications of SNS-TF QKD. We present a SNS-TF QKD against general attacks with the consideration of statistical fluctuations on all the possible parameters, and study the finite data size analysis based on universally composable security definition. And then an optimization model is applied to solve the lower bound of key rates, where the lower bound is the objective function and related parameters are subject to the constraints about observed click rates of detectors. With the same setting of experimental parameters in

*lpy0303@jnu.edu.cn

Ref. [33], the numerical simulation shows key rates overcome the PLOB bound when the transmission distance is far from 350 km, if the number of pulses is fixed as $N = 10^{14}$.

The paper is organized as follows. In Sec. II, we briefly introduce the SNS-TF QKD. The composable security definition and the corresponding security analysis are given in Sec. III. The simulation is shown in Sec. IV, and in Sec. V the conclusion is summarized.

II. SNS-TF QKD SCHEME

The procedure of the SNS-TF QKD scheme is as follows.

A. Preparation stage

Alice (Bob) randomly chooses the X window and Z window with probabilities p_x and $p_z = 1 - p_x$, respectively. In an X window, Alice (Bob) randomly sends out a phase-randomized coherent state from three intensities $u_0 = 0$, u_1, and u_2 with probabilities p_{x0}, p_{x1}, and $p_{x2} = 1 - p_{x0} - p_{x1}$, respectively. In a Z window, Alice (Bob) randomly decides to send a phase-randomized coherent state $|\sqrt{u_z}e^{i\theta_A}\rangle$ ($|\sqrt{u_z}e^{i\theta_B}\rangle$) with probabilities p_{z1} and records a bit 1 (0), or to send nothing (a vacuum state $|0\rangle$) with probability $p_{z0} = 1 - p_{z1}$ and records a bit 0 (1). The X windows are decoy windows, and the Z windows are signal windows.

B. Measurement stage

All the pulses are transmitted through the quantum channel, and sent to Charlie. Charlie is assumed to perform interferometric measurement 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.

C. Sifting stage

According to the clicks, the effective events of Z windows and X windows are defined. It is an effective event of Z windows if one and only one detector clicks. It is an effective event of X windows if one and only one detector clicks, when one party sends the vacuum state, or when Alice and Bob send the coherent states with the same intensity u_i ($i = 0, 1, 2$) and their phases satisfy the following criterion, that is

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

where θ_A and θ_B are the phases of coherent states prepared by Alice and Bob, respectively, and ψ_{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 protocol. The states of the effective events of X windows can be regarded as a probabilistic mixture of different photon-number states, with the two-mode single-photon ingredient $|\psi_1\rangle\langle\psi_1|$, and $|\psi_1\rangle = \frac{1}{\sqrt{2}}(e^{i(\theta_B+\gamma_B)}|01\rangle + e^{i(\theta_A+\gamma_A)}|10\rangle)$, where γ_A and γ_B are the global phases of Alice and Bob, respectively, which are chosen as arbitrary values and published by the strong reference pulses. We only need the value $\gamma_A - \gamma_B$, and denote the difference as ψ_{AB} here. The value of λ in Eq. (1) depends on the size of the phase slice Δ that Alice and Bob choose, and in terms of Δ the condition in Eq. (1) is equivalent to

$$|\theta_A - \theta_B - \psi_{AB}| \leqslant \frac{\Delta}{2} \quad \vee \quad |\theta_A - \theta_B - \psi_{AB} - \pi| \leqslant \frac{\Delta}{2}. \tag{2}$$

Note that in X windows, when one party sends the vacuum state, the event is also an effective event of X windows. The total number of pulses is N, and the number of instances where Alice and Bob send pulses of intensities u_i and u_j, respectively, in X windows is N_{ij}. Considering Charlie's announcements, the set of effective events is $\mathbb{X}_{0i}$ with number n_{0i} or $\mathbb{X}_{ii}$ with number n_{ii}. The set of effective events in Z windows is denoted as $\mathbb{Z}$.

D. Parameter estimation stage

For the events in $\mathbb{Z}$, Alice records bit 0 if she sends a vacuum state and bit 1 if she sends a weak coherent state. At the same time, Bob records different bits. He records bit 1 if he sends a vacuum state and bit 0 if he sends a weak coherent state. Then Alice and Bob choose a random subset of size n of $\mathbb{Z}$ and store the respective bits, as Z_i and Z_i'. The rest of the bits form set $\mathbb{Z}_s$. Next, they compute the average error $e_{pe} = \frac{1}{n}\sum_i Z_i \oplus Z_i'$ where the sum takes over the random subset of size n. If $e_{pe} > Q$, the protocol aborts. The threshold value Q is discussed by Alice and Bob before the protocol starts.

E. Error correction and verification stage

Alice and Bob operate an information reconciliation scheme to correct the rest of Bob's bits Z_S' in $\mathbb{Z}_s$, and Bob obtains an estimate $\hat{Z}_S$ of Z_S from Z_S'. To achieve the goal, Alice would send Bob at most leak_{EC} bits to correct Z_S'. Later, Alice and Bob would operate error verification on Z_S and $\hat{Z}_S$. By a random universal hash function, Alice computes a hash of Z_S of length $\lceil\log(1/\varepsilon_{\text{cor}})\rceil$, and sends the hash function and hash values to Bob. Bob computes the hash of $\hat{Z}_S$ by using the same hash function. Note that if Z_S and $\hat{Z}_S$ are not the same, the probability that the two hash values are equal is less than ε_{cor}. If the two hash values are equal, the protocol continues, otherwise the protocol aborts.

F. Privacy amplification stage

For the sequences Z_S and $\hat{Z}_S$ of length n_s, Alice and Bob estimate the number of bits of n_{s1} caused by the single-photon state $|01\rangle$ or $|10\rangle$ that Alice decides not to send and Bob decides to send or Alice decides to send and Bob decides not to send. The phase error rate $e_{pz}^{(1)}$ of the single-photon state is estimated, according to the events in $\mathbb{X}_{11}$ and $\mathbb{X}_{22}$ as the decoy state. According to the calculation results, they apply a privacy amplification scheme based on two-universal hashing to exact two shorter strings K_A and K_B of length l from Z_S and $\hat{Z}_S$, respectively. K_A and K_B are the secure key strings held by Alice and Bob.

III. SECURITY ANALYSIS OF THE SNS-TF QKD SCHEME

In this section, we will discuss the finite-key security of the SNS-TF QKD scheme. Since the number of pulses sent by each party is finite in practice, the statistical fluctuations due to the finite pulses must not be neglected. Due to statistical fluctuations, the key rate parameters are described by frequencies, instead of probabilities. And the deviation between actual proportion and probability distribution can be deduced by the laws of large number in information theory.

For a phase randomized weak coherent source with intensity u_γ, the number of photons in a pulse is a discrete random variable, denoted as x, the probability distribution of which is $\Pr\{x=k\} = p_{k|u_\gamma} = e^{-u_\gamma} u_\gamma^k / k!$ $(k \in Z)$ and $\sum_{k=0}^{\infty} p_{k|u_\gamma} = 1$. A sequence $x_1, x_2, \dots, x_{N_\gamma}$ is drawn to be independent identically distributed according to the distribution $\Pr\{x=k\} = p_{k|u_\gamma}$. Since the number of pulses sent from a source is finite, the actual proportion of k-photon pulses can be assumed to be $p'_{k|u_\gamma}$, instead of $p_{k|u_\gamma}$. According to the laws of large number shown in Theorem 11.2.1 and Lemma 11.6.1 of Ref. [37], the statistical fluctuation is given in the following lemma [26], tighter than that deduced by Sano *et al.* [38].

Lemma 1. The actual frequency $p'_{k|u_\gamma}$ has the upper bound $\overline{p_{k|u_\gamma}} = \min\{p_{k|u_\gamma} + \xi(N_\gamma, n_\gamma), 1\}$ and lower bound $\underline{p_{k|u_\gamma}} = \max\{p_{k|u_\gamma} - \xi(N_\gamma, n_\gamma), 0\}$ except with the probability $\varepsilon_{\rm PE}$, where $p_{k|u_\gamma}$ is the expected value of $p'_{k|u_\gamma}$, N_γ is the number of samples, n_γ is the number of values of random variable x in samples, and $\xi(N_\gamma, n_\gamma) := \sqrt{[\ln(1/\varepsilon_{\rm PE}) + n_\gamma * \ln(N_\gamma + 1)]/(2N_\gamma)}$.

This lemma shows the absolute fluctuation and has no assumption on the underlying distribution. That is suitable for estimating the fluctuation of parameters in this paper. In the following sections, we will give the finite-key analysis of SNS-TF QKD by applying the notations of the upper bound and the lower bound of the estimated parameter λ' as $\overline{\lambda}$ and $\underline{\lambda}$, respectively.

A. Composable security

In this section, we will give the composable security definition and show the SNS-TF QKD scheme satisfies the composable security.

A QKD protocol outputs a key K_A on Alice's side and an estimate of that key K_B on Bob's side. This key is usually an l-bit string, where l depends on the noise level of the channel, as well as the security and correctness requirements on the protocol. The protocol may also abort, in which case we set $K_A = K_B = \perp$. The secrecy criterion is based on the universally composable security definition. A secure QKD protocol has to, roughly speaking, satisfy two criteria called "correctness" and "secrecy." A QKD protocol is called "correct," if for any strategy of the adversary, $K_A = K_B$. It is called $\varepsilon_{\rm cor}$-correct, if $\Pr[K_A \neq K_B] \leqslant \varepsilon_{\rm cor}$. To define the secrecy of a key, we consider the quantum state $\rho_{\rm SE}$ that describes the correlation between Alice's classical key K_A and the eavesdropper E (for any given attack strategy). A key is called ε_Δ-secret [39] from E if it is ε_Δ close to a uniformly distributed key that is uncorrelated with the eavesdropper, that is, if

$$\tfrac{1}{2}\|\rho_{\rm SE} - \omega_K \otimes \rho_E\|_1 \leqslant \varepsilon_\Delta, \tag{3}$$

where ω_K denotes the fully mixed state on K_A and ρ_E is the marginal state on Eve's system [40]. A QKD protocol is called "secret," if, for any attack strategy, $\varepsilon_\Delta = 0$ whenever the protocol outputs a key. It is called $\varepsilon_{\rm sec}$-secret, if it outputs a ε_Δ-secure key with $(1 - p_{\rm abort})\varepsilon_\Delta \leqslant \varepsilon_{\rm sec}$, where $p_{\rm abort}$ is the probability that the protocol aborts.

A QKD protocol is called "secure" if it is correct and secret. It is called ε-secure, if it is $\varepsilon_{\rm cor}$-correct and $\varepsilon_{\rm sec}$-secret with $\varepsilon_{\rm cor} + \varepsilon_{\rm sec} \leqslant \varepsilon$. Following the definition, our protocol is proven that it is both $\varepsilon_{\rm cor}$-correct and $\varepsilon_{\rm sec}$-secret.

Theorem 1. The protocol is $\varepsilon_{\rm cor}$-correct.

Proof. In the error verification stage, by randomly choosing a hash function F, suppose its length is $\lceil \log(1/\varepsilon_{\rm cor}) \rceil$. Then the probability that K_A is different from K_B is

$$\begin{aligned}\Pr[K_A \neq K_B] &= \Pr[K_A \neq K_B, F(Z_S) = F(\hat{Z}_S)] \\ &\leqslant \Pr[Z_S \neq \hat{Z}_S, F(Z_S) = F(\hat{Z}_S)] \\ &\leqslant \Pr[F(Z_S) = F(\hat{Z}_S) | Z_S \neq \hat{Z}_S] \\ &\leqslant 2^{-\lceil \log(1/\varepsilon_{\rm cor}) \rceil} \leqslant \varepsilon_{\rm cor}.\end{aligned} \tag{4}$$

Note that one defines $K_A = K_B = \perp$ if the protocol aborts. Thus, if $F(Z_S) \neq F(\hat{Z}_S)$, $K_A = K_B = \perp$. ■

Theorem 2. The protocol is $\varepsilon_{\rm sec}$-secret.

Proof. Let E' be Eve's information on Z_S after error verification. Based on the lemmas in Ref. [40], a ε_Δ-secret key K_A of length l can be extracted from Z_S, where

$$\varepsilon_\Delta = \max_{\varepsilon'} \tfrac{1}{2}\sqrt{2^{l - H_{\min}^{\varepsilon'}(Z_S|E')}} + 2\varepsilon'. \tag{5}$$

The conditional smooth min-entropy $H_{\min}^{\varepsilon'}(Z_S|E')$ quantifies the amount of uncertainty that the eavesdropper Eve, holding system E', has on Z_S. Suppose $p_{\rm abort}$ is the probability that the protocol aborts. According to the composable security definition, if the protocol outputs a ε_Δ-secret key of length l satisfying Eq. (5), the protocol is $\varepsilon_{\rm sec}$-secret with $(1 - p_{\rm abort})\varepsilon_\Delta \leqslant \varepsilon_{\rm sec}$. Note that the secrecy definition has been updated in Ref. [40]. This implies that the quantum leftover hash lemma, as stated in Refs. [41,42], should be corrected to Eq. (5). ■

Based on Theorems 1 and 2, since $\varepsilon = \varepsilon_{\rm cor} + \varepsilon_{\rm sec}$, we know the protocol is ε-secure, if ε'-smooth min-entropy $H_{\min}^{\varepsilon'}(Z_S|E')$ satisfies Eq. (5). The first term of the sum in Eq. (5) is the failure probability of privacy amplification, denoted as $\varepsilon_{\rm PA}$. Hence, the length of the final key satisfies

$$l \geqslant H_{\min}^{\varepsilon'}(Z_S|E') + 2\log(2\varepsilon_{\rm PA}), \tag{6}$$

for $\varepsilon_{\rm PA} + 2\varepsilon' \leqslant \varepsilon_\Delta$.

B. Evaluating $H_{\min}^{\varepsilon'}(Z_S|E')$

From Eq. (6), the length of the final key depends on $H_{\min}^{\varepsilon'}(Z_S|E')$. To bound $H_{\min}^{\varepsilon'}(Z_S|E')$, we will use the structure of system E' and chain-rule inequalities for smooth entropies.

First, let E be Eve's information on Alice's system before error correction and error verification, and let C be information leaked during error correction and error verification, thus Eve's information after error correction and error verification is $E' = {\rm EC}$. Actually the information published during error correction is denoted as ${\rm leak}_{\rm EC}$ bits and that leaked during error verification is $\lceil \log(1/\varepsilon_{\rm cor}) \rceil$ bits. Using the chain-rule inequality, we obtain

$$\begin{aligned} H_{\min}^{\varepsilon'}(Z_S|E') &\geqslant H_{\min}^{\varepsilon'}(Z_S|E) - |C| \\ &\geqslant H_{\min}^{\varepsilon'}(Z_S|E) - \mathrm{leak}_{\mathrm{EC}} - \left\lceil \log \frac{1}{\varepsilon_{\mathrm{cor}}} \right\rceil \\ &\geqslant H_{\min}^{\varepsilon'}(Z_S|E) - \mathrm{leak}_{\mathrm{EC}} - \log \frac{2}{\varepsilon_{\mathrm{cor}}}. \end{aligned} \tag{7}$$

Second, Z_S is the system Alice holds after the parameter estimation stage, which can de decomposed into Z_0, Z_1, and Z_{multi} corresponding to the bits generated by vacuum, single-photon, and multiphoton events. Note that Eve knows the decomposition, so the system E includes the decomposition. Based on the generalized chain rule [42], we get

$$\begin{aligned} &H_{\min}^{\varepsilon'}(Z_S|E) \\ &\geqslant H_{\min}^{\hat{\varepsilon}}(Z_1|Z_0Z_{\mathrm{multi}}E) + H_{\min}^{\varepsilon''}(Z_0Z_{\mathrm{multi}}|E) - 2\log\frac{\sqrt{2}}{\bar{\varepsilon}}, \\ &\geqslant H_{\min}^{\hat{\varepsilon}}(Z_1|Z_0Z_{\mathrm{multi}}E) - 2\log\frac{\sqrt{2}}{\bar{\varepsilon}}, \end{aligned} \tag{8}$$

where $\varepsilon' = 2\hat{\varepsilon} + \varepsilon'' + \bar{\varepsilon}$. Mostly, suppose $\varepsilon'' = 0$. In the second inequality, we use $H_{\min}^{\varepsilon''}(Z_0Z_{\mathrm{multi}}|E) \geqslant 0$, since Eve knows all information from multiphoton events by the photon-number splitting attack, and vacuum contributions contain no information about the chosen bit values and generate no key.

To bound $H_{\min}^{\hat{\varepsilon}}(Z_1|Z_0Z_{\mathrm{multi}}E)$, we introduce two bases, the X basis and Z basis. Denote the X basis as $\{(|01\rangle + e^{i\theta}|10\rangle)/2,\ (|01\rangle - e^{i\theta}|10\rangle)/2\}$, and the Z basis as $\{|01\rangle,\ |10\rangle\}$. The raw keys are denoted as Z_S and $\hat{Z}_S$ in the original protocol. We consider a gedanken experiment [41] in which Alice and Bob prepare and measure the single-photon events Z_1 in the X basis, though they choose the bases according to the probabilities p_x and p_z as usual. Since the X basis and Z basis are mutually unbiased, the security follows the fact that, the better Bob is able to estimate Alice's single-photon events if she prepared in the X basis, the worse Eve is able to guess Alice's single-photon events, if she prepared in the Z basis. That is, in terms of smooth entropies,

$$H_{\min}^{\hat{\varepsilon}}(Z_1|Z_0Z_{\mathrm{multi}}E) + H_{\max}^{\hat{\varepsilon}}(X_{s1}|X'_{s1}) \geqslant n_{s1}, \tag{9}$$

where n_{s1} is the length of Z_1, and X_{s1} and X'_{s1} are the strings of Alice and Bob in the gedanken experiment, respectively.

Let $e_{pz}^{(1)}$ be the corresponding phase error rate in Z_1, and let $e_{bx}^{(1)}$ be the bit error rate of single-photon pulses in effective events of X windows. Then we estimate $H_{\max}^{\hat{\varepsilon}}(X_{s1}|X'_{s1})$ by $e_{pz}^{(1)}$ as $H_{\max}^{\hat{\varepsilon}}(X_{s1}|X'_{s1}) \leqslant n_{s1}h(e_{pz}^{(1)})$, when the failure probability is less than $\hat{\varepsilon}$. Furthermore, $e_{pz}^{(1)}$ can be evaluated by the bit error rate of single-photon pulses in X windows, $e_{bx}^{(1)}$, as

$$e_{pz}^{(1)} \leqslant e_{bx}^{(1)} + \delta, \tag{10}$$

with failure probability smaller than ε_{ph}, and

$$\begin{aligned} \delta^2 :&= \frac{\ln 2\left(n_{11}^{(1)} + n_{22}^{(1)} + n_{s1}\right) e_{bx}^{(1)} \left(1 - e_{bx}^{(1)}\right)}{n_{s1}\left(n_{11}^{(1)} + n_{22}^{(1)}\right)} \\ &\times \log_2\left(\frac{n_{11}^{(1)} + n_{22}^{(1)} + n_{s1}}{8\pi\ n_{s1}\ \left(n_{11}^{(1)} + n_{22}^{(1)}\right) \left(e_{bx}^{(1)}\right)^2 \left(1 - e_{bx}^{(1)}\right)^2 (\varepsilon_{ph})^2}\right), \end{aligned} \tag{11}$$

where $n_{ii}^{(1)}$ is the number of single-photon effective events in set $\mathbb{X}$. The calculation of the deviation δ follows the conclusion [43] shown in Appendix A, where we correct some minor errors. Based on Bayes's theorem, we find that

$$\begin{aligned} \Pr\{e_{pz}^{(1)} > e_{bx}^{(1)} + \delta|\text{``pass''}\} &\leqslant \frac{1}{p_{\mathrm{pass}}}\Pr\{e_{pz}^{(1)} > e_{bx}^{(1)} + \delta\} \\ &\leqslant \varepsilon_{ph}/p_{\mathrm{pass}}, \end{aligned} \tag{12}$$

where $p_{\mathrm{pass}} = \Pr\{e_{pe} \leqslant Q\} = 1 - p_{\mathrm{abort}}$. Thus, $H_{\max}^{\hat{\varepsilon}}(X_{s1}|X'_{s1})$ is bounded above by $n_{s1}h(e_{bx}^{(1)} + \delta)$ with failure probability $\hat{\varepsilon} > \varepsilon_{ph}/p_{\mathrm{pass}}$, and $e_{bx}^{(1)}$ is evaluated in the next subsection.

Furthermore, the leaked information during the error correction in Eq. (7) is evaluated by $\mathrm{leak}_{\mathrm{EC}} = f_{\mathrm{EC}}\, n_s\, h(Q)$, where f_{EC} is the efficiency of the error correction code. Q is the threshold value which decides whether the protocol aborts or not. We introduce the robustness $\varepsilon_{\mathrm{rob}}$ which is the probability that the protocol aborts even though the eavesdropper is inactive. The value of $\varepsilon_{\mathrm{rob}}$ is bounded by the probability that the measured error rate e_{pe} exceeds Q. From the statistical fluctuation, we estimate $\varepsilon_{\mathrm{rob}}$ as

$$\Pr\{e_{pe} > Q + \delta_Q\} < \varepsilon_{\mathrm{rob}}, \tag{13}$$

where

$$\begin{aligned} \delta_Q^2 :&= \frac{\ln 2\ (n + n_s)\ e_{pe}\ (1 - e_{pe})}{n\, n_s} \\ &\times \log_2\left(\frac{n + n_s}{8\pi\ n\, n_s\ e_{pe}^2\ (1 - e_{pe})^2 (\varepsilon_{\mathrm{rob}})^2}\right). \end{aligned} \tag{14}$$

Hence, the SNS-TF QKD protocol outputs a key string of length

$$\begin{aligned} l \geqslant\ & n_{s1}\left[1 - h\left(e_{bx}^{(1)} + \delta\right)\right] - 2\log\frac{\sqrt{2}}{\bar{\varepsilon}} - \mathrm{leak}_{\mathrm{EC}} \\ &- \log\frac{2}{\varepsilon_{\mathrm{cor}}} + 2\log(2\varepsilon_{\mathrm{PA}}), \end{aligned} \tag{15}$$

with $\varepsilon_{\mathrm{cor}}$ correctness and $\varepsilon_{\mathrm{sec}}$ secrecy.

C. Evaluating n_{s1} and $e_{bx}^{(1)}$

The effective events in the Z basis are one-clicking events in the Z windows, the number of which is denoted as n_z, while n_{s1} is the number of effective events caused by single-photon states in the Z windows after the parameter estimation stage. In order to evaluate n_{s1}, we consider the events in X windows. Let $\mathbb{X}_{ij}$ be the set of effective events with number n_{ij}, when Alice and Bob send pulses from intensities u_i and u_j, respectively. The set $\mathbb{X}_{0i}(\mathbb{X}_{i0})$ of $n_{0i}(n_{i0})$ includes events that one party sends a pulse with vacuum intensity and the other sends with intensity u_i, if one and only one detector clicks and their phases satisfy the criterion in Eq. (2). Denote n_k as the total number of k-pulse clicking events in sets $\mathbb{X}_{0i}$ and $\mathbb{X}_{i0}$ and the effective events of the Z basis. Thus, the number satisfies

$$\begin{aligned} n_{01} &= n_{10} = \sum_{k=0}^{\infty} p'_{u_1|k} n_k = p_x'^2\, p'_{x0}\, p'_{x1} \sum_{k=0}^{\infty} \frac{p'_{k|u_1}}{q'_k} n_k, \\ n_{02} &= n_{20} = \sum_{k=0}^{\infty} p'_{u_2|k} n_k = p_x'^2\, p'_{x0}\, p'_{x2} \sum_{k=0}^{\infty} \frac{p'_{k|u_2}}{q'_k} n_k, \\ n_{00} &= p'_{u_0|0} n_0 = \frac{p_x'^2\, p_{x0}'^2}{q'_0} n_0, \quad n_z = \sum_{k=0}^{\infty} p'_{u_z|k} n_k, \end{aligned} \tag{16}$$

where $p'_{u_i|k}$ $(i = 0,\ 1,\ 2)$ is the actually conditional frequency of originating intensity u_i given that a k-photon pulse is sent. For convenience, we let $n_{0i} = n_{i0}$ here. Note that they are unequal in practice, but the key rates will not be affected since all the related values are in terms of $n_{0i} + n_{i0}$.

Bayes's rule is used in the first three equations, since

$$\begin{aligned}
p'_{u_0|0} &= \frac{p_x'^2\, p_{x0}'^2}{q'_0},\\
p'_{u_i|k} &= \frac{p_x'^2\, p'_{x0}\, p'_{xi}}{q'_k}\, p'_{k|u_i}, \quad i = 1, 2, \quad k = 0, 1, 2, \dots,\\
p'_{u_z|k} &= \frac{2\, p_z'^2\, p'_{z0}\, p'_{z1}}{q'_k}\, p'_{k|u_z} + \frac{p_z'^2\, p_{z1}'^2}{q'_k}\, p'_{k|u_z u_z}, \quad k = 1, 2, \dots,\\
p'_{u_z|0} &= \frac{2\, p_z'^2\, p'_{z0}\, p'_{z1}}{q'_0}\, p'_{0|u_z} + \frac{p_z'^2\, p_{z1}'^2}{q'_0}\, p'_{0|u_z u_z} + \frac{p_z'^2\, p_{z0}'^2}{q'_0},
\end{aligned} \tag{17}$$

where q'_k is the actual frequency that k-photon pulses are sent in effective sets $\mathbb{X}_{0i}(\mathbb{X}_{i0})$ and $\mathbb{Z}$:

$$\begin{aligned}
q'_0 &= p_x'^2\, p_{x0}'^2 + 2\, p_x'^2\, p'_{x0}\big(p'_{x1}\, p'_{0|u_1} + p'_{x2}\, p'_{0|u_2}\big)\\
&\quad + 2\, p_z'^2\, p'_{z0}\, p'_{z1}\, p'_{0|u_z} + p_z'^2\, p_{z1}'^2\, p'_{0|u_z u_z} + p_z'^2\, p_{z0}'^2,\\
q'_k &= 2\, p_x'^2\, p'_{x0}\big(p'_{x1}\, p'_{k|u_1} + p'_{x2}\, p'_{k|u_2}\big)\\
&\quad + 2\, p_z'^2\, p'_{z0}\, p'_{z1}\, p'_{k|u_z} + p_z'^2\, p_{z1}'^2\, p'_{k|u_z u_z}, k \geqslant 1.
\end{aligned}$$

The key is extracted from the effective events caused by single-photon states in Z windows after privacy amplification, since a powerful eavesdropper will obtain all information on other effective events in Z windows. The lower bound of the key rate can be reached when the lower bounds of $p'_{u_z|1}$ and n_{s1} are obtained. To estimate the bounds of $p_{u_i|k}$, we should find the number of values of random variable x in Lemma 1, which depends on the source's intensity. If a pulse is sent from a vacuum source, the number of photons must be zero, and the number of random variables value is 1. If a pulse is sent from other sources, like u_1, u_2, or u_z, we set the number of random variable values as 10, since the probability of a pulse with more than ten photons is negligible. Thus, all the clicks are divided into 31 classes, according to the intensity of the pulses and the number of photons. For convenience, the statistical fluctuation of each $p_{u_i|k}$ is the same, so $p'_{u_i|k}$ is bounded below by $\underline{p_{u_i|k}} = \max\{p_{u_i|k} - \xi(n_{00} + 2n_{01} + 2n_{02} + n_z, 31), 0\}$ and bounded above by $\overline{p_{u_i|k}} = \min\{p_{u_i|k} + \xi(n_{00} + 2n_{01} + 2n_{02} + n_z, 31), 1\}$. The main task is to find the lower bound of the number n_{s1} of the effective events caused by single-photon states in Z windows and the upper bound of its phase error rate $e_{bx}^{(1)}$. Note that bounding n_{s1} is equivalent to bounding the quantity n_1 since

$$n_{s1} = \frac{n_s}{n_z}\, p'_{u_z|1}\, n_1, \tag{18}$$

where the first fraction n_s/n_z is the residual ratio of set $\mathbb{Z}$ after parameter estimation. To solve the lower bound of n_1, we set up a mathematical model with the minimum n_1 as objective function:

$$\begin{aligned}
&\min\ \ n_1\\
&\text{s.t. } n_{01} = n_{10} = \sum_{k=0}^{\infty} p'_{u_1|k}\, n_k,\\
&n_{02} = n_{20} = \sum_{k=0}^{\infty} p'_{u_2|k} n_k,\\
&n_{00} = p'_{u_0|0} n_0 = \frac{p_x'^2\, p_{x0}'^2}{q'_0} n_0,\\
&p'_{u_z|k} + p'_{u_1|k} + p'_{u_2|k} = 1,\ k \geqslant 1,\\
&p'_{u_z|0} + \sum_{i=0}^{2} p'_{u_i|0} = 1,\\
&\underline{p_{u_i|0}} \leqslant p'_{u_i|0} \leqslant \overline{p_{u_i|0}},\ i = 0, 1, 2, z,\\
&\underline{p_{u_i|k}} \leqslant p'_{u_i|k} \leqslant \overline{p_{u_i|k}},\ k \geqslant 1, i = 1, 2, z.
\end{aligned} \tag{19}$$

In the convex programming, $n_{0i}(n_{i0})$ are experimental data, and $p'_{u_i|k}$ is varied in the continuable interval $[\underline{p_{u_i|k}}, \overline{p_{u_i|k}}]$. Solve the convex programming, and obtain the lower bound of n_1 as

$$n_1 \geqslant \underline{n_1} = \frac{\underline{p_{u_1|2}}\, n_{02} - \overline{p_{u_2|2}}\, n_{01} - (\overline{p_{u_1|2}}\,\overline{p_{u_2|0}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|0}})\overline{n_0}}{\overline{p_{u_1|2}}\,\overline{p_{u_2|1}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|1}}}, \tag{20}$$

under the conditions $u_1 \geqslant u_2$, $n_{10} = n_{01}$, $n_{20} = n_{02}$, $\overline{p_{u_1|2}}\,\overline{p_{u_2|1}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|1}} > 0$, and $\overline{p_{u_1|2}}\,\overline{p_{u_2|0}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|0}} > 0$, where $\overline{n_0} = \min\{n_{00}/\underline{p_{u_0|0}}, 1\}$, $\underline{p_{u_i|k}} = \max\{p_{u_i|k} - \xi(n_{00} + 2n_{01} + 2n_{02} + n_z, 31), 0\}$, and $\overline{p_{u_i|k}} = \min\{p_{u_i|k} + \xi(n_{00} + 2n_{01} + 2n_{02} + n_z, 31), 1\}$. Hence, the lower bound of n_{s1} is bounded below by

$$\underline{n_{s1}} = \frac{n_s}{n_z}\, \underline{p_{u_z|1}}\, \underline{n_1}. \tag{21}$$

Now solve the bit error rate $e_{bx}^{(1)}$ of single-photon pulses in effective events of the X basis. We express the number of error bits in set $\mathbb{X}_{ii}$ as

$$\begin{aligned}
m_{00} &= p'_{u_0u_0|0}\, m_0 = \frac{p_{x0}'^2\, p'_{0|u_0u_0}}{\nu'_0}\, m_0 = \frac{p_{x0}'^2}{\nu'_0}\, m_0,\\
m_{11} &= \sum_{k=0}^{\infty} p'_{u_1u_1|k} m_k = p_{x1}'^2 \sum_{k=0}^{\infty} \frac{p'_{k|u_1u_1}}{\nu'_k}\, m_k,\\
m_{22} &= \sum_{k=0}^{\infty} p'_{u_2u_2|k} m_k = p_{x2}'^2 \sum_{k=0}^{\infty} \frac{p'_{k|u_2u_2}}{\nu'_k}\, m_k,
\end{aligned} \tag{22}$$

where $p'_{u_iu_i|k}$ $(i = 1,\ 2)$ is the actually conditional frequency of both originating intensities u_i given that a bit error of k-photon pulses is obtained, and m_k is the number of bit errors of k-photon pulses in both sets $\mathbb{X}_{ii}$. We use Bayes's rule to express $p'_{u_iu_i|k}$ in the second equations as

$$p'_{u_iu_i|0} = \frac{p'^2_{xi}\, p'_{0|u_iu_i}}{\nu'_0}, i = 0, 1, 2,$$
$$p'_{u_iu_i|k} = \frac{p'^2_{xi}\, p'_{k|u_iu_i}}{\nu'_k},$$
$$i = 1, 2,\ k = 1, 2, \ldots, \tag{23}$$

where $p'_{k|u_iu_i}$ is the actual frequency that a k-photon pulse is sent from the source with intensity $2\,u_i$, the expected value of $p'_{k|u_iu_i}$ is $p_{k|u_iu_i} = e^{-2u_i}(2\,u_i)^k/\,k!$ $(p_{0|u_0u_0} = 1)$, and

$$\nu'_0 = p'^2_{x0} + p'^2_{x1}\, p'_{0|u_1u_1} + p'^2_{x2}\, p'_{0|u_2u_2},$$
$$\nu'_k = p'^2_{x1}\, p'_{k|u_1u_1} + p'^2_{x2}\, p'_{k|u_2u_2}\ (k > 0). \tag{24}$$

Hence, the number of bit errors of single-photon pulses in $\mathbb{X}_{ii}$ is

$$m_1 \leqslant \overline{m_1} = \min\left\{\frac{m_{11} - \underline{p_{u_1u_1|0}}\,\underline{m_0}}{\underline{p_{u_1u_1|1}}}, \frac{m_{22} - \underline{p_{u_2u_2|0}}\,\underline{m_0}}{\underline{p_{u_2u_2|1}}}\right\}, \tag{25}$$

where $\underline{p_{u_iu_i|k}} = \max\{p_{u_iu_i|k} - \xi(m_{00} + m_{11} + m_{22}, 7), 0\}(i = 0, 1, 2;\ k = 0, 1)$, and $\underline{m_0} = m_{00}\,/\,\underline{p_{u_0u_0|0}}$. Furthermore, the upper bound of $e^{(1)}_{bx}$ is given by

$$e^{(1)}_{bx} = \frac{m'_1}{n^{(1)'}_{11} + n^{(1)'}_{22}} \leqslant \overline{e^{(1)}_{bx}} = \frac{\overline{m_1}}{\underline{n^{(1)}_{11} + n^{(1)}_{22}}}, \tag{26}$$

since $\underline{n^{(1)}_{11} + n^{(1)}_{22}} = \underline{n_1}\,\underline{\nu_1}/\,\overline{q_1}$, where $\underline{\nu_1} = \max\{\nu_1 - \xi(m_{00} + m_{11} + m_{22}, 3), 0\}$ and $\overline{q_1} = \min\{q_1 + \xi(n_{00} + 2n_{01} + 2n_{02} + n_z, 10), 1\}$.

IV. SIMULATION OF FINITE-LENGTH KEY RATES AND DISCUSSION

The length of the final key is

$$l = \underline{n_{s1}}\big[1 - h\big(\overline{e^{(1)}_{bx}} + \delta\big)\big] - \text{leak}_{\text{EC}}$$
$$+ 2\log(2\varepsilon_{\text{PA}}) - \log\frac{2}{\varepsilon_{\text{cor}}} - 2\log\frac{\sqrt{2}}{\bar{\varepsilon}}, \tag{27}$$

where $\underline{n_{s1}}$ and $\overline{e^{(1)}_{bx}}$ are given in Eqs. (21) and (26), respectively. Denote the efficiency of the error correction code as f_{EC}, thus the leaked information during the error correction stage is $\text{leak}_{\text{EC}} = f_{\text{EC}}\, n_s\, h(Q)$. If all the stages passed, the protocol is ε_{cor}-correct and ε_{sec}-secret, where $\varepsilon_{\text{sec}} \geqslant (1 - p_{\text{abort}})(\varepsilon_{\text{PA}} + 2\bar{\varepsilon} + 4\, n_{\text{PE}}\, \varepsilon_{\text{PE}}) + 4\,\varepsilon_{ph}$, and $n_{\text{PE}}\, \varepsilon_{\text{PE}}$ is total failure probability for the estimation of $\underline{n_{s1}}$ by using Lemma 1 n_{PE} times. According to the composable security definition, it is ε-secure, where $\varepsilon = \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$. We assume $\varepsilon_{\text{PA}} = \bar{\varepsilon} = \varepsilon_{\text{PE}} = \varepsilon_{\text{cor}} = \varepsilon_{\text{rob}} = p_{\text{abort}} = \kappa$. To estimate $\overline{e^{(1)}_{bx}}$, we should calculate statistical fluctuations of parameters seven times, so the failure probability ε_{ph} is set to 7κ. Similarly, statistical fluctuations of ten times should be estimated to find $\underline{n_{s1}}$, then we let $n_{\text{PE}} = 10$. Thus the security coefficient of the SNS-TF QKD is $\varepsilon = \kappa(72 - 43\kappa)$. The finite-key rate of SNS-TF QKD is $R = (1 - \kappa)l/N$, where N is the total number of pulses sent from sources.

To visualize the finite-key rate, we simulate the performance of our SNS-TF QKD scheme under the reasonable values of parameters [25,26]: the loss coefficient of the quantum channel is $\alpha = 0.2$ dB/km, the detection efficiency is $\eta = 80.0\%$, the dark count rate is $p_{\text{dark}} = 1.0 \times 10^{-10}$, the efficiency of error correction is $f_{\text{EC}} = 1.1$, and the misalignment-error probability is $e_d = 0.15$. Without loss of generality, suppose the distance between Alice and Charlie and that between Bob and Charlie are the same, then the transmittance of the channel is $\eta_{\text{tot}} = \eta \times 10^{-L/100}$, where L is the distance between Alice and Bob. Furthermore, the experimental data are shown as follows:

$$n_z = n_{zs} + n_{ze}, \quad n_{zs} = 4Np_z^2\, p_{z0}\, p_{z1}[(1 - p_{\text{dark}})\, e^{-\eta_{\text{tot}}u_z/2} - (1 - p_{\text{dark}})^2\, e^{-\eta_{\text{tot}}u_z}],$$
$$n_{ze} = 2Np_z^2\, p_{z1}^2\, [(1 - p_{\text{dark}})\, e^{-\eta_{\text{tot}}\, u_z} - (1 - p_{\text{dark}})^2\, e^{-2\,\eta_{\text{tot}}\, u_z}] + 2Np_z^2\, p_{z0}^2\, p_{\text{dark}}\, (1 - p_{\text{dark}}),$$
$$n^R_{\Delta^+i} = n^L_{\Delta^-i} = \frac{\Delta}{2\,\pi}Np_x^2\, p_{xi}^2[T_{Xi}\, e_d + (1 - e_d)\, S_{Xi} - (1 - p_{\text{dark}})^2\, e^{-2\,\eta_{\text{tot}}\, u_i}],\ i = 1, 2,$$
$$m_{ii} = n^R_{\Delta^+i} + n^L_{\Delta^-i},\ i = 1, 2, \quad T_{Xi} = (1 - p_{\text{dark}})\frac{1}{\Delta}\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} e^{-4\eta_{\text{tot}}u_i \sin^2(\delta/2)},\ i = 1, 2,$$
$$S_{Xi} = (1 - p_{\text{dark}})\frac{1}{\Delta}\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} e^{-2\eta_{\text{tot}}u_i(1-\sin\delta)},\ i = 1, 2. \tag{28}$$

With all the actual values, we set the failure probability of statistical fluctuation as $\kappa = 10^{-10}$, and optimize other parameters to maximize the ultimate lower bounds of key rates as functions of transmission distance L. The left figure in Fig. 1 shows the ultimate key rate as a function of the distance between Alice and Bob under three different numbers of pulses $N = 10^{12}$, 10^{14}, and 10^{15}. The key rate drops with the transmission distance increasing, and the number of pulses plays an important role in the key's generation. With the number increasing, the key rates also increase, especially for remote position. Furthermore, the finite SNS-TF QKD could generate the secure key over 600 km. If the number of pulses

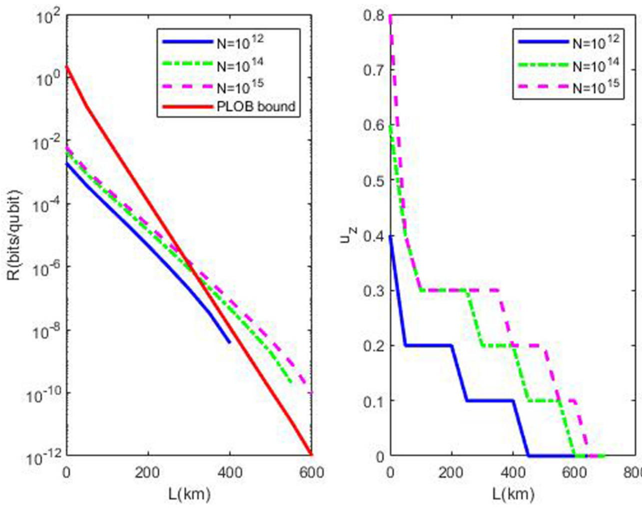

FIG. 1. The lower bounds of key rates for our finite SNS TF-QKD scheme under different numbers of pulses N. Parameters: $\alpha = 0.2$ dB/km, $\eta = 80.0\%$, $p_{\text{dark}} = 1.0 \times 10^{-10}$, $\kappa = 10^{-10}$, and $e_d = 0.15$. Other parameters are optimized to maximize the key rates.

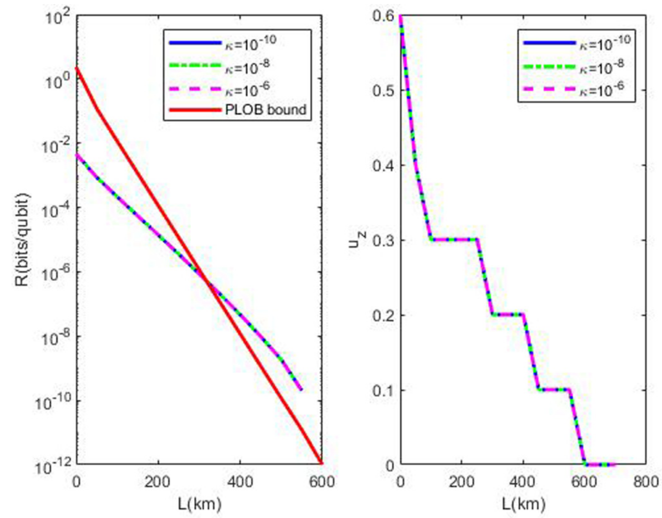

FIG. 2. The lower bounds of key rates and corresponding values of u_z under different values of failure probabilities of statistical fluctuation κ, when the number of pulses is fixed as $N = 10^{14}$.

is smaller than 10^{10}, the protocol could not generate the secure key. When the number of pulses is larger than $N = 10^{14}$, the key rates overcome the PLOB bound far from 350 km.

Compared with Ref. [33], our statistical bounds are slightly tighter. The main reason is that the deviation of probability for a k-photon pulse is introduced in our security analysis. On the other hand, the robustness of a SNS-TF QKD scheme is considered. Hence, the successful probability of the scheme is brought in to evaluate the tighter final key rates. The right figure in Fig. 1 depicts the corresponding optimal intensity of u_z for different numbers of pulses. From the results, we know the intensity u_z is a monotone decreasing function of transmission distance when the number N is fixed.

Now we analyze the corresponding optimal values of some parameters as functions of the distance. The inflection of ε on final key rates is shown in Fig. 2. When the number of pulses is fixed as $N = 10^{14}$, the key rates and the corresponding intensities of u_z are simulated under three different values of failure probabilities of statistical fluctuation $\kappa = 10^{-10}, 10^{-8},$ and 10^{-6}. From the figure, we find that the value of failure probability does not much affect the key rates. Correspondingly, the nonzero intensities of the Z windows are also not affected by the failure probability related to the statistical fluctuations, and decrease over long distances. Furthermore, we discuss the change of probability chosen with a nonzero intensity in a Z window. The value of the probability p_{z1}, much smaller than p_{z0}, is decreasing with the transmission distance increasing. The reason is that many effective events are needed to estimate the error rate and the yield of single-photon pulses for the high lossy channel. When secure distance is the same, the optimal value of p_{z1} increases with N increasing in order to maximize key rate.

V. CONCLUSION

In summary, we analyze the finite-key security for SNS-TF QKD without any assumption on the type of attacks. The lower bound of key rates is simulated with reasonable values of the observed parameters. The numerical simulation shows that the key rates would overcome the PLOB bound, when the transmission distance is far from 350 km, if the number of pulses is fixed as $N = 10^{14}$. Compared with other SNS-TF QKD schemes [31,33], our method is with statistical fluctuations on all possible parameters, and the secure key bounds are valid against general attacks, so our scheme is practical and realizable. Though our strategy gives a tight bound with all statistical fluctuations, the finite-key rates are a little lower, and it is hard to overcome the PLOB bound in a short period of time even with a high-speed QKD system. Thus, other SNS-TF QKD protocols with statistical fluctuations must be designed in the future. Furthermore, in our protocol, Alice and Bob are supposed to have identical distances to the untrusted Charlie, while in practical quantum networks the quantum channels are asymmetric. The phases of pulses after being transmitted in asymmetric-loss channels must be changed. Although one can add additional fibers to each channel to compensate for channel differences, it is not practical to add fibers and maintain symmetry between each pair of users all the time in a scalable network with large numbers of dynamically added or deleted users. Thus, the asymmetric SNS-TF QKD's security must be discussed in the future.

ACKNOWLEDGMENTS

This work is supported by Key R&D Program of Guangdong Province (Grant No. 2019B010136003), Major Program of Guangdong Basic and Applied Research (Grant No. 2019B030302008), Science and Technology Program of Guangzhou (Grant No. 202007040004), Fundamental Research Funds for the Central Universities (Grant No. 21620433, 21619314), and Guangxi Key Laboratory of Cryptography and Information Security (Grant No. GCIS201922).

APPENDIX A: THE CALCULATION OF DEVIATION δ BETWEEN $e_{pz}^{(1)}$ AND $e_{bx}^{(1)}$

Suppose the failure probability that $e_{pz}^{(1)}$ is bounded above by $e_{bx}^{(1)}+\delta$ is less than ε_{ph}. Then we have

$$\Pr\{e_{pz}^{(1)} > e_{bx}^{(1)}+\delta\} \leqslant \varepsilon_{ph}. \tag{A1}$$

To calculate δ, we rewrite the number of effective events and that of corresponding errors in X windows as

$$n_{ii}=\sum_{k=0}^{\infty}\frac{e^{-2u_i}(2u_i)^k}{k!}n_{ii}^{(k)},\quad m_{ii}=\sum_{k=0}^{\infty}\frac{e^{-2u_i}(2u_i)^k}{k!}m_{ii}^{(k)}, \tag{A2}$$

where $n_{ii}^{(k)}$ and $m_{ii}^{(k)}$ are the number of effective events and that of error caused by the k-photon pulses in set $\mathbb{X}_{ii}$. If Bob measures all the single-photon pulses in set $\mathbb{X}_{ii}$ and those of Z windows by the X basis, the number of errors is $m_1=e_{bx}^{(1)}(n_{11}^{(1)}+n_{22}^{(1)})+e_{pz}^{(1)}n_{s1}=m_{11}^{(1)}+m_{22}^{(1)}+e_{pz}^{(1)}n_{s1}$. The first term can be counted accurately after the error verification. Assume Eve chooses a distribution of m_1, $\Pr\{m_1\}$, before Bob's detection. In order to link the probability, $\Pr\{e_{pz}^{(1)}>e_{bx}^{(1)}+\delta\}$, to the quantities, $n_{11}^{(1)}$, $n_{22}^{(1)}$, n_{s1}, and $m_{11}^{(1)}+m_{22}^{(1)}$, we use the security definition of a QKD protocol to show the probability that Eve designs a probability distribution $\Pr\{m_1\}$ and Bob obtains $m_{11}^{(1)}+m_{22}^{(1)}$ bits of errors in the effective X windows. That is,

$$\begin{aligned}\Pr\{e_{pz}^{(1)}>e_{bx}^{(1)}+\delta,\ e_{bx}^{(1)}\} &= \Pr\{e_{pz}^{(1)}\,n_{s1}>e_{bx}^{(1)}\,n_{s1}+\delta\,n_{s1},\ m_{11}^{(1)}+m_{22}^{(1)}\}\\ &=\Pr\{m_1-e_{bx}^{(1)}(n_{11}^{(1)}+n_{22}^{(1)})>e_{bx}^{(1)}n_{s1}+\delta\,n_{s1},\ m_{11}^{(1)}+m_{22}^{(1)}\}\\ &=\Pr\{m_1>m_{11}^{(1)}+m_{22}^{(1)}+(e_{bx}^{(1)}+\delta)n_{s1},\ m_{11}^{(1)}+m_{22}^{(1)}\}\\ &\leqslant \sum_{m_1=m_{11}^{(1)}+m_{22}^{(1)}+(e_{bx}^{(1)}+\delta)n_{s1}}^{m_{11}^{(1)}+m_{22}^{(1)}+n_{s1}}\Pr\{m_{11}^{(1)}+m_{22}^{(1)}|m_1\}\Pr\{m_1\}.\end{aligned} \tag{A3}$$

Though Eve chooses the distribution $\Pr\{m_1\}$, Bob chooses to measure with the X basis randomly, thus

$$\begin{aligned}&\Pr\{m_{11}^{(1)}+m_{22}^{(1)}|m_1\}\\ &=\frac{\binom{n_{11}^{(1)}+n_{22}^{(1)}}{m_{11}^{(1)}+m_{22}^{(1)}}\binom{n_{s1}}{m_1-m_{11}^{(1)}-m_{22}^{(1)}}}{\binom{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}{m_1}}\\ &=\frac{(n_{11}^{(1)}+n_{22}^{(1)})!\cdot n_{s1}!\cdot m_1!\cdot(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}-m_1)!}{(m_{11}^{(1)}+m_{22}^{(1)})!(n_{11}^{(1)}+n_{22}^{(1)}-m_{11}^{(1)}-m_{22}^{(1)})!(m_1-m_{11}^{(1)}-m_{22}^{(1)})!(n_{s1}-m_1+m_{11}^{(1)}+m_{22}^{(1)})!(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})!}\\ &=\frac{\binom{m_1}{m_{11}^{(1)}+m_{22}^{(1)}}\binom{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}-m_1}{n_{11}^{(1)}+n_{22}^{(1)}-m_{11}^{(1)}-m_{22}^{(1)}}}{\binom{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}{n_{11}^{(1)}+n_{22}^{(1)}}}.\end{aligned} \tag{A4}$$

When $m_1>(m_{11}^{(1)}+m_{22}^{(1)})(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})/(n_{11}^{(1)}+n_{22}^{(1)})$, it is easy to prove that $\Pr\{m_{11}^{(1)}+m_{22}^{(1)}|m_1\}$ is a strictly decreasing function on m_1, so Eq. (A3) is bounded by

$$\begin{aligned}\Pr\{e_{pz}^{(1)}>e_{bx}^{(1)}+\delta,\ e_{bx}^{(1)}\} &\leqslant \sum_{m_1=m_{11}^{(1)}+m_{22}^{(1)}+(e_{bx}^{(1)}+\delta)n_{s1}}^{m_{11}^{(1)}+m_{22}^{(1)}+n_{s1}}\Pr\{m_{11}^{(1)}+m_{22}^{(1)}|m_1\}\Pr\{m_1\}\\ &\leqslant \sum_{m_1=m_{11}^{(1)}+m_{22}^{(1)}+(e_{bx}^{(1)}+\delta)n_{s1}}^{m_{11}^{(1)}+m_{22}^{(1)}+n_{s1}}\Pr\{m_{11}^{(1)}+m_{22}^{(1)}|m_1=m_{11}^{(1)}+m_{22}^{(1)}+(e_{bx}^{(1)}+\delta)n_{s1}\}\Pr\{m_1\}\\ &\leqslant \Pr\{m_{11}^{(1)}+m_{22}^{(1)}|m_1=m_{11}^{(1)}+m_{22}^{(1)}+(e_{bx}^{(1)}+\delta)n_{s1}\}\\ &=\frac{(n_{11}^{(1)}+n_{22}^{(1)})!\cdot n_{s1}!\cdot m_1!\cdot(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}-m_1)!}{(m_{11}^{(1)}+m_{22}^{(1)})!(n_{11}^{(1)}+n_{22}^{(1)}-m_{11}^{(1)}-m_{22}^{(1)})!(e_{pz}^{(1)}n_{s1})!(n_{s1}-e_{pz}^{(1)}n_{s1})!(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})!}.\end{aligned} \tag{A5}$$

We will bound the function by the Stirling formula $n! = \sqrt{2\pi n}(\frac{n}{e})^n e^{\lambda_n}$, where $\frac{1}{12n+1} < \lambda_n < \frac{1}{12n}$. Then Eq. (A5) is deduced as

$$\begin{aligned}
&\Pr\{e_{pz}^{(1)} > e_{bx}^{(1)} + \delta,\ e_{bx}^{(1)}\}\\
&\leqslant \frac{1}{\sqrt{2\pi}} 2^{-(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})\xi(\delta)} \frac{\sqrt{n_{s1} m_1 (n_{11}^{(1)}+n_{22}^{(1)})(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}-m_1)}}{\sqrt{(m_{11}^{(1)}+m_{22}^{(1)})(n_{11}^{(1)}+n_{22}^{(1)}-m_{11}^{(1)}-m_{22}^{(1)})(e_{pz}^{(1)}n_{s1})(n_{s1}-e_{pz}^{(1)}n_{s1})(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})}}\\
&= \frac{1}{\sqrt{2\pi}} 2^{-(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})\xi(\delta)} \sqrt{\frac{m_1}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}}\sqrt{1-\frac{m_1}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}}\frac{1}{\sqrt{\frac{m_{11}^{(1)}+m_{22}^{(1)}}{n_{11}^{(1)}+n_{22}^{(1)}}}}\\
&\quad\times \frac{1}{\sqrt{1-\frac{m_{11}^{(1)}+m_{22}^{(1)}}{n_{11}^{(1)}+n_{22}^{(1)}}}} \cdot \frac{1}{\sqrt{e_{pz}^{(1)}(1-e_{pz}^{(1)})}} \frac{\sqrt{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}}{\sqrt{n_{s1}(n_{11}^{(1)}+n_{22}^{(1)})}}\\
&\leqslant \frac{1}{2\sqrt{2\pi}} \frac{\sqrt{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}}{\sqrt{n_{s1}(n_{11}^{(1)}+n_{22}^{(1)})}} \frac{1}{e_{bx}^{(1)}(1-e_{bx}^{(1)})} 2^{-(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})\xi(\delta)},
\end{aligned} \tag{A6}$$

where

$$\begin{aligned}
\xi(\delta) &= H\left(\frac{m_1}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}\right) - \frac{n_{11}^{(1)}+n_{22}^{(1)}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}} H(e_{bx}^{(1)}) - \frac{n_{s1}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}} H(e_{bx}^{(1)}+\delta)\\
&= H\left(e_{bx}^{(1)} + \delta\frac{n_{s1}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}\right) - \frac{n_{11}^{(1)}+n_{22}^{(1)}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}} H(e_{bx}^{(1)}) - \frac{n_{s1}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}} H(e_{bx}^{(1)}+\delta).
\end{aligned} \tag{A7}$$

The last inequality in Eq. (A6) is obtained since function $f(x) = 1/\sqrt{x(1-x)}$ is decreasing on $(0, 1/2)$ and $0 \leqslant e_{bx}^{(1)} < e_{pz}^{(1)} \leqslant 1/2$, where we correct the minor errors in Ref. [43]. Due to the concavity of entropy function $H(x)$, $\xi(\delta)$ is positive. If $n_{11}^{(1)} + n_{22}^{(1)}$ and n_{s1} are large enough, and δ is small enough to $e_{bx}^{(1)}$, $\xi(\delta)$ is expanded by Taylor expansion as

$$\begin{aligned}
\xi(\delta) &= H(e_{bx}^{(1)}) + \frac{n_{s1} H'(e_{bx}^{(1)})}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}\delta + \left(\frac{n_{s1}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}\right)^2 \frac{H''(e_{bx}^{(1)})}{2}\delta^2 - \frac{n_{11}^{(1)}+n_{22}^{(1)}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}} H(e_{bx}^{(1)})\\
&\quad - \frac{n_{s1}}{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}\left[H(e_{bx}^{(1)}) + H'(e_{bx}^{(1)})\delta + \frac{H''(e_{bx}^{(1)})}{2}\delta^2\right] + O(\delta^3)\\
&= -\frac{n_{s1}(n_{11}^{(1)}+n_{22}^{(1)})}{(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})^2}\frac{H''(e_{bx}^{(1)})}{2}\delta^2 + O(\delta^3).
\end{aligned} \tag{A8}$$

Since

$$H(x) = -x\log_2(x) - (1-x)\log_2(1-x), \quad H'(x) = -\log_2(x) + \log_2(1-x), \quad H''(x) = -\frac{1}{\ln 2}\left(\frac{1}{x} + \frac{1}{1-x}\right), \tag{A9}$$

we have

$$\xi(\delta) = \frac{n_{s1}(n_{11}^{(1)}+n_{22}^{(1)})}{(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})^2}\frac{\delta^2}{2\ln 2}\left(\frac{1}{e_{bx}^{(1)}} + \frac{1}{1-e_{bx}^{(1)}}\right) + O(\delta^3), \quad = \frac{n_{s1}(n_{11}^{(1)}+n_{22}^{(1)})}{2\ln 2\, e_{bx}^{(1)}(1-e_{bx}^{(1)})(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})^2}\delta^2 + O(\delta^3). \tag{A10}$$

Hence, if $n_{11}^{(1)} + n_{22}^{(1)}$ and n_{s1} are large enough and δ is sufficiently small, $e_{pz}^{(1)}$ is smaller than $e_{bx}^{(1)} + \delta$ with failure probability smaller than

$$\varepsilon_{ph} := \frac{1}{2\sqrt{2\pi}} \frac{\sqrt{n_{11}^{(1)}+n_{22}^{(1)}+n_{s1}}}{\sqrt{n_{s1}(n_{11}^{(1)}+n_{22}^{(1)})}} \frac{1}{e_{bx}^{(1)}(1-e_{bx}^{(1)})} 2^{-\frac{n_{s1}(n_{11}^{(1)}+n_{22}^{(1)})}{2\ln 2\, e_{bx}^{(1)}(1-e_{bx}^{(1)})(n_{11}^{(1)}+n_{22}^{(1)}+n_{s1})}\delta^2}. \tag{A11}$$

Furthermore, if the failure probability is fixed as ε_{ph}, $e_{pz}^{(1)}$ is bounded above by $e_{bx}^{(1)} + \delta$, where

$$\delta^2 := \frac{\ln 2\,\left(n_{11}^{(1)} + n_{22}^{(1)} + n_{s1}\right) e_{bx}^{(1)}\left(1 - e_{bx}^{(1)}\right)}{n_{s1}\left(n_{11}^{(1)} + n_{22}^{(1)}\right)} \log_2\left(\frac{n_{11}^{(1)} + n_{22}^{(1)} + n_{s1}}{8\pi\, n_{s1}\left(n_{11}^{(1)} + n_{22}^{(1)}\right)\left(e_{bx}^{(1)}\right)^2\left(1 - e_{bx}^{(1)}\right)^2(\varepsilon_{ph})^2}\right). \tag{A12}$$

APPENDIX B: THE LOWER BOUND OF n_1

To solve the convex programming in Eq. (19), we consider a linear combination which eliminates the role of two-photon pulses and gives a strict bound of n_1:

$$\begin{aligned}
\underline{p_{u_1|2}}(n_{02} + n_{20}) - \overline{p_{u_2|2}}\,(n_{01} + n_{10}) &\leqslant p'_{u_1|2}(n_{02} + n_{20}) - p'_{u_2|2}\,(n_{01} + n_{10}) \\
&= 2\sum_{k\neq 2}^{\infty}\left(p'_{u_1|2}\,p'_{u_2|k} - p'_{u_2|2}\,p'_{u_1|k}\right)n_k \\
&\leqslant 2\left(\overline{p_{u_1|2}}\,p'_{u_2|0} - \underline{p_{u_2|2}}\,p'_{u_1|0}\right)n_0 + 2\left(\overline{p_{u_1|2}}\,p'_{u_2|1} - \underline{p_{u_2|2}}\,p'_{u_1|1}\right)n_1 \\
&\quad + 2\sum_{k=3}^{\infty}\left(\overline{p_{u_1|2}}\,p'_{u_2|k} - \underline{p_{u_2|2}}\,p'_{u_1|k}\right)n_k \\
&\leqslant 2\left(\overline{p_{u_1|2}}\,\overline{p_{u_2|0}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|0}}\right)n_0 \\
&\quad + 2\left(\overline{p_{u_1|2}}\,\overline{p_{u_2|1}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|1}}\right)n_1,
\end{aligned} \tag{B1}$$

where $u_1 \geqslant u_2$, and $\overline{p_{u_1|2}}\,p'_{u_2|k} - \underline{p_{u_2|2}}\,p'_{u_1|k} < 0$ for all $k \leqslant 3$. Then the lower bound of n_1 is obtained as

$$n_1 \geqslant \underline{n_1} = \frac{\underline{p_{u_1|2}}\,n_{02} - \overline{p_{u_2|2}}\,n_{01} - \left(\overline{p_{u_1|2}}\,\overline{p_{u_2|0}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|0}}\right)\overline{n_0}}{\overline{p_{u_1|2}}\,\overline{p_{u_2|1}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|1}}}, \tag{B2}$$

under the conditions $n_{10} = n_{01}$, $n_{20} = n_{02}$, $\overline{p_{u_1|2}}\,\overline{p_{u_2|1}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|1}} > 0$, and $\overline{p_{u_1|2}}\,\overline{p_{u_2|0}} - \underline{p_{u_2|2}}\,\underline{p_{u_1|0}} > 0$, where $\overline{n_0} = \min\{n_{00}/\underline{p_{u_0|0}}, 1\}$, $\underline{p_{u_i|k}} = \max\{p_{u_i|k} - \xi(n_{00} + 2n_{01} + 2n_{02} + n_z, 31), 0\}$, and $\overline{p_{u_i|k}} = \min\{p_{u_i|k} + \xi(n_{00} + 2n_{01} + 2n_{02} + n_z, 31), 1\}$. Hence, the lower bound of the number of clicking single-photon pulses n_{s1} in effective events of $\mathbb{Z}$ windows is

$$\underline{n_{s1}} = \frac{n_s}{n_z}\,\underline{p_{u_z|1}}\,\underline{n_1}. \tag{B3}$$

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1985), pp. 175–179.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography Without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[4] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[5] D. Mayers, Quantum key distribution and string oblivious transfer in noisy channels, In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '96 (Springer-Verlag, Berlin, 1996), pp. 343–357.

[6] P. W. Shor and J. Preskill, Simple Proof of Security of the bb84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[7] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[8] H. Inamori, N. Lütkenhaus, and D. Mayers, Unconditional security of practical quantum key distribution, Eur. Phys. J. D **41**, 599 (2007).

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

[10] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).

[11] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[12] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, Phys. Rev. A **75**, 032314 (2007).

[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography

systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[14] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Attacking practical quantum key distribution system with wavelength dependent beam splitter and multi-wavelength sources, Phys. Rev. A **84**, 062308 (2011).

[15] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[16] N. Gisin, S. Pironio, and N. Sangouard, Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier, Phys. Rev. Lett. **105**, 070501 (2010).

[17] M. Curty and T. Moroder, Heralded-qubit amplifiers for practical device-independent quantum key distribution, Phys. Rev. A **84**, 010304(R) (2011).

[18] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, Experimentally Faking the Violation of Bell's Inequalities, Phys. Rev. Lett. **107**, 170404 (2011).

[19] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[20] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[21] R. Y. Q. Cai and V. Scarani, Finite-key analysis for practical implementations of quantum key distribution, New J. Phys. **11**, 045024 (2009).

[22] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita, Security analysis of decoy state quantum key distribution incorporating finite statistics, arXiv:0707.3541 (2007).

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

[24] T.-T. Song, J. Zhang, S.-J. Qin, F. Gao, and Q.-Y. Wen, Finite-key analysis for quantum key distribution with decoy states, Quantum Inf. Comput. **11**, 374 (2011).

[25] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[26] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Finite-key analysis for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 022332 (2012).

[27] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 Km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

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

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

[30] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, Effective eavesdropping to twin field quantum key distribution, arXiv:1805.02272 (2018).

[31] 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).

[32] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[33] 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. Applied **12**, 024061 (2019).

[34] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Applied **11**, 034053 (2019).

[35] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).

[36] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum Key Distribution Through Sending or Not Sending, Phys. Rev. Lett. **123**, 100505 (2019).

[37] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., Wiley Series in Telecommunications and Signal Processing (Wiley, New York, 2006).

[38] Y. Sano, R. Matsumoto, and T. Uyematsu, Secure key rate of the BB84 protocol using finite sample bits, J. Phys. A: Math. Theor. **43**, 495302 (2010).

[39] C. Portmann and R. Renner, Cryptographic security of quantum key distribution, arXiv:1409.3525 (2014).

[40] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, arXiv:1103.4130v2 (2012).

[41] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[42] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[43] C.-H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A **81**, 012318 (2010).