Robust twin-field quantum key distribution through sending or not sending

Cong Jiang\textsuperscript{1,2}, Zong-Wen Yu\textsuperscript{3}, Xiao-Long Hu\textsuperscript{4} and Xiang-Bin Wang \textsuperscript{1,2,5,6,7,*}

ABSTRACT

The sending-or-not-sending (SNS) protocol is one of the most major variants of the twin-field (TF) quantum key distribution (QKD) protocol and has been realized in a 511-km field fiber, the farthest field experiment to date. In practice, however, all decoy-state methods have unavoidable source errors, and the source errors may be non-random, which compromises the security condition of the existing TF-QKD protocols. In this study, we present a general approach for efficiently calculating the SNS protocol's secure key rate with source errors, by establishing the equivalent protocols through virtual attenuation and the tagged model. This makes the first result for TF QKD in practice where source intensity cannot be controlled exactly. Our method can be combined with the two-way classical communication method such as active odd-parity pairing to further improve the key rate. The numerical results show that if the intensity error is within a few percent, the key rate and secure distance only decrease marginally. The key rate of the recent SNS experiment in the 511-km field fiber is still positive using our method presented here, even if there is a $\pm 9.5\%$ intensity fluctuation. This shows that the SNS protocol is robust against source errors.

Keywords: quantum information, quantum key distribution, sending or not sending, twin field, source error

INTRODUCTION

Since the proposal of the twin-field (TF) quantum key distribution (QKD) [1], the longest distance record of QKD has been constantly and rapidly refreshed in recent years [2–9]. The upper bounds of the key rate for previous protocols, such as the BB84 protocol [10–15] and the measurement-device-independent (MDI) QKD protocol [16–22] are limited to the linear scale of channel transmittance, also known as the PLOB bound [23]. Based on single-photon interference, the TF QKD can raise the key rate from a linear scale to a square-root scale of channel transmittance and break the PLOB bound.

As one of the most important variants of TF QKD [24–27], the sending-or-not-sending (SNS) protocol [24] has been extensively studied in theories [28–32] and experiments [2,6–9,33]. Specifically, the 511-km field experiment [8] was done by applying the SNS protocol with the actively odd-parity pairing (AOPP) method, and the 605-km laboratory experiment [9] was done by applying the SNS protocol with the standard two-way classical communication (TWCC) method. The 511-km experiment is the farthest field experiment to date.

Given its great progress [34,35] in both theory and technology, more and more studies of QKD are pointing to real-world applications with various technology limitations.

The TF QKD has typically used with weak coherent state (WCS) sources. The decoy-state method must be used to ensure the security of TF QKD with WCS sources. The intensities of WCS sources are always assumed to be stable in the entire protocol, which is not the fact in experiments where source errors are unavoidable. The source errors, in particular, are not always random. For example, the intensities of the sources can slowly shift over time and are affected by temperature changes in the environment.

Although there are results for decoy-state analysis with source errors for the BB84 and MDI-QKD protocols [36,37], they do not solve the problem for the SNS protocol where encoding is done by the vacuum and single-photon states themselves. To
calculate the key rate, we need a way to estimate the single-photon phase-flip error rate. It is not a trivial task because the single-photon state in the X basis is now different from that in the Z basis. We solve this problem by virtual attenuation and then apply the existing theory for decoy-state analysis with intensity fluctuation.

The work is organized as follows. First, we introduce the real and virtual protocols and demonstrate their equivalence. This shows how to efficiently calculate the secure key rate in a practical application where intensities cannot be controlled exactly. Then we present some numerical results that compare the key rates of the SNS protocol with different degrees of source errors.

THE SECURITY OF THE SNS PROTOCOL WITH SOURCE ERRORS

For ease of presentation, here we introduce the SNS protocol through the four-intensity model. The scientific content is the same as in the earlier literature.

We take the four-intensity SNS protocol as an example to show the security proof. There are four sources with different intensities on Alice’s and Bob’s sides. We denote Alice’s sources by $a_0, a_1, a_2$ and $a_z$, and Bob’s sources by $b_0, b_1, b_2$ and $b_z$, where $a_0$ and $b_0$ are the vacuum sources. WCS sources are typically used to perform the SNS protocol. If the sources are stable, the intensities of sources $a_l$ and $b_r$ are $\mu_{a_l}$ and $\mu_{b_r}$, respectively, for $l, r = 0, 1, 2, z$, where $\mu_{a_0} = \mu_{b_0} = 0$. However, in practice, the sources are always unstable and the intensities are different in different time windows. The intensities of the sources in the $i$th time window are denoted $\mu_{a_i}^l$ and $\mu_{b_i}^l$, where

$$
\mu_{a_i}^l = (1 + \delta_{a_i}^l)\mu_{a_i}, \quad \mu_{b_i}^l = (1 + \delta_{b_i}^l)\mu_{b_i}
$$

(1)

and $|\delta_{a_i}^l| \leq \delta_{a_i}, |\delta_{b_i}^l| \leq \delta_{b_i}$. We assume that $\delta_{a_i}$ and $\delta_{b_i}$ are known values in the protocol. The lower and upper bounds of a physical quantity are represented by superscripts $L$ and $U$, respectively. For instance, $\mu_{a_i}^U$ is the upper bound of the intensity of source $a_i$, and we have $\mu_{a_i}^U = (1 + \delta_{a_i})\mu_{a_i}$.

The real protocol

Alice (Bob) randomly decides whether the $i$th time window is a decoy window or a signal window with probabilities $1 - p_{a_i}$ and $p_{a_i} (1 - p_{b_i}$ and $p_{b_i})$. If it is a decoy window, Alice (Bob) randomly chooses sources $a_0, a_1, a_2, b_0, b_1, b_2$ with probabilities $1 - p_{a_i}, p_{a_i}, 1 - p_{b_i}, p_{b_i}$. Since the sources are unstable, Alice (Bob) actually prepares a WCS pulse in state $|e^{i\theta_{a_i}^l}\sqrt{\mu_{a_i}^l}\rangle (|e^{i\theta_{b_i}^l}\sqrt{\mu_{b_i}^l}\rangle$ if source $a_i (b_i)$ is chosen for $l, r = 1, 2$, where $\theta_{a_i}$ and $\theta_{b_i}$ are random in $[0, 2\pi)$. The imaginary unit is represented here by the symbol $\imath$. If it is a signal window, Alice (Bob) randomly chooses sources $a_0, a_z (b_0, b_z)$ with probabilities $1 - \epsilon_{a}, \epsilon_{a} (1 - \epsilon_{b}, \epsilon_{b})$. Alice (Bob) actually prepares a phase-randomized WCS pulse with intensity $\mu_{a_i}^l (\mu_{b_i}^l)$ if source $a_i (b_i)$ is chosen. Clearly, if Alice (Bob) commits to a signal window at time $i$, Alice’s (Bob’s) choice of source $a_i (b_i)$ indicates a decision of sending whereas the choice of source $a_0 (b_0)$ is a decision of not sending in the SNS protocol.

They (Alice and Bob) send the prepared pulse pair to Charlie, who is assumed to perform interferometric measurements on the received pulse pair. Then Charlie announces the measurement results to them. If only one detector clicks, they would take it as a one-detector heralded event. After they repeat the above process $N$ times and Charlie announces all measurement results, they acquire a series of data. Then they perform the data post-processing, including post-selection of events in $X$ windows and final key distillation.

They first announce the type of time window they choose, i.e. whether it is a decoy window or a signal window. For a time window that both of them decide is a signal window, it is a $Z$ window. The one-detector heralded events in $Z$ windows are effective events, and the corresponding bits of those effective events form the $n_i$-bit raw key strings, which are used to extract the final keys. We also define the $\bar{Z}$ window as a $Z$ window when sources $\{a_0, b_0\}$ or $\{a_z, b_0\}$ are used, i.e. a $Z$ window when one side decides sending and the other side decides not sending. The untagged pulses in the $Z$ windows are that Alice decides not sending and Bob actually sends out a single-photon pulse or Bob decides not sending and Alice actually sends out a single-photon pulse, i.e. the single-photon pulses in the $\bar{Z}$ windows. The untagged bits are the corresponding bits of those untagged pulses that cause effective events. Except the $Z$ windows, they announce the intensities of the pulses in each window, and for time windows that both of them decide sending out a pulse of sources $a_1$ and $b_1$, respectively, they also announce the phases of the pulse pairs. For a time window that both of them decide sending out a pulse of sources $a_1$ and $b_1$, respectively, and their phases satisfy the post-selection criteria [24], it is defined as an $X$ window. The one-detector heralded events in $X$ windows are effective events. The effective events in $X$ windows are used to estimate the phase-flip error rate.
According to Hu and Jiang [30], if the sources are stable, and source $a_z$ ($b_z$) always emits a state of $\rho_{a_z} = \sum_{k=0}^{\infty} q_A^k |k\rangle\langle k|$, $\rho_{b_z} = \sum_{k=0}^{\infty} q_B^k |k\rangle\langle k|$, we can use the following constraint for the source for security:

$$\frac{\mu_{a_i}}{\mu_{b_i}} = \epsilon_a(1 - \epsilon_b)q_A^i / \epsilon_b(1 - \epsilon_a)q_B^i. \quad (2)$$

Here $|k\rangle\langle k|$ represents a $k$-photon Fock state. In particular, when using a phase randomized WCS source with intensity $\mu_{a_z}$ ($\mu_{b_z}$) for source $a_z$ ($b_z$), $q_A^i, q_B^i$ in (2) can be replaced by $\mu_{a_z}\epsilon^{-\mu_{a_z}}, \mu_{b_z}\epsilon^{-\mu_{b_z}}$. Note that, if the constraint above is respected, the density matrix of the single-photon state in $Z$ windows is identical to that of the $X$ basis and hence we can faithfully verify the phase-flip error rate of untaged bits by observing events in $X$ windows.

Given stable sources with the source parameters known, the SNS protocol is still secure and efficient even if (2) does not hold. Most straightforwardly, we can post-select the sending probabilities $\epsilon_a, \epsilon_b$ by randomly deleting some of the time windows [6], i.e. to make (2) hold by post-deletion. (Post-deleting a time window means disregarding the event happening at that time window.) Although the amount of data is reduced by the post-deletion, the key rate will essentially be unchanged if the original bias between the two sides of (2) is not too large, because, after post-deletion, the error rate of raw keys is also decreased.

The more practical situation is that we do not know the exact intensities of the sources of the $Z$ windows but we know the bound values of intensities for each source of $Z$ window. In such a case, we can use the tagged model: replace the intensities of (2) by a lower bound value and make (2) hold.

Most generally, the source intensities of $X$ windows are also unstable. Say, in practice, that none of the sources are stable, and that the intensity errors may be different from time to time and not necessarily random. In such a case, Eve can treat different time windows differently; thus, we cannot treat the $X$ windows as a whole, but have to deal with each time window separately. The intensities of sources $a_1, b_1$ in different time windows are different, which means that, in general,

$$\frac{\mu_{a_i}}{\mu_{b_i}} \neq \frac{\mu_{a_j}}{\mu_{b_j}} \quad (3)$$

if $i \neq j$. When (2) holds, the bit-flip error rate of $X$ windows can be used to estimate the phase-flip error rate of the untaged bits according to the data in $X$ windows. The situation is different for the decoy-state BB84 protocol with source errors [36], or the decoy-state MDI QKD [16,22] where the source errors do not change the encoding states in $X$ windows or $Z$ windows, it affects the decoy-state analysis only [36,37].

In this work, we solve this problem based on the SNS protocol and make the TF QKD robust with imperfect real set-ups.

**Main idea: quantum security from virtual attenuation**

The state preparation stage of the real protocol can be regarded as follows. At every time window $i$, Alice (Bob) has four candidate states emitted from the four sources $a_0, a_1, a_2, a_z (b_0, b_1, b_2, b_z)$. In particular, the intensities of the coherent states emitted by sources $a_0, b_0$ are $\mu_{a_z}, \mu_{b_z}$ for $l = 1, 2, z$, respectively. Sources $a_0, b_0$ emit vacuum only. Alice (Bob) will choose one state from the four candidate states for time window $i$, by the probabilities stated earlier in the real protocol.

Our first major idea is mapping by (virtual) attenuation [38]. We regard the candidate states above as the attenuation outcome from virtual sources $a_0, a_1, a_z (b_0, b_1, b_2, b_z)$ and the intensity of the WCS pulse from virtual source $a_1 (b_1)$ is fixed to $\mu_{a_z}^1 (\mu_{b_z}^1)$ exactly at any time window $i$. This naturally means that the transmittance $\eta_{a_z} = (1 + \delta_{a_z})/(1 + \delta_{a_z})$ $[\eta_{b_z} = (1 + \delta_{b_z})/(1 + \delta_{b_z})]$ in the virtual attenuation of the $i$th time window, and hence the intensities of the WCS pulses from virtual sources $a_z, a_z (b_z, b_z)$ are $\mu_{a_z}^i = \mu_{a_z}^1/\eta_{a_z}$, $\mu_{a_z}^i = \mu_{a_z}^1/\eta_{a_z}$, $\mu_{b_z}^i = \mu_{b_z}^1/\eta_{b_z}$, $\mu_{b_z}^i = \mu_{b_z}^1/\eta_{b_z}$, respectively. For simplicity, we just call the SNS protocol using virtual (real) sources above the virtual protocol (real protocol). Surely, the real protocol above is secure provided that the virtual protocol above is secure. This holds even though Eve knew the exact values of the intensity fluctuation for each source in every time window $i$. Or, equivalently, even though Eve knew the exact values of $\eta_{a_z}, \eta_{b_z}$. If Eve can use scheme $G$ to attack the real protocol, Eve can also attack the virtual protocol by first taking attenuation $[\eta_{a_z}^*, \eta_{b_z}^*]$ to pulses in the virtual protocol and then using attacking scheme $G$. Surely, we can obtain the secure key rate for the real protocol above by calculating the secure key rate of the virtual protocol, because the two protocols cause no difference to the outside lab.

Our second major idea is to treat the intensity fluctuation for states of the $Z$ windows using the tagged model. Consider the key rate calculation for our virtual protocol above. In that protocol, at time
window $i$, the intensity of the pulse from virtual source $a'_z(b'_z)$ is $\mu_{a'_z}^{i}(\mu_{b'_z}^{i})$. This in general does not respect (2). However, in $Z$ windows, there does exist a subset of single-photon pulses that are indistinguishable from the single photons in $X$ windows, and there does exist an efficient method to verify the lower bound of the size of this subset. Thus, the key rate can be effectively calculated.

The third major idea here is to verify the lower bound values of the untagged bits in $Z$ windows and their corresponding upper bound value of the phase-flip error rate, by applying the existing decoy-state method with source errors [36]. Note that in the virtual protocol above, the intensities of the stronger decoy pulses are not stable. According to the existing theory, we only need to use the lower bound values of the photon number distribution coefficients to obtain the worst-case result. With these, the final key rate can be calculated. Furthermore, we can apply the TWCC method such as AOPP to improve the key rate [31,32].

**Virtual protocol 1**

In the $i$th time window of virtual protocol 1, the pulses emitted by sources $a_1, a_2, a_z, (b_1, b_2, b_z)$ are different from those of the real protocol. To avoid confusion, we use the notation $a_0, a'_1, a'_2, a'_z (b_0, b'_1, b'_2, b'_z)$ for Alice’s (Bob’s) sources in virtual protocol 1.

In the $i$th time window, Alice (Bob) randomly decides it is a decoy window or a signal window with probabilities $1 - p_a$ and $p_a$. If it is a decoy window, Alice (Bob) randomly chooses sources $a_0, a'_1, a'_2 (b_0, b'_1, b'_2)$ with probabilities $p_a = 1 - p_{a_1} - p_{a_2}, p_{a_z}, p_{a_0}, p_{b_0} = 1 - p_{b_1} - p_{b_2}, p_{b_1}, p_{b_2}$. If source $a'_i (b'_i)$ is chosen, Alice (Bob) actually prepares a WCS pulse in state $|e^{i\theta_i}\sqrt{\mu_{a'_i}}\rangle \langle e^{i\theta_i}\sqrt{\mu_{b'_i}}\rangle$, where $\mu_{a'_i} = (1 + \delta_{a_i})\mu_{a_i}$ and $\mu_{b'_i} = (1 + \delta_{b_i})\mu_{b_i}$. If source $a'_i (b'_i)$ is chosen, Alice (Bob) actually prepares a WCS pulse in state $|e^{i\theta_i}\sqrt{\mu_{a'_i}}\rangle \langle e^{i\theta_i}\sqrt{\mu_{b'_i}}\rangle$, where

$$\mu_{a_i}^{i} = \frac{1 + \delta_{a_i}}{1 + \delta_{a_i}} \mu_{a_i}, \quad \mu_{b_i}^{i} = \frac{1 + \delta_{b_i}}{1 + \delta_{b_i}} \mu_{b_i}.$$  

(4)

If it is a signal window, Alice (Bob) randomly chooses sources $a_0, a'_z (b_0, b'_z)$ with probabilities $1 - e_{a}, e_{a} (1 - e_{b}, e_{b})$. Alice (Bob) actually prepares a phase-randomized WCS pulse with intensity $\mu_{a'_z}^{i}(\mu_{b'_z}^{i})$ if source $a'_z (b'_z)$ is chosen, where

$$\mu_{a'_z}^{i} = \frac{1 + \delta_{a_z}}{1 + \delta_{a_z}} \mu_{a_z}, \quad \mu_{b'_z}^{i} = \frac{1 + \delta_{b_z}}{1 + \delta_{b_z}} \mu_{b_z}.$$  

(5)

**Figure 1.** Comparison between the (a) real protocol and (b) virtual protocol 1. Here the boxes labeled ‘D’ represent Charlie’s detectors and ATT represents the attenuator. Although the sources of the real protocol and virtual protocol 1 are different, Eve cannot distinguish the differences due to the proper set attenuators.

Then they send out the prepared pulse pair. There are two attenuators between the channel and Alice’s and Bob’s labs, which are controlled by David. To clarify, we define the attenuator on Alice’s side as attenuator $A$ and the attenuator on Bob’s side as attenuator $B$. In the $i$th time window, David sets the transmittance of attenuator $A$ to $\eta_{A}^{i} = (1 + \delta_{a_i})/(1 + \delta_{a_i})$ and the transmittance of attenuator $B$ to $\eta_{B}^{i} = (1 + \delta_{b_i})/(1 + \delta_{b_i})$. Then we have

$$\mu_{a_i}^{i} = \eta_{A}^{i}\mu_{a_i}, \quad \mu_{b_i}^{i} = \eta_{A}^{i}\mu_{b_i}, \quad \mu_{a_i}^{i} = \eta_{A}^{i}\mu_{a_i}, \quad \mu_{b_i}^{i} = \eta_{A}^{i}\mu_{b_i}.$$  

(6)

Equations (6) mean that the real protocol and virtual protocol 1 are equivalent to Eve who is assumed to control the channel and detectors. Thus, the information leakages in the real protocol and virtual protocol 1 are the same and we can use virtual protocol 1 to estimate the key rate of the real protocol. A simple comparison of the real protocol and virtual protocol 1 is shown in Fig. 1.

Note that in virtual protocol 1 sources $a'_i$ and $b'_i$ are stable, bringing us one step closer to the final goal. However, due to the unstable sources in the $Z$ windows, security condition (2) is not always satisfied. Recall that the untagged pulses in the $Z$ windows are the single-photon pulses in the $Z$ windows. This means that we should only need to care about the single-photon pulse of sources $a'_z, b'_z$. The density matrix of a phase-randomized WCS pulse with intensity $\mu$ is

$$\rho_{\mu} = \sum_{k=0}^{+\infty} \frac{\mu^k e^{-\mu}}{k!} |k\rangle \langle k|.$$  

(7)

Although source $a'_z$ is unstable, the density matrix of the pulse from this source in the $i$th time window.
can be expressed in the convex form

\[ \rho_{\mu a_i} = c_{a_i}^1 |1\rangle\langle 1| + (1 - c_{a_i}^1) \rho_{a_i}^i, \quad (8) \]

where

\[ \rho_{a_i}^i = \frac{1}{1 - c_{a_i}^1} \left[ (\mu_{a_i}^U e^{-\mu_{a_i}^U} - c_{a_i}^1)|1\rangle\langle 1| \right. \]

\[ \times |1\rangle + e^{-\mu_{a_i}^U} |0\rangle\langle 0| \]

\[ + \sum_{k=2}^{+\infty} \frac{(\mu_{a_i}^U)^k e^{-\mu_{a_i}^U}}{k!} |k\rangle\langle k| \quad (9) \]

for \( c_{a_i}^1 \leq \mu_{a_i}^U e^{-\mu_{a_i}^U} \). And, if \( c_{a_i}^1 \leq \mu_{a_i}^U e^{-\mu_{a_i}^U} \), the density matrices of all pulses of source \( a_z^c \) have the similar convex form as shown in (8), where the only differences are \( \rho_{a_i}^i \) for different time windows. But, as stated before, we only need to care about the single-photon pulse of source \( a_z^c \); thus, as long as \( c_{a_i}^1 \leq \mu_{a_i}^U e^{-\mu_{a_i}^U} \), we can take the unstable source \( a_z^c \) as the mixture of two sources: one stable source \( a_z^c \) with probability \( c_{a_i}^1 \) and one unstable source \( a_z^c \) with probability \( 1 - c_{a_i}^1 \), where source \( a_z^c \) only emits perfect single-photon pulses and source \( a_z^c \) emits pulses in state \( \rho_{a_i}^i \).

For the unstable source \( b_z^c \), the density matrix of the pulse in the \( i \)th time window is

\[ \rho_{\mu b_z} = c_{b_z}^1 |1\rangle\langle 1| + (1 - c_{b_z}^1) \rho_{b_z}^i, \quad (10) \]

where

\[ \rho_{b_z}^i = \frac{1}{1 - c_{b_z}^1} \left[ (\mu_{b_z}^U e^{-\mu_{b_z}^U} - c_{b_z}^1)|1\rangle\langle 1| \right. \]

\[ \times |1\rangle + e^{-\mu_{b_z}^U} |0\rangle\langle 0| \]

\[ + \sum_{k=2}^{+\infty} \frac{(\mu_{b_z}^U)^k e^{-\mu_{b_z}^U}}{k!} |k\rangle\langle k| \quad (11) \]

for \( c_{b_z}^1 \leq \mu_{b_z}^U e^{-\mu_{b_z}^U} \). As long as \( c_{b_z}^1 \leq \mu_{b_z}^U e^{-\mu_{b_z}^U} \), the unstable source \( b_z^c \) can be regarded as the mixture of two sources: one stable source \( b_z^c \) with probability \( c_{b_z}^1 \) and one unstable source \( b_z^c \) with probability \( 1 - c_{b_z}^1 \), where source \( b_z^c \) only emits perfect single-photon pulses and \( b_z^c \) emits pulses in state \( \rho_{b_z}^i \). With this, we have the following virtual protocol 2.

**Virtual protocol 2**

In the \( i \)th time window, Alice (Bob) randomly decides it is a decoy window or a signal window with probabilities \( 1 - p_{a_i} \) and \( p_{a_i} \). If it is a decoy window, Alice (Bob) randomly chooses sources \( a_0, a_z^c, a_z^c (b_0, b_z^c) \) with probabilities \( p_{a_0} = 1 - p_{a_i} - p_{a_i}, p_{a_i} \). If it is a signal window, Alice (Bob) randomly chooses sources \( a_0, a_z^c, a_z^c (b_0, b_z^c) \) with probabilities \( 1 - p_{b_i}, p_{b_i} \). Then, as stated before, we only need to care about the single-photon pulse of source \( a_z^c \); thus, as long as \( c_{a_i}^1 \leq \mu_{a_i}^U e^{-\mu_{a_i}^U} \), we can take the unstable source \( a_z^c \) as the mixture of two sources: one stable source \( a_z^c \) with probability \( c_{a_i}^1 \) and one unstable source \( a_z^c \) with probability \( 1 - c_{a_i}^1 \), where source \( a_z^c \) only emits perfect single-photon pulses and source \( a_z^c \) emits pulses in state \( \rho_{a_i}^i \). With this, we have the following virtual protocol 2.

\[ p_{a_0} = 1 - p_{a_i} - p_{a_i}, p_{a_i} (p_{b_0} = 1 - p_{b_i} - p_{b_i}, p_{b_i}). \]

Furthermore, only sources \( a_z^c \) and \( b_z^c \) are unstable in virtual protocol 2. The remaining problems are estimating the lower bound of the number of untagged bits and the upper bound of the phase-flip error rate, both of which can be solved by directly applying the conclusion of [36]. Finally, using the method introduced in [28,29], we can obtain the final key rate. We can also use the OAPS method to improve the key rate [31,32]. The calculation details are shown in Section 1 within the online supplementary material.

**Major results**

1. Given the unstable sources as presented in the real protocol, we map them to virtual sources by virtual
attenuation and the tagged model, as shown in virtual protocol 2.

2. In virtual protocol 2, sources $a_1'$ and $b_1'$ are stable, with exactly known intensities, and sources $a_2'$ and $b_2'$ are perfect single-photon sources, while other non-vacuum sources are unstable, with known bounds.

3. Regard the observed values in the real protocol to be those of the virtual protocol, and use decoy-state analysis to verify the values $n_1'$ and $\epsilon_1^{ph,U}$, which are the lower bound value of the number of untagged bits in $Z$ windows and the upper bound value of the phase-flip error rate.

4. Calculate the key rate for the real protocol using the formula

$$R = \frac{1}{N} \left\{ n_1' \left[ 1 - H(\epsilon_1^{ph,U}) \right] - f n_t H(E) \right\} - \log_2 \left( \frac{2}{\epsilon_{cor}} \right) - 2 \log_2 \left( \frac{1}{\sqrt{2E_{PA}\epsilon}} \right),$$

(16)

where $N$ represents the total number of pulse pairs sent by Alice and Bob, $f$ represents the error correction inefficiency, $n_t$ represents the number of effective events in the $Z$ windows and $E$ represents the error rate of the raw keys in the $Z$ windows. As shown in [19,29], the tailing term of $-\log_2 \left( \frac{2}{\epsilon_{cor}} \right) - 2 \log_2 \left( \frac{1}{\sqrt{2E_{PA}\epsilon}} \right)$ is the additional cost for security with finite size. The calculation details are shown in Section 1 within the online supplementary material. As detailed in the online supplementary material, our method does not presume the source errors to be random. Our protocol assumes that Eve can know or even determine the error values of all those candidate states in advance, so they surely are not limited to being random errors only. For security, the decoy-state method requests that Eve has no information in advance about the secret state choice of Alice and Bob, i.e. choosing the pulse of which source to send out by Alice and Bob for each time window. To keep this condition, our method requests that the values of intensity errors that can be known to Eve in advance do not carry any private information about the state choice of Alice and Bob. With this presumption being respected, our method allows whatever dependence of intensity errors from different time windows.

5. The AOPP method is directly applicable here. Suppose that Bob generates the active odd-parity random pairing and then informs Alice of the positions of two bits in raw keys for each pair. Following the parity check, all pairs with odd-parity values at Alice’s side survive, and one bit from each survived pair is chosen at random for final key distillation. That is, in the AOPP, a pair with two untagged bits will always contribute an untagged bit to the final key distillation. Those pairs with even-parity values on Alice’s side will be completely discarded. We have the following final key length formula after AOPP:

$$R' = \frac{1}{N} \left\{ n_1' \left[ 1 - H(\epsilon_1^{ph,U}) \right] - f n_t' H(E') \right\} - \log_2 \left( \frac{2}{\epsilon_{cor}} \right) - 4 \log_2 \left( \frac{1}{\sqrt{2E_{PA}\epsilon}} \right),$$

(17)

Here $n_1'$ is the lower bound of untagged bits after AOPP, $\epsilon_1^{ph,U}$ is the upper bound of the phase-flip error rate after AOPP, $n_t'$ is the number of survived bits after AOPP and $E$ is the bit-flip error rate of the survived bits after AOPP. Details are shown in Section 1 within the online supplementary material.

### NUMERICAL SIMULATION

We use the linear model to simulate the observed values [28], and Charlie’s detectors are assumed to be identical, that is, they have the same detection efficiency and dark counting rate. For simplicity, we assume that the maximum derivations of all sources are the same, i.e. $\delta_{\alpha_0} = \delta_{\beta_0} = \delta$ for $l, r = 1, 2, z$. The experimental parameters are listed in Table 1.

Figures 2 and 3 are the key rates of the original SNS protocol and the SNS protocol with the AOPP method under different degrees of intensity fluctuation. We assume a symmetric channel, which means that the distance between Alice and Charlie, $L_{AC}$, equals the distance between Bob and Charlie, $L_{BC}$. Figures 2 and 3 show that the key rates and farthest distance decrease slightly as the intensity fluctuation range increases. Figure 4 shows the comparison between the key rates of the original SNS protocol and the SNS protocol with the AOPP method under different degrees of intensity fluctuation, where we set $L_{AC} = L_{BC} = 50$ km. The key rates at a distance of 350 km are shown in Table 3 below, where the experimental parameters are the same as those of Fig. 4.

In Figs 2–4, the absolute PLOB bound is for the case of

| $pd$ | $\varepsilon_\beta$ | $\eta_\beta$ | $f$ | $\alpha$ | $\xi$ | $N$ |
|------|----------------|-------------|------|---------|------|-----|
| $1.0 \times 10^{-8}$ | 4% | 60.0% | 1.1 | 0.2 | $1.0 \times 10^{-10}$ | $1.0 \times 10^{13}$ |

Table 1. List of experimental parameters used in numerical simulations. Here $\rho_d$ is the dark counting rate per pulse of Charlie’s detectors, $\varepsilon_\beta$ is the misalignment-error probability, $\eta_\beta$ is the detection efficiency of Charlie’s detectors, $f$ is the error correction inefficiency, $\alpha$ is the fiber loss coefficient (dB/km), $\xi$ is the failure probability while using Chernoff’s bound [39] and $N$ is the number of total pulse pairs sent out in the protocol.
Figure 2. The key rates of the original SNS protocol under different degrees of intensity fluctuation. The absolute PLOB bound is the PLOB bound with 100% detection efficiency detectors. Here we assume the symmetric channel, i.e. the distance between Alice and Charlie, $L_{AC}$, equals the distance between Bob and Charlie, $L_{BC}$. The experimental parameters are listed in Table 1.

Figure 3. The key rates of the SNS protocol with AOPP under different degrees of intensity fluctuation. The absolute PLOB bound is the PLOB bound with 100% detection efficiency detectors. Here we assume the symmetric channel, i.e. the distance between Alice and Charlie, $L_{AC}$, equals the distance between Bob and Charlie, $L_{BC}$. The experimental parameters are listed in Table 1.

Figure 4. Comparison between the key rates of the original SNS protocol and the SNS protocol with AOPP method under different degrees of intensity fluctuation. The absolute PLOB bound is the PLOB bound with 100% detection efficiency detectors. Here we assume the asymmetric channel, where the distance between Alice and Charlie, $L_{AC}$, and the distance between Bob and Charlie, $L_{BC}$, satisfy $L_{AC} - L_{BC} = 50$ km. The experimental parameters are listed in Table 1.

We use a more efficient method to calculate the key rates of the AOPP SNS in Table 3, by scanning the expected value of the counting rate of vacuum sources $\langle S_{00} \rangle$ in its range, which is

$$R'' = \min_{\langle S_{00} \rangle} R'(\langle S_{00} \rangle),$$

and this can improve the non-asymptotic key rate a little bit. The results in Table 3 show that the key rates of AOPP with 5% intensity fluctuation are still higher than those of the original SNS protocol without intensity fluctuation. From Table 3 we can see that every 1% intensity fluctuation causes a 4% drop in the key rate, which shows that the SNS protocol is robust against source errors.

The AOPP method was used in the SNS experiment in a 511-km field fiber to achieve a higher key rate [8]. We calculate the key rate of this experiment if there are source errors using the experimentally observed values shown in [8], and the results show that the key rate is still positive even if $\delta$ is as large as 9.5%.

In the security proof and numerical simulation above, we assume that the intensities of the pulses are in a certain interval. But a more practical case is that very few pulses can exceed the bound values and we can only determine at most the number of pulses outside the interval with a small failure probability. We show how to calculate the key rate under this case in Section 4 within the online supplementary material.
Table 2. The key rates and distances corresponding to the first intersections between the absolute PLOB bound and the key rate curves in Figs 2–4. Here the results of the original method with symmetric channel are the intersections in Fig. 2; the results of the AOPP method with symmetric channel are the intersections in Fig. 3; the results of the AOPP and original methods with asymmetric channel are the intersections in Fig. 4.

| δ     | 0%       | 2%       | 5%       | 0%       | 2%       | 5%       |
|-------|----------|----------|----------|----------|----------|----------|
| Channel | Symmetric | Symmetric | Symmetric | Symmetric | Symmetric | Symmetric |
| Method |          |          |          |          |          |          |
| AOPP   |          |          |          |          |          |          |
| Distance | 233      | 237      | 241      | 263      | 267      | 272      |
| Key rate | \(3.16 \times 10^{-5}\) | \(2.67 \times 10^{-5}\) | \(2.18 \times 10^{-5}\) | \(8.00 \times 10^{-6}\) | \(6.66 \times 10^{-6}\) | \(5.24 \times 10^{-6}\) |
| Channel |          |          |          |          |          |          |
| AOPP   |          |          |          |          |          |          |
| Distance | 246      | 250      | 256      | 280      | 284      | 291      |
| Key rate | \(1.73 \times 10^{-5}\) | \(1.44 \times 10^{-5}\) | \(1.11 \times 10^{-5}\) | \(3.66 \times 10^{-6}\) | \(3.00 \times 10^{-6}\) | \(2.18 \times 10^{-6}\) |

Table 3. The key rates of the original SNS protocol and the AOPP method under different degrees of intensity fluctuation. The distance between Alice and Bob is 350 km, and the experimental parameters are the same as those of Fig. 4. In our simulation, the fluctuation parameter \(\delta\) is between \(-\delta\) and \(\delta\). For example, \(\delta = 10\%\) means a fluctuating range of 20%, from \(-10\%\) to \(+10\%\).

| δ     | 0%       | 2%       | 5%       | 10%      |
|-------|----------|----------|----------|----------|
| Original SNS | \(5.8 \times 10^{-7}\) | \(5.15 \times 10^{-7}\) | \(4.35 \times 10^{-7}\) | \(3.26 \times 10^{-7}\) |
| AOPP SNS    | \(1.33 \times 10^{-6}\) | \(1.20 \times 10^{-6}\) | \(1.05 \times 10^{-6}\) | \(8.46 \times 10^{-7}\) |

CONCLUSION

In this study, we propose a strict method for calculating the key rate of the SNS protocol with source errors, by establishing the equivalent protocols through virtual attenuation and the tagged model. We finally obtain the key rate formulas under the premise of ensuring the protocol’s security. Our method can be combined with the AOPP method to further improve the key rate. The numerical results show that every 1% intensity fluctuation causes a 4% drop in the key rate; additionally, the SNS protocol’s farthest distance slightly decreases as the intensity fluctuation range increases, indicating that the SNS protocol is robust against source errors. Our method can be directly applied to the three-intensity SNS protocol with source error where ‘three intensity’ refers to \(\mu_{a_1} = \mu_{a_2}, \mu_{b_1} = \mu_{b_2}\).

Since our method, on the one hand, allows Eve to know the error values of candidate pulses in advance and, on the other hand, requests no information leakage of the state choice, the errors must be independent of the state choice in applying our method [40]. With this condition being respected, our method applies to errors inside the bound values with whatever patterns or correlations of intensities among different time windows, as shown in the online supplementary material. Our method does not work with crossing correlations between intensity errors and the state choice at different time windows, say, setting-choice-dependent errors [41–43], because such types of crossing correlations obviously lead to the state-choice information leakage to Eve if she knows the error values in advance. It is an interesting problem for future study on the setting-choice-dependent errors [41–43] with TF-QKD protocols.

SUPPLEMENTARY DATA

Supplementary data are available at NSR online.

FUNDING

This work was supported by the Ministry of Science and Technology of China through National Key Research and Development Program of China (2020YFA0309701); National Natural Science Foundation of China (12174215, 12104184, 11774198 and 11974204); Shandong Provincial Natural Science Foundation (ZR2021LLZ007); Key R&D Plan of Shandong Province (2021ZDPT01); Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics (KF202110); and Leading Talents of Quancheng Industry.
AUTHOR CONTRIBUTIONS

C.J. and X.-B.W. conceived the research and developed the security proof. C.J., Z.-W.Y. and X.-L.H. performed the numerical simulation. All authors performed the data analysis and prepared the manuscript.

Conflict of interest statement. None declared.

REFERENCES

1. Lucamarini M, Yuan ZL and Dynes JF et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature 2018; 557: 400–3.
2. Liu Y, Yu ZW and Zhang W et al. Experimental twin-field quantum key distribution through sending or not sending. Phys Rev Lett 2019; 123: 100505.
3. Wang S, He DY and Yin ZQ et al. Beating the fundamental rate–distance limit in a proof-of-principle quantum key distribution system. Phys Rev X 2019; 9: 021046.
4. Zhong X, Hu J and Curty M et al. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. Phys Rev Lett 2019; 123: 100506.
5. Fang XT, Zeng P and Liu H et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. Nat Photonics 2020; 14: 422–5.
6. Chen JP, Zhang C and Liu Y et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. Phys Rev Lett 2020; 124: 070501.
7. Liu H, Jiang C and Zhu HT et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. Phys Rev Lett 2021; 126: 250602.
8. Chen JP, Zhang C and Liu Y et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat Photonics 2021; 15: 570–5.
9. Pittaluga M, Minder M and Lucamarini M et al. 600 km repeater-like quantum communications with dual-band stabilisation. Nat Photonics 2021; 15: 530–5.
10. Bennett CH and Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing 1984; 175–9.
11. Hwang WY. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett 2003; 91: 057901.
12. Wang XB. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett 2005; 94: 230503.
13. Lo HK, Ma X and Chen K. Decoy state quantum key distribution. Phys Rev Lett 2005; 94: 230504.
14. Lim CCW, Curty M and Walenta N et al. Concise security bounds for practical decoy-state quantum key distribution. Phys Rev A 2014; 89: 022307.
15. Boaron A, Bosco G and Rusca D et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett 2018; 121: 190502.
16. Lo HK, Curty M and Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett 2012; 108: 130503.
17. Braunstein SL and Pirandola S. Sidelband-free quantum key distribution. Phys Rev Lett 2012; 108: 130502.
18. Wang XB. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. Phys Rev A 2013; 87: 012320.
19. Curty M, Xu F and Cui W et al. Finite-key analysis for measurement-device-independent quantum key distribution. Nat Commun 2014; 5: 4732.
20. Xu F, Xu H and Lo HK. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. Phys Rev A 2014; 89: 052333.
21. Yu ZW, Zhou YH and Wang XB. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. Phys Rev A 2015; 91: 032318.
22. Zhou YH, Yu ZW and Wang XB. Making the decoy-state measurement-device-independent quantum key distribution practically useful. Phys Rev A 2016; 93: 042324.
23. Pirandola S, Laurenza R and Ottaviani C et al. Fundamental limits of repeaterless quantum communications. Nat Commun 2017; 8: 15043.
24. Wang XB, Yu ZW and Hu XL. Twin-field quantum key distribution with large misalignment error. Phys Rev A 2018; 98: 062323.
25. Tamaki K, Lo HK and Wang W et al. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. arXiv:1805.05511v3.
26. Cui C, Yin ZQ and Wang R et al. Twin-field quantum key distribution without phase postselection. Phys Rev Appl 2019; 11: 034053.
27. Curty M, Azuma K and Lo HK. Simple security proof of twin-field type quantum key distribution protocol. npj Quantum Inf 2019; 5: 64.
28. Yu ZW, Hu XL and Jiang C et al. Sending-or-not-sending twin-field quantum key distribution in practice. Sci Rep 2019; 9: 3080.
29. Jiang C, Yu ZW and Hu XL et al. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. Phys Rev Appl 2019; 12: 024061.
30. Hu XL, Jiang C and Yu ZW et al. Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters. Phys Rev A 2019; 100: 062337.
31. Xu H, Yu ZW and Jiang C et al. Sending-or-not-sending twin-field quantum key distribution: breaking the direct transmission key rate. Phys Rev A 2020; 101: 042330.
32. Jiang C, Hu XL and Yu ZW et al. Composable security for practical quantum key distribution with two way classical communication. New J Phys 2021; 23: 063038.
33. Olivieri C, Meda A and Donadello S et al. Coherent phase transfer for real-world twin-field quantum key distribution. Nat Commun 2022; 13: 157.
34. Pirandola S, Andersen UL and Banchi L et al. Advances in quantum cryptography. Adv Opt Photonics 2020; 12: 1012–236.
35. Xu F, Ma X and Zhang Q et al. Secure quantum key distribution with realistic devices. Rev Mod Phys 2020; 92: 025002.
36. Wang XB, Peng CZ and Zhang J et al. General theory of decoy-state quantum cryptography with source errors. Phys Rev A 2008; 77: 042311.
37. Jiang C, Yu ZW and Wang XB. Measurement-device-independent quantum key distribution with source state errors in photon number spaces. Phys Rev A 2016; 94: 062323.
38. Wang XB, Peng CZ and Pan JW. Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source. *Appl Phys Lett* 2007; **90**: 031110.

39. Chernoff H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann Math Stat* 1952; **23**: 493–507.

40. Mizutani A, Kato G and Azuma K et al. Quantum key distribution with setting-choice-independently correlated light sources. *npj Quantum Inf* 2019; **5**: 8.

41. Pereira M, Kato G and Mizutani A et al. Quantum key distribution with correlated sources. *Sci Adv* 2020; **6**: eaaz4487.

42. Zapatero V, Navarrete Á and Tamaki K et al. Security of quantum key distribution with intensity correlations. *Quantum* 2021; **5**: 602.

43. Sixto X, Zapatero V and Curty M. Security of decoy-state quantum key distribution with correlated intensity fluctuations. arXiv: 2206.06700v2.