Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses

Cong Jiang$^{1,2}$, Zong-Wen Yu$^{1,3}$, Xiao-Long Hu$^{1,2}$ and Xiang-Bin Wang$^{1,2,4}$

$^1$State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, People’s Republic of China

$^2$Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

$^3$Data Communication Science and Technology Research Institute, Beijing 100191, China

$^4$Jinan Institute of Quantum Technology, SAICT, Jinan 250101, Peoples Republic of China

The Sending-or-Not-Sending protocol of the twin-field quantum key distribution (TF-QKD) has its advantage of unconditional security proof under any coherent attack and fault tolerance to large misalignment error. So far this is the only coherent-state based TF-QKD protocol that has considered finite-key effect, the statistical fluctuations. Here we consider the complete finite-key effects for the protocol and we show by numerical simulation that the protocol with typical finite number of pulses in practice can produce unconditional secure final key under general attack, including all coherent attacks. It can exceed the secure distance of 500 km in typical finite number of pulses in practice even with a large misalignment error such as 20%.

I. INTRODUCTION

Quantum key distribution (QKD) could provide an unconditionally secure communication method of two parties, Alice and Bob. But the security in ideal case $\frac{R}{S}$ does not guarantee the security in practice $\frac{R}{S}$. Fortunately, the decoy-state method $\frac{R}{S}$ could help us beating the photon-number-split (PNS) attack $\frac{R}{S}$ and guarantee the security with imperfect light sources. Besides decoy-state method, there are other protocols such as RRDPS protocol $\frac{R}{S}$, proposed to beat PNS attack. Measurement-device-independent (MDI)-QKD $\frac{R}{S}$ can solve all possible loopholes of detection. And the decoy-state MDI-QKD $\frac{R}{S}$ protocol could help us ensure the security of protocol performed by imperfect light sources and detectors.

The 4-intensity protocol $\frac{R}{S}$ together with the joint-constraints $\frac{R}{S}$ has greatly improved the key rate and distance of the MDI-QKD. Using this protocol, a distance exceeding 400 km has been experimentally demonstrated $\frac{R}{S}$ for the MDI-QKD. However, the key rate of all the prior art decoy-state protocols and the MDI-QKD protocols protocols cannot be better than the linear scale of channel transmittance. It cannot exceed the known bound of the repeaterless QKD, such as the PLOB bound $\frac{R}{S}$ or the TGW bound $\frac{R}{S}$. Recently, a QKD protocol named Twin-Field (TF) QKD was proposed $\frac{R}{S}$ whose key rate $R \sim O(\sqrt{\eta})$, where $\eta$ is the channel transmittance, and thus have attracted much attention. But the later announcement of the phase information in Ref $\frac{R}{S}$ will cause security loopholes $\frac{R}{S}$, and many variants of TF QKD have been proposed $\frac{R}{S}$ to close the loophole. A series of experiments $\frac{R}{S}$ have been done to demonstrate those protocols. In particular, an efficient protocol for TF-QKD through sending-or-not-sending (SNS protocol) has been given in Ref. $\frac{R}{S}$. The SNS protocol has been experimentally demonstrated in proof-of-principle in Ref. $\frac{R}{S}$, and realized in real optical fiber with the effects of statistical fluctuation being taken $\frac{R}{S}$. The unconditional security of SNS protocol in the asymptotic case have been proved $\frac{R}{S}$ and SNS protocol relaxes the requirement for single photon interference accuracy. The key rate of SNS is still considerable even if the misalignment error is as large as 35%. Among all those variants of TF QKD with coherent states, the SNS QKD protocol is the only one that takes the effect of statistical fluctuation and finite decoy states into consideration $\frac{R}{S}$. Here we show an analysis of the complete effect of finite-key size of SNS QKD protocol.

The main tool we use to analyse the effect of finite-key size is the universally composable framework $\frac{R}{S}$. An complete QKD protocol usually includes the preparation and distribution of quantum states, measurement of received quantum states, parameter estimation, error correction and private amplification. After the error correction step, Alice gets a bit string $S$, and Bob get an estimate string $S'$ of $S$. If the error rate is too large, the results of error correction is an empty string and the protocol aborts. A protocol is called $\epsilon$-cor-correct if the probability that $S$ and $S'$ aren’t the same, $\Pr(S \neq S') \leq \epsilon_{\text{cor}}$.

Besides, the quantum state of Alice may be attacked by Eve in the distribution and measurement step and some information would be leaked to Eve. To ensure the security of final secret keys, Alice and Bob apply a privacy amplification scheme based on two-universal hashing $\frac{R}{S}$ to extract two shorter strings of length $l$ from $S$ and $S'$. We denote the density operator of the
system of Alice and Eve as $\rho_{AE}$. If
\[
\min_{\rho_E} \frac{1}{2} \| \rho_{AE} - U_A \otimes \rho_E \| \leq \varepsilon_{\text{sec}},
\]
where $U_A$ denotes the fully mixed state of Alice’s system of strings of length $l$, the protocol is called $\varepsilon_{\text{sec}}$-secret [54, 76, 77]. According to the composable framework, a protocol is called $\varepsilon$-secure if it is both $\varepsilon_{\text{cor}}$-correct and $\varepsilon_{\text{sec}}$-secret, and $\varepsilon \leq \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$.

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

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

Here we consider the four-intensity decoy state SNS protocol [68]. In this protocol, Alice and Bob randomly send vacuum state or weak coherent pulse state to the third party, Charlie. In each time, Alice and Bob randomly choose $X$ window or $Z$ window with probabilities $1 - p_z$ and $p_z$. If $X$ window is chosen, Alice (Bob) randomly chooses vacuum state $|0\rangle$, $|e^{i\delta_A + i\gamma_A} \alpha\rangle$ or $|e^{i\delta_A + i\gamma_A} \alpha'\rangle$ (vacuum state $|0\rangle$, $|e^{i\delta_B + i\gamma_B} \alpha\rangle$ or $|e^{i\delta_B + i\gamma_B} \alpha'\rangle$) with probabilities $p_0$, $p_1$ and $1 - p_0 - p_1$ respectively, where $\alpha^2 = \mu_1$ and $\alpha'^2 = \mu_2$ are the intensities of different decoy sources, and $\gamma$ is the public phase and $\delta$ is random in $[0, 2\pi)$ which will be announced in the parameter estimation step. If $Z$ window is chosen, Alice (Bob) randomly chooses vacuum state $|0\rangle$, or phase-randomized weak coherent state $|\alpha_Z\rangle$ with probabilities $p_{z0}$ and $1 - p_{z0}$, where $\alpha_Z^2 = \mu_z$ is the intensity of signal source. Then Alice and Bob prepare the chosen state and send it to Charlie. Charlie is assumed to perform interferometric measurements on the received quantum signals and announces the measurement result to Alice and Bob. If one and only one detector clicks in the measurement process, Charlie will also announces whether the left detector or right detector responds, and Alice and Bob will take it as an effective event.

3. Sifting. Alice and Bob announce whether the signals of effective events are prepared in $X$ window or $Z$ window. Then Alice and Bob divide all the effective events into two sets, $X$ and $Z$ accordingly, where set $Z$ only contains the effective events that both Alice and Bob prepare the quantum signals in $Z$ window and set $X$ contains all other effective events. Then Alice and Bob announce all information of their prepared states, including the intensities and phases, of the effective events of set $X$.

4. Parameter estimation. For the events in set $Z$, Alice will denote it as bit 0 if she sends a vacuum state, and denote it as bit 1 if she sends a phase-randomized weak coherent state. In the same time, Bob will denote it as bit 1 if he sends a vacuum state, and denote it as bit 0 if he sends a phase-randomized weak coherent state. Finally Alice and Bob form the $n_1$ bits strings $Z_x$ and $Z_y$ according to the events in set $Z$. Then Alice and Bob estimate $n_1$ and $\epsilon_1^{\text{ph}}$ according the events in set $X$, where $n_1$ is the lower bound of bits caused by single-photons in $Z_x$ or $Z_y$, and $\epsilon_1^{\text{ph}}$ is the upper bound of phase-flip error rate of single-photons. The details of how to calculate $n_1$ and $\epsilon_1^{\text{ph}}$ are shown in the Methods part.

5. Error correction. Alice and Bob perform an information reconciliation scheme to correct $Z_y$, and Bob will obtain an estimate $\hat{Z}_y$ of $Z_y$. To achieve this goal, Alice sends Bob $\text{leak}_{EC}$ bits of error correction data. Then Alice computes a hash of $Z_x$ of length $\log (1/\varepsilon_{\text{cor}})$ using a random universal hash function, and she sends the hash and hash function to Bob [77]. If the hash of Bob computes is the same with Alice, the probability that $Z_x$ and $\hat{Z}_y$ aren’t the same, $\Pr (Z_x \neq \hat{Z}_y)$, is less than $\varepsilon_{\text{cor}}$. If the hash of Bob computes is not the same with Alice, the protocol aborts.

6. Private amplification. Alice and Bob apply a privacy amplification scheme based on two-universal hashing [77] to extract two shorter strings of length $l$ from $Z_x$ and $Z_y$. Alice and Bob obtain strings $S$ and $\hat{S}$ which is the final secret key after privacy amplification.

The protocol is $\varepsilon_{\text{cor}}$-correct if the error correction step is passed. If the final length of secret keys, $l$, satisfies
\[
l = n_1 [1 - h(e_1^{\text{ph}})] - \text{leak}_{EC} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2 \log_2 \frac{1}{\sqrt{2\xi_{PA}\bar{\varepsilon}}},
\]
the protocol is $\varepsilon_{\text{sec}}$-secret. And according to the composable framework, the security coefficient of the whole protocol is $\xi_{\text{tot}} = \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$, where $\varepsilon_{\text{sec}} = 2\bar{\varepsilon} + 4\varepsilon_{PA} + \varepsilon_{n_1}$, $h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ is the binary Shannon entropy function. Here, $\varepsilon_{\text{cor}}$ is the failure probability of error correction; $\bar{\varepsilon}$ is the accuracy of estimating the smooth min-entropy, which is also the failure probability that the real value of $e_1^{\text{ph}}$ isn’t in the bound that we estimate; $\varepsilon_{PA}$ is the failure probability of privacy amplification; $\varepsilon_{n_1}$ is the failure probability that the real value
of $n_1$ isn’t in the bound that we estimate. The value of $\text{leak}_{EC}$ is related to the specific error correction schemes, and in general $\text{leak}_{EC} = f n_1 h(E_2)$, where $f$ is the error correction inefficiency and $E_2$ is the error rate of strings $Z_s$ and $Z'_s$.

### III. NUMERICAL SIMULATION

If an experiment of SNS protocol is done, we can first calculate the lower and upper bound of $\langle S_{jk} \rangle$ with Eqs. (10), (14)-(18) from their observed values. And we can get the upper bound of $\langle e_{ph}^j \rangle$ in a similar way. Then we can get the lower bound of $\langle s_{1j}^2 \rangle$ and the upper bound of $\langle e_{ph}^j \rangle$ with Eqs. (12) and (13). Then we can get the lower bound of $n_1$ and the upper bound of $\varepsilon_{ph}^j$ with Eqs. (19)-(22). Finally, we can get how many bits of secret keys we could extract from this experiment with Eq. (2). The problem is we do not have such observed values and we need to simulate what values we would observe in the experiment with the experimental parameters list in Table I. All symbols appearing in this paragraph is defined in Sec. IV B.

We use the linear model to simulate the observed values of experiment with the experimental parameters list in Table I. Without loss of generality, we assume the distance between Alice and Charlie and the distance between Bob and Charlie are the same, and we assume the property of Charlie’s two detectors are the same. If the total transmittance of the experiment set-ups is $\eta = 10^{-L/100} \eta_d$, where $L$ is the distance between Alice and Bob. The simulation of those observed values are shown in Sec. IV C which are related to $\eta$ and other parameters list in Table I.

Here we set $\varepsilon_{cor} = \bar{\varepsilon} = \varepsilon_{PA} = \xi$, $\bar{\varepsilon} = 4\xi$ and $\varepsilon_{n_1} = 4\xi$, and thus security coefficient of the whole protocol is $\varepsilon_{tot} = 24\xi = 2.4 \times 10^{-9}$. The reason we set $\bar{\varepsilon} = 4\xi$ and $\varepsilon_{n_1} = 4\xi$ is we use the Chernoff bound for four times to estimate $\varepsilon_{ph}$ and $n_1$ (Notice that we could handle $\langle S_{21} \rangle + \langle S_{10} \rangle$ together and we could handle $\langle S_{02} \rangle + \langle S_{20} \rangle$ together in Eq. (18)). In order to fairly compare the performance of generating final keys of different total pulse numbers, $N$, we define the key rate of per sending pulse, $R = l/N$.

![Key rates (per pulse) versus transmission distance](image)

**Fig. 1:** The optimal key rates (per pulse) versus transmission distance (the distance between Alice and Bob) with the results of this work and Ref. [68] under the experimental parameters listed in Table I. The dashed lines are results of Ref. [68] and the solid lines are the results of this work. Here we simulate three groups of results where $N = 1 \times 10^4, 1 \times 10^8, 1 \times 10^{10}$. Here the red solid line is the PLOB bound.

This work and Ref. [68] with the experimental parameters list in Table I. The only difference of Fig. I and Fig. 2 is that $\varepsilon_d = 15\%$ of Fig. 1 and $\varepsilon_d = 20\%$ of Fig. 2. The results of this work and Ref. [68] is almost overlap while we set $N = 1 \times 10^4$, but the difference of the results is obvious while we set $N = 1 \times 10^{10}$, especially in the end of the lines. Still, the secure distance of SNS protocol can still reach up to 500 km with 20% misalignment error and $1 \times 10^{12}$ total pulses, even if we take all the effects of finite-key size into consideration.

### IV. CONCLUSION

In this paper, we show an analysis of the finite-key size effect of SNS protocol and get the relation of final key length $l$ and the security coefficient, as shown in Eq. (2). Eq. (2) is derived by the method proposed in Ref. [11], and thus it can produce unconditional secure final key under general attack, including all coherent attacks. The numerical results show that the secure distance of SNS protocol can still reach up to 500 km with 20% misalignment error and $1 \times 10^{12}$ total pulses, even if we take all the effects of finite-key size into consideration. This clearly shows that the SNS protocol of TF-QKD is on the one hand secure under general attack, i.e., as secure as the existing decoy-state MDI-QKD, on the other hand more efficient than the existing decoy-state MDI-QKD by many orders of magnitudes in key rate at long distance domain.

**Acknowledgement:** We thank Hai Xu for discussions. We acknowledge the financial support in part by

| $p_d$ | $e_0$ | $e_d$ | $\eta_d$ | $f$ | $\alpha_f$ | $\xi$ |
|-------|-------|-------|----------|-----|------------|-------|
| $1.0 \times 10^{-10}$ | 0.5 | 15% | 80.0% | 1.1 | 0.2 | $1.0 \times 10^{-10}$ |
FIG. 2: The optimal key rates (per pulse) versus transmis-
sion distance (the distance between Alice and Bob) with the re-
results of this work and Ref. 68 under the experimental parame-
ters listed in Table I except we set εd = 20%. The dashed lines
are results of Ref. 68 and the solid lines are the results of
this work. Here we simulate three groups of results where
are results of Ref. 68 and the solid lines are the results of
this work. Here we simulate three groups of results where
N = 1 × 10^{14}, 1 × 10^{12}, 1 × 10^{10}. Here the red solid line is the
PLOB bound.

Ministration of Science and Technology of China through
The National Key Research and Development Program
of China grant No. 2017YFA0303901; National Natu-
ral Science Foundation of China grant No. 11474182,
11774198 and U1738142.

Methods

A. The relation of the length of final key and εsec

In this protocol, any attack to quantum channel and
detectors is allowed only if it doesn’t break the rules of
quantum mechanics, and we call the attacker as Eve. We
denote the system of Eve after error correction as E'.
If Alice and Bob apply a privacy amplification scheme
based on two-universal hashing to extract two shorter
strings of length l from Zs, the protocol is εsec-secret. 75
78

εsec ≤ 2ε + 1√2\left(1−H_{min}^ε(Z|E')\right),

(3)

where H_{min}^ε(Z|E') is the ε-smooth min entropy. It mea-
sures the max probability of guessing Zs right giving E'.
E' could be decomposed as CE, where C is the system of
leakage information while Alice and Bob perform er-
ror correction and E is the system of Eve before error
correction. According to the chain rules 79, we have

H_{min}^ε(Z|E') ≥ H_{min}^ε(Zs|E) − |C|,

(4)

where |C| < leakEC + log_2(\frac{Z}{\varepsilon}). And we could decom-
pose the string Zs as Z_1, Z_{rest}, where Z_1 is the bits caused
by single-photon and Z_{rest} is the other bits of Z. 

Thus according to the chain rules 79, we have

H_{min}^ε(Z_1|E) ≥ H_{min}^ε(Z_1|Z_{rest}E) + H_{min}^ε(Z_{rest}|E)

− 2\log_2 \frac{\sqrt{\varepsilon}}{\varepsilon},

(5)

where ε = 2ε + ε' + 2\varepsilon \text{ and } H_{min}^ε(Z_{rest}|E) ≥ 0.

To get the lower bound of H_{min}^ε(Z_1|Z_{rest}E), we need
to use the uncertainty relation of smooth min and max
entropy 77, 80. It says that if the single-photon states
preparing in X-basis and Z-basis are orthogonal unbiased,
and if the states originally measured under the Z-basis are
now measured under the X-basis and obtained strings X_1
and X_1^* by Alice and Bob respectively, then we have

H_{min}^ε(Z_1|Z_{rest}E) ≥ n_1 − H_{max}^ε(X_1|X_1^*)

≥ n_1 – n_1 \text{h}(e_{ph}^{10}).

Finally we have

H_{min}^ε(Z_1|Z_{rest}E) ≥ n_1[1 − \text{h}(e_{ph}^{10})] − \text{leak}_{EC}

− 2\log_2 \frac{\sqrt{\varepsilon}}{\varepsilon}

(7)

Combining Eqs. (2), (3) and (7) and setting ε' = 0, we have

εsec ≤ 2\varepsilon + 4\varepsilon + \varepsilon_{PA}.

(8)

Finally, containing the failure probability that the real
value of n_1 isn’t in the bound that we estimate, ε_{n_1}, we have

εsec ≤ 2\varepsilon + 4\varepsilon + \varepsilon_{PA} + \varepsilon_{n_1}.

(9)

B. The calculation method of n_1 and e_{ph}^{10}

The method we use here is similar with Ref. 68.
To introduce our calculation method clearly, we denote
\rho = |0\rangle\langle 0|, \rho_1 = \sum_{k=0}^{n} \frac{\rho_{jk}}{\alpha_{jk}} |k\rangle\langle k|, \rho_2 = \sum_{k=0}^{n} \frac{\rho_{jk}}{\alpha_{jk}} |k\rangle\langle k|
and \rho_3 = \sum_{k=0}^{n} |k\rangle\langle k|. It is easy to check that the density
operator of |e^{i\delta_{A}' + i\gamma_{A}}\rangle\langle A| and |e^{i\delta_{A}' + i\gamma_{A}}\rangle\langle A|
if Alice chooses δ_A and δ_A' randomly, is \rho_1 and \rho_2.
And this also apply to Bob's quantum state. In the whole protocol, Alice
and Bob obtain N_{jk}(j,k = 1, 2, z) instances when Al-
\ice sends state \rho_1 and Bob sends states \rho_2. And after the
\text{sifted step, Alice and Bob obtain n_{jk} effective events.}

We denote the counting rate of source jk as S_{jk} = n_{jk}/N_{jk}.
The sending or not sending information of set Z is not
announced, and thus we don’t know the value of n_{0z}, n_{00} and n_{zz}.
But the number of total effective events of set Z, n_z, and other n_{jk} are known values. With all those
definitions, we have

\[
N_{00} = [(1 - p_z)^2 p_0^2 + 2(1 - p_z)p_z p_0 p_{20}] N,
\]

\[
N_{01} = N_{10} = [(1 - p_z)^2 p_0 p_1 + (1 - p_z)p_z p_2 p_0 p_1] N,
\]

\[
N_{02} = N_{20} = [(1 - p_z)^2 (1 - p_0 - p_1) p_0 + (1 - p_z)p_z p_{20} (1 - p_0 - p_1)] N.
\]  

(10)

Besides, we need define two new sets \( C_{\Delta^+} \) and \( C_{\Delta^-} \). \( C_{\Delta^+} \) contains all the instance that both Alice and Bob prepare \( |e^{i\phi_A + i\varphi_A} \rangle \) and \( |e^{i\phi_B + i\varphi_B} \rangle \) and \( |\delta_A - |\delta_B| \leq \Delta \). \( C_{\Delta^-} \) contains all the instance that both Alice and Bob prepare \( |e^{i\phi_A + i\varphi_A} \rangle \) and \( |e^{i\phi_B + i\varphi_B} \rangle \) and \( |\delta_A - |\delta_B - \pi| \leq \Delta \). The number of instances in \( C_{\Delta^+} \) is

\[
N_{\Delta^+} = \frac{\Delta}{2} (1 - p_z)^2 p_1^2 N.
\]  

(11)

We denote the number of effective events of right detectors responding from \( C_{\Delta^+} \) as \( n_{\Delta^+} \), and the number of effective events of left detectors responding from \( C_{\Delta^-} \) as \( n_{\Delta^-} \). And we get the counting error rate of \( \Delta^+ \),

\[
T_{\Delta^+} = \frac{n_{\Delta^+}}{n_{\Delta^+} + n_{\Delta^-}}.
\]

If we denote the expected value of the counting rate of single-photons state, \( \frac{1}{2} (|01\rangle(|01\rangle + |10\rangle|10\rangle) \), in Z basis as \( \langle s_1^Z \rangle \), the lower bound of \( \langle s_1^Z \rangle \) is

\[
\langle s_1^Z \rangle \geq \langle s_1^Z \rangle = \frac{1}{2 \mu_1 \mu_2 (\mu_2 - \mu_1)} [\mu_2^2 e^{i\mu_1} (\langle S_{01} \rangle + \langle S_{10} \rangle)

- \mu_1^2 e^{i\mu_2} (\langle S_{02} \rangle + \langle S_{20} \rangle) - 2(\mu_2 - \mu_1)^2 (\langle S_{00} \rangle)],
\]  

(12)

where \( \langle S_{jk} \rangle \) is the expected value of \( S_{jk} \), and \( \langle S_1^Z \rangle \) and \( \langle S_2^Z \rangle \) are the upper bound and lower bound of \( \langle S_{jk} \rangle \) when we estimate the expected value from its observed value.

The expected value of the phase-flip error rate of the single-photons in the Z basis satisfies \( ^868 \)

\[
\langle e^{i\phi_1} \rangle \leq \langle e^{i\phi_1} \rangle = \frac{(\langle T_{\Delta^+} \rangle - \frac{1}{2} e^{-2\mu_1} (\langle S_{00} \rangle)}{2 \mu_1 e^{-2\mu_1} (\langle s_1^Z \rangle)}.
\]  

(13)

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

Chernoff bound. The formulas of \( \langle s_1^Z \rangle \) and \( \langle e^{i\phi_1} \rangle \) are represented by expected values, but the values we get in experiment are observed values. To close the gap between the expected values and observed values, we need Chernoff bound \( ^868, ^81 \). Let \( X_1, X_2, \ldots, X_n \) be \( n \) random samples, detected with the value 1 or 0, and let \( X \) denote their sum satisfying \( X = \sum_{i=1}^{n} X_i \). \( \phi \) is the expected value of \( X \). We have

\[
\phi^L(X) = \frac{X}{1 + \delta_1(X)},
\]

\[
\phi^U(X) = \frac{X}{1 - \delta_2(X)},
\]  

(14)

(15)

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

\[
\left( \frac{e^{\delta_1}}{(1 + \delta_1)^{1 + \delta_1}} \right)^{X_{\Delta^+}} = \frac{\xi}{2},
\]

(16)

\[
\left( \frac{e^{-\delta_2}}{(1 - \delta_2)^{1 - \delta_2}} \right)^{X_{\Delta^-}} = \frac{\xi}{2},
\]  

(17)

where \( \xi \) is the failure probability. Thus we have

\[
\phi^L(N_{jk} s_{jk}) = N_{jk} (\langle s_{jk} \rangle), \phi^U(N_{jk} s_{jk}) = N_{jk} (\langle s_{jk} \rangle).
\]  

(18)

Still Eqs. (12) and (13) are the lower bound of the expected values of the counting rate and the upper bound of phase flip error rate of single-photons. The final question is what their real values are in this specific experiment, and we need the Chernoff bound to help us estimate their real values from their expected values. Similar to Eqs. (14) - (17), the observed value, \( \varphi \), and its expected value, \( Y \), satisfy

\[
\varphi^U(Y) = [1 + \delta_1(Y)]Y, \varphi^L(Y) = [1 - \delta_2(Y)]Y,
\]  

(19)

(20)

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

\[
\left( \frac{e^{\delta_1}}{(1 + \delta_1)^{1 + \delta_1}} \right)^{Y_{\Delta^+}} = \frac{\xi}{2},
\]

(21)

\[
\left( \frac{e^{-\delta_2}}{(1 - \delta_2)^{1 - \delta_2}} \right)^{Y_{\Delta^-}} = \frac{\xi}{2},
\]  

(22)

We define \( N_1 = 2p_z p_{20}(1 - p_{p20}) \mu_z e^{-\mu_z} N \), and we have \( ^868 \)

\[
n_1 = \varphi^L(N_1 (\langle s_1^Z \rangle (\langle e^{i\phi_1} \rangle))), \quad e^{i\phi_1} = \frac{\varphi^U(N_1 (\langle s_1^Z \rangle (\langle e^{i\phi_1} \rangle)))}{N_1 (\langle s_1^Z \rangle (\langle e^{i\phi_1} \rangle))}.
\]  

(23)

This ends the estimate of \( n_1 \) and \( e^{i\phi_1} \).

C. The simulation of observed values

We use the linear model to simulate the observed values of experiment with the experimental parameters list in Table. \( ^\boxed{} \). Without loss of generality, we assume the distance between Alice and Charlie and the distance between Bob and Charlie are the same, and we assume the property of Charlie’s two detectors are the same. If the total transmittance of the experiment set-ups is \( \eta \), then
we have

\[ n_{00} = 2p_d(1 - p_d)N_{00}, \]
\[ n_{01} = n_{10} = 2[(1 - p_d)e^{\eta \mu_1/2} - (1 - p_d)^2e^{-\eta \mu_1}]N_{01}, \]
\[ n_{02} = n_{20} = 2[(1 - p_d)e^{\eta \mu_2/2} - (1 - p_d)^2e^{-\eta \mu_2}]N_{02}, \]
\[ n_t = n_{\text{signal}} + n_{\text{error}}, \]
\[ E_z = \frac{n_{\text{error}}}{n_t}, \]
\[ n_{\Delta +}^R = n_{\Delta -}^L = [T_X(1 - 2e_d) + e_dS_X]N_{\Delta z}, \]

where \( N_{00}, N_{01}, N_{10}, N_{02}, N_{20}, N_{\Delta z} \) are defined in Eqs. \((10)\) and \((11)\) and

\[ n_{\text{signal}} = 4N_{P_z}^2p_d0(1 - P_{z0})(1 - p_d)e^{-\eta \mu_z/2} \]
\[ - (1 - p_d)^2e^{-2\eta \mu_z}, \]
\[ n_{\text{error}} = 2N_{P_z}^2(1 - p_{d0})^2[(1 - p_d)e^{-\eta \mu_z} I_0(\eta \mu_z) \]
\[ - (1 - p_d)^2e^{-2\eta \mu_z}] + 2N_{P_z}^2p_d0p_d(1 - p_d), \]
\[ T_X = \frac{1}{2} \int_{-\pi}^{\pi} (1 - p_d)e^{-2\eta \mu_1 \cos^2\frac{\delta}{2}}\sin^2\frac{\delta}{2} \text{d}\delta \]
\[ - (1 - p_d)^2e^{-2\eta \mu_1}, \]
\[ S_X = \frac{1}{2} \int_{-\pi}^{\pi} (1 - p_d)e^{-2\eta \mu_1 \sin^2\frac{\delta}{2}}\cos^2\frac{\delta}{2} \text{d}\delta \]
\[ - (1 - p_d)^2e^{-2\eta \mu_1} + T_X, \]

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

[1] C. Bennett, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (1984), pp. 175-179.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of modern physics 74, 145 (2002).
[3] N. Gisin and R. Thew, Nature photonics 1, 165 (2007).
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of modern physics 81, 1301 (2009).
[5] P. W. Shor and J. Preskill, Physical review letters 85, 441 (2000).
[6] M. Koashi, New Journal of Physics 11, 045018 (2009).
[7] K. Tamaki, M. Koashi, and N. Imoto, Physical review letters 90, 167904 (2003).
[8] B. Kraus, N. Gisin, and R. Renner, Physical review letters 95, 080501 (2005).
[9] B. Hüttner, N. Imoto, N. Gisin, and T. Mor, Physical Review A 51, 1863 (1995).
[10] H. P. Yuen, Quantum and Semiclassical Optics: Journal of the European Optical Society Part B 8, 939 (1996).
[11] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Physical Review Letters 85, 1350 (2000).
[12] N. Lütkenhaus, Physical Review A 61, 052304 (2000).
[13] N. Lütkenhaus and M. Jahma, New Journal of Physics 4, 44 (2002).
[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature photonics 4, 686 (2010).
[15] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature communications 2, 349 (2011).
[16] M. Hayashi, Physical Review A 76, 012329 (2007).
[17] V. Scarani and R. Renner, Physical review letters 100, 200501 (2008).
[18] W.-Y. Hwang, Physical Review Letters 91, 057901 (2003).
[19] X.-B. Wang, Physical Review Letters 94, 230503 (2005).
[20] H.-K. Lo, X. Ma, and K. Chen, Physical review letters 94, 230504 (2005).
[21] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Physics reports 448, 1 (2007).
[22] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Physical review letters 98, 010503 (2007).
[23] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, et al., Physical Review Letters 98, 010504 (2007).
[24] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Physical review letters 98, 010505 (2007).
[25] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, et al., Nature 549, 43 (2017).
[26] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda,
