SCIENTIFIC REPORTS

OPEN

Sending-or-not-sending twin-field quantum key distribution in practice

Received: 6 September 2018
Accepted: 16 January 2019
Published online: 28 February 2019

Zong-Wen Yu[1,2], Xiao-Long Hu[1], Cong Jiang[1], Hai Xu[1] & Xiang-Bin Wang[1,3,4,5]

Recently, the twin field quantum key distribution (TF-QKD) protocols have been investigated extensively. In particular, an efficient protocol for TF-QKD with sending or not sending the coherent state has been given in. Here in this paper, we present results of practical sending-or-not-sending (SNS) twin field quantum key distribution. In real-life implementations, we need consider the following three requirements, a few different intensities rather than infinite number of different intensities, a phase slice of appropriate size rather than infinitely small size and the statistical fluctuations. We first show the decoy-state method with only a few different intensities and a phase slice of appropriate size. We then give a statistical fluctuation analysis for the decoy-state method. Numerical simulation shows that, the performance of our method is comparable to the asymptotic case for which the key size is large enough. Our method can beat the PLOB bound on secret key capacity. Our results show that practical implementations of the SNS quantum key distribution can be both secure and efficient.

Quantum key distribution (QKD) allows two parties, Alice and Bob, to share unconditional secret keys based on the laws of quantum physics[1–6], even in the presence of an eavesdropper, Eve. However, in real-life implementations of QKD, its practical security is still questionable due to the device imperfections, such as the imperfect source[7–9] and detectors. Fortunately, by using the decoy-state method[10–25], it has been shown that the unconditional security of QKD can still be assured with an imperfect single-photon source. To avoid the detector side channel attacks, the measurement-device-independent QKD (MDI-QKD) was proposed[26,27]. The decoy-state MDI-QKD can remove all detector side-channel attacks with imperfect single-photon sources[28–33].

With the developments[10–44] in both theory and experiment, QKD is more and more hoped to be extensively applied in practice, though there are barriers for doing so. Among them, the transmission loss of photons for long distance QKD has become the major obstacle in practical implementations. Very recently, a milestone breakthrough was made under the name of twin-field quantum key distribution (TF-QKD)[45] for long distance QKD with a key rate scales in square root of channel transmittance. To offer the information-theoretic-security, a number of upgraded variants were then proposed[1,46–48]. In particular, an efficient protocol for TF-QKD with sending or not sending the coherent state has been given in ref.[1]. In the sending-or-not-sending (SNS) protocol[1], Alice and Bob do not take post selection for the bits in Z basis (signal pulses) and hence the traditional calculation formulas directly apply. Also, it is fault tolerant to misalignment errors in the long distance single-photon interference.

In practice, we need consider the situations with a few different intensities rather than infinite number of different intensities, a phase slice of appropriate size and the statistical fluctuations. It should be interesting to see whether the advantage in the twin-field QKD still holds with these conditions in practice. In this paper, we proceed further and analyse the performance of the SNS TF-QKD under the above real-life assumptions and we show that the advantage in distance and key rate still holds..

First, we reveal the decoy-state method with only a few different intensities and a phase slice of appropriate size to estimate the lower bound of the yield and the upper bound of the phase-flip error rate for the single-photon

[1]State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing, 100084, People's Republic of China. [2]Data Communication Science and Technology Research Institute, Beijing, 100191, People's Republic of China. [3]Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, 230026, People's Republic of China. [4]Shandong Academy of Information and Communication Technology, Jinan, 250101, People's Republic of China. [5]Department of Physics, Southern University of Science and Technology, Shenzhen, 518055, People's Republic of China. Zong-Wen Yu and Xiao-Long Hu contributed equally. Correspondence and requests for materials should be addressed to X.-B.W. (email: xbwang@mail.tsinghua.edu.cn)

state. Furthermore, we also need to consider the statistical fluctuations. In order to improve the results, the instances for basis unmatched are also used to estimate the lower bound of the yield for the single-photon state, such as in Eq. (1).

Results

The decoy-state method with a few different intensities and a phase slice of appropriate size. In the four-intensity decoy-state SNS protocol, Alice and Bob randomly choose the X-window (decoy pulses) and Z-window (signal pulses) to send or not to send a phase-randomized coherent pulse to an untrusted party, Charlie, who is expected to perform interference measurement. The protocol is detailed below.

1. Alice and Bob repeat Steps 2–3, N times. All the public announcements by the legitimate users Alice and Bob are done over an authenticated channel.
2. Alice and Bob randomly choose X-window and Z-window with probabilities p_X and $1-p_X$ respectively. Alice (Bob) prepares and sends the decoy pulses in her (his) X-window. Explicitly she (he) randomly choose one of three sources ρ_{α_i} with probability p_i for $i=0, 1, 2$, where $\rho_{\alpha_0} = |0\rangle\langle 0|$ is the vacuum source, ρ_{α_1} and ρ_{α_2} are two phase-randomized coherent sources with intensity μ_1 and μ_2 ($\mu_1 < \mu_2$) respectively. In Z-window, Alice (Bob) puts down a bit value 1 and prepares and sends the phase-randomized coherent state ρ_{α_z} with probability p_z, or puts down a bit value 0 and sends nothing else, i.e., sends the vacuum pulse with probability $1-p_z$.
3. Charlie measures the incoming signals and records which detector clicks. When the quantum communication is over, he publicly announces all the information about the detection event. The situation when one and only one detector (detector 0 or detector 1) makes a count is denoted as an effective event. Alice and Bob collect all the data with effective events and discard all the others.
4. Alice and Bob announce the basis information (X-window or Z-window) firstly. Then they announce the bit values and phase information corresponding to the effective events when Alice or Bob choose X-window. With these information, Alice and Bob obtain the observable $N_{jk}(j, k=0, 1, 2, z)$ being the number of instances when Alice and Bob send state ρ_{α_j} and ρ_{α_k} respectively. Correspondingly, the lowercases n_{jk} are used to denote the number of effective events. The yields can be defined as $S_{jk}=n_{jk}/N_{jk}$. Explicitly, we have N_{11}, N_{22} and N_{zz} are the number of instances when Alice and Bob send state ρ_{α_1}, ρ_{α_2} and ρ_{α_z} respectively. Furthermore, In order to improve the results, the instances for basis unmatched are also considered and

$$\begin{aligned} N_{00} &= p_0^2 N_X + 2p_0(1-p_z)N_{XZ}, \\ N_{01} &= N_{10} = p_0 p_1 N_X + (1-p_z)p_1 N_{XZ}, \\ N_{02} &= N_{20} = p_0 p_2 N_X + (1-p_z)p_2 N_{XZ}, \end{aligned} \tag{1}$$

   where $p_0=1-p_1-p_2$ is the probability to send a vacuum pulse in X-window, $N_X = p_X^2 N$ is the number of instances when both Alice and Bob choose X-window and $N_{XZ}=p_X(1-p_X)N$ is the number of instances when Alice chooses X-window and Bob chooses Z-window.
5. Define two sets C_{Δ^+} and C_{Δ^-} that contain the instances when both Alice and Bob send ρ_{α_1} in X-window with the phase information θ_A and θ_B falling into the slice $|\theta_A-\theta_B| \le \Delta/2$ and $|\theta_A-\theta_B-\pi| \le \Delta/2$ respectively. The number of instances in $C_{\Delta^\pm}$ are $N_{11}^{\Delta^\pm} = \frac{\Delta}{2\pi}N_{11}$. The number of effective events corresponding to $C_{\Delta^\pm}$ are denoted by $n_{11}^{\Delta_0^\pm}$ and $n_{11}^{\Delta_1^\pm}$ for detector 0 and detector 1 respectively.
6. With these observables, Alice and Bob can estimate the lower bound of n_1 and the upper bound of e_1^{ph} by using the decoy-state methods shown below. Then the post-processing can be performed and the final key length is

$$N_f = n_1[1 - H(e_1^{ph})] - f n_t H(E_Z), \tag{2}$$

where N_f is the number of final bits, n_1 is the number of effective events caused by single-photon states in Z-basis when Alice decides sending while Bob decides not sending or Alice decides not sending while Bob decides sending, e_1^{ph} is the phase-flip error rate for instances of n_1, $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function, f is the correction efficiency, n_t is the number of effective events when both Alice and Bob choose Z-window and E_Z is the corresponding bit-flip error rate.

Alternatively, we also have the equivalent formula for key rate per time window as shown in the section Methods.

In the above, for conciseness, we have omitted those mismatching time windows in a real protocol. For example, when Alice commits to a decoy window and Bob commits to a signal window. Although the events of these windows cannot be used for the final key distillation, the data for heralded events from these time windows can be used in the decoy-state analysis. The bit value encoding is defined by Alice or Bob's decision on sending or not-sending in a signal window. As shown in ref.[1], we can relate the bit values with local ancillary states in the virtual protocol. Clearly, there isn't any definition confusion[47] in the SNS protocol[1].

A tricky point in the SNS protocol is that the traditional decoy-state method can still work. In this protocol, the random phase information of Z-windows are never announced therefore we can regard pulses of Z-basis as classical mixture of different photon number states properly. Note that, very importantly, the random phase information in Z windows can never been announced because otherwise, the elementary concepts such as the

p_d	η_d	f	ε	e_a
1.0×10^{-10}	50%	1.1	1.0×10^{-10}	15%

Table 1. List of experimental parameters used in numerical simulations. p_d: the dark count rate, η_d: the detection efficiency of all detectors, f: the error correction inefficiency, ε: the security bound considered in the statistical fluctuation analysis, e_a: the misalignment error.

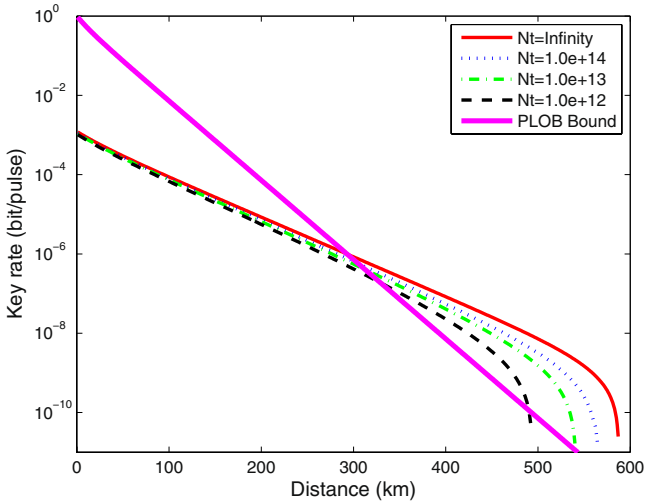

Figure 1. Optimal key rate (bits per pulse) as a function of the distance by 4-inensity decoy-state method. The asymptotic result is shown in the red solid line. The blue dotted line, the green dash-dot line and the black dashed line are the results with $N = 10^{14}$, $N = 10^{13}$ and $N = 10^{12}$, respectively. The solid magenta thick line illustrates the PLOB bound.

number of single-photon counts are *illy* defined. But, as shown in details in ref.[1], the random phase information in X-windows can be post announced. Because we only want to verify the phase-flip error rate of Z windows. The phase-flip rate of Z windows is an objective fact, once it is verified, it is there. The post announced phase information does not change this objective facts because no matter how Eve takes action with the post announced information, the action is just Eve's local action which can not make a difference to anything detectable to Alice and Bob.

Numerical simulation. In this section, we present some results of the numerical simulation. In order to show the efficiency of our method, without any loss of generality, we focus on the symmetric case where the two channel transmissions from Alice to Charlie and from Bob to Charlie are equal. We also assume that Charlie's detectors are identical, i.e., they have the same dark count rates and detection efficiencies, and their detection efficiencies do not depend on the incoming signals. The results for the asymmetric case will be considered in the coming work. We shall estimate what values would be probably observed in the normal cases by the linear models as previously. The values of the experimental parameters used in the simulations are listed in Table 1.

We optimize all parameters, p_X, p_1, p_2 p_z, μ_1, μ_2, μ_z and Δ by the method of full optimization. The results of optimized key rate with different N by four-inensity decoy-state method and the result with theoretical PLOB bound[49] are shown in Fig. 1. In it, we use the red solid line to denote the asymptotic results with infinite number of pulses. The optimal key rate with $N = 10^{14}$, $N = 10^{13}$ and $N = 10^{12}$ are shown by the blue dotted line, the green dash-dot line and the black dashed line respectively. The result with theoretical PLOB bound is plotted by the thick magenta solid line. The numerical simulations show that the finite-size SNS protocol can overcome the PLOB bound. In Fig. 2, we plot the final key rates by the four-intensity and the three-intensity decoy-state methods with $N = 10^{12}$. We can see that the optimal key rates for the three-intensity decoy-state method is nearly equal to the results for the four-intensity decoy-state method when we are aim for practically useable key-rates (such as 10^{-6} per-pulse). In Fig. 3, we plot the optimal value of Δ for different distances with $N = 10^{12}$ by four-inensity decoy-state method. With this, we know that the optimal value of Δ are changed with different communication distance between Alice and Bob. The optimal value of Δ monotonically increases, to reduce the impact of statistical fluctuations, until it reaches a peak where the optimal key rate becomes decreasing dramatically and the error rate has a greater impact on the key rate than the statistical fluctuation.

Also, according to the observed data there[36], we use a linear loss model to estimate the actual loss in the experiment for 404 km of ultralow-loss optical fiber (0.16 dB/km). Assuming the same device parameters ($p_d = 7.2 \times 10^{-8}$, $\eta_d = 0.5525$, $f = 1.16$, $\varepsilon = 10^{-10}$, $e_a = 2\%$ and $N = 6.0 \times 10^{14}$), we make the optimization by using our SNS protocol with the four-intensity decoy-state method shown above. We obtain a final key rate of 141 bit per second (bps), which is more than 4.4×10^5 times higher than the reported experimental result, 3.2×10^{-4} bps. Similarly, assuming the same device parameters ($p_d = 4.0 \times 10^{-11}$, $\eta_d = 0.5$, $f = 1.1$, $\varepsilon = 5.0 \times 10^{-11}$, $e_a = 2\%$

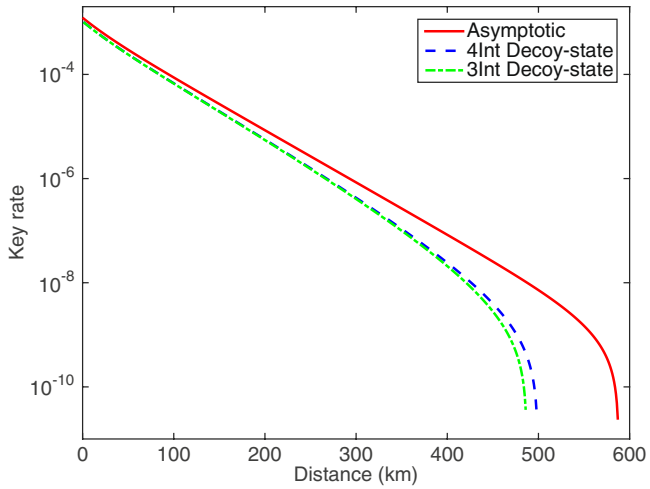

Figure 2. Optimal key rate (bits per pulse) as a function of the distance. The asymptotic result is shown in the red solid line. The blue dashed line and the green dash-dot line are the results for 4-intensity and 3-intensity decoy-state methods with $N = 10^{12}$, respectively.

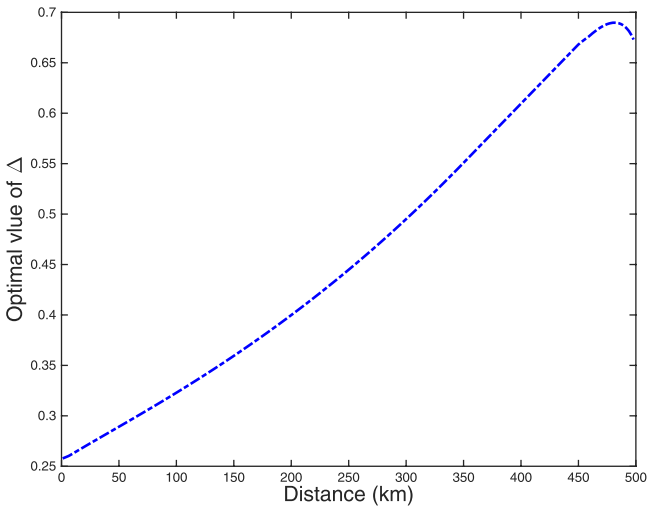

Figure 3. Optimal value of Δ (radians) corresponding to the optimal key rate by 4-intensity decoy-state method with $N = 10^{12}$.

and $N = 2.178 \times 10^{14}$) for 421 km of ultralow-loss optical fiber (0.17 dB/km) in ref.[50], we obtain a final key rate of 2.62×10^3 bit per second (bps), which is more than 1.05×10^4 times higher than the reported experimental result, 0.25 bps.

Discussion

In real setups of QKD, the practical situations with a few different intensities rather than infinite number of different intensities, a phase slice of appropriate size rather than infinitely small size and the statistical fluctuations must be considered. We first present the decoy-state method with a few different intensities and a phase slice of appropriate size. Then we show that the SNS protocol is a highly practical scheme even when the statistical fluctuations are considered. Numerical simulation shows that, the finite-size SNS protocol can exceed the PLOB bound. Our results show that practical implementations of the SNS TF-QKD can be both secure and efficient.

Methods

Decoy-state method analysis. In the protocol, Alice and Bob prepare and send the coherent pulses with randomized phase. The traditional formulas of decoy-state method can be applied directly. The coherent state whose phase is selected uniformly at random can be regard as a mixture of photon number states

$$\rho_{\alpha_j} = e^{-\mu_j} \sum_{n=0}^{\infty} \frac{\mu_j^n}{n!} |n\rangle\langle n|, \qquad (j = 0, 1, 2, z) \tag{3}$$

where $\mu_j = |\alpha_j|^2$ is the intensity of the coherent state $|\alpha_j\rangle$. Then the state when Alice decides not sending and Bob decides to send ρ_{α_k} is $\rho_{\alpha_0\alpha_k} = e^{-\mu_k}\sum_{n=0}^{\infty}\mu_k^n/n!|0n\rangle\langle 0n|$. With these convex forms, the lower bound of the yield of the state $\rho_{z_{01}} = |01\rangle\langle 01|$ can be written into the following form[30]

$$s_{z_{01}} \geq s_{z_{01}}^L = \frac{\mu_2^2 e^{\mu_1} S_{01} - \mu_1^2 e^{\mu_2} S_{02} - (\mu_2^2 - \mu_1^2) S_{00}}{\mu_1\mu_2(\mu_2 - \mu_1)}, \tag{4}$$

where S_{0k} are the yield of the sources $\rho_{\alpha_0\alpha_k}$ for $k = 1, 2$, S_{00} is the yield when both Alice and Bob send the vacuum state. Similarly, the lower bound of the yield of the state $\rho_{z_{10}} = |10\rangle\langle 10|$ can be written as

$$s_{z_{10}} \geq s_{z_{10}}^L = \frac{\mu_2^2 e^{\mu_1} S_{10} - \mu_1^2 e^{\mu_2} S_{20} - (\mu_2^2 - \mu_1^2) S_{00}}{\mu_1\mu_2(\mu_2 - \mu_1)}, \tag{5}$$

where S_{j0} are the yield of the sources $\rho_{\alpha_j\alpha_0}$ for $j = 1, 2$. With Eqs (4) and (5), the lower bound of the yield of single-photon state in Z-basis, i.e., the state $\rho_1^Z = \frac{1}{2}\left(\rho_{z_{01}} + \rho_{z_{10}}\right)$, has the following form

$$s_1^Z \geq s_1^Z = \frac{1}{2}\left(s_{z_{01}}^L + s_{z_{10}}^L\right). \tag{6}$$

Note: Replacing the source ρ_2 used in Eqs (4–6) with the source ρ_z, we obtain the other lower bound of s_1^Z. With this replacement, source ρ_2 is not used actually, then the four-intensity decoy-state method can be simplified to a three-intensity decoy-state method by taking $p_2 = 0$. On the one hand, the three-intensity decoy-state method can be carried out easily in experiment. On the other hand, interested more in terms of practical key-rates instead of achieving the longest distance QKD possible (such as 10^{-6} per-pulse), the key rate of the three-intensity decoy-state method is only a little lower than (less than one percent for the cases discussed in the numerical simulation) the results for the four-intensity decoy-state method.

In the rest of this section, we show the formula to estimate the upper bound of e_1^{ph} in Eq. (2) with the observable. The state of pulse pair when Alice sends the coherent state $\left|\alpha_1^A = \sqrt{\mu_1}e^{i\theta_A}\right\rangle$ and Bob sends the coherent state $\left|\alpha_1^B = \sqrt{\mu_1}e^{i\theta_B}\right\rangle$ is

$$\begin{aligned}
|\alpha_1^A\rangle|\alpha_1^B\rangle &= |\sqrt{\mu_1}e^{i\theta_A}\rangle|\sqrt{\mu_1}e^{i\theta_B}\rangle = e^{-\mu_1}\sum_{k_1,k_2}\frac{\left(\sqrt{\mu_1}e^{i\theta_A}\right)^{k_1}\left(\sqrt{\mu_1}e^{i\theta_B}\right)^{k_2}}{\sqrt{k_1!}\sqrt{k_2!}}|k_1\rangle|k_2\rangle \\
&= e^{-\mu_1}\left[|00\rangle + \sqrt{\mu_1}(e^{i\theta_B}|01\rangle + e^{i\theta_A}|10\rangle) + \mu_1\left(\frac{e^{2i\theta_B}}{\sqrt{2}}|02\rangle\right.\right. \\
&\quad \left.\left. + e^{i(\theta_A+\theta_B)}|11\rangle + \frac{e^{2i\theta_A}}{\sqrt{2}}|20\rangle\right) + \cdots\right] \\
&= e^{-\mu_1}\left[|00\rangle + \sqrt{2\mu_1}e^{i\theta_B}|\psi_1^{\delta^+}\rangle + \frac{\left(\sqrt{2\mu_1}e^{i\theta_B}\right)^2}{\sqrt{2}}|\psi_2^{\delta^+}\rangle + \cdots\right] \\
&= e^{-\mu_1}\sum_{n=0}^{\infty}\frac{\left(\sqrt{2\mu_1}e^{i\theta_B}\right)^n}{\sqrt{n!}}|\psi_n^{\delta^+}\rangle.
\end{aligned} \tag{7}$$

Similarly, we also have

$$|\alpha_1^A\rangle| - \alpha_1^B\rangle = e^{-\mu_1}\sum_{n=0}^{\infty}\frac{\left(-\sqrt{2\mu_1}e^{i\theta_B}\right)^n}{\sqrt{n!}}|\psi_n^{\delta^-}\rangle. \tag{8}$$

In Eqs (7) and (8), the n-photon twin-field state $\left|\psi_n^{\delta^\pm}\right\rangle$ is defined as follows

$$|\psi_n^{\delta^+}\rangle = \frac{1}{\sqrt{2^n}}\sum_{m=0}^{n}\frac{\sqrt{n!}\,e^{im\delta}}{\sqrt{m!(n-m)!}}|m\rangle|n-m\rangle, \tag{9}$$

$$|\psi_n^{\delta^-}\rangle = \frac{1}{\sqrt{2^n}}\sum_{m=0}^{n}\frac{(-1)^m\sqrt{n!}\,e^{im\delta}}{\sqrt{m!(n-m)!}}|m\rangle|n-m\rangle, \tag{10}$$

where $\delta = \theta_A - \theta_B$. For the state in set C_{Δ^+}, the phase is selected uniformly at random in the slice with $|\theta_A - \theta_B| \leq \Delta/2$. Equivalently, in set C_{Δ^+}, the phase θ_B chosen by Bob in $|\alpha_1^A\rangle|\alpha_1^B\rangle$ can be regarded as uniformly distributed in $[0, 2\pi)$ and the phase θ_A chosen by Alice satisfies the condition $|\delta| \leq \Delta/2$. For any fixed value δ, we have

$$\rho_{\delta^+} = \frac{1}{2\pi}\int_0^{2\pi} |\alpha_1^A\rangle|\alpha_1^B\rangle\langle\alpha_1^A|\langle\alpha_1^B|d\theta_B = e^{-2\mu_1}\sum_{n=0}^{\infty}\frac{(2\mu_1)^n}{n!}|\psi_n^{\delta^+}\rangle\langle\psi_n^{\delta^+}|. \tag{11}$$

Similarly, we also have

$$\rho_{\delta^-} = \frac{1}{2\pi}\int_0^{2\pi} |\alpha_1^A\rangle|-\alpha_1^B\rangle\langle\alpha_1^A|\langle-\alpha_1^B|d\theta_B = e^{-2\mu_1}\sum_{n=0}^{\infty}\frac{(2\mu_1)^n}{n!}|\psi_n^{\delta^-}\rangle\langle\psi_n^{\delta^-}|. \tag{12}$$

Considering the single-photon twin-field states in $C_\Delta = C_{\Delta^+} \cup C_{\Delta^-}$ for a fixed δ, we have

$$\rho_1^{\delta} = \frac{1}{2}(|\psi_1^{\delta^+}\rangle\langle\psi_1^{\delta^+}| + |\psi_1^{\delta^-}\rangle\langle\psi_1^{\delta^-}|) = \rho_1^Z. \tag{13}$$

So we know that the single-photon states in set C_Δ and in Z-basis have the same density matrices. The probability to emit a single-photon pulse from C_Δ is $q_1 = 2\mu_1 e^{-2\mu_1}$. With this relations, we know that the bit-flip error rate of single-photon state in set C_Δ is equal to the phase-flip error rate e_1^{ph} asymptotically. The bit-flip error yield for all instances in set C_Δ is

$$T_\Delta = \frac{1}{2}(T_{\Delta^+} + T_{\Delta^-}) = \frac{1}{2}(n_{11}^{\Delta_1^+}/N_{11}^{\Delta^+} + n_{11}^{\Delta_0^-}/N_{11}^{\Delta^-}). \tag{14}$$

where T_k, $k = \Delta, \Delta^+, \Delta^-$ is the proportion of wrong effective events in C_k, e.g. in N_{11}^k. Attribute all the error to the single-photon state and the vacuum state, the upper bound of phase-flip error rate e_1^{ph} can be estimated by

$$e_1^{ph} \le \bar{e}_1^{ph} = \frac{T_\Delta - 1/2e^{-2\mu_1}S_{00}}{2\mu_1 e^{-2\mu_1}\underline{s}_1^Z}, \tag{15}$$

where $\underline{s}_1^Z$ is the lower bound of s_1^Z given in Eq. (6). Then the final key rate of per pulse can be calculated with

$$R = (1 - p_X)^2\{2p_z(1 - p_z)a_1 s_1[1 - H(e_1^{ph})] - fS_Z H(E_Z)\}, \tag{16}$$

where R is the final key rate, $a_1 = \mu_z e^{-\mu_z}$ is the probability to emit a single-photon state from source ρ_z, s_1 is the yield of the single-photon state in Z-window when one party from Alice and Bob decides to send a signal states, e_1^{ph} is the phase-flip error rate for those instance of s_1, S_Z and E_Z are the yield and bit-flip error rate for instances when both Alice and Bob choose Z-window.

Statistical fluctuation analysis. In the real protocol with finite data size, in order to extract the secure final key, we have to consider the effect of statistical fluctuations. To obtain the lower bound value for s_1 and the upper bound value for e_1^{ph} in the real protocol with finite N, one can implement the idea of ref.[25], i.e., treating the averaged yield. Accordingly, define $\langle S\rangle$ as the mean value of yield S. Note that even though $S_{jk}(j, k = 0, 1, 2, z)$ are known values directly observed in the experiment, the mean values $\langle S_{jk}\rangle$ are not. However, given the observed values S_{jk} and the corresponding number of pulse pairs, the confidence lower and upper limits of $\langle S_{jk}\rangle$ can be calculated.

In order to obtain a tighter lower bound of $\langle s_1^Z\rangle$, we need introduce the following two yields

$$S_1 = \frac{1}{2}(S_{01} + S_{10}) = \frac{n_{01}}{2N_{01}} + \frac{n_{10}}{2N_{10}}, \tag{17}$$

$$S_2 = \frac{1}{2}(S_{02} + S_{20}) = \frac{n_{02}}{2N_{02}} + \frac{n_{20}}{2N_{20}}, \tag{18}$$

Replacing the observed yields with their mean values in Eqs (6) and (15), we can formulate the lower bound of $\langle s_1^Z\rangle$ and the upper bound of $\langle e_1^{ph}\rangle$ respectively. Explicitly, we have

$$\langle s_1^Z\rangle \ge \langle \underline{s}_1^Z\rangle = \frac{\mu_2^2 e^{\mu_1}\underline{S}_1 - \mu_1^2 e^{\mu_2}\overline{S}_2 - (\mu_2^2 - \mu_1^2)\overline{S}_{00}}{\mu_1\mu_2(\mu_2 - \mu_1)}, \tag{19}$$

and

$$\langle e_1^{ph}\rangle \le \langle \bar{e}_1^{ph}\rangle = \frac{\overline{T}_\Delta - 1/2e^{-2\mu_1}\underline{S}_{00}}{2\mu_1 e^{-2\mu_1}\langle \underline{s}_1^Z\rangle}. \tag{20}$$

with

$$\underline{\mathcal{U}}_k = \mathcal{U}_k/(1+\delta_k),\ \overline{\mathcal{U}}_k = \mathcal{U}_k/(1-\delta'_k), \tag{21}$$

for $\mathcal{U} = S,\ T$ and $k = 00, 1, 2$ and Δ. By using the multiplicative form of the Chernoff bound[29,33], with a fixed failure probability ε, we can give an interval of $\langle S_k\rangle$ with the observable $S_k, [\underline{S}_k,\ \overline{S}_k]$, which can bound the value of $\langle S_k\rangle$ with a probability of at least $1-\varepsilon$. Explicitly, with the function $f_\delta(x,\ y) = [-\ln(y/2) + \sqrt{(\ln(y/2))^2 - 8\ln(y/2)x}]/(2x)$, we have $\delta_{00} = f_\delta(N_{00}S_{00}, \varepsilon)$, $\delta_j = f_\delta((N_{0j}+N_{j0})S_j, \varepsilon)$, $j = 1$, 2 and $\delta_\Delta = f_\delta((N_{11}^{\overline{\Delta}} + N_{11}^{\underline{\Delta}})T_\Delta,\ \varepsilon)$.

With the mean values $\langle \underline{s}_1^Z\rangle$ and $\langle \bar{e}_1^{ph}\rangle$ defined in Eqs (19) and (20), the lower bound of the yield $\underline{s}_1$ and the upper bound of the phase-flip error rata $\bar{e}_1^{ph}$ corresponding to s_1 in Eq. (16) can be estimated by[29,33]

$$\underline{s}_1 = \langle \underline{s}_1^Z\rangle(1-\delta_1^c), \quad \bar{e}_1^{ph} = \langle \bar{e}_1^{ph}\rangle(1+\delta_1^{\prime c}), \tag{22}$$

where $\delta_1^c = f_\delta(a_1 N_{zz}^c \langle \underline{s}_1^Z\rangle,\ \varepsilon)$ and $\delta_1^{\prime c} = f_\delta(a_1 N_{zz}^c \underline{s}_1 \langle \bar{e}_1^{ph}\rangle,\ \varepsilon)$ with $N_{zz}^c = 2p_z(1-p_z)N_{zz}$ and $a_1 = \mu_z e^{-\mu_z}$ being the probability to emit a single-photon state from source ρ_z.

With the lower bound of s_1 and the upper bound of e_1^{ph} in Eq. (22), the final key rate can be calculated with Eq. (16).

References

1. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Physical Review A* **98**, 062323 (2018).
2. Bennett, C. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (1984).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Reviews of modern physics* **74**, 145 (2002).
4. Gisin, N. & Thew, R. Quantum communication. *Nature photonics* **1**, 165 (2007).
5. Dušek, M., Lütkenhaus, N. & Hendrych, M. Quantum cryptography. *Progress in Optics* **49**, 381–454 (2006).
6. Scarani, V. *et al*. The security of practical quantum key distribution. *Reviews of modern physics* **81**, 1301 (2009).
7. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Physical Review Letters* **85**, 1330 (2000).
8. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Physical Review A* **61**, 052304 (2000).
9. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics* **4**, 44 (2002).
10. Inamori, H., Lütkenhaus, N. & Mayers, D. Unconditional security of practical quantum key distribution. *The European Physical Journal D* **41**, 599 (2007).
11. Gottesman, D., Lo, H.-K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, 136 (IEEE, 2004).
12. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters* **91**, 057901 (2003).
13. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters* **94**, 230503 (2005).
14. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Physical review letters* **94**, 230504 (2005).
15. Adachi, Y., Yamamoto, T., Koashi, M. & Imoto, N. Simple and efficient quantum key distribution with parametric down-conversion. *Physical review letters* **99**, 180503 (2007).
16. Hayashi, M. Practical evaluation of security for quantum key distribution. *Physical Review A* **74**, 022307 (2006).
17. Hayashi, M. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Physical Review A* **76**, 012329 (2007).
18. Rosenberg, D. *et al*. Long-distance decoy-state quantum key distribution in optical fiber. *Physical review letters* **98**, 010503 (2007).
19. Schmitt-Manderbach, T. *et al*. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters* **98**, 010504 (2007).
20. Peng, C.-Z. *et al*. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Physical review letters* **98**, 010505 (2007).
21. Yuan, Z., Sharpe, A. & Shields, A. Unconditionally secure one-way quantum key distribution using decoy pulses. *Applied physics letters* **90**, 011118 (2007).
22. Wang, X.-B., Peng, C.-Z., Zhang, J., Yang, L. & Pan, J.-W. General theory of decoy-state quantum cryptography with source errors. *Physical Review A* **77**, 042311 (2008).
23. Hu, J.-Z. & Wang, X.-B. Reexamination of the decoy-state quantum key distribution with an unstable source. *Physical Review A* **82**, 012331 (2010).
24. Wang, X.-B., Hiroshima, T., Tomita, A. & Hayashi, M. Quantum information with gaussian states. *Physics reports* **448**, 1–111 (2007).
25. Wang, X.-B., Yang, L., Peng, C.-Z. & Pan, J.-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New Journal of Physics* **11**, 075006 (2009).
26. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Physical review letters* **108**, 130502 (2012).
27. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Physical review letters* **108**, 130503 (2012).
28. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A* **87**, 012320 (2013).
29. Curty, M. *et al*. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature communications* **5**, 3732 (2014).
30. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Three-intensity decoy-state method for measurement-device-independent quantum key distribution. *Physical Review A* **88**, 062339 (2013).
31. Xu, F., Xu, H. & Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Physical Review A* **89**, 052333 (2014).
32. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Physical Review A* **91**, 032318 (2015).
33. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Physical Review A* **93**, 042324 (2016).
34. Comandar, L. *et al*. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics* **10**, 312 (2016).

35. Wang, C. *et al*. Measurement-device-independent quantum key distribution robust against environmental disturbances. *Optica* **4**, 1016–1023 (2017).
36. Yin, H.-L. *et al*. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical review letters* **117**, 190501 (2016).
37. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics* **11**, 045018 (2009).
38. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475 (2014).
39. Chau, H. Quantum key distribution using qudits that each encode one bit of raw key. *Physical Review A* **92**, 062324 (2015).
40. Azuma, K., Tamaki, K. & Munro, W. J. All-photonic intercity quantum key distribution. *Nature communications* **6**, 10171 (2015).
41. Takesue, H., Sasaki, T., Tamaki, K. & Koashi, M. Experimental quantum key distribution without monitoring signal disturbance. *Nature Photonics* **9**, 827 (2015).
42. Roberts, G. *et al*. Experimental measurement-device-independent quantum digital signatures. *Nature Communications* **8**, 1098 (2017).
43. Liao, S.-K. *et al*. Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
44. Liao, S.-K. *et al*. Satellite-relayed intercontinental quantum network. *Physical review letters* **120**, 030501 (2018).
45. Lucamarini, M., Yuan, Z., Dynes, J. & Shields, A. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018).
46. Tamaki, K., Lo, H. -K., Wang, W. & Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv preprint arXiv:1805.05511* (2018).
47. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Physical Review X* **8**, 031043 (2018).
48. Cui, C. *et al*. Phase-matching quantum key distribution without phase post-selection. *arXiv preprint arXiv:1807.02334* (2018).
49. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nature communications* **8**, 15043 (2017).
50. Boaron, A. *et al*. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters* **121**, 190502 (2018).

Acknowledgements

We acknowledge the financial support in part by Ministration of Science and Technology of China through The National Key Research and Development Program of China grant No. 2017YFA0303901; National Natural Science Foundation of China grant No. 11474182, 11774198 and U1738142.

Author Contributions

X.B.W. and Z.W.Y. proposed this work. X.L.H., C.J. and H.X. did the calculations and drew the figures. Z.W.Y. and X.L.H. wrote the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.