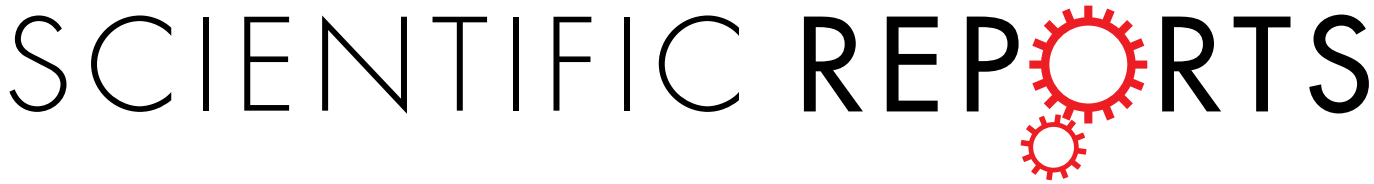

OPEN

Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources

Received: 27 January 2015
Accepted: 21 September 2015
Published: 16 October 2015

Ting-Ting Song[1,2], Su-Juan Qin[2], Qiao-Yan Wen[2], Yu-Kun Wang[2] & Heng-Yue Jia[3]

In quantum communication, passive decoy-state QKD protocols can eliminate many side channels, but the protocols without any finite-key analyses are not suitable for in practice. The finite-key securities of passive decoy-state (PDS) QKD protocols with two different unstable sources, type-II parametric down-convention (PDC) and phase randomized weak coherent pulses (WCPs), are analyzed in our paper. According to the PDS QKD protocols, we establish an optimizing programming respectively and obtain the lower bounds of finite-key rates. Under some reasonable values of quantum setup parameters, the lower bounds of finite-key rates are simulated. The simulation results show that at different transmission distances, the affections of different fluctuations on key rates are different. Moreover, the PDS QKD protocol with an unstable PDC source can resist more intensity fluctuations and more statistical fluctuation.

Since the rapid development of quantum information, based on quantum mechanics and classical communication to achieve unconditional security, quantum cryptography has become the most important field of quantum information. The first proposed quantum key distribution (i.e., QKD) protocol, BB84 protocol[1], was proved to be unconditionally secure under the perfect conditions[2], which include perfect single-photon source, perfect measurement devices.

Also, the unconditional security of BB84 protocol is with the assumption "Alice and Bob exchange infinite pulses". Actually, this assumption is inconsistent with the practical situation. The length of exchanged pulses is limited by the link duration constraints and memory resources on one side and efficiency on the other. In the use with satellites, the communication between the orbiting terminal and the ground station is restricted to a few minutes in the case of low-earth-orbit satellite[3,4] or to about one hour for the medium-earth-orbit ones[5]. Furthermore, many researches on the finite-key BB84 protocols with decoy states[6–8] showed that the finite pulses make an ideal remote QKD protocol into a short-distance but practical QKD protocol. Hence, for the practical application of QKD protocols, it is of crucial importance to analyze the security in the finite-key scenario, which should consider the affection of finite number of pulses.

Following the statistical fluctuation theory, the security of decoy-state QKD protocol is reflected by the lower bound of the key rate for the finite-key model. Suppose the eavesdropper operates the collective attack, the general formula for the lower bound of the final key rate with statistical fluctuations is

$$r = q\left\{p_0^L Y_0^L + p_1^L Y_1^L [1 - h(e_1^U)] - f_{EC} Qh(E^U)\right\} - \Delta, \quad (1)$$

where q is the number of raw key per pulse received by Bob, p_0^L and p_1^L are the lower bounds of probability of the vacuum state and that of single-photon state sent from the signal source, Y_0^L and Y_1^L are the

[1]Department of Computer Science, College of Information Science and Technology, Jinan University, Guangzhou, 510632, China. [2]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [3]School of Information, Central University of Finance and Economics, Beijing, 100081, China. Correspondence and requests for materials should be addressed to T.-T.S. (email: tingtingsong@jnu.edu.cn.)

lower bounds of clicking rate for vacuum state and single-photon state, e_1^U is the upper bound of error rate for single-photon state, f_{EC} reflects the deviation of practical error-correction codes from the Shannon limit, Q and E^U are the gain and the upper bound of the error rate for signal pulses generated to the final key, $h(\cdot)$ is the Shannon entropy, $h(E^U)$ shows part of the information leaked to Eve during the error correction step, and the other part is included in Δ. Δ is comprised by the fluctuations of practical key rate induced by the "smoothing" level of min- and max-entropy $\bar{\varepsilon}$[6,7,9], the failure probability of privacy amplification ε_{PA} and the failure probability of error correction ε_{EC}. As refs 6,7,10 pointed out, Δ can be quantified by

$$\Delta = 7\sqrt{\frac{qQ}{2N}\log_2(2/\bar{\varepsilon})} + \frac{2}{N}\log_2(1/\varepsilon_{PA}) + \frac{1}{N}\log_2(2/\varepsilon_{EC}), \tag{2}$$

where N is the number of signal pulses sent from the source. The finite-key QKD protocol is called ε-secure, i.e., $\varepsilon = \varepsilon_{PA} + \varepsilon_{EC} + \bar{\varepsilon} + n_{PE}\varepsilon_{PE}$, where n_{PE} is the number of parameters that must be estimated, and ε_{PE} is the failure probability of parameter estimation.

For the practical finite QKD protocols, there also exist two side channels. One follows the intensity modulator. In decoy-state QKD protocol, Alice modulates actively the weak laser into two weak coherent sources with different intensities. This is an elegant solution to implement the BB84 protocol, but some loopholes emerge in the practical implementations with Plug & Play systems[11]. So the finite passive-decoy-state (PDS) QKD protocols are thus desirable. Two, all the sources mentioned above are stable, i.e., the intensities are fixed. Actually, there exists the intensity fluctuations[12] in practical sources. This is induced by the practical unstable sources[13–16]. No source can be perfectly stable. So does the sources in the finite PDS QKD protocols. That the sources are unstable means, at each time i, the intensity of source prepared by sender is $u_i = (1 + \epsilon_i)u$ where u is the expected intensity of the source, and ϵ_i reflects the intensity fluctuation varying with the time i. The imperfection leaves a backdoor to eavesdropper, so the finite security of PDS QKD protocols with intensity fluctuations must be analyzed. In order to make sure the practical security of QKD protocols, this paper analyzes the finite securities of PDS QKD protocols with two unstable sources, type-II parametric down-convention (PDC) source[17–19] and weak coherent pulses (WCPs)[20,21].

Results

This paper concerns on two kinds of fluctuations, intensity fluctuation and photon-number distribution fluctuation. Imprecise intensity control generates sources with intensity fluctuations. Because of the finite number of pulses in practical experiment, some parameters are to be with photon-number distribution fluctuations. We propose two finite PDS QKD protocols under different unstable sources, PDC source and WCPs. The process of two protocols and corresponding security analyses are as follows.

Passive decoy-state QKD protocol with an unstable PDC source. Type-II PDC source could send out two pulses with the same number of photons at one time, but the polarizations of photons in the two pulses are different. Since the errors of PDC source[12], especially the intensity fluctuations, the initial states sent from the source are different from the assumed states that Alice wants. Here, we only consider the affection of intensity fluctuations on the security of the QKD protocol with finite keys.

PDC source would send a pair of pulses at each integer time. If N pairs of pulses are sent, time i belongs to the integer set $[1, N]$. At time i, the intensity of PDC source is $u_i = u(1 + \epsilon_i)$ where u is the expected intensity and ϵ_i reflects the intensity fluctuations and its value belongs to the set $[-\epsilon, \epsilon]$ except with a small probability, so the initial state sent from the unstable PDC source at time i is $|\Psi_i\rangle = \sum_{k=0}^{\infty}\sqrt{u_i^k/(1+u_i)^{k+1}}\,|k\rangle\,|k\rangle$ where the k-photon pulse is sent with the probability $p_{ki} = u_i^k/(1+u_i)^{k+1}$. The two pulses go to different paths. The first pulse is sent to the polarization-independent detector located in Alice's lab. The polarization of the second pulse is modulated according to Alice's secret. Then the modulated pulse is sent to Bob through a high loss quantum channel. Bob receives the pulse, does the measurement with the basis randomly chosen by him, and records the result.

The transmitted part of quantum-state is finished, and the following part is the classical information post-process. After comparing the basis published by Bob, Alice tells Bob whether the bit is kept. If the bases used by Alice and Bob are same, the bit is kept, otherwise it is dropped. Then Alice and Bob repeat the previous steps many times until they get a string of bits. All the kept bits form the sifted bit sequence. According to the results of Alice's detections, the sifted key bits are divided into two classes, the sifted bits with triggered and the sifted bits without triggered, as "trigger" and "non-trigger"[17–19], respectively. Half of the sifted trigger pulses are the raw keys generated to the final keys, and the other half is used to estimate the bit error rate. The sifted non-trigger pulses are used to estimate the phase error rate.

The security analysis of the protocol is as follows. The trigger pulses and the non-trigger pulses are classified passively according to the results of corresponding pulses at Alice's detector. Before the corresponding pulses arrived at her detector, Alice has no information about the classification of the pulses, so the eavesdropper has no information on the pulses before they arrive at Alice's detectors, either. Thus

the classifying method is passive and secure to any powerful eavesdropper. The security of the following steps in PDS QKD protocol with an unstable PDC source is equivalent to that of standard BB84 protocol with decoy method. The protocol introduced above is secure.

Now we show that how to get the lower bound of the finite-key rate with the affections of intensity fluctuations and photon-number distribution fluctuations. In the PDS QKD protocol with an unstable PDC source, whatever the intensity fluctuation is at each time, Alice knows the maximum and the minimum of the expected intensity, and the two boundary values should be estimated with statistical fluctuation. The failure probability of parameter estimation is denoted as ε_{PE}. According to the statistical fluctuation of photon-number distribution, we can get the lower bound of the key rate for the PDS QKD protocol. In the following, we give the particular analysis on that how to get the lower bound of the finite-key rate with the affections of intensity fluctuations and statistical fluctuations.

In our analysis, we assumed the worst case that eavesdropper knows exactly the intensity fluctuation of each pulse, as Refs 13–16, so the clicking rate of k-photon pulses at Bob's detector and the error rate of k-photon pulses are both changed with time i, which is different from earlier work[6–8]. Thus the number of sifted trigger pulses received by Bob is $N^t = \sum_{k=0}^{\infty} N_k^t = \frac{1}{2}\sum_{k=0}^{\infty}\sum_{i=1}^{N} p_{ki}\gamma_k Y_{ki}$, and the number of sifted non-triggered pulses received by Bob is $N^{nt} = \sum_{k=0}^{\infty} N_k^{nt} = \frac{1}{2}\sum_{k=0}^{\infty}\sum_{i=1}^{N} p_{ki}(1-\gamma_k) Y_{ki}$, where N is the total number of pulses sent from the source, p_{ki} is the probability that Alice sends a pair of k-photon pulse to Bob at time i, γ_k is the clicking rate of Alice's detector for k-photon pulse, and Y_{ki} is the clicking rate of Bob's detectors at time i when Alice sends Bob a k-photon pulse. Note that here we suppose that the clicking rate γ_k doesn't vary with time. Denote the number of bit errors and that of phase errors checked by Alice and Bob as n^t and n^{nt} respectively. There have $n^t = \sum_{k=0}^{\infty} n_k^t = \frac{1}{2}\sum_{k=0}^{\infty}\sum_{i\in T} p_{ki}\gamma_k Y_{ki} e_{ki}$ and $n^{nt} = \sum_{k=0}^{\infty} n_k^{nt} = \frac{1}{2}\sum_{k=0}^{\infty}\sum_{i=1}^{N} p_{ki}(1-\gamma_k) Y_{ki} e_{ki}$, where set T has $N/2$ elements randomly chosen from the index set $[1, N]$, and e_{ki} is the error rate of Bob's sifted results when Alice sends Bob a k-photon pulse at time i.

Generally speaking, the probability of k-photon trigger pulses is different from that of k-photon non-trigger pulses, thus the sifted trigger pulses and the sifted non-trigger pulses could give the lower bound of the key rate by the economic estimated method[15]. But here has another problem: any expect value as $\langle N^t\rangle$, $\langle N^{nt}\rangle$, $\langle n^t\rangle$, $\langle n^{nt}\rangle$, and their bound values with intensity fluctuation $\langle N^t\rangle^{U(L)}$, $\langle N^{nt}\rangle^{U(L)}$, $\langle n^t\rangle^{U(L)}$, $\langle n^{nt}\rangle^{U(L)}$ do not be applied in practice directly. Practical implementation needs the practical values of these parameters, which should consider the influence of finite-number of pulses. We give the lower bounds and the upper bounds of these parameters by statistical fluctuation theory[8], as follows,

$$N^{tU} = \langle N^t\rangle^U + N\cdot\xi(N, 2),\ N^{ntL} = \langle N^{nt}\rangle^L - N\cdot\xi(N, 2), \tag{3}$$

$$n^{tU} = \langle n^t\rangle^U + \frac{\langle N^t\rangle}{2}\cdot\xi(\langle N^t\rangle/2, 2),\ n^{ntU} = \langle n^{nt}\rangle^U + \langle N^{nt}\rangle\cdot\xi(\langle N^{nt}\rangle, 2), \tag{4}$$

where $\xi(m, d) := \sqrt{\frac{\ln(1/\varepsilon_{PE}) + d\cdot\ln(m+1)}{2m}}$. Following Eq. (1), the lower bound of key rate for this PDS QKD protocol will be

$$r^L = -\Delta_{PDC} + \frac{1}{2N}\{N_1^{tL}[1 - h(e_1^U)] - f_{EC}N^{tU}h(E^U)\}, \tag{5}$$

where $\Delta_{PDC} = \frac{7}{2N}\sqrt{N^{tU}\log_2(2/\bar{\varepsilon})} + \frac{2}{N}\log_2(1/\varepsilon_{PA}) + \frac{1}{N}\log_2(2/\varepsilon_{EC})$, ε_{PA} and ε_{EC} are the failure probabilities of privacy amplification and the error correction respectively, N_1^{tL} is the lower bound of N_1^t, e_1^U is the upper bound of e_{1i}, and $E^U = 2n^{tU}/N^{tL} + \xi(N^{tU}/2, 2)$ is the upper bound of phase error rate of raw key. The rigorous proof of Eq. (5) is in Methods. Note that the lower (upper) bound of the expected value $\langle\star\rangle^{L(U)}$ mentioned here represents the lower (upper) bound of parameter $\star$with intensity fluctuation only, and the lower (upper) bound of the observed value $\star^{L(U)}$ represents the lower (upper) bound of parameter $\star$with both intensity fluctuation and statistical fluctuation.

Passive decoy-state QKD protocol with unstable WCPs. The requirement of PDS method is to have correlations between the photon number statistics of two signals. Curty *et al.*[22] pointed out that the photon numbers of outgoing pulses are classically relevant when two phased randomized WCPs interfere at a beam splitter. Based on this, we propose a PDS QKD protocol with unstable phased randomized WCPs, which could be realized easily by linear optical components. The setups are shown in Fig. 1.

The protocol is described below. Alice prepare one phase randomized weak coherent father source whose expected intensity is u. Due to intensity fluctuations, the output state from the father source at time i is $\rho_i = \sum_k e^{-u(1+\epsilon_i)}[u(1+\epsilon_i)]^k/k!|k\rangle\langle k|$, where ϵ_i gives the fluctuation of intensity, and its value belongs to $[-\epsilon, \epsilon]$ except with a small probability ε_{PE}. Through the beam splitter BS1, the pulses are separated into two parts, one to the upper path, and the other to the lower path. The upper part would

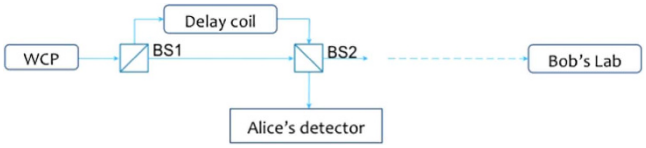

Figure 1. The apparatuses in PDS QKD protocol with an unstable WCP source.

interfere with the lower part on another beam splitter BS2 after the upper part transmitted through a delay coil. And there is a polarization independent detector at one of the outputs of BS2 which is located in Alice's lab. The pulses coming out from the other output of BS2 are sent to the receiver Bob. After receiving the pulses, Bob does the measurement with randomly chosen bases. The quantum distribution is finished, and the following process is classical process, including sifting data, error corrections and privacy amplification. Comparing the bases for each pulse, Alice and Bob keep the bits with same bases, and the bit sequence becomes the sifted key. To be concerned, the pulses sent to Bob are also passively classified into two kinds, "trigger" and "non-trigger", according to the results of the detector in Alice's lab. During the error correction process, all the sifted non-trigger pulses estimate the phase error rate, and half of the sifted trigger pulses estimates the bit error rate. According to the privacy amplification, the other half of the sifted trigger pulses is generated to the final key.

Note that there should be an intensity modulation (IM) before Bob's Lab, and its operation is correlated with the length of delay coil. Denote the state of the upper path and that of the lower path after BS1 at time i as ρ_{1i} and ρ_{2i}. We can adjust the length of the delay coil on the upper path to make the pulse $\rho_{1,i-1}$ sent at time $i-1$ and the pulse ρ_{2i} sent at time i interfere at BS2. In order to eliminate all the possible correlations between the results hold by Bob, IM should block the pulses arrived at even time or at odd time. Now the signal states that go to Bob are guaranteed to be tensor products of mixtures of Fock states.

The protocol would resist against the side channels on modulators and detectors. Suppose BS1 is with transitivity rate t_1, the state of the upper path and that of the lower path at time i are as follows:

$$\begin{aligned}\rho 1i &= \sum_{k=0}^{\infty}\frac{e^{-u(1+\varepsilon_i)(1-t_1)}[u(1+\varepsilon_i)(1-t_1)]^k}{k!}|k\rangle\langle k|,\\ \rho 2i &= \sum_{k=0}^{\infty}\frac{e^{-u(1+\varepsilon_i)t_1}[u(1+\varepsilon_i)t_1]^k}{k!}|k\rangle\langle k|.\end{aligned} \tag{6}$$

After through BS2 with transitivity rate t_2, the joint probability that k-photon pulse is sent to Bob and the m-photon pulse is sent to Alice's detector at time i is denoted as $p_{k,m,i}$, so the probability that k-photon pulse is sent to Bob at time i is denoted as $Q_{k,i}=\sum_{m=0}^{\infty}p_{k,m,i}$. If Alice's detector at the end of one output of BS2 responses with the probability γ_m for m-photon pulse, at time i the probability of non-triggered k-photon pulse sent to Bob is $Q_{k,i}^{nt}=\sum_{m=0}^{\infty}p_{k,m,i}(1-\gamma_m)$, and the probability of triggered k-photon pulse sent to Bob is $Q_{k,i}^{t}=Q_{k,i}-Q_{k,i}^{nt}$. At time i, the distributions $\{Q_{k,i}^{t}\}_{k=1}^{\infty}$ and $\{Q_{k,i}^{nt}\}_{k=0}^{\infty}$ are different but classical correlated. The pulses sent to Bob are passively classified into two classes, "trigger" and "non-trigger". During the pulses transmitted through the quantum channels, eavesdropper would get no information about the classification, no matter which kind of attack operated by her. Thus the PDS QKD protocol is secure without any information leakages.

Furthermore, same as the PDS QKD protocol with an unstable PDC source, whatever intensity fluctuates is at each time in the PDS QKD protocol with unstable WCPs, Alice only know the maximum and the minimum of the expected intensity. The failure probability of intensity-fluctuation estimation is also defined as ε_{PE}, then according to Eq. (1) we would get the lower bound of the key rate.

Suppose that the number of the pulses sent from the source is N, so time i is the integer in the set $[1, N]$, and IM blocks all the pulses sent at odd time. Same as the process of the PDS QKD protocol with an unstable PDC source, in this with unstable WCPs, both the clicking rate of k-photon pulses at Bob's side Y_{ki} and the error rate of k-photon pulses e_{ki} are correlated with time i, so the number of sifted trigger pulses and that of sifted non-trigger pulses received by Bob, respectively, are

$$N^t=\sum_{k=0}^{\infty}N_k^t=\sum_{k=0}^{\infty}\sum_{i=1}^{N/2}\frac{1}{2}Q_{k,2i}^{t}Y_{k,2i},\quad N^{nt}=\sum_{k=0}^{\infty}N_k^{nt}=\sum_{k=0}^{\infty}\sum_{i=1}^{N/2}\frac{1}{2}Q_{k,2i}^{nt}Y_{k,2i}, \tag{7}$$

where half of the sifted trigger pulses estimates the bit error rate, all the odd pulses are blocked by IM. The number of bit errors and that of phase errors are

$$n^t = \sum_{k=0}^{\infty} n_k^t = \sum_{k=0}^{\infty}\sum_{i\in T}\frac{1}{2}Q_{k,2i}^t Y_{k,2i} e_{k,2i}, \quad n^{nt} = \sum_{k=0}^{\infty} n_k^{nt} = \sum_{k=0}^{\infty}\sum_{i=1}^{N/2}\frac{1}{2}Q_{k,2i}^{nt} Y_{k,2i} e_{k,2i}, \tag{8}$$

where the set T has $N/4$ elements chosen randomly from the index set $[1, N/2]$. The expected values of above parameters can be calculated without considering the statistical fluctuations, and with statistical fluctuations we can get the practical values of these parameters. The relationship between the expected value and the practical values are same as Eq. (3). Based on the bounds of practical values $N^{tU(L)}$, $N^{ntU(L)}$, $n^{tU(L)}$, $n^{ntU(L)}$, the lower bound of key rate is received

$$r^L = -\Delta_{WCP} + \frac{1}{2N}\left\{N_1^{tL}[1 - h(e_1^U)] - f_{EC} N^{tU} h(E^U)\right\}, \tag{9}$$

where $\Delta_{WCP} = 7\sqrt{\frac{Q^{tU}}{16N}\log_2(2/\bar{\varepsilon})} + \frac{2}{N}\log_2(1/\varepsilon_{PA}) + \frac{1}{N}\log_2(2/\varepsilon_{EC})$, ε_{PA} and ε_{EC} are the failure probabilities of privacy amplification and the error correction respectively, N_1^{tL} is the lower bound of N_1^t, e_1^U is the upper bound of $e_{1,2i}$, and $E^U = 2n^{tU}/N^{tL} + \xi(N^{tU}/2, 2)$ is the upper bound of phase error rate of raw key. As described earlier, $\langle\star\rangle^{L(U)}$ denotes the lower (upper) bound of the expected value, and $\star^{L(U)}$ represents the lower (upper) bound of the observed value. Note that the formula of failure probability applied in this work is actually for a stable source while here we are studying the performance of QKD with an unstable. This issue should be further studied in the future. The rigorous process to get the parameters in Eq. (9) is in Methods.

Discussion

In this section, we will discuss the asymptotic finite-key rate with the unstable PDC source and that with the unstable WCPs. For this purpose, we firstly establish the models for quantum setups. In both PDS QKD protocols, the model for Alice's detector and that for quantum channel including Bob's detectors are same. Suppose Alice's detector is with efficiency η_A and dark count rate d_A. The detector is triggered by the k-photon pulse with the rate $\gamma_k = 1 - (1 - d_A)(1 - \eta_A)^k$, so the non-triggered rate is $1 - \gamma_k = (1 - d_A)(1 - \eta_A)^k$. Furthermore, we establish the model for the expected value $\langle Y_k\rangle$, and this simplification wouldn't affect the accuracy of the following discussion because the finite-key rates are related with the boundary values. The k-photon pulse that Alice sends to Bob would click on Bob's detectors with the expected probability $\langle Y_k\rangle = 1 - (1 - d_B)(1 - \eta)^k$, where d_B is the dark count rate of Bob's detectors, $\eta = \eta_B\eta_C = \eta_B 10^{-\alpha l/10}$ is the total transmission rate, η_B is the efficiency of Bob's detector, η_C is the transmittance of quantum channels, α (dB/km) is the lossy rate of quantum channels, and l (km) is the transmission distance. Then the different models and simulation results for two PDS QKD protocols are as follows.

Model for an unstable PDC source. Based on the model of detectors described before, we would get the gains and error rates for the PDS QKD protocol with an unstable PDC source

$$\begin{aligned}
\langle N^t\rangle^U &= \frac{N}{2}\left[1 - \frac{1 - d_A}{1 + u^U\eta_A} - \frac{1 - d_B}{1 + u^U\eta} + \frac{(1 - d_A)(1 - d_B)}{1 + u^U(\eta_A + \eta - \eta_A\eta)}\right]\\
\langle N^{nt}\rangle^L &= \frac{N}{2}\left[\frac{1 - d_A}{1 + u^L\eta_A} - \frac{(1 - d_A)(1 - d_B)}{1 + u^L(\eta_A + \eta - \eta_A\eta)}\right],\\
\langle n^t\rangle^U &= e_d\cdot\frac{\langle N^t\rangle^U}{2} + \frac{N}{4}\cdot\frac{(1 - 2e_d)(u^U\eta_A + d_A)d_B}{2(1 + u^U\eta_A)},\\
\langle n^{nt}\rangle^U &= e_d\cdot\langle N^{nt}\rangle^U + \frac{N}{2}\cdot\frac{(1 - 2e_d)(1 - d_A)d_B}{2(1 + u^U\eta_A)},
\end{aligned} \tag{10}$$

where e_d is the error rate of Bob's detectors. The upper bounds are all obtained when the intensity of the source reaches the maximum value u^U with a large probability. Correspondingly, the lower bound is received with minimum value of the intensity u^L.

Model for an unstable WCP source. Following the models of quantum setups and the protocol in Results, we obtain the probability that Alice's detectors at time i are non-triggered, i.e., $Q_{pro,i}^{nt} = \sum_{k=0}^{\infty} Q_{k,i}^{nt} = (1 - d_A)e^{-\eta_A\chi_i} I_{0,\eta_A\beta_i}$, where $\beta_i = 2u\sqrt{(1 + \varepsilon_{i-1})(1 - t_1)(1 - t_2)(1 + \varepsilon_i)t_1t_2}$, $\chi_i = u(1 + \varepsilon_i)t_1(1 - t_2) + u(1 + \varepsilon_{i-1})(1 - t_1)t_2$, $I_{x,z}$ represents the modified Bessel function of first kind and is defined as $I_{x,z} = \frac{1}{2\pi i}\oint e^{\frac{z}{2}(t + \frac{1}{t})}t^{-x-1}dt$. Supplementary Material shows the calculating process that how to get $Q_{pro,i}^{nt}$ and the upper bounds of some expect values except the followings,

$$\begin{aligned}
\langle N'\rangle^U &= \frac{N}{4}\Big[1-(1-d_B)e^{-\eta\langle w\rangle^U}I_{0,\eta\langle w\rangle^U}\Big],\\
\langle N^{nt}\rangle^L &= \frac{N}{4}\Big[\Big\langle Q_{pro}^{nt}\Big\rangle^L-(1-d_A)(1-d_B)e^{(\eta_A-\eta)\langle w\rangle^L-\eta_A u^L}I_{0,(\eta_A-\eta)\langle\beta\rangle^L}\Big],\\
\langle n'\rangle^U &= e_d\langle N'\rangle^U+\frac{N}{4}\Big(\frac{1}{2}-e_d\Big)d_B,\\
\langle n^{nt}\rangle^U &= e_d\langle N^{nt}\rangle^U+\frac{N}{4}\Big(\frac{1}{2}-e_d\Big)d_B\Big\langle Q_{pro}^{nt}\Big\rangle^U,
\end{aligned}\tag{11}$$

where N' is the number of pulses received by Bob, n' is the number of error bits in the pulses received by Bob, and

$$\begin{aligned}
\langle w\rangle^U &= u^U t_1 t_2+u^U(1-t_1)(1-t_2),\ \Big\langle Q_{pro}^{nt}\Big\rangle^U=(1-d_A)e^{-\eta_A\langle\chi\rangle^L}I_{0,\eta_A\langle\beta\rangle^L},\\
\langle\chi\rangle^U &= u^U-\langle w\rangle^U,\ \langle\beta\rangle^U=2u^U\sqrt{(1-t_1)(1-t_2)t_1t_2}.
\end{aligned}\tag{12}$$

Simulation Results. We simulate the finite-key rates for both of PDS QKD protocols based on the models. The values of some experimental parameters in Eqs (10,11) are supposed to be as follows. Assume Alice's detector is a typical silicon avalanche photodiode with $d_A=3.2*10^{-7}$ and $\eta_A=0.12$. Other experimental parameters are chosen as Refs 10,23–30: the detection efficiency of Bob's detectors $\eta_B=0.045$, the dark count rate of Bob's detectors $d_B=1.7*10^{-6}$, the loss coefficient of the quantum channel $\alpha=0.21$, the error rate of the optical system $e_d=0.015$, and the efficiency of error correction code $f=1.22$. The sum of all failure probabilities is $\varepsilon=10^{-5}$, and the failure probability of parameter estimation is $\varepsilon_{EC}=10^{-10}$. Followed the equations about the lower bounds of finite-key rates, the other parameters are optimized to maximize the finite-key rates, including the expected intensity u, the failure probabilities ε_{PA}, ε_{PE}, the transmission rates of beam splitters t_1, t_2.

Figure 2 (Left) shows the lower bounds of key rates for PDS QKD protocols with a PDC source under the conditions that Bob receives 10^9, 10^{10}, 10^{11} and infinite pulses, when the transmission distance is fixed as 50 km. The corresponding optimal number of pulses sent from the PDC source is shown in Fig. 2(Right). From the curves in Fig. 2(Left), we know that the lower bounds of key rates without intensity fluctuations are all with the order of 10^{-5}. With the intensity fluctuations increasing, the key rates decrease, and the finite-key rates approach to the infinite-key rates with the number of pulses increasing too much. Furthermore, in order to find the main affection on key rates[15], we give the lower bounds of key rates without intensity fluctuations or without photon-number-distribution fluctuation in Fig. 3. When there is no photon-number-distribution fluctuation, the protocol has positive key rates with intensity fluctuations $\varepsilon<0.2$, and the key rates without intensity fluctuations are about 10 times than the key rates with $\varepsilon=0.15$ if the transmittance distance is shorter than 100 km. Moreover, if the PDC source is stable, the lower bound of finite-key rates in the PDS QKD protocol are positive with the number of pulses more than 10^7 in Fig. 3(Right). Compared two figures, if the transmittance distance is shorter than 10 km, as the number of pulses increasing from 10^7 to its 9 times, the key rates increase less than that as the intensity fluctuation decreasing from $\varepsilon=0.15$ to its 9 times, but that is to be contrary if the transmittance distance is farther than 10 km. So, the photon-number-distribution fluctuations introduced by finite-number of pulses are the main cause, if the distance between communication parties is farther than 10 km. Within 10 km, the intensity fluctuation is the main cause. Note that this is deduced within the scope of the resistible intensity fluctuations and the scope of the number of pulses that can yield secure keys in the protocol.

For the PDS QKD protocol with unstable WCPs, we simulate the key rates when the numbers of pulses received by Bob are 10^{10}, 10^{11}, 10^{12}, infinite, and the transmission distance is fixed as 50 km in Fig. 4(Left). The finite-key rates are arbitrarily close to the key rates with infinite number of pulses as the number of pulses sufficiently close to infinite. If Bob receives less than 10^{10} pulses, secure keys can not be obtained. Figure 4(Right) shows the corresponding optimal number of pulses sent from Alice when the transmission distance is 50 km and Bob receives 10^{10}, 10^{11}, 10^{12} pulses. For the curves in Fig. 4(Right), the least number of pulses sent from Alice is 10^{13}, which needs that 10G High-speed QKD system runs more than 1000 seconds without stop. We also describe the affections of intensity fluctuations on key rates and that of the photon-number-distribution fluctuations on key rates in Fig. 5(Left) and Fig. 5(Right) respectively. Within the resistible intensity fluctuations, Fig. 5(Left) shows that for different intensity fluctuations the decreasing velocities of the key rates at same transmission distance is much same, but the curves in Fig. 5(Right) do not have the same characters. Comparing the two figures in Fig. 5, we know that if the transmittance distance is shorter than 50 km, as the number of pulses increasing from 10^{10} to its 9 times, the key rates are changed less than that with the intensity fluctuation decreasing from $\varepsilon=0.15$ to its 9 times. Therefore, if the distance between communication parties is farther than 50 km, the photon-number-distribution fluctuations are the main affections on the key rates. Within 50 km, the

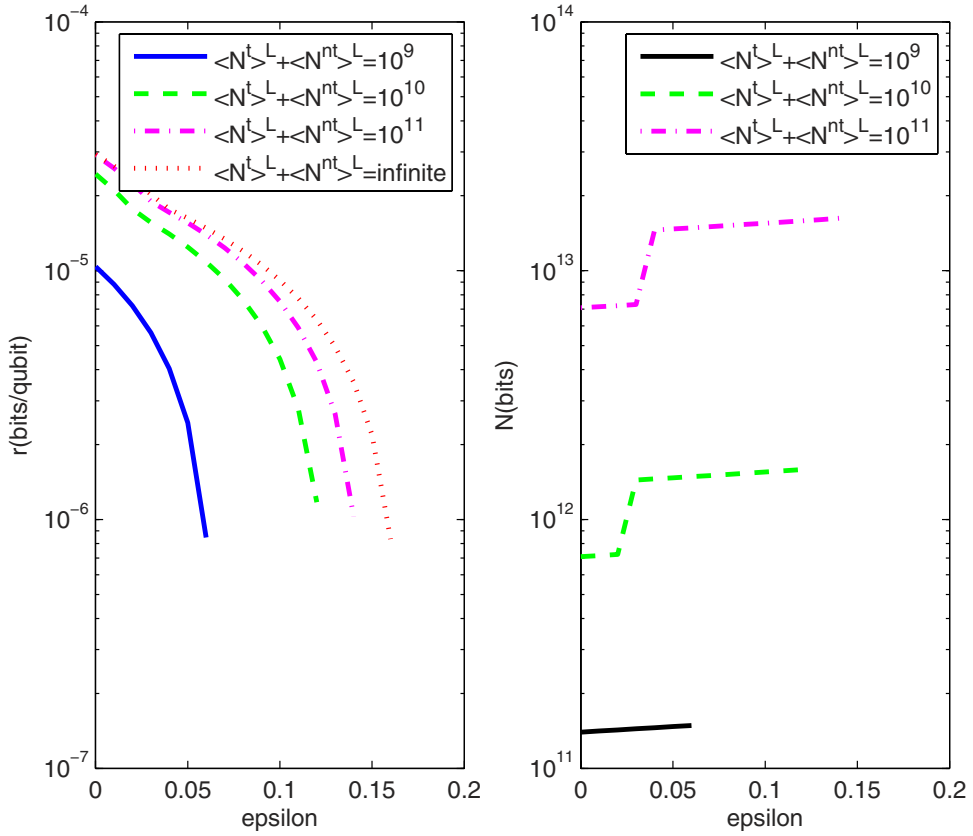

Figure 2. (Left) The lower bounds of key rates for PDS QKD protocols with an unstable PDC source under different numbers of pulses that Bob receives, when the transmission distance is fixed as 50 km; (Right) The corresponding optimal number of pulses sent from the PDC source with the transmission distances 50 km, when the numbers of pulses received by Bob is 10^9, 10^{10}, and 10^{11}.

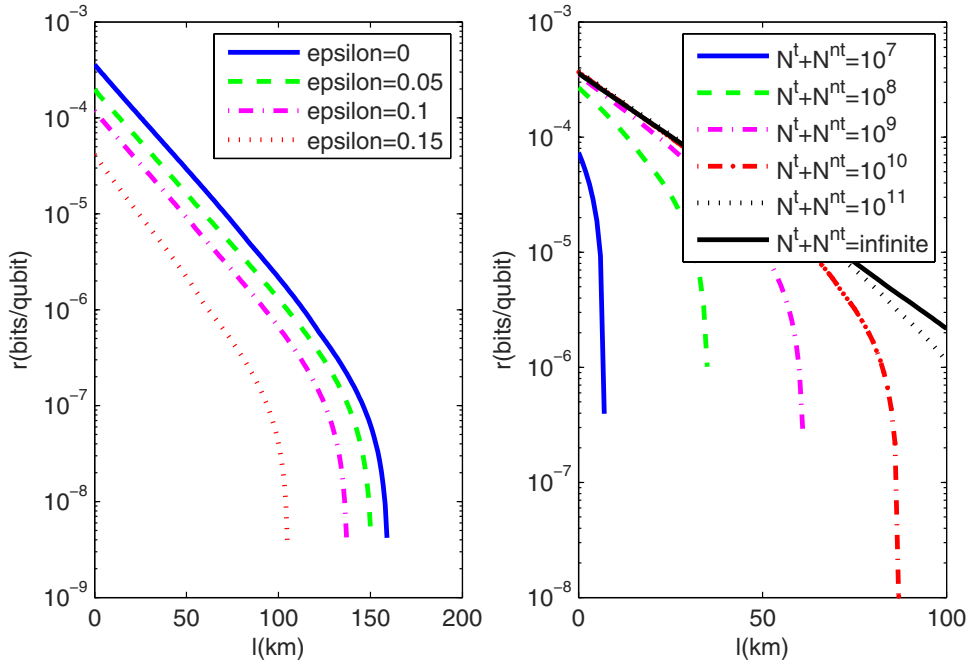

Figure 3. (Left) The lower bounds of key rates for PDS QKD protocols when the intensity fluctuations are 0, 0.05, 0.1, 0.15 and the number of pulses are infinite; (Right) The lower bounds of key rates for PDS QKD protocols with a stable PDC source under different numbers of pulses that Bob receives.

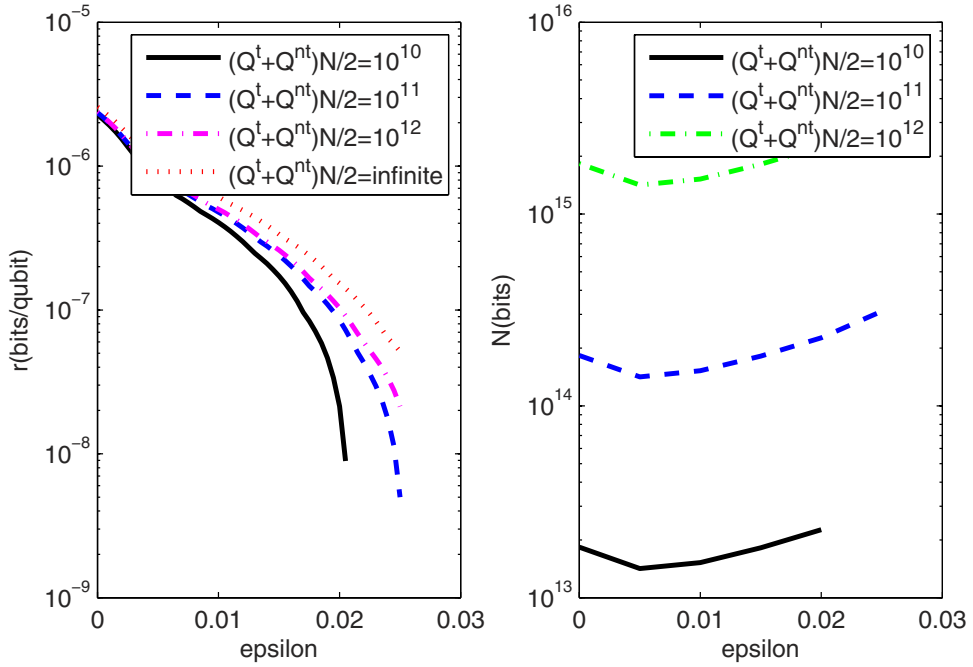

Figure 4. (Left) The lower bounds of key rates for PDS QKD protocols with unstable WCPs under different numbers of pulses that Bob receives, when the transmission distance is fixed as 50 km; (Right) The corresponding optimal number of weak coherent pulses sent from the source with the transmission distances 50 km.

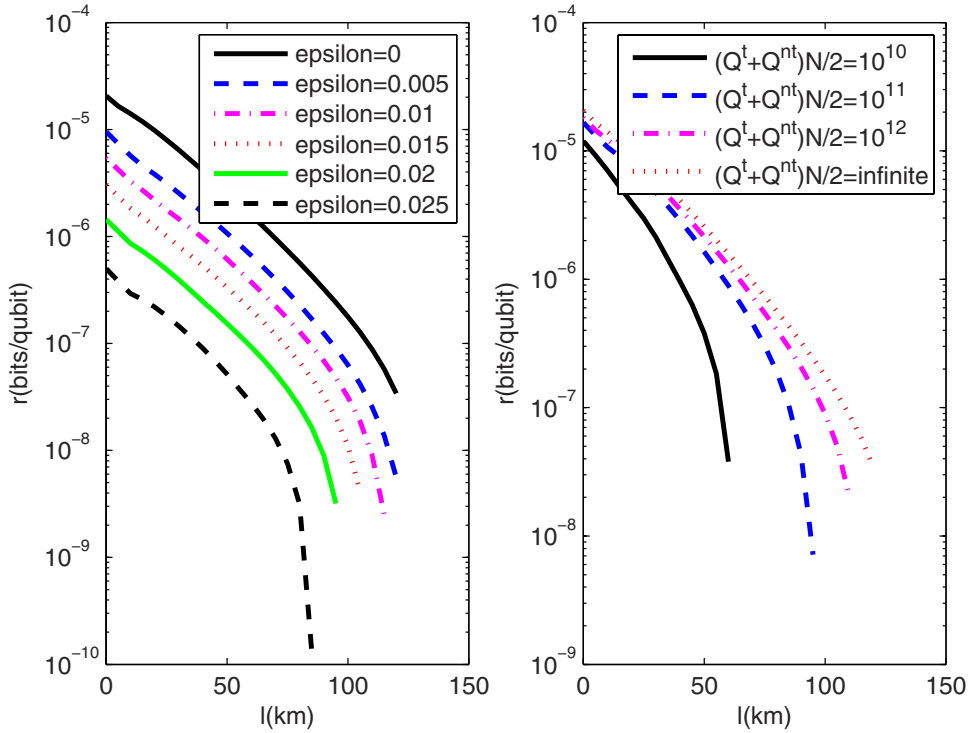

Figure 5. (Left) The lower bounds of key rates for PDS QKD protocols when the intensity fluctuations are 0, 0.005, 0.01, 0.015, 0.02, 0.025 and the number of pulses are infinite; (Right) The lower bounds of key rates for PDS QKD protocols with stable WCPs under different numbers of pulses that Bob receives.

intensity fluctuation is changed into the main cause. This is deduced within the scope of the resistible intensity fluctuations and the number of pulses that can yield positive key-rates in the protocol.

Comparison. We study the applications of two different sources in PDS QKD protocols. In both of protocols, the finite-key rates are all affected by intensity fluctuations and the photon-number-distribution fluctuations. Comparing Fig. 2(Left) and Fig. 4(Left), we know that while the protocol with an unstable PDC source even can resist intensity fluctuations with $\varepsilon < 0.15$, the PDS QKD protocol with unstable WCPs resist much less intensity fluctuations, and it cannot generate secure key with the number of pulses less than 10^{10}. With the same intensity fluctuations and the same transmission distances, the finite-key rates of PDS QKD protocol with PDC source are much higher than that with WCPs. Moreover, for large scale of transmission distances, the PDS QKD protocol with unstable PDC source is mainly affected by the photon-number-distribution fluctuations, which are in the control of communicating parties.

Methods

It is difficult to obtain the values of Y_1^L and e_1^U in the key rates of Eq. (1), but the authors in Refs 14–16 have introduced many methods to obtain the two values. The methods are general and can be applied to any fluctuation of parameters in the source state. Following the models established in Discussion Section, we will show how to get each parameter in the formula of final finite-key rate. Both the methods are inspired by the idea in Refs 14–16.

Finite-key rates for an unstable PDC source. In order to get the lower bound of the sifted trigger number of the single-photon pulses N_1^{tL} and the upper bound of error rate of the single-photon pulses e_1^U, we introduce the influences of statistical fluctuations and intensity fluctuations on some expected parameters.

The lower bound and the upper bound of the source intensity u_i are $u^L = u(1-\epsilon)$ and $u^U = u(1+\epsilon)$, respectively. In the following, $\langle\star\rangle^{L(U)}$ is the lower bound (the upper bound) of the expected value of parameter $\star$, and $\star^{L(U)}$ is the lower bound (the upper bound) of the observed value of parameter $\star$.

According to ref. 15, the lower bound of N_1^t is

$$N_1^{tL} = \frac{N^{ntL} - \frac{1-\gamma_2}{\gamma_2}N^{tU} + \left(\frac{1-\gamma_2}{\gamma_2} - \frac{1-\gamma_0}{\gamma_0}\right)N_0^{tU}}{\frac{1-\gamma_1}{\gamma_1} - \frac{1-\gamma_2}{\gamma_2}}, \tag{13}$$

if there exists $max_{k\in(2,\infty)_Z}\{\frac{1-\gamma_k}{\gamma_k}\} \le \frac{1-\gamma_2}{\gamma_2} \le \frac{1-\gamma_1}{\gamma_1} \le \frac{1-\gamma_0}{\gamma_0}$, where

$$N^{tU} = \langle N^t\rangle^U + N\cdot\xi(N,2), \quad N^{ntL} = \langle N^{nt}\rangle^L - N\cdot\xi(N,2), \tag{14}$$

$$n^{tU} = \langle n^t\rangle^U + \frac{\langle N^t\rangle}{2}\cdot\xi\left(\frac{\langle N^t\rangle}{2},2\right), \quad n^{ntU} = \langle n^{nt}\rangle^U + \langle N^{nt}\rangle\cdot\xi(\langle N^{nt}\rangle,2). \tag{15}$$

And also we can get the upper bound of the clicking number of sifted trigger vacuum pulses N_0^t and the error rate of single-photon pulse e_{1i}

$$N_0^{tU} = min\left\{8n^{tU}, 4n^{ntU}\frac{\gamma_0}{1-\gamma_0}\right\}, \; e_1^U = min\left\{\frac{n^{ntU}}{N_1^{tL}}\frac{\gamma_1}{1-\gamma_1}, \frac{2n^{tU}}{N_1^{tL}}\right\}. \tag{16}$$

Followed the upper bound of error rate $E^U = \frac{2n^{tU}}{N^{tL}} + \xi\left(\frac{\langle N^t\rangle^U}{2},2\right)$, the lower bound of finite-key rate is obtained

$$r^L = -\Delta_{PDC} + \frac{1}{2N}\left\{N_1^{tL}[1-h(e_1^U)] - f_{EC}N^{tU}h(E^U)\right\}, \tag{17}$$

where $\Delta_{PDC} = 7\sqrt{\frac{Q^{tU}}{8N}\log_2(2/\bar{\varepsilon})} + \frac{2}{N}\log_2(1/\varepsilon_{PA}) + \frac{1}{N}\log_2(2/\varepsilon_{EC})$. Note that the key rate without photon-number-distribution fluctuations in Fig. 2(Left) is easily obtained from above discussion, i.e.,

$$r_{inf} = \frac{1}{4}\left\{r_1(1-h(e_1^U)) - f_{EC}Q^{tU}h(E^{tU}/Q^{tU})\right\}, \tag{18}$$

where

$$r_1 = \frac{Q^{ntL} - \frac{1-\gamma_2}{\gamma_2}Q^{tU} + \left(\frac{1-\gamma_2}{\gamma_2} - \frac{1-\gamma_0}{\gamma_0}\right)r_0}{\frac{1-\gamma_1}{\gamma_1} - \frac{1-\gamma_2}{\gamma_2}}, \quad r_0 = \min\left\{2E^{tU}, 2E^{ntU}\frac{\gamma_0}{1-\gamma_0}\right\},$$
$$Q^{tU} = \frac{2\langle N^t\rangle^U}{N}, Q^{ntL} = \frac{2\langle N^{nt}\rangle^L}{N}, \quad E^{tU} = \frac{4}{N}\langle n^t\rangle^U, \quad E^{ntU} = \frac{2}{N}\langle n^{nt}\rangle^U. \tag{19}$$

$\langle N^t\rangle^U$, $\langle N^{nt}\rangle^L$, $\langle n^t\rangle^U$ and $\langle n^{nt}\rangle^U$ are shown in Eq. (10).

Finite-key rates for an unstable WCP source. In order to make our paper complete, we apply the results in ref. 13 to obtain the values of N_1^{tL} and e_1^U here, through replacing the observed values by the expected values of each quantities there[13].

The lower bound of N_1^t is

$$N_1^{tL} = \frac{4}{\langle Q_2\rangle^L Q_1^{tU} - \langle Q_2^t\rangle^U Q_1^L}[\langle Q_2\rangle^L\langle N^t\rangle^L - \langle Q_2^t\rangle^U\langle N'\rangle^U - (\langle Q_2\rangle^L Q_0^{tU} - \langle Q_2^t\rangle^U Q_0^L)N_0^{tU}], \tag{20}$$

under the conditions $\langle Q_2\rangle^L Q_0^{tU} - \langle Q_2^t\rangle^U Q_0^L > 0$ and $\langle Q_2\rangle^L Q_1^{tU} - \langle Q_2^t\rangle^U Q_1^L > 0$, where

$$N_0^{tU} = \min\left\{8n^{tU}, \frac{4n^{ntU}Q_0^{tU}}{Q_0^{ntL}}\right\}. \tag{21}$$

Similarly, we can obtain the upper bound of error rate of single-photon pulses, i.e.,

$$e_1^U = \min\left\{\frac{n^{ntU}}{N_1^{tL}}\frac{Q_1^{tU}}{Q_1^{ntL}}, \frac{2n^{tU}}{N_1^{tL}}\right\}. \tag{22}$$

Note that in the right hand side of Eq. (20), all quantities are expected values, while in the practical implementation, they are actually observed values.

Now the final finite-key rate is received as follows:

$$r^L = -\Delta_{WCP} + \frac{1}{2N}\left\{N_1^{tL}[1 - h(e_1^U)] - f_{EC}N^{tU}h(E^U)\right\}, \tag{23}$$

where $\Delta_{WCP} = 7\sqrt{\frac{Q^{tU}}{16N}\log_2(2/\bar{\varepsilon})} + \frac{2}{N}\log_2(1/\varepsilon_{PA}) + \frac{1}{N}\log_2(2/\varepsilon_{EC})$. According to the discussion, we also can obtain the key rate without photon-number-distribution fluctuations, i.e.,

$$r_{inf} = \frac{1}{8}\left\{\langle Q_1^t\rangle^L Y_1^L(1 - h(e_1^U)) - f_{EC}\langle Q^t\rangle^U h(2\langle n^t\rangle^U/\langle N^t\rangle^L)\right\}, \tag{24}$$

where $Y_1^L = \frac{1}{\langle Q_2\rangle^L\langle Q_1^t\rangle^U - \langle Q_2^t\rangle^U\langle Q_1\rangle^L}[\langle Q_2\rangle^L\langle Q^t\rangle^L - \langle Q_2^t\rangle^U\langle Q'\rangle^U - (\langle Q_2\rangle^L\langle Q_0^t\rangle^U - \langle Q_2^t\rangle^U\langle Q_0\rangle^L)Y_0^U]$,
$Y_0^U = \min\left\{\frac{2E^{ntU}}{\langle Q_0^{nt}\rangle^L}, \frac{2E^{tU}}{\langle Q_0^t\rangle^L}\right\}$, $Q^{tU} = \frac{4\left(\langle N'\rangle^U - \langle N^{nt}\rangle^U\right)}{N}$, $Q^{ntL} = \frac{4\langle N^{nt}\rangle^L}{N}$, $E^{tU} = \frac{4\left(\langle n'\rangle^U - \langle n^{nt}\rangle^U\right)}{N}$, $E^{ntU} = \frac{4}{N}\langle n^{nt}\rangle^U$.
$\langle N'\rangle^U$, $\langle N^{nt}\rangle^U$, $\langle n'\rangle^U$ and $\langle n^{nt}\rangle^U$ are from in Eq. (11). The simulation results of infinite-key rates are shown in Fig. 4 (Left).

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* 175–179 (1984).
2. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441 (2000).
3. Villoresi, P. *et al.* Experimental verification of the feasibility of a quantum channel between space and Earth. *New J. Phys.* **10,** 033038 (2008).
4. Bonato, C., Tomaello, A., Deppo, V. D., Naletto, G. & Villoresi, P. Feasibility of satellite quantum key distribution. *New J. Phys.* **11,** 045017 (2009).
5. Tomaello, A., Bonato, C., Deppo, V. D., Naletto, G. & Villoresi, P. Link budget and background noise for satellite quantum key distribution. *Adv. Space Res.* **47,** 802–810 (2011).
6. Scarani, V. & Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100,** 200501 (2008).
7. Scarani, V. & Renner, R. Security bounds for quantum cryptography with finite resources. In *Theory of Quantum Computation, Communication, and Cryptography, Lecture Notes in Computer Science* **5106,** 83–95 (2008).
8. Song, T. T., Zhang, J., Qin, S. J., Gao, F. & Wen, Q. Y. Finite-key analyses for quantum key distribution with decoy-states. *Quant. Inf. Comp.* **11,** 374–389 (2011).
9. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **6,** 1 (2008).

10. Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11,** 045024 (2009).
11. Zhao, Y., Qi, B., Ma, X. F., Lo, H. K. & Qian, L. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.* **96,** 070502 (2006).
12. Wang, X. B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A* **75,** 052301 (2007).
13. Wang, X. B., Peng, C. Z., Zhang, J., Yang, L. & Pan, J. W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **77,** 042311 (2008).
14. Wang, X. B., Yang, L., Peng, C. Z. & Pan, J. W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **11,** 075006 (2009).
15. Hu, J. Z. & Wang, X. B. Reexamination of the decoy-state quantum key distribution with an unstable source. *Phys. Rev. A* **82,** 012331 (2010).
16. Chi, H. H., Yu, Z. W. & Wang, X. B. Decoy-state method of quantum key distribution with both source errors and statistics fluctuations *Phys. Rev. A* **86,** 042307 (2012).
17. Mauerer, W. & Silberhorn, C. Quantum key distribution with passive decoy state selection. *Phys. Rev. A* **75,** 050305 (2007).
18. Adachi, Y., Yamamoto, T., Koashi, M. & Imoto, N. Simple and efficient quantum key distribution with parametric down-conversion. *Phys. Rev. Lett.* **99,** 180503 (2007).
19. Ma, X. F. & Lo, H. K. Quantum key distribution with triggering parametric down-conversion sources. *New J. Phys.* **10,** 073018 (2008).
20. Curty, M., Moroder, T., Ma, X. F. & Lütkenhaus, N. Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution. *Opt. Lett.* **34,** 3238 (2009).
21. Curty, M., Ma, X. F., Qi, B. & Moroder, T. Passive decoy-state quantum key distribution with practical light sources. *Phys. Rev. A* **81,** 022310 (2010).
22. Curty, M., Ma, X. F., Lo, H. K. & Lütkenhaus, N. Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals. *Phys. Rev. A* **82,** 052325 (2010).
23. Gobby, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84,** 3762–3764 (2004).
24. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
25. Zhou, C. *et al.* Tight finite-key analysis for passive decoy-state quantum key distribution under general attacks. *Phys. Rev. A* **89,** 052328 (2014).
26. Li, Y., Bao, W. S., Li, H. W., Zhou, C. & Wang, Y. Passive decoy-state quantum key distribution using weak coherent pulses with intensity fluctuations. *Phys. Rev. A* **89,** 032329 (2014).
27. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108,** 130502 (2012).
28. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111,** 130502 (2013).
29. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111,** 130501 (2013).
30. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Commun.* **5,** 3732 (2013).

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grants No. 61502200, 61309029, 61272057, 61572081), the Natural Science Foundation of Guangdong Province under Grant No. 2014A030310245, the Fundamental Research Funds for the Central Universities under Grant No. 21615313, the Beijing Higher Education Young Elite Teacher Project (Grants No. YETP0475, YETP0477).

Author Contributions

T.T.S. proposed the theoretical method. H.Y.J. simulated the protocols. T.T.S. and Y.K.W. wrote the main manuscript text. S.J.Q. and Q.Y.W. reviewed the manuscript.

Additional Information

Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Song, T.-T. *et al.* Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources. *Sci. Rep.* **5**, 15276; doi: 10.1038/srep15276 (2015).