Practical issues of twin-field quantum key distribution

Feng-Yu Lu, Zhen-Qiang Yin, Rong Wang, Guan-Jie Fan-Yuan, Shuang Wang, De-Yong He, Wei Chen, Wei Huang, Bing-Jie Xu, Guang-Can Guo, and Zheng-Fu Han

1 CAS Key Laboratory of Quantum Information, CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, People’s Republic of China
2 State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, People’s Republic of China
3 Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, Sichuan 610041, People’s Republic of China
4 Author to whom any correspondence should be addressed

E-mail: yinzq@ustc.edu.cn

Keywords: quantum key distribution, twin-field quantum key distribution, finite-key size effect

Abstract

Twin-field quantum key distribution (TF-QKD) protocol and its variants, such as phase-matching QKD, sending-or-not-sending QKD, and no phase post-selection TF-QKD (NPP-TFQKD), are very promising for long-distance applications. However, there are still some gaps between theory and practice in these protocols. Concretely, a finite-key size analysis is still missing, and the intensity fluctuations are not taken into account. To address the finite-key size effect, we first give the key rate of NPP-TFQKD against collective attack in finite-key size region and then prove it can be against coherent attack. To deal with the intensity fluctuations, we present an analytical formula of 4-intensity decay state NPP-TFQKD and a practical intensity fluctuation model. Finally, through detailed simulations, we show NPP-TFQKD can still keep its superiority of high key rate and long achievable distance.

1. Introduction

Quantum key distribution (QKD) [1, 2] is one of the most mature applications among the emerging quantum technologies. It allows two remote users, called Alice and Bob, to share random secret keys even if there is an eavesdropper, Eve [3–5]. Due to the loss of channel, both the key rate and achievable distance of QKD are limited. Although increasing the secret key rate (SKR) and achievable distance are essentially significant for the real applications of QKD, the theorists proved there are some limits on the improvement of SKR [6, 7]. In particular, for the channel of transmission η, the linear bound [7], i.e. $R \leq -\log_2(1 - \eta)$, gives the precise SKR bound for any point-to-point QKD without quantum repeaters. Surprisingly, a revolutionary protocol called twin-field quantum key distribution (TF-QKD) [8] was recently proposed to beat this bound. Inspired by the novel idea of TF-QKD, researchers proposed some variants and completed the corresponding security proofs [9–14]. From the view of experiments, these variants, i.e. phase-matching QKD [10], sending-or-not-sending QKD [11] and no phase post-selection TF-QKD (NPP-TFQKD) [12–14], are simpler. Indeed, both the sending-or-not-sending QKD and NPP-TFQKD have been successfully demonstrated [15–18].

However, there are still some gaps between theory and implementation of TF-QKD. In [12–14], asymptotic SKR of NPP-TFQKD is proposed, but the SKR in finite-key region is not given. On the other hand, the key-size in a practical implementation is always finite, thus a framework to deal with the finite-key size effect in TF-QKD is indispensable.

Another problem we will discuss is a potential security loophole of TF-QKD and its variants. Although the [8–14] have proved the TF-QKD and its variants are information-theoretically secure even with untrusted measurement device just like the original measurement-device-independent protocol [19–22], the imperfections of laser source may spoil the security. One of the intractable loopholes of source is the intensity fluctuation [23–25]. In this work, we also propose a countermeasure to tackle the intensity fluctuation of NPP-TFQKD.
TFQKD. A key step of our method is proposing the analytical formulas to deal with the 4-intensity decoy states in NPP-TFQKD. In the original NPP-TFQKD [12], one must use linear programing to solve linear equations of decoy states [26–30]. Compared with linear programing, analytical formula has superiorities on some special situations. More importantly, the proposed analytical formulas are particularly convinient to be incorporated to our intensity fluctuation. Another key step of our method is introducing a new intensity fluctuation model in finite-key size regime. The model makes TF-QKD robustner to intensity fluctuation.

The rest of this paper is organized as followoing. Firstly, In section 2, we briefly review the procedure of NPP-TFQKD protocol. In section 3, we analyze the finite-key size effect of NPP-TFQKD, give the SKR formula against coherent attack and evaluate the performance of TF-QKD in finite-key regime. In section 4, the analytical formulas for 4-intensity decoy state method are given. Then we introduce the intensity fluctuation model and its countermeasure. Finally, a complete simulation which takes into account both the finite-key size effects and the intensity fluctuations is presented.

2. Protocol definition

The setup of NPP-TFQKD [12] protocol is illustrated in figure 1 and the procedure is as following:

State preparation: this step will be repeated by N trials. In each trial, Alice(Bob) chooses code mode or decoy mode with probabilities $P_c$ and $P_d = 1 - P_c$ respectively, sends corresponding quantum state to untrusted Charlie.

When code mode is selected, Alice(Bob) prepares a phase-locked weak coherent pulse(WCP) $|\pm \sqrt{\mu}_{A}(\pm \sqrt{\mu}_{B})\rangle$, where the plus or minus of the quantum state depends on the bit value of Alice(Bob)’s random key of this trial.

When decoy mode is selected, Alice(Bob) prepares a phase randomized WCP, whose intensity $\nu_{A}(\nu_{B})$ is randomly choosen from a pre-decided set. Alice(Bob) actually prepares a mixed state since the randomized phase in the decoy mode will never be publicly announced. For instance, the density matrix of Alice’s WCP in decoy mode can be denoted as:

$$\rho_{n} = \sum_{n=0}^{\infty} e^{-\nu_{n}/2} \frac{\nu_{n}^{n}}{n!} |n\rangle \langle n|$$

(1)

where $|n\rangle$ is the Fock state.

Measurement: for each trial of the state preparation step, the untrusted Charlie must publicly announce a single click of his single photon detector(SPD) ‘SPD-L’ or ‘SPD-R’ or non-click meassage. Note that Charlie is untrusted, thus he is not necessarily to make the measurement shown in figure 1.

Sifting: Alice and Bob publicly announce which trials are code mode and which are decoy mode. For the trials they both choose code mode and Charlie announce ‘SPD-L’ or ‘SPD-R’ clicked, Alice and Bob will retain this key bit. According to Charlie’s measurement result, Bob may decide to flip his key bit or not. After this step, Alice and Bob generate sifted key bit string $Z$ and $Z'$ respectively.

Error correction: Alice sends $\lambda_{EC} = nH(E_2)$ bits of classical error correction data to Bob. Here $n = |Z| = |Z'|$ is the size of sifted key bits, $H(p) = -p \log_{2} p - (1 - p) \log_{2}(1 - p)$ is the Shannon entropy,
\( E \) is the error rate of sifted key bits and \( f \geq 1 \) denotes error correction efficiency. Depending on the error correction data and \( Z' \), Bob obtains an estimated \( \hat{Z} \) of \( Z \). Next, by applying universal hash function, Alice sends \( \lambda_{EV} = \log_{2 \epsilon_{EV}} \) bits of error verification information to Bob. If the error verification fails, they output an empty string and abort the protocol. Otherwise, they assume the error correction successes and \( Z = Z' \).

Parameter estimation and privacy amplification: Alice and Bob accumulate data to estimate gain \( Q \), of trials that they both choose code mode, gains \( Q_{xy} \) of trials they choose decoy mode with intensity \( x \) and \( y \) respectively. With these parameters and \( \lambda_{EC}, \lambda_{EV} \), Alice and Bob perform privacy amplification, say, apply a random universal hash function to \( Z \) and \( \hat{Z} \) respectively to generate \( l_{sec} \)-length secure bit string \( S \) and \( S' \) respectively. The SKR per pulse is defined as \( R = l_{sec}/N \).

3. Finite-key analysis of NPP-TFQKD

Previous work [12–14] of NPP-TFQKD are based on the asymptotic situation. However, since it is impossible for Alice and Bob to send infinite pulses to generate their secure key in reality, the finite-key size effect [31–34] must be taken into account. In this section, we first extend the asymptotic SKR formula of [12] to non-asymptotic one against collective attack. Then based on the postselection technique developed in [31], a formula against coherent attack is present.

3.1. Security definition and SKR against collective attack

As discussed above, in the end of NPP-TFQKD, Alice and Bob obtain a pair of bit string \( S \) and \( S' \) respectively. Ideally, the bit strings are secure and applicable to any cryptosystem if two fundamental conditions are met, namely correctness and secrecy. The correctness is, in simple terms, \( S = S' \), which is guaranteed by the error verification. The secrecy requires Eve’s system \( E \) is decoupled from Alice’s key \( S \), which is met when

\[
\sum_{s} (|s\rangle \langle s| \otimes \rho_E^s) = U_A \otimes \rho_E, \quad (2)
\]

where \( \sum_{s} (|s\rangle \langle s| \otimes \rho_E^s) \) denotes the density matrix of Alice and Eve’s quantum state; the \( U_A = \sum_{s} \frac{1}{|S|} |s\rangle \langle s| \) denotes the uniform mixture of all possible value of \( S \); \( \{ |s\rangle \} \) denotes the orthonormal basis of Alice’s key \( S \); \( \rho_E \) is Eve’s the density matrix and \( \rho_E^s \) is Eve’s the density matrix of Eve’s system conditioned that Alice’s key \( S \) is in the state \( |s\rangle \). Clearly, Alice’s key \( S \) is completely unknown to Eve in this ideal case.

However, in finite-key size regime, the ideal condition, namely, equation (2), usually cannot be perfectly met. In [35], a composable security criterion is proposed. This criterion introduces secure parameters to describe some small probabilities of the keys \( S \) and \( S' \) varying from the ideal case. The protocol is \( \epsilon_{EC} \)-correct if \( P(S = S') \leq \epsilon_{EC} \), i.e. the probability of \( S \neq S' \) is less than \( \epsilon_{EC} \). Similarly, the protocol is \( \epsilon_{PA} \)-secret if \( \frac{1}{N} \sum_{s} (|s\rangle \langle s| \otimes \rho_E^s) - U_A \otimes \rho_E \) is \( \epsilon_{PA} \)-close to the ideal situation \( U_A \otimes \rho_E \), where the symbol \( \| . \| \) denotes trace norm of a matrix. In general, if a protocol is \( \epsilon \)-secure, \( \epsilon_{EC} + \epsilon_{PA} \leq \epsilon \) must hold. To meet this criterion, with the same manner of [32], the SKR formula of NPP-TFQKD against collective is given by

\[
R_{col} = \frac{n}{N} [1 - \Gamma_{AE}] - \frac{1}{N} \lambda_{EC} - \frac{1}{N} \lambda_{EV} - \frac{2}{N} \log_{2 \epsilon_{PA}} - \frac{7}{N} \sqrt{n \log(n/\epsilon)}, \quad (3)
\]

where \( n = P^2 N, N \) is the size of sifted key bits, \( \Gamma_{AE} \) is the upper bound of Eve’s information on the sifted key bit if she launches collective attack, \( \lambda_{EV} = \log_{2 \epsilon_{EV}} \) implies that \( P(S = S') \leq \epsilon_{EC} \), \( \epsilon_{PA} \) accounts for the probability of failure of privacy amplification, and \( \epsilon \) measures the accuracy of the estimating the smooth min-entropy [32]. As shown in [12], the estimation of \( \Gamma_{AE} \) against collective attack depends on some experimentally observed parameters including the gains \( Q \), and \( Q_{xy} \). When the number of trials is finite, the expectations of these gains may vary from the experimentally observed values due to statistical fluctuations. Thus, another secure parameter \( \epsilon_{PE} \) [34] characterizing the probability that parameter estimation fails must be taken into account. For instance, consider a set of i.i.d. random variables \( X, X_2, ..., X_N \) with \( X \in \{ 0, 1 \} \), the observed frequency of bit 1 is usually not equal to its expectation \( E(X) \), provided \( N \) is finite. To solve this problem, we apply large deviation theory, specifically, the Chernoff bound to estimate a confidence interval of \( X \) according to the observed value. In NPP-TFQKD, we can apply Chernoff bound [34, 36, 37] to estimate expected value \( \hat{Q} \) and \( \hat{Q}_{xy} \) through the observed gains \( \hat{Q} \) and \( \hat{Q}_{xy} \) with a failure probability \( \epsilon_{PE} \). We take \( Q_{xy} \) as an example:

\[
Q_{xy} = \hat{Q}_{xy} (1 + \delta_{xy}), \quad -\frac{\Delta}{\sqrt{N_{xy}}} \leq \delta_{xy} \leq \frac{\hat{\Delta}}{\sqrt{N_{xy}} \hat{Q}_{xy}}, \quad (4)
\]

where the \( \Delta = f ((\epsilon_{PE}/2)^{3/2}) \), \( \hat{\Delta} = f ((\epsilon_{PE}/2)^{3/4}) \), and \( f (x) = \sqrt{2 \ln(x^{-1})} \). The \( N_{xy} \) denotes the total number of trials which Alice and Bob select decoy mode with intensity \( x \) and \( y \).
The upper and lower bound of $Q_{xy}$ are:

$$Q_{xy} \leq Q_{xy}' = \hat{Q}_{xy} \left( 1 + \frac{f \left( (\epsilon_{PE}/2)^4/16 \right)}{N_{xy} Q_{xy}} \right),$$

$$Q_{xy} \geq Q_{xy}' = \hat{Q}_{xy} \left( 1 - \frac{f \left( (\epsilon_{PE}/2)^4/16 \right)}{N_{xy} Q_{xy}} \right).$$

(5)

In [2], the $I_{AE}$ is bounded by $Y_{in}$ and $Q_c$. We estimated upper and lower bound of $Y_{in}$ by linear programming, whose constraints are:

$$Q_{xy} \geq \sum_{i=0}^{8} \sum_{j=0}^{8} p_i^x p_j^y Y_{ij},$$

$$Q_{xy} \leq \sum_{i=0}^{8} \sum_{j=0}^{8} p_i^x p_j^y Y_{ij} + \sum_{i=9}^{\infty} \sum_{j=9}^{\infty} p_i^x p_j^y.$$  

(6)

As introduced in [12], there are 10 different $Q_{xy}$ in equation (6), thus there are 20 constraints in total.

When fluctuation analyses are applied, the $Q_{xy}'$ should be replaced with its worst-case in equation (6). The equation (6) is modified as:

$$Q_{xy}^+ \geq \sum_{i=0}^{8} \sum_{j=0}^{8} p_i^x p_j^y Y_{ij},$$

$$Q_{xy}^- \leq \sum_{i=0}^{8} \sum_{j=0}^{8} p_i^x p_j^y Y_{ij} + \sum_{i=9}^{\infty} \sum_{j=9}^{\infty} p_i^x p_j^y.$$  

(7)

By applying the new constraints, we can estimate secure $Y_{in}^+$ and $Y_{in}^-$ in non-asymptotic scenario. With these $Y_{in}^+$, $Y_{in}^-$, and $Q_{xy}^+$, $Q_{xy}^-$, an estimation of $I_{AE}$ with acceptable failure probability $(11\epsilon_{PE})$ can be obtained.

Finally, Alice and Bob generate $NR_{col}$ bits secret key against collective attack with $\epsilon_{col}$-security. Obviously, $\epsilon_{col}$ is not exceeding the sum of failure probabilities of error verification, privacy amplification, accuracy of smooth min-entropy and parameters estimation, say

$$\epsilon_{col} \leq \epsilon_{PA} + \epsilon_{EC} + \epsilon_s + 11\epsilon_{PE}. \tag{8}$$

Now we have introduced how to generate $\epsilon_{col}$-security keys against collective attack in NPP-TFQKD with finite-key effect. Next, we discuss how to obtain $\epsilon_{coh}$-security keys against coherent attack.

### 3.2. Countermeasure of coherent attack

There are two ways to deal with security under coherent attack in finite-key scenarios. One way is to use uncertainty relation for smooth entropies [38, 39] or complementarity relation [40]. In this context, collective attack is not assumed, thus the data used in parameter estimation can be arbitrarily correlated. The other way, which we follow here, is to firstly assume collective attack (i.i.d.) then convert its security to be against coherent attack. In real-life, the i.i.d. assumption may be not satisfied. Fortunately, [31] has proved that one can always assume i.i.d. in the security proof (including parameter estimation) to get a key rate against collective attack, then calculate a key rate against coherent attack. In this work, we introduce the following corollary from the theorem 1 of [31] to tackle coherent attack in finite-key region.

**Corollary.** The key rate $R_{coh}$ against coherent attack could be given by

$$R_{coh} = R_{col} - \frac{126 \log_2(N + 1)}{N}, \tag{9}$$

while the key is $\epsilon_{coh}$-secure and

$$\epsilon_{coh} = \epsilon_{col}(N + 1)^{0.5}. \tag{10}$$

**Proof.** The proof is based on the theorem 1 of [31] and very similar proofs can be found in [31] and the appendix B of [32]. We denote $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{M}$ are the Hilbert space of Alice’s ancilla $A$, Bob’s ancilla $B$ and Charlie’s message $M$ respectively. Without compromising the security, Charlie’s message $M$ (click or not) can be treated as a quantum stated shared by Alice and Bob. The NPP-TFQKD protocol using equation (3) to generate keys could be viewed as a map $\mathcal{E}$ transforming $A, B$ and $M$ into keys $S$ and $S'$ [$|S| = |S'| = NR_{col}$] respectively. Let $S$ be a hypothetical map transforming imperfect keys $S$ and $S'$ into perfect ones and define $\mathcal{F} = S \circ \mathcal{E}$. Recall last subsection, it asserts that $||(\mathcal{E} \otimes \mathcal{I}) \tau_{TFQKD}||_1 \leq \epsilon_{coh}$ holds when equation (3) is used to generate keys,
where the de Finetti–Hilbert–Schmidt state \( \tau_{\psi^{kn}} = \sum_{\mu} \sigma_{\psi^{kn}}^\mu \sigma(\mu) \), \( \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{M} \), \( \sigma_{\psi^{kn}}^\mu \) is the pure state shared by Alice, Bob and Eve induced by any collective attack, and \( \mu(\sigma_{\psi^{kn}}) \) is the Haar measure on the pure state \( \sigma_{\psi^{kn}} \).

Next, we consider Eve may control another ancilla \( R \) to obtain the purification \( \tau_{\psi^{kn}^{\otimes r}} \) of \( \tau_{\psi^{kn}} \). For such a purification, \( \text{dim}(R) \) is not larger than \( (N + 1)^{d-1} \) [31] where \( d = \text{dim}(\mathcal{H}) = 8 \). Through controlling ancilla \( R \), Eve’s min-entropy on sifted key is decreased at most \( 2(d^2 - 1) \log_2(N + 1) \) bits. To meet the security, Alice and Bob may perform protocol \( \mathcal{E} \), in which privacy amplification shortens the sifted key into \( NR_{\text{col}} \approx 2(d^2 - 1) \log_2(N + 1) \). Then we have \( \|((\mathcal{E} - \mathcal{F}^i) \otimes \text{id}_{\mathcal{H}_B^{\otimes r}}) \tau_{\psi^{kn}^{\otimes r}} \| \leq \epsilon_{\text{col}} \) still holds, where \( \mathcal{F} \) is a hypothetical map generating perfect keys.

Finally, we apply the theorem 1 of [31] and obtain
\[
\|((\mathcal{E} - \mathcal{F}^i) \otimes \text{id}_{\mathcal{H}_B^{\otimes r}}) \rho_{\psi^{kn}^{\otimes r}} \| \leq (N + 1)^{d-1} \|((\mathcal{E} - \mathcal{F}^i) \otimes \text{id}_{\mathcal{H}_B^{\otimes r}}) \tau_{\psi^{kn}^{\otimes r}} \| \leq \epsilon_{\text{col}}(N + 1)^{d-1}.
\]

Since \( \rho_{\psi^{kn}^{\otimes r}} \) is any state shared by Alice, Bob and Eve, this inequality clearly shows that the protocol \( \mathcal{E} \) is \( \epsilon_{\text{col}}(N + 1)^{d-1} \)-secure for any coherent attack. Substituting \( d = 8 \), we end the proof. □

According to the corollary, if Alice and Bob want to generate \( \epsilon_{\text{coh}} \)-secure keys against any attack, they will calculate the parameter \( \epsilon_{\text{col}} \) with equation (10), and generate keys with equations (9), (3) and (8).

Before proceeding, we review the logic of our proof and clarify why the difference between code mode and decoy mode does not compromise the security. In the analysis of collective attack, one can assume the quantum system shared by Alice, Bob and Eve is collective, i.e. Eve always treats each code round or decoy round with an identical operation, which implies that the parameter estimation can safely assume the statistical parameters corresponding to a same measurement are i.i.d for any round. In other words, the distinguishability between code states and decoy states has no effects on the parameter estimation in the context of collective attack, provided the security proof against collective attack has considered the fact that the emitted states used for key generation and the ones for testing are not exactly the same. Indeed, the [12] has considered this issue, namely, the security proof is suitable for all collective attacks. Consequently, parameter estimation with random sampling and its security parameter \( \epsilon_{\text{EQ}} \) are applicable when only collective attack is taken into account. Of course, analysis against collective attack is not sufficient in the finite-key region. Fortunately, based on the [31, 32], security proof of a discrete-variable QKD protocol against collective attack can be expanded into a proof against coherent attack (note that this theory only applies in permutation-invariant protocols, and evidently this is the case in TF-QKD by treating measurement message \( M \) as a part of quantum system). Following this, we proved that the security of coherent attack with \( \epsilon_{\text{coh}} \)-secure can be obtained from collective attack with \( \epsilon^{\prime} \)-secure, where \( \epsilon_{\text{coh}} = \epsilon^{\prime}(N + 1)^{d_3} \). Note that \( \epsilon^{\prime} \) is the overall security parameter against collective attack, and thus includes the security parameter of parameter estimation in the context of collective attack. Recall that we have clarified random sampling is relevant if collective attack is considered.

To evaluate the performance of NPP-TFQKD in finite-key region, simulations in fiber channel are performed here. The experimental parameters such as dark count rate, detection efficiency are listed in table 1.

| Dark count rate | Detection efficiency | Misalignment | Fiber loss | Total secure parameter \( \epsilon_{\text{coh}} \) |
|----------------|----------------------|--------------|------------|------------------|
| 10^{-8} per pulse | 60% | 1.5% | 0.2 dB km^{-1} | 10^{-10} |

Table 1. Experimental parameters [16, 41].

In addition to fixed parameters in table 1, there are some parameters should be optimized to maximize the SKR. There are 10 parameters should be optimized in total. The first set is decoy intensities \( \mu, \nu, \omega \). The second set is probabilities of modes and intensities. \( P_{\text{d}} \) denote probabilities of choosing code mode and \( P_{\text{d}c} = P_{ \mu } + P_{\nu } - P_{\omega } = P_{\mu }^{\text{d}} + P_{\nu }^{\text{d}} - P_{\omega }^{\text{d}} \). The number of pulses they both select code mode is \( N_{\text{p}}^{\text{d}} \) and they select decoy mode with intensity \( x \) and \( y \) respectively is \( N_{\text{p}}^{\text{d}c} P_{\omega }^{\text{d}} \). The other set is \( \epsilon_{\text{PA}}, \epsilon_{\text{EC}}, \epsilon_{\text{c}} \) satisfying \( \epsilon_{\text{PA}} + \epsilon_{\text{EC}} + \epsilon_{\text{c}} \leq \epsilon_{\text{coh}} \). The secure parameter \( \epsilon_{\text{PE}} = (\epsilon_{\text{col}} - \epsilon_{\text{PA}} - \epsilon_{\text{EC}} - \epsilon_{\text{c}})/11 \).

The optimal parameters can be regarded as a vector \( \vec{v} = [\mu, \nu, \omega, P_{\text{d}}, P_{\text{d}c}, P_{\text{d}c}, \epsilon_{\text{PA}}, \epsilon_{\text{EC}}, \epsilon_{\text{c}}] \). Noting that the convex form of function \( R_{\text{coh}} = F(\vec{v}) \) [42, 43] is not guaranteed, we choose particle swarm optimization algorithm (PSO) which can optimize the non-smooth function and non-convex function [44] to search the best \( \vec{v} \) to maximize the \( R_{\text{coh}} \).

The results of the simulations are illustrated in figures 2 and 3. In figure 2, we simulate the SKR as a function of distance between Alice and Bob while the pulses number \( N \) is fixed to be 10^{12}, 10^{13}, 10^{14}. In figure 3, we simulate the SKR as a function of \( N \) while the distance is fixed to be 50, 100 and 150 km. The results show that
compared with asymptotic situation, the protocol still works well in non-asymptotic situations and the linear bound is still overcome when $N \geq 10^{12}$. Some optimal parameters and SKRs are listed in Table 2.

4. NPP-TFQKD with both large random intensity fluctuation and finite-key size effect

Except for finite-key size effect, a ubiquitous loophole in practical QKD system is intensity fluctuation [23–25]. When applying decoy state technique, accurate intensity values are required to ensure the correct estimation of $Y_{nm}$ [12]. The uncertain intensities bring uncertain Poisson distribution of photon numbers in linear programming equations [12, 33], which leads to incorrect estimation of $Y_{nm}$ and may allow Eve to perform sophisticated attacks. Unfortunately, it is very difficult to control the intensity of WCP exactly in practical QKD system since noise, time jitter, problem of modulation and other imperfections of devices. In this section, we discuss the NPP-TFQKD with large random intensity fluctuation in finite-key size regime, where the ‘random’ means that the distribution of the intensity fluctuation can be arbitrary. The main contribution of this section is that we present a countermeasure of both large random intensity fluctuation and finite-key size effect of NPP-TFQKD. Since the Poisson distribution $P_n = e^{-x} x^n / n!$, where $x$ is the intensity of WCP, is not certain anymore, we

---

![Figure 2](image2.png)

**Figure 2.** SKR versus distance between Alice and Bob for three different pulses number ($N = 10^{12}$: blue, $N = 10^{13}$: red, $N = 10^{14}$: yellow). The purple dot-dash line is asymptotic SKR and the green dot line is the linear bound [7].

![Figure 3](image3.png)

**Figure 3.** Secret key rate in logarithmic scale as a function of pulses number $N$ for three different distance between Alice and Bob (50 km: yellow, 100 km: red, 150 km: blue). The solid lines denote non-asymptotic SKR and the dash lines show corresponding asymptotic SKR.

---

New J. Phys. 21 (2019) 123030 F-Y Lu et al
Table 2. Optimal parameters in non-asymptotic situations.

| Distance (km) | $\mu$       | $\nu$       | $\omega$     | $P_{\text{code}}$ | $P_\mu$     | $P_\nu$     | $P_\omega$ | $P_o$   | $R$       |
|---------------|-------------|-------------|--------------|-------------------|-------------|-------------|-------------|---------|----------|
|               | $N = 10^{12}$ |             |              |                   |             |             |             |         |          |
| 50            | 0.029 7041  | 0.677 129  | 0.266 772   | 0.932 176         | 0.014 8199 | 0.003 083 81| 0.017 5695 | 0.032 3505| 0.003 4352|
| 150           | 0.019 8943  | 0.707 745  | 0.305 501   | 0.915 991         | 0.024 1014 | 1e-05       | 0.023 0336 | 0.036 8643| 0.000 281 217|
| 250           | 0.012 4843  | 0.366 036  | 0.349 51    | 0.848 271         | 0.027 2353 | 1e-05       | 0.030 8167 | 0.093 6666| 1.030 32e-05|
| 350           | 0.006 068 51| 0.657 897  | 0.148 403   | 0.676 692         | 0.000 702 66| 0.023 3539  | 0.064 0229 | 0.235 229 | 6.756 24e-08|
|               | $N = 10^{13}$ |             |              |                   |             |             |             |         |          |
| 50            | 0.033 2228  | 0.662 703  | 0.284 533   | 0.956 632         | 0.008 317 12| 0.003 951 61| 0.012 0011 | 0.019 0981| 0.003 970 85|
| 150           | 0.022 4138  | 0.663 411  | 0.221 007   | 0.936 998         | 0.013 7466 | 1e-05       | 0.017 2474 | 0.031 9979| 0.000 263 338|
| 250           | 0.013 9126  | 0.642 318  | 0.273 503   | 0.902 825         | 0.018 6833 | 1e-05       | 0.021 0388 | 0.057 4429| 1.510 76e-05|
| 350           | 0.007 833 72| 0.533 179  | 0.121 501   | 0.818 001         | 1e-05      | 0.013 0499  | 0.043 094 | 0.125 845 | 4.475 01e-07|
|               | $N = 10^{14}$ |             |              |                   |             |             |             |         |          |
| 50            | 0.034 9457  | 0.516 41   | 0.218 549   | 0.967 932         | 0.004 461 75| 0.002 915 53| 0.009 783 82| 0.014 8868| 0.004 401 35|
| 150           | 0.023 292   | 0.543 888  | 0.160 051   | 0.953 002         | 0.009 144 17| 0.000 603 937| 0.014 1559 | 0.023 0941| 0.000 300 084|
| 250           | 0.015 3936  | 0.575 305  | 0.215 113   | 0.936 372         | 0.012 4987 | 1e-05       | 0.014 3871 | 0.036 7325| 1.871 65e-05|
| 350           | 0.008 299 56| 0.443 138  | 0.102 584   | 0.898 058         | 1e-05      | 0.009 399 55| 0.023 6518 | 0.068 8805| 7.341 52e-07|
present a new method to estimate \( p_n^{\pm} \) which denote, respectively, upper and lower bound of \( p_n \) and replace \( p_n \) by its worst case in our analytical formula. The analytical formula is presented to estimate \( Y_{\text{sum}} \) and is introduced in the next subsection. It worth noting that, by measuring the average intensity and upper and lower bound of fluctuation, our method can estimate tighter \( p_n^{\pm} \), which helps to improve the SKR in large random intensity fluctuation scenario.

### 4.1. Analytical formula of 4-intensity decoy state method of NPP-TFQKD

Before proposing the intensity fluctuation model of NPP-TFQKD, we will introduce our analytical formula of 4-intensity decoy state method. In ‘Parameter estimation and privacy amplification’ step, the n-photon yield can be estimated by linear programming or analytical formula [29, 30]. However, the analytical formula of NPP-TFQKD is not given. In our countermeasure of imperfect WCP source loophole in next section, the analytical formula is needed. To make the NPP-TFQKD more practical, the analytical formula of 4-intensity decoy state method is proposed.

Define \( q_{\text{sum}} = p_n^{\mu} p_n^{\nu} Y_{\text{sum}} \) where \( \mu, \nu \) is the Alice’s (Bob’s) intensity of the code mode. To estimate the upper bound of \( I_{\text{AB}} \), we have to estimate the upper bound of \( q_{00} + q_{01} + q_{20} + q_{21} \) and lower bound of \( q_{\text{sum}} = q_{00} + q_{01} + q_{20} + q_{21} + q_{11} \). The upper and lower bound of \( Y_{\text{sum}} \) can be estimated by applying linear programming [12, 33] whose constraints are joint of:

\[
Q_{xy} = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} p_n^x p_m^y Y_{\text{sum}} \quad (x, y \in \{ \mu, \nu, \omega, \sigma \}),
\]

(11)

where \( 0 \leq Y_{\text{sum}} \leq 1 \). Noting that these \( p_n^x \) depend on the intensity \( x \), it’s obvious that the \( p_n^x \) in equation (11) are uncertain and the linear programming will not be valid any more if we cannot control intensities exactly. Intuitively, we can still get secure bound of key rate if we correctly replace coefficients \( p_n^x \) by its upper and lower bound in analytical formula. Thus we present an analytical formula before building the fluctuation model.

We will use superscript or subscript ‘+’ and ‘−’ to express, respectively, upper and lower bound of a variable. We denote Alice’s (Bob’s) intensity in decoy mode by \( \mu, \nu, \omega, \mu', \nu', \omega' \) and \( \phi \) where \( \mu > \nu > \omega > \phi \) (\( \mu' > \nu' > \omega' > \phi \)) and \( \phi \) is the vacuum state. Alice’s (Bob’s) intensity of code mode is denoted by \( \mu, \nu, \omega \).

It is worth noting that, \( \mu, \nu, \omega \) should be the same as one of \( \mu, \nu, \omega, \mu', \nu', \omega' \). To make our formula more clear, we denote \( p_n^{\mu}, p_n^{\nu} \) and \( p_n^{\phi} \) by, respectively, \( a_n, b_n, \) and \( c_n, d_n, e_n, f_n \).

Here we will demonstrate how to estimate n-photon yield by analytical formulas as follows. The details are shown in appendix.

**Estimation of \( q_{00} \):**

\[
q_{00}^{\pm} = p_0^{\mu} p_0^{\nu} Q_{00}.
\]

**Upper bound of \( q_{01} \) and \( q_{01} \):**

\[
q_{01}^{\pm} = p_1^{\mu} p_0^{\nu} \left( K_1 c_2 - c_1 a_2 + K_1 (b_2 e_3 - b_3 e_2) + K_1 (a_2 b_3 - a_3 b_2) \right),
\]

(12)

where \( K_1 = Q_{00} - a_0 Q_{00} \), \( K_2 = Q_{00} - b_0 Q_{00} \) and \( K_3 = Q_{00} - c_0 Q_{00} \).

Similarly

\[
q_{20}^{\pm} = p_0^{\mu} p_2^{\nu} \left( H_1 c_1 - L_3 a_0 \right),
\]

(14)

where \( H_1 = Q_{00} - a_0 Q_{00}, L_3 = Q_{00} - c_0 Q_{00} \), \( \sum_{n=0}^{\infty} c_n \).

Similarly

\[
q_{02}^{\pm} = p_2^{\mu} p_0^{\nu} \left( H_1 c_1 - L_3 a_0 \right),
\]

(15)

where \( H_1 = Q_{00} - a_0 Q_{00}, L_3 = Q_{00} - c_0 Q_{00} \), \( \sum_{n=0}^{\infty} c_n \).

**Upper bound of \( q_{11} \):**

\[
q_{11}^{\pm} = Q_{11} c_1 - a_0 Q_{00} + p_0^{\mu} Q_{00} c_1 + p_0^{\mu} Q_{00} c_1 + p_0^{\mu} Q_{00} c_1.
\]

(16)

**Lower bound of \( q_{\text{sum}} \):**

We take two steps to calculate the \( q_{\text{sum}}^{\pm} \). Define \( q_{\text{sum}} = q_0 + q_{12} \), where \( q_0 = q_{00} + q_{01} + q_{20} + q_{21} \) and \( q_{12} = q_{11} \) and...
Figure 4. The main structure of simple tomography technique is showed in the red dash line box. Alice (Bob) does all operations as usual except attenuate intensity to 2x when she (he) actually wants x, then she (he) splits it by a 50:50 BS. One of the pulse is sent to Charlie and the other is measured by a local low dark-count SPD. By observing the count rate of the local SPD, Alice (Bob) can estimate the bound of average intensity. PM denotes phase modulator, decoy-IM denotes intensity modulator. VA denotes variable attenuator. BS denotes 50:50 beam splitter and SPD denotes single photon detector.

\[
q^{-}_1 = p_0^{\mu} \left( Q_{0|x_0} - \sum_{n=3}^{\infty} p_n^{x_0} \right) + p_0^{\mu'} (Q_{0|x_0'} - \sum_{n=3}^{\infty} p_n^{x_0'}) - p_0^{\mu} p_0^{\mu'} Q_{0|0},
\]
\[
q^{-}_2 = p_1^{\mu} p_1^{\mu'} T_1 b_1 b_1' - T_2 a_1 a_1' a_1 b_1 b_1' - b_1 b_1' a_1 a_1',
\]
(17)

where \( T_1 = Q_{0|x_0'} - a_0 Q_{0|x_0'} - a_0' Q_{0|0} + a_0 a_0' Q_{0|0} \) and \( T_2 = Q_{0|x_0'} - b_0 Q_{0|x_0'} - b_0' Q_{0|0} + b_0 b_0' Q_{0|0} \).

The lower bound of \( q_{\text{sum}} \) is

\[
q_{\text{sum}}^- = q^{-}_1 + q^{-}_2.
\]
(18)

4.2. Estimation of average intensity

In this subsection, we briefly introduce the simple tomography technique proposed by [24]. Based on this work, we propose a large random intensity fluctuation model in finite-key size regime.

As illustrated in figure 4, Alice (Bob) should firstly produce a WCP with intensity 2x when she (he) actually wants x. Before sending the WCP to Charlie, she (he) splits it by a 50:50 BS. One of the pulse is sent to Charlie and the other one is measured by a local low dark-count SPD whose detection efficiency is \( \eta \). After sending \( N_x \) x-intensity WCPs, the local detector’s count number is \( n_x \) and the \( \hat{n}_x \) denotes the observed \( n_x \). The dark count is ignored since it’s orders of magnitude lower than light count. Because of the random fluctuations, whenever Alice (Bob) wants to modulate intensity x, she (he) actually modulates \( \bar{x} = (1 + \delta_i)x \), where \( \bar{x} \) is the average intensity and the instantaneous fluctuation \( \delta_i \) is an unknow value. Mathematically, the click rate \( h_x \) is:

\[
h_x = \sum_{i=0}^{N_x} (1 - e^{-\eta \bar{x}}) / N_x.
\]
(19)

As proof in [24], the upper and lower bound of \( \bar{x} \) is:

\[
\bar{x} \leqslant \bar{x}_+ = 1 - \sqrt{1 - 2h_x (1 + \zeta)} / \eta (1 + \zeta),
\]
\[
\bar{x} \geqslant \bar{x}_- = h_x / \eta + h_x^2 / 2\eta - \eta^2 \bar{x}_+^2 / 3!,
\]
(20)

where \( \zeta = \sum \delta_i^2 / N_x \leqslant (\max \{|\delta_i|\})^2 \).

However, this conclusion in [24] cannot be used in non-asymptotic situations directly. Here we apply large deviation theory to make the method met practice.

Noting that the distribution of intensity fluctuation is not independent identically distributed in most cases, we choose Azuma’s inequality [45–47] rather than Chernoff bound to estimate the confidence interval of \( h_x \). The upper and lower bound of \( h_x \) is:
\[ h_x \leq h_x^+ = \left( \hat{a}_x + \sqrt{2\hat{a}_x \ln \frac{1}{\epsilon_0}} \right) / N_x, \]
\[ h_x \geq h_x^- = \left( \hat{a}_x - \sqrt{2\hat{a}_x \ln \frac{1}{\epsilon_0}} \right) / N_x, \]

where the \( \epsilon_0 \) is secure parameter of estimation. Then the bound of the average intensity is corrected as
\[ \bar{x} \leq \bar{x}_+ = 1 - \frac{\sqrt{1 - 2h_x^+(1 + \zeta)}}{\eta(1 + \zeta)}, \]
\[ \bar{x} \geq \bar{x}_- = h_x^- / \eta + (h_x^-)^2 / 2\eta - \eta^2 \bar{x}_+^2 / 3!. \]  

4.3. Model of NPP-TFQKD with both intensity fluctuation and finite-key size effect

In this subsection, we will propose our countermeasure model.

When we want sent x-intensity WCP, we actually prepare \( x_i = \bar{x}(1 + \delta_i) \) since the intensity fluctuation. The intensity range is \( x^+ = \bar{x}(1 + \delta^+) \) where \( \delta^+ = \max \{ \delta_i \} \) and \( \delta^- = \min \{ \delta_i \} \).

With definitions above, the density matrix of the source with fluctuation can be describe by:
\[ \rho_x = \sum_{i=1}^{N_x} e^{-x_i} x_i^n / n! \langle n \rangle / N_x. \]

Thus the \( p_n^x \) is re-written as:
\[ p_n^x = \frac{1}{N_x} \sum_{i=1}^{N_x} e^{-x_i} x_i^n / n! = \bar{x}e^{-\bar{x}} \sum_{i=1}^{N_x} e^{-\delta x_i}(1 + \delta_i)^n. \]

By applying Taylor expansion to equation (24), we obtain:
\[ p_n^x = \frac{\bar{x}e^{-\bar{x}}}{n! N_x} \left( 1 + \frac{n}{1} \delta_i + \frac{n^2}{2} \delta_i^2 + \ldots \right) \left( 1 + \frac{n}{1} \delta_i + \frac{n^2}{2} \delta_i^2 + \ldots \right).
\[ = \frac{\bar{x}e^{-\bar{x}}}{n! N_x} \left( 1 + \sum_{i=1}^{N_x} (n - \bar{x}) \delta_i + o(\delta_i) \right). \]

Since \( \bar{x} = \sum_{i=1}^{N_x} x_i(1 + \delta_i) \), we notice an important fact that \( \sum_{i=1}^{N_x} \delta_i = 0 \), namely, the \( \sum_{i=1}^{N_x} (n - \bar{x}) \delta_i = 0 \).

We have known that \( p_n^x = \frac{\bar{x}e^{-\bar{x}} \sum_{i=1}^{N_x} e^{-\delta x_i}(1 + \delta_i)^n}{n! N_x} \) from equation (24) in the article. The \( p_n^x \) can be rewritten as:
\[ p_n^x = p_n^x - 0 = p_n^x - \sum_{i=1}^{N_x} (n - \bar{x}) \delta_i = \frac{\bar{x}e^{-\bar{x}}}{n! N_x} \sum_{i=1}^{N_x} e^{-\delta x_i}(1 + \delta_i)^n - (n - \bar{x}) \delta_i. \]

By defining \( f_n(\delta, \bar{x}) = \frac{\bar{x}e^{-\bar{x}}}{n!} \sum_{i=1}^{N_x} e^{-\delta x_i}(1 + \delta_i)^n - (n - \bar{x}) \delta_i \), \( p_n^x \) can be rewritten as:
\[ p_n^x = \frac{1}{N_x} \sum_{i=1}^{N_x} f_n(\delta_i, \bar{x}). \]

Define \( a_n^+ = \max f_n(\delta_i, \bar{x}) \) and \( a_n^- = \min f_n(\delta_i, \bar{x}) \), where \( \delta \in [\delta^-, \delta^+] \) and \( \bar{x} \in [\bar{x}_-, \bar{x}_+] \). The \( a_n^+ \) and \( a_n^- \) is the upper and lower bound of \( a_n \). The upper and lower bound of \( f_n(\delta_i, \bar{x}) \) can be obtained by optimization algorithms.

Espacially, when \( n = 0 \)
\[ a_0 \geq a_0^- = e^{-\mu^+}; \quad a_0 \leq a_0^+ = e^{-\mu^ -}. \]
\[ b_n^+ \text{ and } c_n^+ \text{ in the analytical formula can be obtained similarly.} \]
However, without introduction of average intensity, when \( n \geq 1 \):
\[ a_n \geq a_n^- = a_n^+ = \frac{e^{-\mu}}{n!} \mu^n, \]
\[ \text{and when } n = 0: \]
\[ a_0 \geq a_0^- = e^{-\mu^-}; \quad a_0 \leq a_0^+ = e^{-\mu^+}. \]

The difference between introducing average intensity or not is showed in figure 5, it indicates that the introduction of average intensity can significantly tighten the bound.

By replacing coefficients \( p_n^x \) (namely, \( a_n, b_n, c_n, a_n^+, b_n^+, c_n^+, p_n^+ \) and \( p_n^- \)) and \( Q_{xy} \) by their upper or lower bound, the analytical formula is rewritten as:
Upper bound of $q_{00}$:

$$q_{00}^+ = p_{00}^+ p_{00}^{l+} Q_{00}^+,$$

Upper bound of $q_{10}$ and $q_{01}$:

$$q_{10}^+ = p_{10}^+ p_{00}^{l+} K_1^+(c_2^+ a_2^+ - c_2^- a_2^-) - K_2^+(b_2^- c_2^- - b_2^+ c_2^+) - K_3^+(a_3^- b_2^- - a_3^+ b_2^+) ,$$

where $K_1^+ = Q_{10}^+ - a_0^+ Q_{00}^+ , K_2^+ = Q_{01}^+ - b_0^+ Q_{00}^+ , K_3 = Q_{00}^+ - c_0^+ Q_{00}^+ .

Similarly

$$q_{01}^+ = p_{01}^+ p_{10}^{l+} K_3^+(c_2^+ a_2^+ - c_2^- a_2^-) - K_1^+(b_2^- c_2^- - b_2^+ c_2^+) - K_2^+(a_3^- b_2^- - a_3^+ b_2^+) ,$$

where $K_1^- = Q_{01}^- - a_0^- Q_{00}^- , K_2^+ = Q_{01}^- - b_0^+ Q_{00}^- , K_3^- = Q_{00}^- - c_0^+ Q_{00}^- .

Upper bound of $q_{20}$ and $q_{02}$:

$$q_{20}^+ = p_{20}^+ p_{00}^{l+} H_1^+ c_1^+ - L_3^- a_2^- ,$$

where $H_1^+ = Q_{00}^+ - a_0^+ Q_{00}^+ , L_3^- = Q_{00}^- - c_0^+ Q_{00}^- - (\sum_{n=5}^{\infty} \epsilon_n) .

Similarly

$$q_{02}^+ = p_{02}^+ p_{20}^{l+} \frac{H_1^+ c_1^+ - L_3^- a_2^-}{a_2^- c_1^+ - a_1^+ c_2^-} ,$$

where $H_1^+ = Q_{00}^+ - a_0^+ Q_{00}^+ , L_3^- = Q_{00}^- - c_0^+ Q_{00}^- - (\sum_{n=5}^{\infty} \epsilon_n) .

Figure 5. We compare the upper and lower bound of $q_{n0}$ with two methods. The intensity is fixed at 0.5 and $n = 0, 1, 2, 3$ in different figures. In these figures, the blue and red lines denote the upper and lower bound respectively. The solid lines denote the model only considering fluctuation range and dash lines are our method which introducing the average intensity. It’s obvious that our method estimates the bound much tighter.
Upper bound of $q_{11}$:

$$q_{11}^+ = Q_{\mu_1}^{++} - P_{Q_{\mu_1}}^{+} + Q_{Q_\mu}^{+} + P_{Q_\mu}^{+} + P_{Q_\mu}^{+} + Q_{Q_\mu}^{+}$$  \hspace{1cm} (35)$$

Lower bound of $q_{\text{sum}}$:

$$q_{\text{sum}}^- = q_{i1}^- + q_{i2}^-,$$  \hspace{1cm} (36)$$

where

$$q_{i1}^- = P_{Q_{\mu_1}}^{+} - P_{Q_{\mu_1}}^{-} - \sum_{n=3}^{\infty} P_{\mu_1}^{-} + Q_{Q_\mu}^{+} - \sum_{n=3}^{\infty} P_{Q_{\mu_1}}^{-} - P_{Q_{\mu_1}}^{+} + P_{Q_\mu}^{+},$$  \hspace{1cm} (37)$$

and

$$T_{1} = Q_{\mu_1}^{-} - a_0^+ Q_{Q_\mu}^+ + a_0^+ Q_{Q_\mu}^+ + a_0^+ Q_{Q_\mu}^+, \hspace{1cm} T_{2} = Q_{Q_\mu}^- - b_0^+ Q_{Q_\mu}^- + b_0^+ Q_{Q_\mu}^- + b_0^+ Q_{Q_\mu}^-.$$  \hspace{1cm} (38)$$

The simulation of NPP-TFQKD with both large random intensity fluctuation and finite-key size effect is shown in figure 6. The experimental parameters are listed in table 1 and the secure parameter of Azuma’s inequality in equation (21), namely, $\epsilon_0$ is fixed to $10^{-10}$. To emphasize the countermeasure of intensity fluctuation, we simulate the SKR as a function of distance for different intensity fluctuation range. Similar to the optimization introduced in section 3, we maximize SKR by using PSO algorithm to optimize $\rho_{mnw}$. The optimal parameters are listed in table 3.

The result of NPP-TFQKD indicates that by applying our countermeasure model, the large random intensity fluctuation has very limited influence on the performance of NPP-TFQKD.

5. Discussion

In this article, we have discussed some practical issues of NPP-TFQKD based on [12]. We firstly analyzed the issue of finite-key size effect and solve this problem by applying post-selection technique for quantum channels.
Table 3. Some optimal parameters when finite-key size effect and intensity fluctuation are taken into consider.

| distance (km) | $\mu$   | $\nu$   | $\omega$ | $P_{\text{code}}$ | $P_{\mu}$ | $P_{\nu}$ | $P_{\omega}$ | $P_{R}$ | $R$     |
|--------------|---------|---------|----------|-------------------|-----------|-----------|-----------|---------|---------|
| $N = 10^{14}, \delta_{N} = 0\%$ |
| 50           | 0.028 419 | 0.224 84 | 0.269 07 | 0.954 54 | 0.003 5100 | 1e-05 | 0.002 606 | 0.039 3296 | 0.004 1441 |
| 200          | 0.018 25  | 0.256 81 | 0.259 53 | 0.936 86 | 0.024 225  | 1e-05 | 0.005 4998 | 0.033 398  | 7.950 5e-05 |
| 350          | 0.009 8314 | 0.3232 | 0.037 000 | 0.822 33 | 0.012 643  | 0.017 298 | 0.000 142 61 | 0.1475 | 5.589 4e-07 |
| $N = 10^{14}, \delta_{N} = \pm 20\%$ |
| 50           | 0.032 226 | 0.642 47 | 0.514 82 | 0.927 70 | 0.000 808 17 | 0.026 791 | 1e-05 | 0.044 685 | 0.003 5298 |
| 200          | 0.017 263 | 0.5499  | 0.420 25 | 0.929 33 | 0.017 880  | 0.006 6488 | 1e-05 | 0.046 1267 | 7.428 06e-05 |
| 350          | 0.007 7948 | 0.530 21 | 0.435 65 | 0.914 24 | 0.017 224  | 0.004 639 | 1e-05 | 0.063 883  | 5.908 6e-07 |
| $N = 10^{14}, \delta_{N} = \pm 50\%$ |
| 50           | 0.031 897 | 0.218 34 | 0.494 98 | 0.948 46 | 0.012 816  | 0.015 244 | 0.003 6931 | 0.019 782 | 0.003 3357 |
| 200          | 0.020 452 | 0.275 06 | 0.467 05 | 0.958 99 | 0.004 0597 | 1e-05 | 0.012 359  | 0.024 572  | 6.623 3e-05 |
| 350          | 0.006 2331 | 0.175 99 | 0.5395 | 0.859 18 | 0.015 274  | 1e-05 | 0.020 731  | 0.104 80  | 4.828 5e-07 |
Another contribution of this work is we propose a countermeasure of intensity fluctuation. We introduce an analytical formula of decoy state method to meet the needs of our fluctuation model. Then we propose our intensity fluctuation model to deal with large random intensity fluctuation problem in the source side. Our model is practical since it doesn’t contain any assumption about distribution of fluctuation. It only need average intensity and fluctuation range, which can be measured by local detectors. Our simulation results suggest that by applying our method, the non-asymptotic SKR can still break the linear bound even if the large random intensity fluctuation is taken into account.

Some work have discussed the TF-QKD with coherent attack, we briefly discuss them here.

The [9] is the earliest work mentioned coherent attack which we can find. This work independently proposed a very similar idea with [12]. The [9] also proposed that by applying Azuma inequality, their proof is against coherent attack. However, they do not give a detailed quantitative analysis on coherent attack in finite-key region.

Indeed, Azuma inequality is a general tool to deal with coherent attack and finite-key effects. However, since Azuma inequality converges slowly with the number of rounds, we conjecture this technique may be a not good solution.

Another work [48] is based on sending-or-not-sending QKD. By applying entropic uncertainty relations method [38, 39], the key rate of sending-or-not-sending QKD against coherent attack is proposed. Their method is a powerful way to deal with coherent attack and finite-key effects, but seems to be not applicable in NPP-TFQKD.

From the view of performance, the sending-or-not-sending QKD features its robustness against large misalignment error and finite-key effects. It seems that NPP-TFQKD is more sensitive to finite-key effects. However, when the misalignment error is small and key size is large, NPP-TFQKD may perform better.

It worth noting that, in order to simplify the simulation, we suppose that all experimental parameters are symmetric, namely, parameters such as dark count rate, detection efficiency, distance to Charlie, misalignment and intensity fluctuation of Alice and Bob are same. However, the experimental setups are usually asymmetric. It is an open question that how to optimize intensity and probability parameters to efficiently maximize the secure key rate. Reference [49] is a recently published work about the asymmetric sending-or-not-sending QKD.

Another open question is if the vacuum state $o$ can be removed or replace by other intensities. In our simulation, we set vacuum state to estimate $Y^o_{\infty}$ tighter. However, the IM in a real implementation has a finite extinction ratio, it would be very challenging to obtain approximate vacuum state. The [50] demonstrates an approach to generate stable and high extinction ratio light pulses with an extinction ratio $>80 \text{ dB}$ by cascading two IM, which can attenuate coherent pulse to approximate vacuum state. It is worth to study if the vacuum state can be removed to make the protocol more practically useful.

Note added.—Recently, we found that [31, 52] discussed the finite-key size effect and [53, 54] discussed the security of TF-QKD under intensity fluctuation.

6. Funding information

This work has been supported by the National Key Research and Development Program of China (Grant No. 2016YFA0302600), the National Natural Science Foundation of China (Grant Nos. 61822115, 61775207, 61702469, 61771439, 61622506, 61627820, 61575183), National Cryptography Development Fund (Grant No. MMJJ20170120) and Anhui Initiative in Quantum Information Technologies.

Appendix. Proof of analytical formula

Before introduce our analytical formula, we should introduce some important conclusions. The first improtant conclusion is:

$$\frac{P_m^x}{P_n^x} \geq \frac{P_m^y}{P_n^y} \quad (A.40)$$

where $x \geq y$ and $m \geq n$. The details can be found in [29, 30].

The next is:

$$Q_{xy} = \sum_{n,m=0}^{\infty} P_n^x P_m^y Y_{mn} \quad (A.41)$$

where $x \in \{ \mu, \nu, \omega, o \}$ and $y \in \{ \mu', \nu', \omega', o \}$. 

[31] and using Chernoff Bound to estimate fluctuations of observed values. The simulation shows that NPP-TFQKD works well in non-asymptotic situations.
Especially, when one of the user select vacuum state, there are:

\[ Q_{\omega} = \sum_{n} p_{n}^{\omega} Y_{0n}, \]  
\[ (A.42) \]

and

\[ Q_{\varphi} = \sum_{m} p_{m}^{\varphi} Y_{0m}. \]  
\[ (A.43) \]

Based on above conclusions, we can estimate upper and lower bound of some important \( q_{nm} \), the proofs are showed as follows:

**Upper bound of \( q_{00} \):**
The \( Y_{00} = Q_{\omega} \) since \( \sigma \) is vacuum state. Thus:

\[ q_{00} = p_{0}^{\mu} p_{0}^{\nu} Y_{00} = p_{0}^{\mu} p_{0}^{\nu} Q_{\omega}. \]  
\[ (A.44) \]

**Upper bound of \( q_{01} \) and \( q_{10} \):**
We take \( +q_{10} \) as an example. The proof of \( +q_{01} \) is similar.

We define \( K_{1} = Q_{\omega} - a_{0} Q_{\omega}, K_{2} = Q_{\omega} - b_{0} Q_{\omega}, K_{3} = Q_{\omega} - c_{0} Q_{\omega}. \) Using equation \( (A.42) \), we obtain:

\[
\begin{align*}
K_{1} &= a_{1} Y_{10} + a_{2} Y_{20} + a_{3} Y_{30} + \ldots, \\
K_{2} &= b_{1} Y_{10} + b_{2} Y_{20} + b_{3} Y_{30} + \ldots, \\
K_{3} &= c_{1} Y_{10} + c_{2} Y_{20} + c_{3} Y_{30} + \ldots.
\end{align*}
\]  
\[ (A.45) \]

By defining \( \tau = \sum_{k=3}^{\infty} b_{k} Y_{k0} \) and applying conclusion equations \( (A.40) \)--\( (A.45) \), we can derive inequalities that:

\[ Y_{10}^{+} = \frac{K_{2}(c_{2} a_{3} - c_{3} a_{2}) + K_{1}(b_{2} c_{3} - b_{3} c_{2}) + K_{3}(a_{2} b_{3} - a_{3} b_{2})}{b_{2}(a_{1} c_{3} - c_{1} a_{3}) + b_{1}(a_{2} c_{3} - c_{2} a_{3}) + b_{3}(a_{2} c_{1} - a_{1} c_{2})}. \]

The \( q_{10}^{+} \) is:

\[ q_{10}^{+} = p_{1}^{\mu} p_{1}^{\nu} Y_{10}^{+}. \]  
\[ (A.48) \]

**Upper bound of \( q_{02} \) and \( q_{20} \):**
We take \( q_{20}^{+} \) as an example. Based on equation \( (A.42) \), we obtain:

\[
Q_{\omega} \geq Q_{\omega} \geq Q_{\omega} \\
Q_{\omega} \leq Q_{\omega} \leq Q_{\omega}. \]  
\[ (A.49) \]

By defining \( H_{1} = Q_{\omega} - a_{0} Q_{\omega} \) and \( L_{3} = Q_{\omega} - c_{0} Q_{\omega} - (c_{3} + c_{4} + c_{5} + \ldots) \), the equation \( (A.49) \) can be written as:

\[
\begin{align*}
H_{1} > Y_{10} a_{1} + Y_{20} a_{2} \\
L_{3} < Y_{10} c_{1} + Y_{20} c_{2}.
\end{align*}
\]  
\[ (A.50) \]

Solving the equation \( (A.50) \), we obtain:

\[ Y_{20}^{+} = \frac{H_{1} c_{1} - L_{3} a_{1}}{a_{2} c_{1} - a_{1} c_{2}}. \]  
\[ (A.51) \]

The \( q_{20}^{+} \) is:

\[ q_{20}^{+} = p_{2}^{\mu} p_{2}^{\nu} Y_{20}^{+}. \]  
\[ (A.52) \]

**Upper bound of \( q_{11} \):**
Observing equation \( (A.44) \), we obtain:

\[ q_{11} < \sum_{n=1, m=1}^{\infty} p_{n}^{\mu} p_{m}^{\nu} Y_{nm} = Q_{\mu_{1}, \nu_{1}} - p_{0}^{\mu_{1}} Q_{\mu_{0}, \nu_{0}} - p_{0}^{\mu_{2}} Q_{\mu_{0}, \nu_{2}} + p_{0}^{\mu_{3}} p_{0}^{\nu_{3}} Q_{\omega}. \]  
\[ (A.53) \]
Thus the upper bound of $q_{11}$ is:
\[ q^+_{11} = Q_{\nu, \nu'} - p^\mu_0 Q_{\nu, \nu} + p^\mu_0 Q_{\mu', \nu} + p^\mu_0 p^\mu_0 Q_{\nu, \nu}. \]  
(A.54)

Lower bound of $q_{00} + q_{01} + q_{02} + q_{03} + q_{04} + q_{05} + q_{11}$: define $q_{\text{sum}} = q_{00} + q_{01} + q_{02} + q_{03} + q_{04} + q_{05} + q_{11}$, we estimate lower bound of $q_{11}$ as $q_{00} + q_{01} + q_{02} + q_{03} + q_{04} + q_{05} + q_{11}$ separately. Firstly, we estimate the $q^+_{11}$. By applying equations (A.42) and (A.43), we obtain:
\[ q^+_{11} = \left( Q_{\nu, \nu} - \sum_{n=3}^{\infty} q_{0n} \right) + \left( Q_{\mu', \nu} - \sum_{m=3}^{\infty} q_{0m} \right) - p^\mu_0 p^\mu_0 Q_{\nu, \nu} \]
\[ \geq \left( Q_{\nu, \nu} - \sum_{n=3}^{\infty} p^\mu_0 \right) + \left( Q_{\mu', \nu} - \sum_{m=3}^{\infty} p^\mu_0 \right) - p^\mu_0 p^\mu_0 Q_{\nu, \nu} = q^+_{11}. \]  
(A.55)

Then we estimate the $q^-_{11}$, namely, the $q^+_{11}$. Similar to the estimation of $q^+_{11}$, we define:
\[ T_1 = Q_{\nu, \nu'} - a_0 Q_{\nu, \nu'} + a_0 Q_{\nu, \nu}, \]  
(A.56)
\[ T_2 = Q_{\nu, \nu} - b_0 Q_{\nu, \nu} + b_0 Q_{\nu, \nu}, \]  
(A.57)
\[ \tau' = \sum_{n, m=1}^{\infty} b_n b_m Y_{nm} - b_n b_m Y_{11}. \]  
(A.58)

By applying above equations, we obtain an inequality set:
\[ \begin{align*}
E_{11} &< \frac{a_1 b_1 b_1 Y_{11}}{a_2} + \tau'; \\
T_2 & = b_1 b_1 Y_{11} + \tau'.
\end{align*} \]  
(A.59)

Solving the equation (A.59), we obtain:
\[ Y_{11} = \frac{T_2 b_1 b_1 - T_1 a_1 a_1}{a_1 a_1 b_1 b_1 - b_1 b_1 a_1 a_1}, \]  
(A.60)
and
\[ q^-_{11} = p^\mu_0 p^\mu_0 Y_{11}. \]  
(A.61)

It is obviously that $q_{\text{sum}} = q^-_{11} + q^-_{11}$.

ORCID iDs

Zhen-Qiang Yin \( \text{https://orcid.org/0000-0002-3486-3934} \)

References

[1] Bennett C H and Brassard G 2014 Theor. Comput. Sci. 560 7
[2] Ekert A K 1991 Phys. Rev. Lett. 67 661
[3] Mayers D 2001 Jo. ACM (JACM) 48 351
[4] Lo H-K and Chau H F 1999 Science 283 2050
[5] Shor P W and Preskill J 2000 Phys. Rev. Lett. 85 411
[6] Takeoka M, Guha S and Wilde M M 2014 Nat. Commun. 5 5235
[7] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Nat. Commun. 8 15043
[8] Lucamarini M, Yuan Z, Dyines J and Shields A 2018 Nature 557 400
[9] Tamaki K, Lo H-K, Wang W and Lucamarini M 2018 arXiv:1805.05511
[10] Ma X, Zeng P and Zhou H 2018 Phys. Rev. X 8 031043
[11] Wang X-B, Yu Z-W and Hu X-L 2018 Phys. Rev. A 98 062323
[12] Cui C, Yin Z-Q, Wang R, Chen W, Wang S, Guo G-C and Han Z-F 2019 Phys. Rev. Appl. 11 034053
[13] Curty M, Azuma K and Lo H-K 2019 npj Quantum Inf. 5 64
[14] Lin J and Lütkenhaus N 2018 Phys. Rev. A 98 042332
[15] Minder M, Pittaluga M, Roberts G, Lucamarini M, Dyines J, Yuan Z and Shields A 2019 Nat. Photon. 13 1334
[16] Wang S, He D-Y, Yin Z-Q, Lu F-Y, Cui C-H, Chen W, Zhou Z, Guo G-C and Han Z-F 2019 Phys. Rev. X 9 021046
[17] Liu Y et al 2019 Phys. Rev. Lett. 123 100505
[18] Zhong X, Hu J, Curty M, Qian L and Lo H-K 2019 Phys. Rev. Lett. 123 100506
[19] Lo H-K, Curty M and Qian L 2012 Phys. Rev. Lett. 108 130503
[20] Wang C, Song X-Y, Yin Z-Q, Wang S, Chen W, Zhang C-M, Guo G-C and Han Z-F 2015 Phys. Rev. Lett. 115 160502
[21] Lu Y et al 2013 Phys. Rev. Lett. 111 130502
[22] Ma X and Razavi M 2012 Phys. Rev. A 86 062319
[23] Wang X-B, Yang L, Peng C-Z and Pan J-W 2009 New J. Phys. 11 075006
[24] Wang X-B 2007 Phys. Rev. A 75 052301
[25] Zhou X-Y, Zhang C-M and Wang Q 2017 JOSA B 34 1518
[26] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[27] Wang X-B 2005 Phys. Rev. A 72 012322
[28] Wang X-B 2005 Phys. Rev. Lett. 94 230503
[29] Wang X-B 2013 Phys. Rev. A 87 012320
[30] Yu Z-W, Zhou Y-H and Wang X-B 2015 Phys. Rev. A 91 032318
[31] Christandl M, König R and Renner R 2009 Phys. Rev. Lett. 102 020504
[32] Sheridan J, Le T P and Scarani V 2010 New J. Phys. 12 123019
[33] Ma X, Fung C-H F and Razavi M 2012 Phys. Rev. A 86 052305
[34] Curty M, Xu F, Cui W, Lim C C W, Tamaki K and Lo H-K 2014 Nat. Commun. 5 3732
[35] Müller-Quade J and Renner R 2009 New J. Phys. 11 085006
[36] Wang C, Yin Z-Q, Wang S, Chen W, Guo G-C and Han Z-F 2017 Optica 4 1016
[37] Tang Y-L et al 2014 Phys. Rev. Lett. 113 190501
[38] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 Nat. Commun. 3 634
[39] Tomamichel M and Renner R 2011 Phys. Rev. Lett. 106 110506
[40] Koashi M 2009 New J. Phys. 11 045018
[41] Boaron A et al. 2018 Phys. Rev. Lett. 121 190502
[42] Lu F-Y, Yin Z-Q and Wang C 2019 JOSA B 36 92
[43] Wang W and Lo H-K 2018 arXiv:1812.07724
[44] Shi Y and Eberhart R C 1999 Proc. 1999 Congress on Evolutionary Computation pp 1945–50
[45] Yin Z-Q, Li H W, Chen W, Han Z F and Guo G C 2010 Phys. Rev. A 82 042335
[46] Boileau J C, Tamaki K, Batuwantudawe J, Laflamme R and Renes J M 2005 Phys. Rev. Lett. 94 040503
[47] Azuma K 1967 Tohoku Math. J. 19 357
[48] Xu H, Yu Z-W, Jiang C, Hu X-L and Wang X-B 2019 arXiv:1904.06331
[49] Zhou X-Y, Zhang C-H, Zhang C-M and Wang Q 2019 Phys. Rev. A 99 062316
[50] Wang X, Liu J, Li X and Li Y 2015 IEEE J. Quantum Electron. 51 5200206
[51] Yin H-L and Chen Z-B 2019 arXiv:1903.09093
[52] Maeda K, Sasaki T and Koashi M 2019 Nat. Commun. 10 3140
[53] Grasselli F and Curty M 2019 New J. Phys. 21 073001
[54] Federico Grasselli M C and Navarrete A 2019 New J. Phys. 21 113032