# Security of the traditional quantum key distribution protocols with finite-key lengths

Bao Feng(冯宝)[1,2], Hai-Dong Huang(黄海东)[3], Yu-Xiang Bian(卞宇翔)[1,2], Wei Jia(贾玮)[1,2], Xing-Yu Zhou(周星宇)[4,†], and Qin Wang(王琴)[4]

[1] *State Grid Electric Power Research Institute, Nanjing* 211000, *China*
[2] *NRGD Quantum CTEK Co., Ltd., Nanjing* 211000, *China*
[3] *State Grid Jiangsu Electric Power Co., Ltd., Nanjing* 210000, *China*
[4] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 19 July 2022; revised manuscript received 29 September 2022; accepted manuscript online 19 October 2022)

Quantum key distribution (QKD) in principle can provide unconditional secure communication between distant parts. However, when finite-key length is taken into account, the security can only be ensured within certain security level. In this paper, we adopt the Chernoff bound analysis method to deal with finite-key-size effects, carrying out corresponding investigations on the relationship between the key generation rate and security parameters for different protocols, including BB84, measurement-device-independent and twin-field QKD protocols. Simulation results show that there exists a fundamental limit between the key rate and the security parameters. Therefore, this study can provide valuable references for practical application of QKD, getting a nice balance between the key generation rate and the security level.

**Keywords:** quantum key distribution, BB84, measurement-device-independent quantum key distribution, twin-field quantum key distribution

**PACS:** 03.67.Dd, 03.67.Hk, 42.65.Lm **DOI:** 10.1088/1674-1056/ac9b33

## 1. Introduction

The conventional power system widely adopts the national secret algorithm based on computational complexity to realize the encrypted transmission of business data. At the meantime, the increase of computing power, especially the rapid development of quantum computers threatens the security of conventional encryption systems. Luckily, quantum key distribution (QKD) has attracted wide attention since the first QKD protocol (BB84) was proposed in 1984.[1] Based on the laws of quantum physics, QKD has been proven to possess unconditional security in theory.[2–4] Since 2012, State Grid Corporation of China had introduced QKD technology into the power system, and successively built demonstration networks in Nanjing, Hefei, Beijing, Shanghai, Tianjin, Wuhan and other cities in China, realizing the verification in various power control systems. In these demonstrations, BB84 protocol based on decoy-state method,[5–7] an efficient countermeasure of photon-number-splitting attacks, is applied wildly. Considering the influence of overhead optical cable lines in real-life facilities, the encoding methods in power systems include: (i) polarization encoding method for buried optical cable lines; (ii) fast polarization feedback encoding method for medium and short distance overhead lines; (iii) phase encoding method with overhead lines for long distances. Generally, the distance between the power system business sites is far away from each other and the optical cable has a fixed attenuation, usually 0.2 dB/km–0.4 dB/km. When the distance reaches a certain distance, it will be difficult to meet the requirements of power business applications. In order to solve those problems, people proposed the measurement-device-independent quantum key distribution (MDI-QKD)[8,9] and the twin-field quantum key distribution (TF-QKD) protocols[10–12] to enhance the transmission distance.

In practical implementations, considering the number of pulses sent by the communicated parties is finite, the finite-key-size effect should be taken into consideration regardless of the chosen protocols. Up to now, several methods have been proposed to deal with the statistical fluctuation, such as the Gaussian approximation analysis,[13] the Hoeffding inequality,[14,15] the Chernoff bound,[16,17] etc. With the above analyzing methods, we can deduce out secure keys with certain failure probability. However, we cannot arbitrarily choose security parameters to one-side pursue either a higher key rate or a higher-level security. In this paper, we will show that there has a fundamental limit between the key generation rate and the security parameter when finite-key length is taken into account.

In this paper, we will illustrate the conclusions through utilizing three practical QKD protocols, i.e., the BB84, the MDI-QKD and the TF-QKD. We hope that our present work could provide valuable references for choosing proper security parameters under practical environments.

†Corresponding author. E-mail: xyz@njupt.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd 

## 2. The BB84 protocol

BB84 was proposed by Bennett and Brassard in 1984.[1] In general, it contains two parts, the sender (Alice) and the receiver (Bob). Even today, it still has wide applications due to its simplicity and practicality. Below let us illustrate the processes of the specific protocol.

(i) Alice randomly modulates her pulses into three different intensities, i.e., signal state $\mu$, decoy state $v$ and vacuum state $o$, with a probability of $P_\mu$, $P_v$, and $P_o$ individually. Meanwhile, the signal state ($\mu$) and the decoy state ($v$) will also be randomly prepared in $Z$ or $X$ basis with certain conditional probability.

(ii) Upon receiving the light pulses sent by Alice, Bob randomly chooses one of the bases ($Z$ or $X$) with certain probability ($P_Z$ or $P_X$) to do projection measurement.

(iii) After the transmission process is completed, Alice and Bob compare their basis choices through an authenticated classic channel. The bits using the same basis will be retained. Otherwise, they will be discarded.

(iv) Alice and Bob carry out post-processing processes, i.e., error corrections and privacy amplifications, to obtain the final secure keys.

In the asymptotic case, the gain of decoy state and signal state in the $W$ ($W \in \{Z,X\}$) basis can be expressed as

$$Q_\xi^W = \sum_{i=0}^{\infty} Y_i P_\xi(i), \tag{1}$$

where $Y_i$ represents the yield of $i$-photon state and $P_\xi(i)$ ($\xi \in \{o,v,\mu\}$) denotes the photon number distribution of certain light source. Furthermore, the average quantum-bit error-rate (QBER) of decoy state in $W$ basis can be expressed as

$$E_\xi^W Q_\xi^W = \sum_{i=0}^{\infty} e_i Y_i P_\xi(i), \tag{2}$$

in which $e_i$ is the error rate of the $i$-photon state.

According to the definitions above, we can obtain the lower bound of the single-photon counting rate in $X$ ($Z$) basis and the upper bound of the quantum bit error rate of single-photon pulses in $X$ basis

$$\begin{aligned} Y_1^W &\geq Y_1^{W,L} \\ &= \frac{P_\mu(2)Q_v^W - P_v(2)Q_\mu^W - (P_v(0)P_\mu(2) - P_v(2)P_\mu(0))Y_0}{P_v(1)P_\mu(2) - P_v(2)P_\mu(1)}, \end{aligned} \tag{3}$$

$$e_1^{bX} \leq e_1^{bX,U} = \frac{E_v^X Q_v^X - e_0 P_v(0) Y_0}{P_v(1) Y_1^{X,L}}, \tag{4}$$

where $Y_0$ is the dark count rate and $e_0$ corresponds to the error rate of a vacuum pulse. Furthermore, the phase error rate $e_1^{pZ}$ [18] can be written as

$$e_1^{pZ} = e_1^{bX} + \theta_X, \tag{5}$$

where $\theta_X$ is the deviation of the phase error rate from the tested value due to the statistical fluctuation, which can be referred in Ref. [19].

In nonasymptotic case, however, the number of pulses sent by Alice is finite. Thus, we must take statistical fluctuation into consideration for the observed value.[20] In this manuscript, the Chernoff bound analysis method will be adopted to deal with the deviations between the expected and observed values. We can estimate the statistical fluctuation range with a probability $1-2\varepsilon$, i.e.,

$$X = \mathbb{E}[X] + \delta, \tag{6}$$

where $\delta \in [\Delta, -\hat{\Delta}]$ with $\Delta = F(X, \varepsilon^4/16)$, $\hat{\Delta} = F(X, \varepsilon^{3/2})$, and $F(x,y) = \sqrt{2x\ln(y^{-1})}$. And in here, the system gain and system bit error are affected by the finite key-length to produce statistical fluctuations, it means the $X$ can be considered as sysytem gain or QBER. Specifically, Eq. (6) can be written as

$$\begin{aligned} &Q_{x,y}^W - \frac{F(N_{x,y}^W \hat{Q}_{x,y}^W, \varepsilon^4/16)}{N_{x,y}^W} \\ &\leq \hat{Q}_{x,y}^W \leq Q_{x,y}^W - \frac{F(N_{x,y}^W \hat{Q}_{x,y}^W, \varepsilon^{3/2})}{N_{x,y}^W}, \end{aligned} \tag{7}$$

$$\begin{aligned} &E_{x,y}^W Q_{x,y}^W - \frac{F(N_{x,y}^W \hat{E}_{x,y}^W \hat{Q}_{x,y}^W, \varepsilon^4/16)}{N_{x,y}^W} \\ &\leq \hat{E}_{x,y}^W \hat{Q}_{x,y}^W \leq E_{x,y}^W Q_{x,y}^W - \frac{F(N_{x,y}^W \hat{E}_{x,y}^W \hat{Q}_{x,y}^W, \varepsilon^{3/2})}{N_{x,y}^W}, \end{aligned} \tag{8}$$

where $N_{x,y}^W$ being the number of pulses in the $W$ basis, with the intensities of $x$ and $y$ sent by Alice and Bob, respectively. Besides, $Q_{x,y}^W$ and $E_{x,y}^W Q_{x,y}^W$ are system gain and QBER when Alice and Bob use intensities $x$ and $y$, respectively.

Finally, the formula of the key generation rate is given by

$$R \geq q\left\{-f Q_\mu^Z H\left(E_\mu^Z\right) + Y_1^{Z,L} P_\mu(1)\left[1 - H\left(e_1^{pZ,U}\right)\right]\right\}, \tag{9}$$

where $q$ ($:= P_\mu P_{Z|\mu} P_Z$) is the raw data sift factor, $f$ is the bidirectional error correction efficiency, $H(x)$ is the binary Shannon information function.

According to the formulas above, we can do numerical simulations between the key rate and security parameter. Here we reasonably set $\mu = 0.65$, $v = 0.06$, $P_\mu = 0.92$, $P_v = 0.07$, $P_{X|\mu} = 0.01$, $P_{X|v} = 0.81$, and $P_Z = 0.84$. The WCS is chosen as the light source and the specific experimental parameters used in our simulation are listed in Table 1.

As we can see from Fig. 1(a), the key generation rate $R$ depends on the security parameter $\varepsilon$. When the number of pulses is sufficiently large, we can increase the security of the system appropriately and obtain a considerably high key rate. If the number of pulses $N \leq 10^8$, there is a limit in reducing $\varepsilon$. Consequently, we cannot obtain a secure key when the security parameter is smaller than the limit. Furthermore, the value of $\varepsilon$ cannot be set to 1, which means that the key rate obtained is

not secure at all. On the other hand, the transmission loss can influence the final key rate greatly. In Fig. 1(b), we calculate the key rate at the distance of 50 km with different number of pulses and the limit between the key rate and security parameter is still hold. Owing to the transmission loss, the key rate cannot be obtained if $\varepsilon < 10^{-43}$ when the number of pulses $N = 10^9$. However, if $N \geq 10^{10}$ we can appropriately enhance the security parameter and achieve a high key rate.

**Table 1.** List of practical parameters for simulations in BB84. $\eta_{\rm d}$ and $Y_0$ are the detection efficiency and dark count rate of detectors. $e_{\rm d}$ is the misalignment error rate. $e_0$ is the error rate of a vacuum pulse. $\alpha$ is the transmission fiber loss constant. $f$ is the error correction efficiency.

| $\eta_{\rm d}$ (%) | $Y_0$ | $e_{\rm d}$ (%) | $e_0$ | $\alpha$ (dB/km) | $f$ |
|---|---|---|---|---|---|
| 14.5 | $3\times10^{-6}$ | 1.5 | 0.5 | 0.2 | 1.16 |

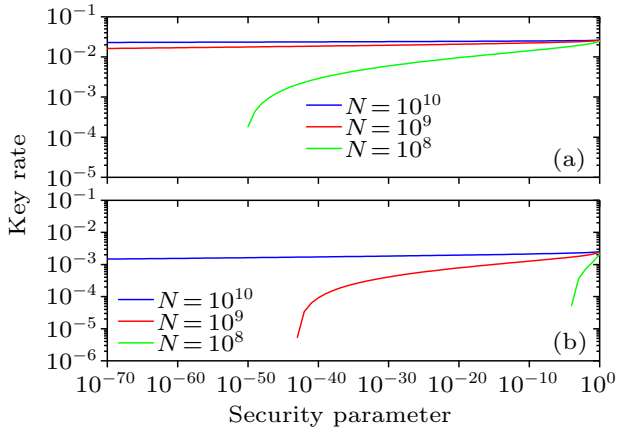



**Fig. 1.** Key generation rate of BB84 protocol versus security parameter with different number of pulses at the distance of 0 km (a) and 50 km (b).

## 3. MDI-QKD

The measurement-device-independent quantum key distribution (MDI-QKD) can remove all the side-channel attacks and obtain a higher transmission distance. In recent years, the decoy-state MDI-QKD has been extensively studied both theoretically and experimentally. In MDI-QKD, Alice and Bob respectively send their pulses to the untrusted third party, Charlie, which can be controlled by the eavesdropper. Upon receiving, Charlie does Bell-state projection measurement on the pulse pairs and records the measurement results. After finishing all the signal transmission, Charlie announces his detection results through a certified channel. According to Charlie's announcement, Alice and Bob do the bit flip and obtain the sifted keys.

In three-intensity decoy-state MDI-QKD, where Alice and Bob send pulses with intensity $l$ ($l \in \{o,v,\mu\}$), the corresponding average counting rate ($Q_{lr}$) and the average quantum-bit error-rate ($E_{lr}$) can be expressed as

$$Q_{lr}^{W} = \sum_{n,m=0}^{\infty} P_n^l P_m^r Y_{nm}^{W}, \tag{10}$$

$$E_{lr}^{W} Q_{lr}^{W} = \sum_{n,m=0}^{\infty} P_n^l P_m^r e_{nm}^{W} Y_{nm}^{W}, \tag{11}$$

where $W$ denotes the $X$ or the $Z$ basis and can be omitted without causing any confusion. $Y_{nm}$ and $e_{nm}$ represent the yield and the error-rate given that Alice sends an $n$-photon state and Bob sends an $m$-photon state, respectively.

According to the observed values above, we can obtain the lower bound of the counting rate for single-photon-pair pulses in $W$ basis

$$Y_{11}^{W} \geq Y_{11}^{W,L} = \frac{P_1^{\mu} P_2^{\mu} (Q_{vv}^{W} - \widetilde{Q}_{oo}) - P_1^{v} P_2^{v} (Q_{\mu\mu}^{W} - \widehat{Q}_{oo})}{P_1^{\mu} P_1^{v} (P_1^{v} P_2^{\mu} - P_1^{\mu} P_2^{v})}, \tag{12}$$

where $\widetilde{Q}_{oo} = Q_{vo} + Q_{ov} - Q_{oo}$ and $\widehat{Q}_{oo} = Q_{\mu o} + Q_{o\mu} - Q_{oo}$.

Similarly, we can deduce the upper bound of the QBER for single-photon state in the $X$ basis

$$e_{11}^{X} \leq e_{11}^{X,U} = \frac{E_{\mu\mu}^{X} Q_{\mu\mu}^{X} - E_{\mu o}^{X} Q_{\mu o}^{X} - E_{o\mu}^{X} Q_{o\mu}^{X} + E_{oo}^{X} Q_{oo}^{X}}{(P_1^{\mu})^2 Y_{11}^{X}}. \tag{13}$$

In practical situation, we also need to take statistical fluctuation into consideration for the observed value in Eqs. (12) and (13). Finally, the key generation rate is given by

$$R \geq (P_\mu)^2 (P_{Z|\mu})^2 \times \left\{ (P_1^{\mu})^2 Y_{11}^{Z,L} \left[ 1 - H\left( e_{11}^{X,U} \right) \right] - Q_{\mu\mu}^{Z} f H\left( E_{\mu\mu}^{Z} \right) \right\}. \tag{14}$$

Next, we also do numerical simulations for the key rate and security parameter. Here we reasonably set $\mu = 0.5$, $v = 0.1$, $P_\mu = 0.5$, $P_v = 0.3$, $P_{X|\mu} = 0.5$, and $P_{X|v} = 0.7$. The specific parameters used in simulation are listed in Table 2.

From Fig. 2(a), we can see that the key rate $R$ depends on security parameter $\varepsilon$ as well in MDI-QKD. When the number of pulses is larger than $10^{12}$, we can increase the security at the expense of slight influence of key rate. If the number of pulses is not sufficiently large, there is a visible key rate limit with the reducing of $\varepsilon$. For example, the secure key can not be generated if the security parameter is smaller than $10^{-42}$ with $10^{11}$ pulses. In Fig. 2(b), we also calculate the key rate at the distance of 30 km with different number of pulses. Due to the transmission loss, the key rate declines obviously with the decrease of the security parameter $\varepsilon$. Therefore, if someone needs to obtain a high secure key, the number of pulses should larger than $10^{11}$.

**Table 2.** List of practical parameters for simulations in MDI-QKD. $\eta_{\rm d}$ and $Y_0$ are the detection efficiency and dark count rate of detectors. $e_{\rm d}$ is the misalignment error rate. $e_0$ is the error rate of a vacuum pulse. $\alpha$ is the transmission fiber loss constant. $f$ is the error correction efficiency.

| $\eta_{\rm d}$ (%) | $Y_0$ | $e_{\rm d}$ (%) | $e_0$ | $\alpha$ (dB/km) | $f$ |
|---|---|---|---|---|---|
| 14.5 | $6.02\times10^{-6}$ | 1.5% | 0.5 | 0.2 | 1.16 |

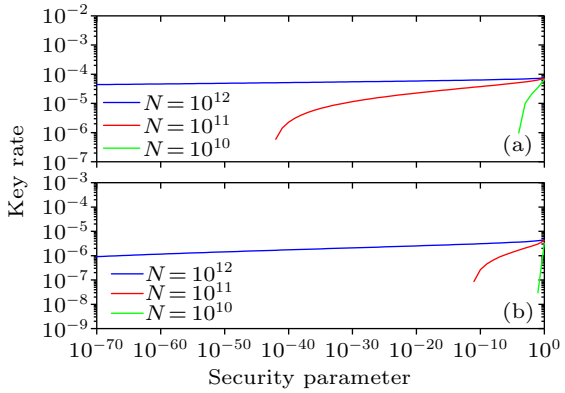



**Fig. 2.** Key generation rate versus security parameter with different number of pulses for the MDI-QKD at the distance of 0 km (a) and 30 km (b).

## 4. Sending-or-not TF-QKD

In BB84 or MDI-QKD protocols, the key generation rates are linear dependent on the channel loss which results in a limited secure transmission distance. Recently, Lucamarini *et al.* proposed a novel twin-field QKD (TF-QKD) which can break through the limit without quantum repeater.[10] After that, many interesting variants were proposed. Among those variants, Wang *et al.* proposed a sending-or-not TF-QKD protocol[12] which can tolerate the largest misalignment errors and make up the loophole of original TF-QKD. Below, we briefly describe the process of the sending-or-not TF-QKD protocol.

(i) Firstly, before signal transmission, Alice and Bob send out a strong reference light to the untrusted third party, Charlie, for the phase compensation.

(ii) For each time window, Alice or Bob randomly chooses a signal window ($Z$-window) or decoy window ($X$-window) with probabilities of $P_Z$ and $1-P_Z$. In $Z$-window, Alice (Bob) sends out a signal pulse with intensity of $\mu$ to Charlie with a probability of $\kappa$ and not to send with $1-\kappa$. For the $X$-window, Alice (Bob) sends out a decoy pulse with intensity of $l$ ($r$) ($l,r\in\{o,w,v\}$) to Charlie with a random phase shift $\delta_{\rm A}$ ($\delta_{\rm B}$). It should be noted that the phases $\delta_{\rm A}$ and $\delta_{\rm B}$ need to satisfy

$$|\delta_{\rm A}-\delta_{\rm B}-m\pi|\leq\frac{2\pi}{M}, \tag{15}$$

where $m\in\{0,1\}$ and $M$ denotes the total number of phase slices pre-chosen by Alice and Bob.

(iii) Upon receiving, Charlie does the twin-field measurements on the pulses and records all the measurement results.

(iv) According to Charlie's measurement outcomes, Alice and Bob announce whether it is a $Z$-window or an $X$-window. For the $X$-window, the users also need to announce the detailed phase values $\delta_{\rm A}$ and $\delta_{\rm B}$.

(v) The bits obtained in $X$ basis are used for parameter estimations and the bits in $Z$ basis are employed for distilling the final secure keys.

According to Refs. [21–23], we can obtain the average gain and QBER in $X$-window

$$Q_{lr}=\frac{M^2}{4\pi^2}\int_{\delta_0}^{\frac{2\pi}{M}+\delta_0}\int_0^{\frac{2\pi}{M}}Q_{lr}^{\delta_{\rm a}\delta_{\rm b}}\,{\rm d}\delta_{\rm a}\,{\rm d}\delta_{\rm b}, \tag{16}$$

$$Q_{lr}E_{lr}=\frac{M^2}{4\pi^2}\int_{\delta_0}^{\frac{2\pi}{M}+\delta_0}\int_0^{\frac{2\pi}{M}}Q_{lr}^{\delta_{\rm a}\delta_{\rm b}}E_{lr}^{\delta_{\rm a}\delta_{\rm b}}\,{\rm d}\delta_{\rm a}\,{\rm d}\delta_{\rm b}, \tag{17}$$

where $\delta_0=\arccos(1-2e_{\rm opt})$ and $e_{\rm opt}$ represents the optical misalignment error. Furthermore, the $Q_{lr}^{\delta_{\rm a}\delta_{\rm b}}$ and $E_{lr}^{\delta_{\rm a}\delta_{\rm b}}Q_{lr}^{\delta_{\rm a}\delta_{\rm b}}$ can be given by

$$\begin{aligned}Q_{lr}^{\delta_{\rm a}\delta_{\rm b}}=&(1-P_{\rm d})\,{\rm e}^{-\frac{l\eta}{2}-\frac{r\eta}{2}}\Big({\rm e}^{-\cos(\delta_{\rm a}-\delta_{\rm b})\sqrt{lr\eta^2}}\\&+{\rm e}^{\cos(\delta_{\rm a}-\delta_{\rm b})\sqrt{lr\eta^2}}\Big)-2(1-P_{\rm d})^2\,{\rm e}^{-(l+r)\eta},\end{aligned} \tag{18}$$

$$\begin{aligned}E_{lr}^{\delta_{\rm a}\delta_{\rm b}}Q_{lr}^{\delta_{\rm a}\delta_{\rm b}}=&(1-P_{\rm d})\,{\rm e}^{-\frac{l\eta}{2}-\frac{r\eta}{2}-\cos(\delta_{\rm a}-\delta_{\rm b})\sqrt{lr\eta^2}}\\&-(1-P_{\rm d})^2\,{\rm e}^{-(l+r)\eta},\end{aligned} \tag{19}$$

here $\eta=10^{\frac{-\alpha L/2}{10}}$ and $P_{\rm d}$ is the dark count rate.

Through the formulas above, we can estimate the single-photon yield and the error rate

$$Y_1\geq Y_1^L=\frac{P_2^{2v}Q_{ww}-P_2^{2w}Q_{vv}+(P_2^{2w}P_0^{2v}-P_2^{2v}P_0^{2w})Y_0}{P_2^{2v}P_1^{2w}-P_2^{2w}P_1^{2v}}, \tag{20}$$

$$e_1\leq e_1^U=\frac{Q_{ww}E_{ww}-P_0^{2w}e_0Y_0}{P_1^{2w}Y_1}, \tag{21}$$

where $P_2^{2v}$ is the photon number distribution when Alice and Bob send two photon pulses $v$ at the same time. Similarly, the $P_2^{2w},P_0^{2v}$, and $P_0^{2w}$ represent the distribution of the number of photons sent by the communicating parts with different numbers and intensities of photons.

In addition, the average gain and QBER in $Z$-window can be given by

$$\begin{aligned}Q_{\mu\mu}=&\,2P_{\rm d}(1-P_{\rm d})(1-\kappa)^2+4(1-P_{\rm d})\,{\rm e}^{-\frac{\mu\eta}{2}}\\&\times\left[1-(1-P_{\rm d})\,{\rm e}^{-\frac{\mu\eta}{2}}\right]\kappa(1-\kappa)\\&+2(1-P_{\rm d})\,{\rm e}^{-\mu\eta}\left[1-(1-P_{\rm d})\,{\rm e}^{-\mu\eta}\right]\kappa^2,\end{aligned} \tag{22}$$

$$\begin{aligned}E_{\mu\mu}Q_{\mu\mu}=&\,2P_{\rm d}(1-P_{\rm d})(1-\kappa)^2\\&+2(1-P_{\rm d})\,{\rm e}^{-\mu\eta}\left[1-(1-P_{\rm d})\,{\rm e}^{-\mu\eta}\right]\kappa^2.\end{aligned} \tag{23}$$

Similarly, we also need to take statistical fluctuation into consideration for the observed values in Eqs. (20) and (21). Finally, the key generation rate can be expressed as

$$R\geq(P_Z)^2\{2\kappa(1-\kappa)\mu\,{\rm e}^{-\mu}Y_1^L[1-H(e_1^U)]-Q_{\mu\mu}fH(E_{\mu\mu})\}. \tag{24}$$

Next, we do simulation for the key rate and security parameter in sending-or-not TF-QKD. Here we set $\mu=0.7$, $v=0.5$, $w=0.04$, $P_\mu=0.8$, $P_v=0.01$, $P_w=0.1$, and $\kappa=0.01$. The specific parameters used in simulation are listed in Table 3.

**Table 3.** List of practical parameters for simulations in sending-or-not TF-QKD. $\eta_d$ and $P_d$ are the detection efficiency and dark count rate of detectors. $e_{opt}$ is the optical misalignment error. $e_0$ is the error rate of a vacuum pulse. $\alpha$ is the transmission fiber loss constant. $f$ is the error correction efficiency. $M$ is the number of phase slices.

| $\eta_d$ (%) | $P_d$ | $e_{opt}$ (%) | $e_0$ | $\alpha$ (dB/km) | $f$ | $M$ |
|---|---|---|---|---|---|---|
| 50 | $10\times10^{-10}$ | 15 | 0.5 | 0.2 | 1.1 | 16 |

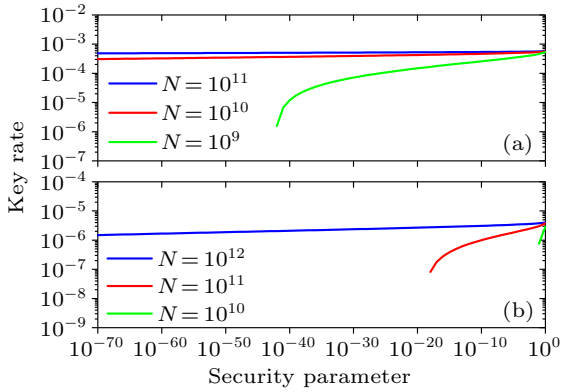



**Fig. 3.** Key generation rate versus security parameter with different number of pulses for the sending-or-not TF-QKD at the distance of 0 km (a) and 200 km (b).

As we can see in Fig. 3(a), the key generation rate depends on security parameter as well in sending-or-not TF-QKD. When the number of pulses is larger than $10^{10}$, we can obtain a considerable key rate with a high level security. However, if the number of pulses is smaller than $10^{10}$, there still exist sharp key rate decrease with the reducing of $\varepsilon$. Therefore, when the number of pulses is not large enough, we should reasonably choose the $\varepsilon$. In addition, we also calculate the key rate at the distance of 200 km with different number of pulses. Due to the transmission loss, the security parameter more obviously limits the key rate. Therefore, in this situation, if someone needs to obtain a considerable key rate with a high level security, the number of pulses should larger than $10^{11}$.

## 5. Conclusion

In summary, we have shown the relationship between the key generation rate and the security parameter when the finite-key length is taken into account. The conclusion has been illustrated by the simulations for three common QKD protocols. In practical QKD experiments, thus, we cannot freely set the value of the security parameter to obtain a considerable key rate or a high-level security. This work will provide a valuable reference for the choice of the security parameter in complicated power business applications QKD systems when the finite-key-size effect is taken into consideration. It is worth noting that the guessing probability[24] describes the probability that Eve can correctly guess the final keys and it is also related to the finite key length effect. Furthermore, the $\varepsilon_{sec}$, characterized by the trace distance inequality,[25] represents the protocol's security and contains the security parameter discussed in this work. How the two security targets influence the key rate will be studied in future works.

## Acknowledgment

Project supported by the Research on Key Technology and Equipment Development of Autonomous and Controllable Lightweight Endogenous Safety of Power Monitoring System (Grant No. 5108-202118056A-0-0-00).

## References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 1984, New York, pp. 175–179
[2] Lo H K and Chau H F 1999 *Science* **283** 2050
[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[4] Mayers D and Assoc J 2001 *Comput. Mach.* **48** 351
[5] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[6] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[7] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[8] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[9] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[10] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[11] Ma X F, Zeng P and Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[12] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[13] Ma X, Fung C H F and Razavi M 2012 *Phys. Rev. A* **86** 052305
[14] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 *Phys. Rev. A* **89** 022307
[15] Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2016 *Phys. Rev. A* **94** 032335
[16] Curty M, Xu F, Cui W, Lim C C W, Tamaki K and Lo H K 2014 *Nat. Commun.* **5** 3732
[17] Li H, Jiang H, Gao M, Ma Z, Ma C and Wang W 2015 *Phys. Rev. A* **92** 062344
[18] Yin H L and Chen Z B 2019 *Sci. Rep.* **9** 17113
[19] Fung C H F, Ma X and Chau H F 2010 *Phys. Rev. A* **81** 012318
[20] Yin H L, Zhou M G and Gu J 2020 *Sci. Rep.* **10** 14312
[21] Yin H L and Fu Y 2019 *Sci. Rep.* **9** 3045
[22] Zhang C H, Zhang C M and Wang Q 2019 *Opt. Lett.* **44** 1468
[23] Zhou X Y, Zhang C H, Zhang C M and Wang Q 2019 *Phys. Rev. A* **99** 062316
[24] Wang X B, Wang J T, Qin J Q, Jiang C and Yu Z W 2020 *NPJ Quantum Inform.* **6** 45
[25] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634