


# Finite-key analysis of practical time-bin high-dimensional quantum key distribution with afterpulse effect

Yu Zhou(周雨), Chun Zhou(周淳), Yang Wang(汪洋), Yi-Fei Lu(陆宜飞), Mu-Sheng Jiang(江木生), Xiao-Xu Zhang(张晓旭), and Wan-Su Bao(鲍皖苏)

**Citation:**Chin. Phys. B, 2022, 31 (**8**): 080303. DOI: 10.1088/1674-1056/ac6017
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Coherence migration in high-dimensional bipartite systems

Zhi-Yong Ding(丁智勇), Pan-Feng Zhou(周攀峰), Xiao-Gang Fan(范小刚),Cheng-Cheng Liu(刘程程), Juan He(何娟), and Liu Ye(叶柳)

Chin. Phys. B, 2022, 31 (**6**): 060308. DOI: 10.1088/1674-1056/ac48f8

## Probabilistic resumable quantum teleportation in high dimensions

Xiang Chen(陈想), Jin-Hua Zhang(张晋华), and Fu-Lin Zhang(张福林)

Chin. Phys. B, 2022, 31 (**3**): 030302. DOI: 10.1088/1674-1056/ac1efb

## Majorana stellar representation for mixed-spin (*s*, 1/2) systems

Yu-Guo Su(苏玉国), Fei Yao(姚飞), Hong-Bin Liang(梁宏宾), Yan-Ming Che(车彦明), Li-Bin Fu(傅立斌), and Xiao-Guang Wang(王晓光)

Chin. Phys. B, 2021, 30 (**3**): 030303. DOI: 10.1088/1674-1056/abc2bc

## New semi-quantum key agreement protocol based on high-dimensional single-particle states

Huan-Huan Li(李欢欢), Li-Hua Gong(龚黎华), and Nan-Run Zhou(周南润)

Chin. Phys. B, 2020, 29 (**11**): 110304. DOI: 10.1088/1674-1056/abaedd

## Attacking a high-dimensional quantum key distribution system with wavelength-dependent beam splitter

Ge-Hai Du(杜舸海), Hong-Wei Li(李宏伟), Yang Wang(汪洋), Wan-Su Bao(鲍皖苏)

Chin. Phys. B, 2019, 28 (**9**): 090301. DOI: 10.1088/1674-1056/ab343c

---

# Finite-key analysis of practical time-bin high-dimensional quantum key distribution with afterpulse effect

Yu Zhou(周雨)[1,2], Chun Zhou(周淳)[1,2,†], Yang Wang(汪洋)[1,2], Yi-Fei Lu(陆宜飞)[1,2], Mu-Sheng Jiang(江木生)[1,2], Xiao-Xu Zhang(张晓旭)[1,2], and Wan-Su Bao(鲍皖苏)[1,2,‡]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou* 450001, *China*

[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 27 January 2022; revised manuscript received 18 March 2022; accepted manuscript online 23 March 2022)

High-dimensional quantum resources provide the ability to encode several bits of information on a single photon, which can particularly increase the secret key rate rate of quantum key distribution (QKD) systems. Recently, a practical four-dimensional QKD scheme based on time-bin quantum photonic state, only with two single-photon avalanche detectors as measurement setup, has been proven to have a superior performance than the qubit-based one. In this paper, we extend the results to our proposed eight-dimensional scheme. Then, we consider two main practical factors to improve its secret key bound. Concretely, we take the afterpulse effect into account and apply a finite-key analysis with the intensity fluctuations. Our secret bounds give consideration to both the intensity fluctuations and the afterpulse effect for the high-dimensional QKD systems. Numerical simulations show the bound of eight-dimensional QKD scheme is more robust to the intensity fluctuations but more sensitive to the afterpulse effect than the four-dimensional one.

**Keywords:** high-dimensional, time-bin, finite-key analysis, intensity fluctuations, afterpulse effect

**PACS:** 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/ac6017

## 1. Introduction

The unpredictable development of quantum computation undoubtedly threatens the security of classical cryptographic systems. Alternative cryptosystems must be found to safely transmit sensitive data and confidential information under serious threat of quantum computer. Quantum key distribution (QKD) is an efficient and reliable technique to resist high-performance computing attacks. It enables two legitimate parties, Alice and Bob, to share common secret key under the interference of noise and eavesdropper (Eve).[1] Basic principles of quantum mechanics including measurement-collapse theory, the Heisenberg uncertainty principle and quantum no-cloning theorem guarantee the unconditional security of QKD.[2] In recent years, the experiment of QKD has developed rapidly and made a lot of progress. The world's first quantum satellite "Mozi" was launched in 2016[3] and a 2000-km quantum link from Beijing to Shanghai was built in 2017,[4] which initially formed a prototype of the space-ground integration quantum network. The measurement-device-independent network scheme was also proposed to connect untrusted node networks.[5] In addition, the latest experimental quantum key distribution system can reach a safe distance of 833.8 kilometers,[6] which is a breakthrough in building quantum network. However, the secret key rate of engineering prototype of QKD systems is still low. How to promote the key rate and broaden the application fields of QKD public issues requiring urgent solutions. Hardware constraints of QKD systems such as optical state generation speed, photon-counting rates and detecting dead time limit the key rate. Besides, a large fraction of photons is lost in the quantum channel due to optical absorption and scattering. Such physical and practical limitations drive researchers to seek new QKD protocols that can outperform two-dimensional protocols in both secure key rate and distance. Recent years, several high-dimensional QKD (HD-QKD) schemes has been proposed.[7–10] Photonic degrees of freedom such as position–momentum,[11] time–energy,[12] and orbital angular momentum[13,14] are proven to have a high-dimensional information loading capability, which can immensely improve the secret key rate of QKD. Generally, QKD systems using high-dimensional qudits have several superiorities than the ones using classical two-dimensional qubits. Firstly, they can effectively increase the secret key rate. $n = \log_2(d)$ bits of information can be safely encoded on each single photon in HD-QKD systems.[15] Secondly, HD-QKD systems have higher resistance to quantum channel noise, which means they can tolerate a higher quantum bit error rate.[16] An attractive implementation has been proposed and its security analysis was given based on entropic uncertainty relations by Islam *et al.*[17] They use temporal and phase states to realize the $d$-dimensional protocol, in which temporal states are used to generate the key and phase states are used to guarantee the security of QKD system. The first challenge is how to prepare and measure the phase states under certain experimental resources. An equivalent protocol based on entanglement was proposed which simplifies the detector

[†]Corresponding author. E-mail: zc@qiclab.cn

[‡]Corresponding author. E-mail: bws@qiclab.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd 

requirements for measurement.[18] Lately, another alternative scheme for four-dimensional QKD with time-bin and phase encoding was presented[19] with a simplified and compact detecting system, which presents an efficient performance than previous HD-QKD schemes and appears a broad prospects in future application.

However, the condition of its theoretical security can not be well satisfied in practical engineering conditions. Several quantum hacking attacks have been proposed by exploiting the imperfections of photoelectric devices.[22–29] Since the ideal single photon source is difficult to realize, the weak coherent-state (WCS) source is usually used in practical systems. The WCS source contains multiphoton part, which may be used by Eve through the photon-number-splitting (PNS) attack.[21] The decoy-state method[30–32] is one of means to tackle the multi-photon in WCS source. This method can estimate the counting rate and bit error of the single photon part of the WCS source, so as to estimate the secure key rate. Besides, the equipment defects of practical systems will lead to the leakage of information. The existing set-ups use the imperfect WCS source, and the intensity fluctuations[33,34] caused by intensity modulation is a nonnegligible imperfection. The avalanche photodiode single photon detectors (APD) have the nonnegligible afterpulse effect, which is created by former ignition avalanche and related to the avalanche duration time, hold-off time, lifetime of detrapping carriers. Several schemes that analyze the impact of afterpulse on QKD have also been proposed.[35–37]

Since the secret key rate in the practical protocol is limited, it is necessary to reconsider the security bound of the asymptotic region, and several methods based on finite-length key have been given.[38–40] These imperfections will lead to the correlation of detection results. Therefore, in the case of finite key and related random samples,[41] how to comprehensively take both the afterpulse and the intensity fluctuations into account in the security proof of high-dimensional schemes remains to be solved. Here, we limit the intensity fluctuations of the sources to a certain range by setting the intensity fluctuations parameters. We also introduce the afterpulse probabilities into the formula of secret key rate with different dimensions. Considering finite-length effects, we apply Azuma's inequality to tackle the statistical fluctuations of relevant random samples in the security bound.[42]

In this paper, we give the implementation process of the four-dimensional time-bin protocol and extend it to the eight-dimensional protocol in Section 2. Then we analyze the impact of the afterpulse effect and the intensity fluctuations on the secret key rate in practical protocols in Section 3. In addition, the simulations of key rates for the different afterpulse effect and intensity fluctuations in two schemes are provided in Section 4.

## 2. Protocol description

Firstly, we introduce the four-dimensional scheme based on time-phase states. The eight states of four-dimensional (4D) scheme and the experimental setup have been given in Ref. [19]. Time-bin qudits can be easily created by weak coherent pulses. Pulses in different time slots form the different bases and the superposition among these pulses is devised by controlling the relative phase of the pulses. The analysis of one-decoy protocol has been given and it has been proved that the one-decoy protocol has better performance in the practical protocol.[20] Let the choesn probabilities of $Z$ and $X$ bases are $p_Z$ and $p_X$ respectively. The secret key is extracted only when two parties both select $Z$ basis, while the information leakage is estimated from the events when two parties both select $X$ basis. The specific protocol process is shown below.

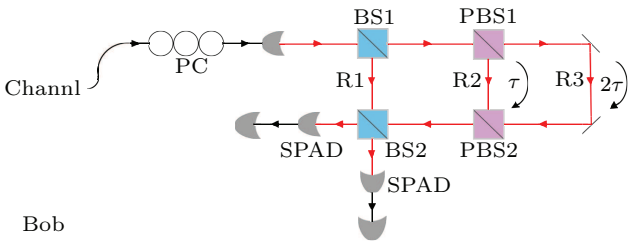



**Fig. 1.** Experimental setup for measurement.[19] PC: polarization controller; BS: beam splitter; PBS: polarizing beam splitter. After the qudit is polarized, it interfered at BS2. The delay ($\tau$ or $2\tau$) of the interference depends on the polarization. The specific interference results are shown in Fig. 2.

(i) Preparation

Alice selects $Z(X)$ basis with probability $p_Z^{\text{Alice}}$ ($p_X^{\text{Alice}}$). She modulates the intensity $k \in \{\mu_1, \mu_2\}$ through intensity modulator with probabilities $p_{\mu_1}, p_{\mu_2}$ respectively, where $\mu_1$ is the signal setting and $\mu_2$ is the decoy setting. The eigenstates of $Z$ basis are denoted by $|t_n\rangle\,(n = 0,1,2,3)$ and $|f_n\rangle$ $(n = 0,1,2,3)$ for $X$ basis. Each eigenstate is represented by two photonic wave packets within a frame of four contiguous time bins. We employ intensity modulators and phase modulator to control the relative interval and phase of the two photonic wave packets respectively. Then, Alice sends her phase-randomized weak laser pulses to Bob.

(ii) Measurement

Bob uses polarization controller (PC) and polarizing beam splitter (PBS) to realize the selection of basis $Z(X)$ with probabilitiy $p_Z^{\text{Bob}}(p_X^{\text{Bob}})$. He firstly applies polarizations to states by PC, then the polarized states will be divide by PBS to realize the basis selection (see Fig. 1). Bob applies $\tau$ and $2\tau$ delays to the states under $Z$ basis and $X$ basis, respectively. States interfere at the second beam splitter (BS) and both outputs of the interferometer are monitored by two single-photon avalanche detectors (SPADs). The interference of states can be observed in the second and fourth time bins for the $Z$-basis measurements (see Fig. 2), and in the third and fourth time bins for the $X$-basis measurements.

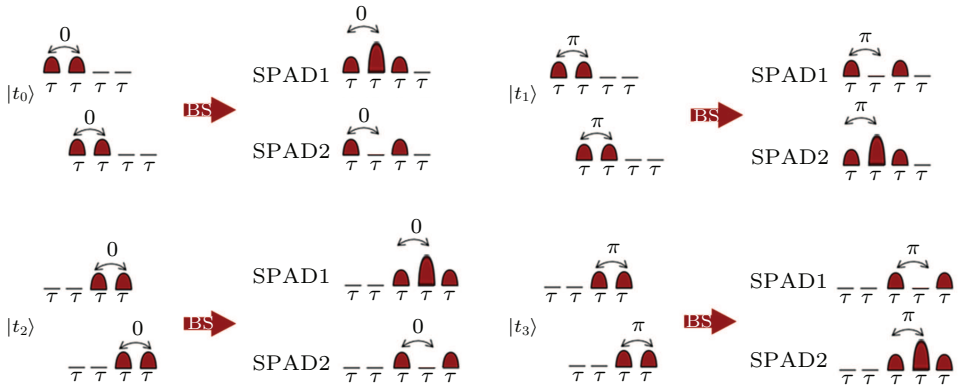



**Fig. 2.** $\tau$ is the time-bin duration. Alice and Bob both select $Z$ basis and here is the interference of the four states respectively. We can distinguish the four states by the response of detectors and the arrival time. For example, the SPAD 1 responds in the second time slot, we believe that the state received by Bob at this time is $|t_1\rangle$.

(iii) Basis reconciliation

Alice and Bob announce their bases and intensity choices over an authenticated public channel. Then they record the number of the detected pulses under $k$ intensity when they choose the same basis, where $n_{Z,k}$ and $n_{X,k}$ correspond to the $Z$ basis and the $X$ basis, respectively.[41]

(iv) Parameter estimation

Alice and Bob calculate the bit errors $m_{X,k}$ for intensity $k$ when they both choose the $X$ basis. Then they calculate the lower bound of single-photon events $s_{Z,1}$, $s_{X,1}$, the lower bound of vacuum photon events $s_{Z,0}$ and the upper bound of the errors $c_{Z,1}$ for the single-photon events in the $Z$ basis. If the phase error rate $\phi = c_{Z,1}/s_{Z,1}$ is lower than the predetermined phase error rate $\bar{\phi}$, Alice and Bob accept the the raw key and perform post-processing, or they abandon the protocol.

(v) Postprocessing

Alice and Bob carry out the error correction, which consumes at most $\text{Leak}_{\text{EC}}$ bits. Then they carry out the error verification and privacy amplification to obtain the secret key length $\ell$.

The protocol can be extended to higher level. We realize the protocol expansion from four-dimension to eight-dimension without adding detectors and other devices and here are the eight qudits of $Z$ basis (see Fig. 3). In the preparation, we expand two photonic wave packets within a frame of four contiguous time bins to four photonic wave packets within a frame of eight contiguous time bins, and two sets of random numbers are required to edit the phases of adjacent photonic wave packets. In order to ensure that the eight qudits are perfectly orthogonal, we assume that the ratio of time-bin duration to pulse width is greater than 7.7[43] and we neglect the problem of time jitter in this situation. Also, the time-bin duration should be adjusted to ensure that the dead time of the SPADs is shorter than the time slot between two peaks.[44] realizes the minimum dead time of avalanche photodiode of 12.4 ns, so we can set the minimum dead time as the duration between two peaks ideally. Therefore, the minimum duration of each qudit can reach approximately 24.8 ns. Here, we have analyzed the scheme that the qudit have 6 or 7 time bins. When there are 6 or 7 time bins per qudit, it is possible for the eight states belonging to any basis orthogonal to each other. However, it cannot satisfy the condition that the two bases are mutually unbiased. Therefore, we coding the qudits in eight contiguous time bins.

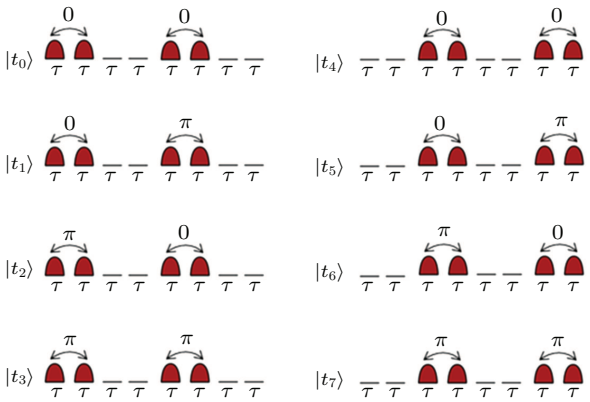



**Fig. 3.** The eight states of $Z$ basis belonging to the eight-dimensional (8D) protocol, 0 and $\pi$ specify the relative phase between the different time bins occupied by the photon. When two SPADs response twice in total, we can distinguish the current state according to the response of the two detectors and the arrival time of clicks. The specific process is similar to the four-dimensional protocol.

**Table 1.** The method of distinguishing eight signal states in measurement.

| States | Detectors | Clicks |
|---|---|---|
| $\|t_0\rangle$ | SPAD1 | 2nd time bin and 6th time bin |
| | SPAD2 | none |
| $\|t_1\rangle$ | SPAD1 | 2nd time bin |
| | SPAD2 | 6th time bin |
| $\|t_2\rangle$ | SPAD1 | 6th time bin |
| | SPAD2 | 2nd time bin |
| $\|t_3\rangle$ | SPAD1 | none |
| | SPAD2 | 2nd time bin and 6th time bin |
| $\|t_4\rangle$ | SPAD1 | 4th time bin and 8th time bin |
| | SPAD2 | none |
| $\|t_5\rangle$ | SPAD1 | 4th time bin |
| | SPAD2 | 8th time bin |
| $\|t_6\rangle$ | SPAD1 | 8th time bin |
| | SPAD2 | 4th time bin |
| $\|t_7\rangle$ | SPAD1 | none |
| | SPAD2 | 4th time bin and 8th time bin |

In the measurement, we distinguish the eight states by the response of the two detectors and arrival time of the clicks (see Table 1).

## 3. Security analyses

The security analysis is based on the composable security definition, we say our protocol is $\varepsilon$-secure means $\varepsilon_{\rm sec}+\varepsilon_{\rm cor}\leq\varepsilon$, where $\varepsilon_{\rm cor}$ is the correctness parameter and $\varepsilon_{\rm sec}$ is the secrecy parameter.[45] The length of secret key per privacy amplification block in the $Z$ basis can be given by[17]

$$\begin{aligned}\ell_{\rm 4D} \leq\ & 2s^{\rm L}_{Z,0}+s^{\rm L}_{Z,1}[c-H(\phi^{\rm U}_Z)]-{\rm Leak}_{\rm EC}\\ & -6\log_2(19/\varepsilon_{\rm sec})-2\log_2(2/\varepsilon_{\rm cor}),\end{aligned}\tag{1}$$

where $s^{\rm L}_{Z,0}, s^{\rm L}_{Z,1}$ are the lower bound of the vacuum events and the single-photon events, $\phi^{\rm U}_Z$ is the upper bound of the phase error rate, ${\rm Leak}_{\rm EC}$ is the number of bits consumed in error correction. $H(x)=-x\log_2(x/3)-(1-x)\log_2(1-x)$ is the Shannon entropy in a 4D Hilbert space. Since the two bases are ideally mutually unbiased, $c=2$.

In 8D scheme, the secret key per privacy amplification block in the $Z$ basis can be inferred by

$$\begin{aligned}\ell_{\rm 8D} \leq\ & 3s^{\rm L}_{Z,0}+s^{\rm L}_{Z,1}[c-H(\phi^{\rm U}_Z)]-{\rm Leak}_{\rm EC}\\ & -6\log_2(19/\varepsilon_{\rm sec})-2\log_2(2/\varepsilon_{\rm cor}),\end{aligned}\tag{2}$$

where $H(x)=-x\log_2(x/7)-(1-x)\log_2(1-x)$ is the Shannon entropy in an 8D Hilbert space and $c=3$ in the ideal case. Each afterpulse in the 8D scheme will bring 87.5% error bit.

Let $s_{Z,n}$ is the number of detections observed by Bob when Alice sent n-photon states in the $Z$ basis and $\sum_{n=0}^{\infty} s_{Z,n}=n_Z$. In the asymptotic limit, for the intensity $k$, we have

$$n^*_{Z,k}=\sum_0^\infty p_{k|n}s_{Z,n}, {\rm k}\in\{\mu_1,\mu_2\},\tag{3}$$

where $n^*_{Z,k}$ is the expected value of $n_{Z,k}$. The $p_{k|n}$ is the conditional probability of choosing the intensity $k$ when Alice sent an $n$-photon states,

$$p_{k|n}=\frac{p_k}{\tau_n}p_{n|k}=\frac{p_k}{\tau_n}\frac{{\rm e}^{-k}k^n}{n!},\tag{4}$$

where $\tau_n=\sum p_k\,{\rm e}^{-k}k^n/n!$ is the probability that Alice prepares an $n$-photon state.

We also take the afterpulse effect of SPADs into consideration. When the afterpulse effect is not considered, the loss of quantum channel is determined by loss coefficient $a$ and fiber length $l$. Let $\eta_{\rm c}=10^{-al/10}$ is channel transmission efficiency. The detection efficiency of $n$ photons can be expressed as $\eta_n=1-(1-\eta_{\rm c})^n$. The rate of $n$-photon detection can be expressed as $Y_n=Y_0+\eta_n$, where $Y_0$ is the background counting rate. The count rate $Q_\mu$ can be expressed as

$$Q_\mu=\sum_{n=0}^{\infty}Y_n\frac{\mu^n}{n!}{\rm e}^{-\mu}=Y_0+1-{\rm e}^{-\mu\eta_{\rm c}}.\tag{5}$$

The error rate of the $n$-photon states and the overall quantum bit error rate (QBER) is given by[46]

$$e_n=\frac{e_0Y_0+e_{\rm d}\eta_n}{Y_n},\tag{6}$$

$$E_\mu=\frac{e_{\rm d}(1-{\rm e}^{-\mu\eta_{\rm c}})+e_0Y_0}{Q_\mu},\tag{7}$$

where $e_{\rm d}$ is the baseline system error rate, $e_0$ is the error rate of the background. We assume the $e_0$ of four-dimensional scheme to be random and $e_0=3/4$.

Then we consider the afterpulse effect. Considering the dead time of SPADs, not all afterpulse can be detected. Based on the previous work,[35] we propose another method to calculate the afterpulse probability. Let $p_i$ represent the probability that the next $i$-th gate triggers an avalanche after an avalanche trigger. Here, we no longer consider the high-order afterpulse, but directly counting the probability of generating clicks in a period of time after a trigger. Then, we can obtain the overall probability of the afterpulse

$$p_{\rm ap}=\frac{\sum_{i=1}^{\infty}p_i}{1-\sum_{i=1}^{\infty}p_i}Q_\mu,,\tag{8}$$

where $\sum_{i=1}^{\infty}p_i$ is the overall probability that the SPADs generate afterpulses in a period of time after a trigger.

Next, combined with the obtained the overall probability of the afterpulse, we can characterize the count rate $Q_\mu$ and the overall QBER $E_\mu$. Here, we assume that the triggers caused by the background count also cause the afterpulse, and it can be expressed as follows:

$$Q_\mu=(1-{\rm e}^{-\mu\eta_{\rm c}}+Y_0))(1+p_{\rm ap}),\tag{9}$$

$$E_\mu=\frac{e_0Y_0+(e'_{\rm d}+e_0p_{\rm ap})(1-{\rm e}^{-\eta_{\rm c}\mu})}{Q_\mu},\tag{10}$$

where $e'_{\rm d}$ is the baseline system error rate which does not include the afterpulse phenomenon.[37] In the numerical simulation, we can derive $n_{\alpha,k}$ and $n_{\alpha,k}$ ($\alpha\in\{Z,X\}$) by

$$n_{\alpha,k}=Np_kp^{\rm Alice}_\alpha p^{\rm Bob}_\alpha Q_{\alpha,k},\tag{11}$$

$$m_{\alpha,k}=Np_kp^{\rm Alice}_\alpha p^{\rm Bob}_\alpha E_{\alpha,k}Q_{\alpha,k},\tag{12}$$

where $p_k, p_\alpha, Q_{\alpha,k}, E_{\alpha,k}$ are the ratio of the states of intensity $k$, the selecting probability in the $\alpha$ basis, the gain of the intensity $k$ state in the $\alpha$ basis, and the QBER of the intensity $k$ state in the $\alpha$ basis, respectively.

In practical time-bin HD-QKD system, the imperfections of practical devices should be considered. The laser sources and the intensity modulators will bring the intensity fluctuations.[47,48] In this work, we take the intensity fluctuations $k\in\{\mu_1,\mu_2,\mu_3\}$ into account. Assuming that the intensity fluctuations of source is within a certain range and we can

introduce the parameter $\delta$ to characterize the intensity fluctuations with $\mu_i \in [\mu_i^-, \mu_i^+]$. The lower and upper bounds of $\mu_i$ can be expressed as $\mu_i^- = (1-\delta)\mu_i$ and $\mu_i^+ = (1+\delta)\mu_i$. Due to the intensity fluctuations, a certain detection event may be mutually related by prior detection events. According to the finite-key effect,[41] we establish a relationship between the asymptotic values and the observed statistics by Azuma's inequality.[42] For dependent random samples, applying the Azuma's inequality we have

$$|n^*_{Z,k} - n_{Z,k}| \leq \delta_{\mathrm{A}}(n_Z, \varepsilon_1) \tag{13}$$

with probability at least $1-2\varepsilon_1$, where $\delta_{\mathrm{A}}(x,y) = \sqrt{2x\ln(1/y)}$. The same relationship can also be made for the expected number of errors. Let $\nu_{Z,n}$ is the number of errors associated with $s_{Z,n}$ and $\sum_{n=0}^{\infty} \nu_{Z,n} = m_Z$. In the asymptotic limit, for the intensity $k$, we have

$$m^*_{Z,k} = \sum_{0}^{\infty} p_{k|n}\nu_{Z,n}, \quad k \in \{\mu_1, \mu_2\}, \tag{14}$$

where $m^*_{Z,k}$ is the expected value of $m_{Z,k}$. Using the Azuma's inequality we have

$$|m^*_{Z,k} - m_{Z,k}| \leq \delta_{\mathrm{A}}(m_Z, \varepsilon_2) \tag{15}$$

with probability at least $1-2\varepsilon_2$, where $\delta_{\mathrm{A}}(x,y) = \sqrt{2x\ln(1/y)}$. From the analysis above, we can estimate the upper bound and lower bound of $n_{Z,k}$ and $m_{X,k}$, as same as the $n_{X,k}$ and $m_{Z,k}$.

For one-decoy protocol, we can refer to Ref. [20]. According to the one-decoy protocol we can derive

$$s^{\mathrm{U}}_{Z,0} = \frac{1}{e_0}\left(\tau_0 \frac{\mathrm{e}^k}{p_k} m^{\mathrm{L}}_{Z,k} + \delta_{\mathrm{A}}(n_Z, \varepsilon_1)\right), \tag{16}$$

$$s^{\mathrm{U}}_{X,0} = \frac{1}{e_0}\left(\tau_0 \frac{\mathrm{e}^k}{p_k} m^{\mathrm{L}}_{X,k} + \delta_{\mathrm{A}}(n_X, \varepsilon_1)\right), \tag{17}$$

$$s^{\mathrm{L}}_{Z,0} = \frac{\tau_0}{\mu_1^+ - \mu_2^-}(\mu_1^- n^{\mathrm{L}}_{Z,\mu_2} - \mu_2^+ n^{\mathrm{U}}_{Z,\mu_1}), \tag{18}$$

$$s^{\mathrm{L}}_{Z,1} = \frac{\tau_1\mu_1^-}{\mu_2^+(\mu_1^+ - \mu_2^-)}\left(n^{\mathrm{L}}_{Z,\mu_2} - \frac{(\mu_2^+)^2}{(\mu_1^-)^2} n^{\mathrm{U}}_{Z,\mu_1} - \frac{((\mu_1^+)^2 - (\mu_2^-)^2)}{(\mu_1^-)^2}\frac{s^{\mathrm{U}}_{Z,0}}{\tau_0}\right), \tag{19}$$

$$s^{\mathrm{L}}_{X,1} = \frac{\tau_1\mu_1^-}{\mu_2^+(\mu_1^+ - \mu_2^-)}\left(n^{\mathrm{L}}_{X,\mu_2} - \frac{(\mu_2^+)^2}{(\mu_1^-)^2} n^{\mathrm{U}}_{X,\mu_1} - \frac{((\mu_1^+)^2 - (\mu_2^-)^2)}{(\mu_1^-)^2}\frac{s^{\mathrm{U}}_{X,0}}{\tau_0}\right), \tag{20}$$

$$\nu^{\mathrm{U}}_{X,1} = \frac{\tau_1}{(\mu_1^- - \mu_2^+)}(m^{\mathrm{U}}_{X,\mu_1} - m^{\mathrm{L}}_{X,\mu_2}). \tag{21}$$

$$\phi^{\mathrm{U}}_Z = \frac{\upsilon^{\mathrm{U}}_{X,1}}{s^{\mathrm{L}}_{X,1}} + \gamma\left(\varepsilon_{\mathrm{sec}}, \frac{\upsilon^{\mathrm{U}}_{X,1}}{s^{\mathrm{L}}_{X,1}}, s^{\mathrm{L}}_{X,1}, s^{\mathrm{L}}_{Z,1}\right), \tag{22}$$

where

$$\gamma(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cd\ln 2}\log_2\left(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2}\right)}.$$

By adding the Eq. (16)–(22) to Eq. (1) we can obtain the lower bound of secret key length $\ell_{4\mathrm{D}}$ of the two-decoy state protocol. This method can also be applied to the 8D protocol.

## 4. Simulation

In this section, the QKD schemes are tested over different channel lengths of standard single-mode fiber. In simulation, we traverse the $Z$ basis selection probabilities, the emission proportions of signal light and the intensities of signal (decoy) light to obtain a optimal secret key rate. The values of parameters are listed in Table 2.

**Table 2.** The parameters values of simulation. $N$ is the total number of pulses, $f_{\mathrm{e}}$ is the error-correction efficiency, $\varepsilon_{\mathrm{sec}}$ and $\varepsilon_{\mathrm{cor}}$ are the security parameters, $Y_0$ is the background counting rate, $e_{\mathrm{d}}$ is the misalignment-error probability.

| $N$ | $f_{\mathrm{a}}$ | $\varepsilon_{\mathrm{sec}}$ | $\varepsilon_{\mathrm{cor}}$ | $Y_0$ | $\eta_{\mathrm{B}}$ | $e_{\mathrm{d}}$ |
|---|---|---|---|---|---|---|
| $10^9$ | 1.16 | $10^{-9}$ | $10^{-15}$ | $10^{-8}$ | 0.1 | $10^{-2}$ |

For the case with the intensity fluctuations, we simulated the effect of the different intensity fluctuation parameters $\delta$ on the secure key rate of one-decoy protocol. The generation of key rate decreases evidently with the intensification of source intensity fluctuations. The secure key rate decreases sharply when the parameter exceeds 20%, and almost no key is generated when the parameter $\delta$ exceeds 25%. In practical QKD system, the afterpulse of detectors also affects the secure key rate. The afterpulse effect will lead to bit error, and each detected afterpulse in the 4D protocol will bring 75% error bit. The increase of afterpulse probability and transmission distance will directly lead to the increase of overall QBER in Eq. (10). And the longer the transmission distance, the more sensitive the QBER is to the afterpulse probability. Therefore, the afterpulse indirectly raise the upper bound of the phase error rate $\phi^{\mathrm{U}}_Z$ in Eq. (1). Figure 4 shows the curve of secure key rate with the different afterpulse probability. As shown in the figure that the maximum transmission distance decreases with the increase of the afterpulse probability. When the afterpulse probability reaches 3%, the key rate decreases rapidly, and the intense afterpulse of detectors will lead to a sharp reduction in key rate.

According to Fig. 5, the line represents the 4D scheme and the dotted line represents the 8D scheme, we provide the key rate curves of the two schemes under different parameters. The eight-dimensional scheme generates more secure keys under normal attenuation, the key rate of 8D scheme is at least 1.5 times higher than that of 4D scheme. However, in the case of extreme attenuation, the performance of 8D scheme is gradually inferior to that of 4D scheme. When we consider the two

parameters on the key rate, it will aggravate the decline of the key rate. As shown in Fig. 4, when only the afterpulse effect is considered in the 4D scheme, there will be a significant attenuation of the transmission distance when $p_{\text{ap}} = 3\%$. However, when the intensity fluctuations is considered at the same time, the tolerance for the afterpulse effect is greatly weakened and the sharp reduction occurs when $p_{\text{ap}} = 2\%$.

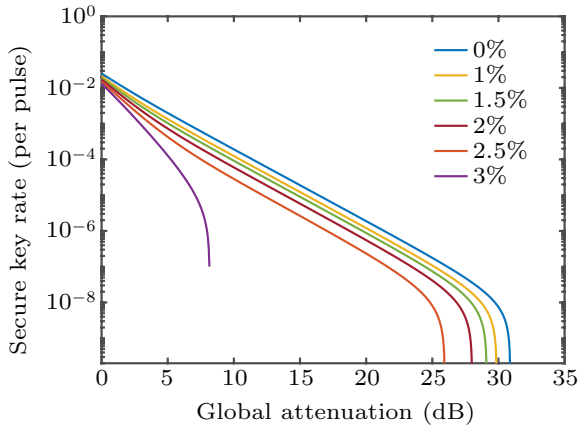



**Fig. 4.** Optimal secure key rate (per pulse) of one-decoy approach for different values of the afterpulse probability with no intensity fluctuations. The key rate and the longest transmission distance decrease sharply after the afterpulse probability exceeds 2.5%.

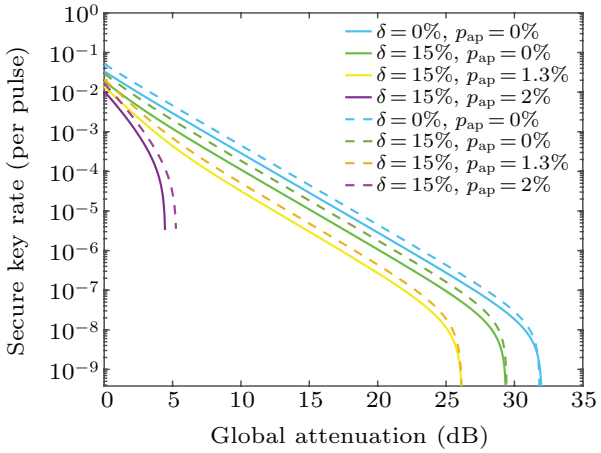



**Fig. 5.** The solid line represents the 4D scheme and the dotted line represents the eight-dimensional scheme, we provide the changes of the key rate curves of the two schemes under the strength fluctuations parameter $\delta = 0\%$, 15% and the afterpulse probability $p_{\text{ap}} = 0\%$, 1.3%, 2%.

In addition, we compare the effects of the intensity fluctuations and the afterpulse effect to schemes in different dimensions. We propose the ratios $\theta_{\text{int}}$ and $\theta_{\text{pap}}$ to characterize them, where $\theta_{\text{int}}$ is the ratio before and after considering the strength fluctuations and $\theta_{\text{pap}}$ is the ratio before and after considering the afterpulse effect (see Fig. 6). As can be seen from the figure, the key rate reduction of the 8D scheme before and after considering the strength fluctuations is obviously better than that of the 4D scheme, while 4D scheme performs better only considering the afterpulse effect. This is because the 8D scheme's error rate of the background $e_0$ is greater than the 4D ones. From Eq. (10), we know that the 8D scheme has greater overall QBER considering the afterpulse. The stronger the afterpulse effect, the greater the overall QBER, which increases the estimation of phase error rate $\phi_Z^{\text{U}}$. Therefore, the tolerance of 8D scheme to afterpulse effect is not as good as that of 4D scheme. In conclusion, the 8D protocol has stronger tolerance to the intensity fluctuations, but is more sensitive to the afterpulse.

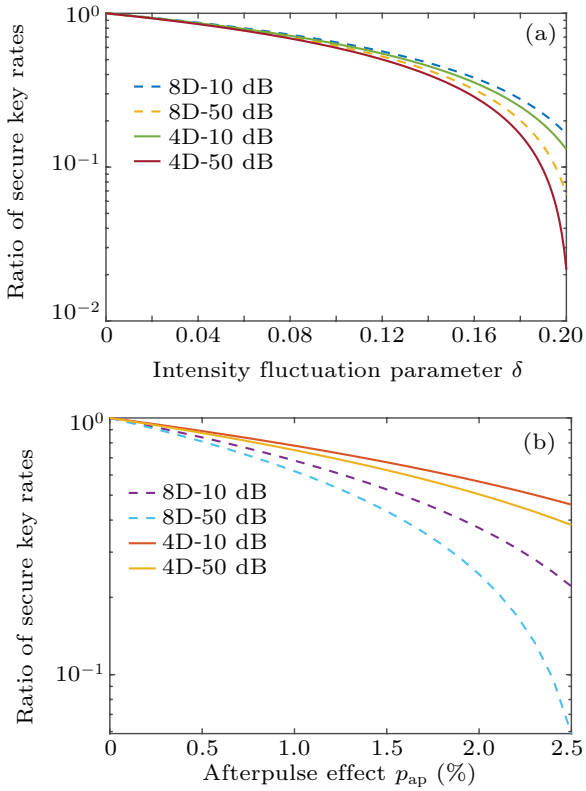



**Fig. 6.** The two ratios to characterize the effects of the intensity fluctuations and afterpulse. (a) Efficiency of the intensity fluctuations $\theta_{\text{int}}$, and $\delta$ is the fluctuations parameter. (b) Efficiency of the afterpulse $\theta_{\text{pap}}$, and $p_{\text{ap}}$ is the overall probability of the afterpulse.

## 5. Conclusion

For the practical HD-QKD, the flaws of source and detector restrict the key rate of practical high-dimensional protocols. In this paper, we extended the 4D time-bin protocol, and the effect of the intensity fluctuations and afterpulse have been mainly considered. We utilized parameters to limit the intensity and applied Azuma's inequality to establish the relationship between the expected and practical value. Besides, the afterpulse probability is introduced to quantify its effect to the generation of secure key rate. In numerical simulation, we simulated the effect of two flaws to schemes with different dimensions. It is found that both two flaws will reduce the key rate, but the 8D scheme is more sensitive to the afterpulse and has better robustness than the 4D scheme. Form the simulation, our results emphasized the significance of the stable source and high-performance detector in practical HD-QKD. In conclusion, we derived an analytical model to the variant practical time-bin QKD protocol considering the intensity fluctuations and the afterpulse effect. It provides a theoretical reference for secure analysis of practical high-dimensional protocols.

## Acknowledgements

Project supported by the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the National Natural Science Foundation of China (Grant Nos. 62101597, 61605248, 61675235, and 61505261), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan Province, China (Grant Nos. 202300410534 and 202300410532), and the Anhui Initiative Fund in Quantum Information Technologies.

## References

[1] Bennett C H and Brassard G 1984 *Theor. Comput. Sci.* **560** 7
[2] Lo H K and Chau H F 1999 *Science* **283** 2050
[3] Raska M 2016 *Nanyang Technological University RSIS* **223**
[4] Courtland R 2016 *IEEE Spectrum* **53** 11
[5] Fan-Yuan G J, Lu F Y, Wang S, Yin Z Q, He D Y, Zhou Z, Teng J, Chen W, Guo G C and Han Z F 2021 *Photon. Res.* **9** 1881
[6] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan-Yuan G J, Wang F X and Zhu Y G 2022 *Nat. Photon.* **16** 154
[7] Mower J, Zhang Z, Desjardins P, Lee C, Shapiro J H and Englund D 2013 *Phys. Rev. A* **87** 062322
[8] Mirhosseini M, Magana-Loaiza O S, O sullivan M N, Rodenburg B, Malik M, Lavery M P, Padgett M J, Gauthier D J and Boyd R W 2015 *New J. Phys.* **17** 033033
[9] Ding Y, Bacco D, Dalgaard K, Cai X, Zhou X, Rottwitt K and Oxenlowe L K 2017 *npj Quantum Information* **3** 1
[10] Sit A, Bouchard F, Fickler R, Gagnon-Bischoff J, Larocque H, Heshami K, Elser D, Peuntinger C, Gunthner K and Heim B 2017 *Optica* **4** 1006
[11] Zhang L, Silberhorn C and Walmsley I A 2008 *Phys. Rev. Lett.* **100** 110504
[12] Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737
[13] Mair A, Vaziri A, Weihs G and Zeilinger A 2001 *Nature* **412** 313
[14] Zhang Y, Roux F S, Konrad T, Agnew M, Leach J and Forbes A 2016 *Sci. Adv.* **2** e1501165
[15] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
[16] Erhard M, Krenn M and Zeilinger A 2020 *Nat. Rev. Phys.* **2** 365
[17] Islam N T, Cahall C, Aragoneses A, Lezama A, Kim J and Gauthier D J 2017 *Phys. Rev. Appl.* **7** 044010
[18] Islam N T, Lim C C W, Cahall C, Qi B, Kim J and Gauthier D J 2019 *Quantum Science and Technology* **4** 035008
[19] Vagniluca I, Da Lio B, Rusca D, Cozzolino D, Ding Y, Zbinden H, Zavatta A, Oxenlowe L K and Bacco D 2020 *Phys. Rev. Appl.* **14** 014051
[20] Rusca D, Boaron A, Grunenfelder F, Martin A and Zbinden H 2018 *Appl. Phys. Lett.* **112** 171104
[21] Brassard G, Lutkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[22] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
[23] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev. A* **74** 022313
[24] Lamas-Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388
[25] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
[26] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[27] Li H W, Wang S, Huang J Z, Chen W, Yin Z Q, Li F Y, Zhou Z, Liu D, Zhang Y, Guo G C, Bao W S and Han Z F 2011 *Phys. Rev. A* **84** 062308
[28] Bugge A N, Sauge S, Ghazali A M M, Skaar J, Lydersen L and Makarov V 2014 *Phys. Rev. Lett.* **112** 070503
[29] Huang A, Navarrete A, Sun S H, Chaiwongkhot P, Curty M and Makarov V 2019 *Phys. Rev. Appl.* **12** 064043
[30] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[31] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[32] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[33] Wang X B, Peng C Z, Zhang J, Yang L and Pan J W 2008 *Phys. Rev. A* **77** 042311
[34] Zhou C, Bao W and Fu X 2010 *Science China Information Sciences* **53** 2485
[35] Fan-Yuan G J, Wang C, Wang S, Yin Z Q, Liu H, Chen W, He D Y, Han Z F and Guo G C 2018 *Phys. Rev. Appl.* **10** 064032
[36] Fan-Yuan G J, Wang S, Yin Z Q, Chen W, He D Y, Guo G C and Han Z F 2020 *Quantum Engineering* **2** e56
[37] Papapanos C, Zavitsanos D, Giannoulis G, Raptakis A, Kouloumentas C and Avramopoulos H 2020 arXiv: 201003358 [hep-ph]
[38] Hayashi M and Tsurumaru T 2012 *New J. Phys.* **14** 093014
[39] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[40] Hayashi M and Nakayama R 2014 *New J. Phys.* **16** 063009
[41] Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2016 *Phys. Rev. A* **94** 032335
[42] Azuma K 1967 *Tohoku Mathematical J. Second Series* **19** 357
[43] Sedziak-Kacprowicz K, Czerwinski A and Kolenderski P 2020 *Phys. Rev. A* **102** 052420
[44] Peronio P, Acconcia G, Rech I and Ghioni M 2015 *Rev. Sci. Instrum.* **86** 113101
[45] Muller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006
[46] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[47] Wang X B, Yang L, Peng C Z and Pan J W 2009 *New J. Phys.* **11** 075006
[48] Wang S, Zhang S L, Li H W, Yin Z Q, Zhao Y B, Chen W, Han Z F and Guo G C 2009 *Phys. Rev. A* **79** 062309