

Improved model on asynchronous measurement-device-independent quantum key distribution with realistic devices

Mingshuo Sun(孙铭烁), Chun-Hui Zhang(张春辉), Rui Zhang(章睿), Xing-Yu Zhou(周星宇), Jian Li(李剑), and Qin Wang(王琴)

Citation: Chin. Phys. B, 2024, 33 (**11**): 110302. DOI: 10.1088/1674-1056/ad757a
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Preparation of entangled W states based on the cavity QED system

Ke Li(李可) and Jun-Long Zhao(赵军龙)
Chin. Phys. B, 2024, 33 (**9**): 090306. DOI: 10.1088/1674-1056/ad50bf

Effects of quantum noise on teleportation of arbitrary two-qubit state via five-particle Brown state

Ao Wang(汪澳), Yu-Zhen Wei(魏玉震), Min Jiang(姜敏), Yong-Cheng Li(李泳成), Hong Chen(陈虹), and Xu Huang(黄旭)
Chin. Phys. B, 2024, 33 (**8**): 080307. DOI: 10.1088/1674-1056/ad3dc8

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)
Chin. Phys. B, 2022, 31 (**8**): 080303. DOI: 10.1088/1674-1056/ac6017

Detection efficiency characteristics of free-running InGaAs/InP single photon detector using passive quenching active reset IC

Fu Zheng(郑福), Chao Wang(王超), Zhi-Bin Sun(孙志斌), Guang-Jie Zhai(翟光杰)
Chin. Phys. B, 2016, 25 (**1**): 010306. DOI: 10.1088/1674-1056/25/1/010306

Afterpulsing characteristics of InGaAs/InP single photon avalanche diodes

Ma Hai-Qiang (马海强), Yang Jian-Hui (杨建会), Wei Ke-Jin (韦克金), Li Rui-Xue (李瑞雪), Zhu Wu (朱武)
Chin. Phys. B, 2014, 23 (**12**): 120308. DOI: 10.1088/1674-1056/23/12/120308

SPECIAL TOPIC — Quantum communication and quantum network

Improved model on asynchronous measurement-device-independent quantum key distribution with realistic devices

Mingshuo Sun(孙铭烁)[1,2], Chun-Hui Zhang(张春辉)[1,2,†], Rui Zhang(章睿)[3], Xing-Yu Zhou(周星宇)[1,2], Jian Li(李剑)[1,2], and Qin Wang(王琴)[1,2,‡]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

[2] *Broadband Wireless Communication and Sensor Network Technology, Key Laboratory of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

[3] *Changqing Oilfield Company Digital and Intelligent Business Division, China National Petroleum Corporation, Xi'an* 710299, *China*

(Received 8 July 2024; revised manuscript received 26 August 2024; accepted manuscript online 30 August 2024)

In principle, the asynchronous measurement-device-independent quantum key distribution (AMDI-QKD) can surpass the key rate capacity without phase tracking and phase locking. However, practical imperfections in sources or detections would dramatically depress its performance. Here, we present an improved model on AMDI-QKD to reduce the influence of these imperfections, including intensity fluctuation, the afterpulse effect, and the dead time of detectors. Furthermore, we carry out corresponding numerical simulations. Simulation results show that, by implementing our present work, it can have more than 100 km longer secure transmission distance and one order of magnitude enhancement in the key generation rate after 320 km compared with the standard method. Moreover, our model can still break the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound even under realistic experimental conditions.

Keywords: asynchronous measurement-device-independent quantum key distribution, intensity fluctuations, afterpulse, dead time

PACS: 03.67.Hk, 03.67.Dd, 03.67.–a, 03.67.Lx **DOI:** 10.1088/1674-1056/ad757a

1. Introduction

Quantum key distribution (QKD) could provide secure and effective keys between two legitimate users (Alice and Bob) at a remote distance.[1] Despite the security of QKD being guaranteed by quantum physical theory, the malicious attacker, Eve, is still able to make use of some potential loopholes of practical devices, i.e., in either the source part or the detection part, to hack the actual QKD system.

To protect the detection part of the QKD system, the measurement-device-independent quantum key distribution (MDI-QKD) protocol was proposed.[2,3] MDI-QKD is a three-party protocol, including a third untrusted party, Charlie, which is immune to all side-channel attacks directed at measurement devices. However, the transmission distance of MDI-QKD is still limited and cannot break the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound.[4]

Recently, the twin-field protocol and many varied TF-QKD protocols have been proposed,[5–9] and many experiments have proved their extraordinary performances.[10,11] On the one hand, TF-QKD inherits the advantages of MDI-QKD; on the other hand, TF-QKD utilizes single-photon interference of two independent sources to successfully break the PLOB bound.

However, TF-QKD is very sensitive to channel length drift and frequency differences between two users, which makes the phase-tracking and phase-locking techniques very important. To reduce the complexity of the TF-QKD system, the asynchronous measurement-device-independent QKD (AMDI-QKD) was proposed, with its key feature lying in post-matching two interference detection events.[12–14] As a result, even without phase-tracking techniques, AMDI-QKD could still surpass the secret key capacity. Successful experiments and advanced theoretical works have also been achieved.[15–18]

However, in real life, device imperfections may inevitably affect the performance of AMDI-QKD.[19] For example, the intensity of the laser source is not stable, which reduces the accuracy of parameter estimation.[20–24] Besides, the afterpulse and the deadtime effects often exist in practical QKD systems, especially in high-speed systems, resulting in increased quantum bit error rate (QBER).[25–27] To reduce the influence of device imperfections, including fluctuations in light source intensity, the afterpulse and the deadtime effects in single-photon detectors, here we present an improved model on AMDI-QKD systems.

This paper is arranged as follows. We first describe the procedures of decoy-sate AMDI-QKD step by step in Section 2. In Section 3, we present our improved model on AMDI-QKD by taking both fluctuations in light source inten-

[†]Corresponding author. E-mail: chz@njupt.edu.cn

[‡]Corresponding author. E-mail: qinw@njupt.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

sity, the afterpulse and the dead time effects in detectors into account. Numerical simulations are carried out in Section 4, and finally conclusions and outlooks are given in Section 5.

2. Procedures of decoy-sate AMDI-QKD

The protocol steps of decoy-state AMDI-QKD are presented as follows:[12]

Step 1 Alice and Bob independently prepare weak coherent states (WCS) $|\mathrm{e}^{\mathrm{i}(\theta_a^i+r_a^i\pi)}\sqrt{k_a^i}\rangle$ and $|\mathrm{e}^{\mathrm{i}(\theta_b^i+r_b^i\pi)}\sqrt{k_b^i}\rangle$ with probabilities P_{k_a} and P_{k_b}, respectively, where k_a^i $(k_b^i)\in\{\mu_{a(b)},\nu_{a(b)},\omega_{a(b)},o_{a(b)},\hat{o}_{a(b)}\}$ corresponding to the signal, decoy, preserve-vacuum, and declare-vacuum intensities. Here, $i\in\{1,2,\ldots,N\}$ denotes the time bin, $\theta_{a(b)}^i$ denotes the randomized phase and $r_{a(b)}^i\in\{0,1\}$ is the classical bit randomly chosen by Alice or Bob.

Step 2 For each time bin i, Charlie performs an interference measurement on the two received pulses. Charlie obtains an effective detection event whereas an effective event means only one detector clicks. Then, Charlie publicly announces whether an effective event is obtained and which detector clicks. In the following, we define $\{k_a^ik_a^j,k_b^ik_b^j\}$ that Alice and Bob choose $\{k_a^i,k_b^i\}$ as a match at the i-th time slot and Alice and Bob choose $\{k_a^j,k_b^j\}$ as a match at the j-th time slot.

Step 3 Before the specific steps, we define two cases in the protocol:

Case 1: Within T_{c} time slots, other detection events can be found around it.

Case 2: Within T_{c} time slots, no detection events can be found around it.

Alice and Bob first check the number of case 2. If case 2 is smaller than or equal to Δ, the data of case 2 can be discarded, where Δ is a preset threshold; otherwise, they abort the protocol. Regarding case 1, Alice or Bob will announce the intensity and phase information through a trusted channel when they choose decoy or declare-vacuum intensity. In the Z-basis, the data comes from the events including $\{\mu_a,\mu_b\},\{o_a,\mu_b\},\{\mu_a,o_b\},\{o_a,o_b\}$. Among these events, Alice randomly chooses intensity μ_a at the i-th time bin to match with intensity o_a at the j-th time bin. The events which can not find a matchable peer will be discarded. If $i<j$ $(i>j)$, Alice will set bit 1 (0) and inform Bob of the serial number ij. As a result, if Bob chooses $k_b^{\min(i,j)}=\mu_b(o_b)$ and $k_b^{\max(i,j)}=o_b(\mu_b)$, his bit will be set as 0 (1). Then Bob announces an event where $k_b^i=k_b^i=o_b$ or μ_b. Thus, the valid events in the Z-basis are $\{\mu_ao_a,o_b\mu_b\}$, $\{\mu_ao_a,\mu_bo_b\}$,$\{o_a\mu_a,o_b\mu_b\}$ and $\{o_a\mu_a,\mu_bo_b\}$.

In the X-basis, the data comes from the events including $\{\nu_a,\nu_b\}$, $\{o_a,\nu_b\}$, $\{\nu_a,o_b\}$, $\{o_a,\hat{o}_b\}$ and $\{\hat{o}_a,o_b\}$. The global phase between Alice and Bob is $\varphi^i=\varphi_a^i-\varphi_b^i$. Alice and Bob randomly choose two events that satisfy $k_a^i=k_a^j,k_b^i=k_b^j$, and $|\varphi^i-\varphi^j|=0$ or π. They then match the two events as $\{k_a^ik_a^j,k_b^ik_b^j\}$. Alice and Bob could get a bit value in the X-basis by calculating the bit $r_a^i\oplus r_a^j$ and $r_b^i\oplus r_b^j$, respectively. Afterwards, in the Z-basis, Bob always flips his bit. In the X-basis, Bob flips his bit as follows: when the phase difference is 0 and different detectors click; or when the phase difference is π and the same detector clicks twice.

Step 4 Alice and Bob exploit the bits from the Z-basis to form the n_z raw key bits and calculate the bit error rate E_z. Then, they reveal all bit values in the X-basis to obtain the total number of errors. We also utilize the decoy-state method to estimate the vacuum events in the Z-basis $s_{o\mu}^z$, the number of single-photon pairs s_{11}^z, the bit error rate in the X-basis e_{11}^x and the phase error rate of single-photon pairs in the Z-basis ϕ_{11}^z.

Step 5 Alice and Bob distill the final keys as

$$\begin{aligned} l \;=\; & s_{o\mu}^z+s_{11}^z[1-H(\phi_{11}^z)]-n_zfH(E_z) \\ & -\log_2\frac{2}{\varepsilon_{\mathrm{cor}}}-2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}}-2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}, \end{aligned} \tag{1}$$

where $H(x)$ is the binary Shannon entropy function. f is the error correction efficiency. $\varepsilon_{\mathrm{cor}}$ is the failure probability of error verification; $\varepsilon_{\mathrm{PA}}$ refers to the failure probability of privacy amplification; ε' and $\hat{\varepsilon}$ represent the coefficients when using the chain rules of smooth min-entropy and max-entropy, respectively.[28–30]

3. Improved AMDI-QKD model considering device imperfections

Before describing device imperfections, we first introduce the mathematical model for AMDI-QKD and some important parameters, including the counting rate and the quantum bit error rate. When Alice and Bob send light pulses with intensities k_a and k_b, respectively, with a phase difference of φ, the counting rate for one and only one detector (L or R) clicking is

$$q_{k_ak_b}^{\mathrm{L}\varphi}=y_{k_ak_b}(\mathrm{e}^{w_{k_ak_b}\cos\varphi}-y_{k_ak_b}), \tag{2}$$

$$q_{k_ak_b}^{\mathrm{R}\varphi}=y_{k_ak_b}(\mathrm{e}^{-w_{k_ak_b}\cos\varphi}-y_{k_ak_b}), \tag{3}$$

where $y_{k_ak_b}=\mathrm{e}^{-(\eta_ak_a+\eta_bk_b)/2}(1-P_{\mathrm{d}})$ and $w_{k_ak_b}=\sqrt{\eta_ak_a\eta_bk_b}$. Here, $\eta_{a(b)}$ is the transmission loss and P_{d} is the dark count rate. Then the overall gain is

$$Q_{k_ak_b}=\frac{1}{2\pi}\int_0^{2\pi}(q_{k_ak_b}^{\mathrm{L}\varphi}+q_{k_ak_b}^{\mathrm{R}\varphi})\,\mathrm{d}\varphi. \tag{4}$$

Denote $QE_{2\nu,2\nu}$ as the overall error rate in the X-basis when both Alice and Bob send pulses with intensity ν; $QE_{2\nu,0}(QE_{0,2\nu})$ corresponds to the case when Alice (Bob) sends pulses with intensity ν and Bob (Alice) with intensity 0. $QE_{0,0}$ refers to the case when both Alice and Bob send vacuum states. They can be expressed as

$$QE_{2\nu,2\nu}=\frac{1}{4\pi}\int_0^{2\pi}\frac{q_{\nu\nu}^{\mathrm{L}\varphi}q_{\nu\nu}^{\mathrm{R}\varphi+\sigma}+q_{\nu\nu}^{\mathrm{L}\varphi+\sigma}q_{\nu\nu}^{\mathrm{R}\varphi}}{q_{\nu\nu}^{\mathrm{L}\varphi+\sigma}+q_{\nu\nu}^{\mathrm{R}\varphi+\sigma}}\,\mathrm{d}\varphi, \tag{5}$$

$$QE_{2\nu,0} = QE_{0,2\nu} = \frac{e_0\, e^{-2\nu} Q_{\nu,0}^2}{4\pi} \int_0^{2\pi} \frac{1}{q_{\nu\nu}^{L\varphi} + q_{\nu\nu}^{R\varphi}} \mathrm{d}\varphi, \quad (6)$$

$$QE_{0,0} = \frac{e_0\, e^{-4\nu} Q_{00}^2}{4\pi} \int_0^{2\pi} \frac{1}{q_{\nu\nu}^{L\varphi} + q_{\nu\nu}^{R\varphi}} \mathrm{d}\varphi, \quad (7)$$

where σ refers to the misaligned angle in the X basis.

3.1. Intensity fluctuation

In most decoy-state AMDI-QKD protocols, it assumes that the signal and the decoy states have stable intensities. However, in practical experiments, the light intensities always fluctuate, inevitably degrading the QKD performance. Moreover, it is very hard to know the exact value of intensity fluctuations for every single light pulse. Instead, we usually know the upper and the lower bounds of the intensity fluctuations[20]

$$\mu_{a(b)}^i = (1 \pm \delta_i)\mu, \quad \nu_{a(b)}^i = (1 \pm \delta_i)\nu, \quad (8)$$

where $|\delta_i| \leq \delta$, and δ is the maximum fluctuation that could be determined before experiments.

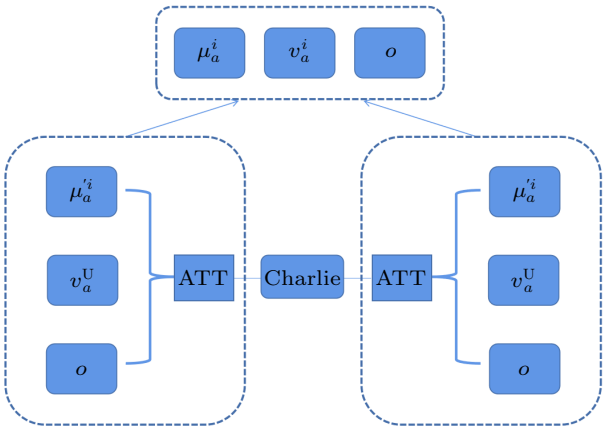


Fig. 1. The schematic of the virtual AMDI-QKD protocol. ATT is the attenuator. The upper box represents the sources as shown in Eq. (8). Both the dashed sides represent the virtual sources as shown in Eq. (9).

In QKD, a stable attenuator and an upper-bounded source allow for the application of the method proposed in Refs. [22, 24] to uphold both the security and efficiency of the QKD system. To enhance the robustness of AMDI-QKD, we introduce a virtual AMDI-QKD protocol. This protocol utilizes three sources, each emitting a single intensity state. Notably, the decoy state ν is fixed at the upper value ν^U and coupled with a virtual attenuator $\eta_i = \frac{1+\delta_i}{1+\delta}$, ensuring that the intensity of all sources can be concluded as[24]

$$\nu_i' = \nu^U, \quad (9)$$

$$\mu_i' = \mu_i \frac{1+\delta}{1+\delta_i} \leq \mu_i \frac{1+\delta}{1-\delta}. \quad (10)$$

Correspondingly, the density matrices of decoy states and signal states are changed to

$$\rho_\nu = \sum_{k=0}^{\infty} P_\nu^n |k\rangle\langle k| = \sum_{k=0}^{\infty} \frac{(\nu^U)^k e^{-\nu^U}}{k!} |k\rangle\langle k|, \quad (11)$$

$$\rho_\mu = \sum_{k=0}^{\infty} P_\mu^n |k\rangle\langle k| = \sum_{k=0}^{\infty} \frac{(\mu_i')^k e^{-\mu'}}{k!} |k\rangle\langle k|. \quad (12)$$

With the above, the single-photon yield and error rate with intensity fluctuation could be written as

$$Y_{01} \geq Y_{01}^L = \frac{P_\mu^{2,L} Q_{0\nu}^L - P_\nu^2 Q_{0\mu}^U - (P_\nu^0 P_\mu^{2,L} - P_\mu^{0,L} P_\nu^2) Q_{oo}}{P_\nu^2 P_\mu^{1,L} - P_\nu^1 P_\mu^{2,L}}, \quad (13)$$

$$Y_{10} \geq Y_{10}^L = \frac{P_\mu^{2,L} Q_{\nu 0}^L - P_\nu^2 Q_{\mu 0}^U - (P_\nu^0 P_\mu^{2,L} - P_\mu^{0,L} P_\nu^2) Q_{oo}}{P_\nu^2 P_\mu^{1,L} - P_\nu^1 P_\mu^{2,L}}. \quad (14)$$

Suppose that the global phase difference φ is a randomly and uniformly distributed value, the expected number of single-photon pairs in the X-basis can be given by

$$s_{11}^x \geq \nu_a \nu_b e^{-2\nu_a - 2\nu_b} Y_{01} Y_{10} \int_0^{2\pi} \frac{1}{2\pi (q_{k_a k_b}^{L\varphi} + q_{k_a k_b}^{R\varphi})} \mathrm{d}\varphi. \quad (15)$$

For single-photon pairs, the expected phase error rate in the Z basis ϕ_{11}^z equals the expected value of the bit error rate in the X basis e_{11}^x, and e_{11}^x is concluded as

$$e_{11}^x \leq e_{11}^U = t_{11}/s_{11}^x, \quad (16)$$

where t_{11} is the error in X-basis which is relevant to the decoy state intensity ν. The t_{11} can be expressed as

$$t_{11} = QE_{2\nu,2\nu} - QE_{2\nu,0} - QE_{0,2\nu} + QE_{0,0}. \quad (17)$$

3.2. Afterpulse effects and dead time

One of the most important factors to qualify the performance of single-photon avalanche diodes (SPADs) is the afterpulse rate. The generation of an afterpulse originates from the accumulation of carriers caused by a previous detection event, potentially causing a 'false' detection event. Especially in the high-rate QKD system, such false detection events contribute to an additional QBER.

An effective method to mitigate the impact of afterpulses is to extend the dead time. This method capitalizes on the fact that during the dead time interval, no detection events occur. However, blinding increasing the dead time results in a reduced counting rate, consequently decreasing the key generation rate. Here, we propose a novel AMDI-QKD calculation model which considers both the afterpulse rate and dead time. Accounting for the presence of afterpulse effects and the fact that the prior pulse detection may influence the subsequent matching pulse detection, we correct the gains as follows:

$$q_{k_a k_b}'^{L\varphi} = q_{k_a k_b}^{L\varphi} + (1 - q_{k_a k_b}^{L\varphi})(1 - q_{k_a k_b}^{R\varphi}) P_{ap}(1 - P_{ap}), \quad (18)$$

$$q_{k_a k_b}'^{R\varphi} = q_{k_a k_b}^{R\varphi} + (1 - q_{k_a k_b}^{L\varphi})(1 - q_{k_a k_b}^{R\varphi}) P_{ap}(1 - P_{ap}), \quad (19)$$

where P_{ap} is the average afterpulse response probability of the system and is estimated as

$$P_{ap} = \frac{q}{1-q} \hat{D}, \quad (20)$$

where $\hat{D} = \sum_{k_a}\sum_{k_b} P_{k_a}P_{k_b}Q_{k_ak_b}$ and q is the overall afterpulse rate.

Next, adding the dead time into account, the corresponding gain is

$$\hat{q}^{\mathrm{L}\varphi}_{k_ak_b} = \frac{q'^{\mathrm{L}\varphi}_{k_ak_b}}{1+\tau\sum\sum_{k_ak_b}[P_{k_a}P_{k_b}(q'^{\mathrm{L}\varphi}_{k_ak_b}+q'^{\mathrm{R}\varphi}_{k_ak_b})]}, \tag{21}$$

$$\hat{q}^{\mathrm{R}\varphi}_{k_ak_b} = \frac{q'^{\mathrm{R}\varphi}_{k_ak_b}}{1+\tau\sum\sum_{k_ak_b}[P_{k_a}P_{k_b}(q'^{\mathrm{L}\varphi}_{k_ak_b}+q'^{\mathrm{R}\varphi}_{k_ak_b})]}, \tag{22}$$

where τ denotes the ratio between the dead time and the system pulse interval period[31] and $P_{k_a}(P_{k_b})$ represents the probability of sending a pulse with intensity k_a (k_b).

Finally, the gain considering afterpulse and dead time is concluded as

$$\hat{Q}_{k_ak_b} = 1/2\pi\int_0^{2\pi}(\hat{q}^{\mathrm{L}\varphi}_{k_ak_b}+\hat{q}^{\mathrm{R}\varphi}_{k_ak_b})\,\mathrm{d}\varphi. \tag{23}$$

4. Simulation results

In this section, we present some numerical simulations focusing on the symmetric case where the untrusted party, Charlie, is located midway between Alice and Bob. Considering statistical fluctuations, we apply the Chernoff method to enhance practicality.[32] Further simulation results are based on the parameters in Table 1.

Table 1. List of experimental parameters used in numerical simulations. Here, P_{d} denotes the dark count rate of single-photon detectors; e_{d} is the misalignment probability of the optical system; N is the number of transmitted signals. η_{d} is the efficiency of single-photon detectors; f is the error correction inefficiency; ξ is the failure probability of statistical fluctuation analysis;[32] α is the fiber loss coefficient.

e_{d}	P_{d}	N	η_{d}	ξ	f	α (dB/km)
0.015	10^{-8}	10^{13}	0.6	10^{-10}	1.16	0.2

Simulation results with different models of intensity fluctuation are shown in Fig. 2. It is evident that our present method outperforms the standard method, demonstrating an order of magnitude higher key generation rate and an extended transmission distance of 60 km. Here, the standard method denotes the method introduced in Ref. [20]. Furthermore, compared to the ideal model that neglects intensity fluctuations, the key generation rate and transmission distance of our scheme are only marginally reduced.

Under the influence of afterpulse effects and dead time, we simulate various methods as illustrated in Fig. 3. The solid line represents the ideal AMDI-QKD model, i.e., without considering the afterpulse effect or dead time, while the dash-dot lines depict our present method by incorporating the afterpulse effect and the dead time effect. The two pairs of q and τ values are derived from the experimental data in Ref. [26]. Notably, the intersection of the two lines around 75 km indicates that blindly increasing the dead time does not necessarily enhance the key generation rate at any distance. This observation highlights the importance of selecting an appropriate dead time to optimize the performance of AMDI-QKD.

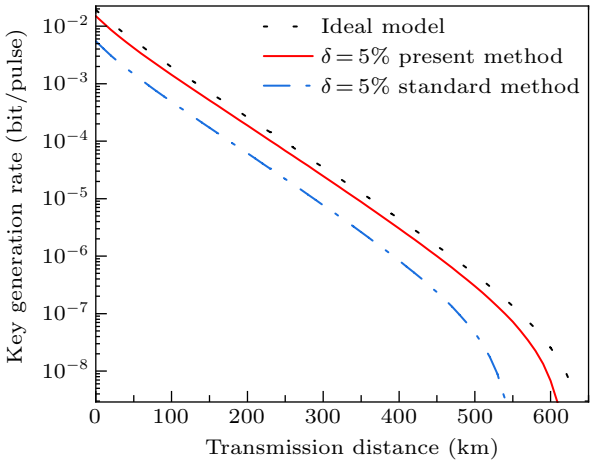


Fig. 2. Comparison of the key generation rate for the AMDI-QKD with different intensity fluctuation models, setting the intensity fluctuation at 5%. The dotted line denotes the model without considering any intensity fluctuation. The dash-dot line denotes the standard model, and the solid line denotes our present model.

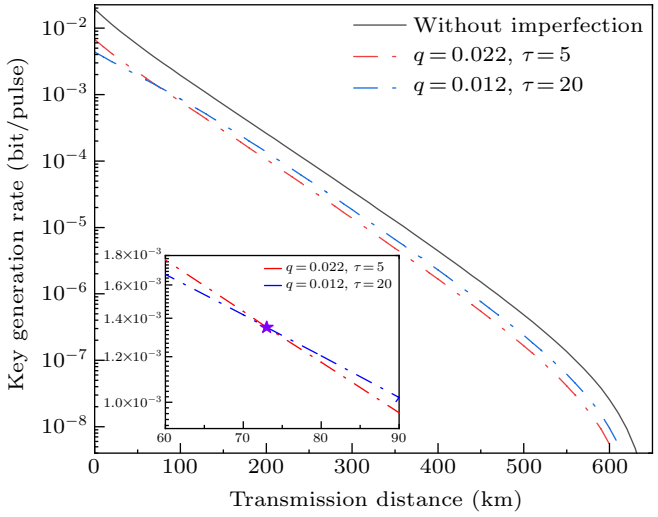


Fig. 3. The key generation rates versus transmission distance with different afterpulse probabilities q and dead time τ. The solid line denotes the ideal model without considering the afterpulse effect and dead time. The two dash lines denote our present model with reasonable parameters.[26]

Finally, we compare the ideal model, the standard method and our present method by comprehensively accounting for all those practical imperfections in AMDI-QKD, including intensity fluctuation, afterpulse effect, and dead time, as shown in Fig. 4. We can see from Fig. 4 that our present approach can have 100 km longer transmission distance and one order of magnitude enhancement in the key generation rate after 320 km compared with the standard method. Besides, it could still surpass the PLOB bound while maintaining performance close to the ideal model.

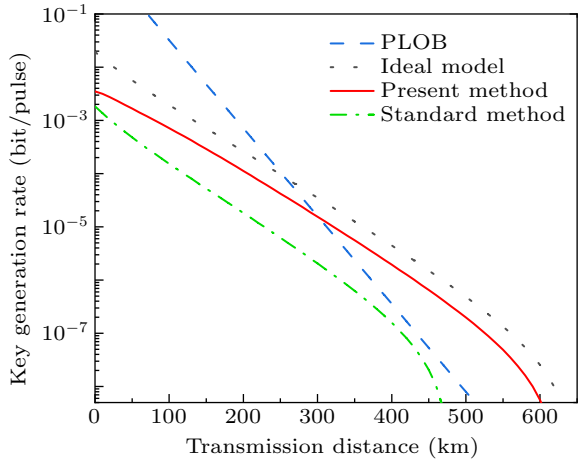


Fig. 4. Comparison of the key generation rate for the AMDI-QKD with different intensity fluctuation or afterpulse models, setting the intensity fluctuation at 7.5%. The dashed line denotes the PLOB.[4] The other dotted, solid, and dash-doted lines represent using the ideal model, our present method with $q = 0.012$, $\tau = 20$, and the standard method, respectively.

5. Conclusion and perspectives

In this paper, we carry out investigations on the imperfections of practical AMDI-QKD systems, including intensity fluctuation, afterpulse effect, and dead time. To depress the influence of intensity fluctuations on AMDI-QKD protocol, we present an improved method by establishing the equivalent protocols with a virtual attenuation. Furthermore, we take the dead time and the afterpulse effect into account, and give a more general model for practical AMDI-QKD. Besides, we carry out corresponding numerical simulations and demonstrate that our present work can show significant enhancement in both the key generation rate and the secure transmission distance compared with the standard method. Therefore, our work can pave a way towards practical implementations of AMDI-QKD in the near future.

Acknowledgments

Project supported by Natural Science Foundation of Jiangsu Province (Grant Nos. BE2022071 and BK20192001), the National Natural Science Foundation of China (Grant Nos. 12074194, 62101285, 62471248, and 12104240), and Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX22_0954).

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* pp. 175–179
[2] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[3] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[4] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[5] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[6] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[7] Cui C H, Yin Z Q, Wang R, *et al.* 2019 *Phys. Rev. Appl.* **11** 034053
[8] Ma X F, Zeng P and Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[9] Han Y X, Sun Z Q, Ma H Q, *et al.* 2022 *Chin. Phys. Lett.* **39** 070301
[10] Wang S, Yin Z Q, Han Z F, *et al.* 2022 *Nat. Photon.* **16** 154
[11] Liu Y, Zhang W J, Pan J W, *et al.* 2023 *Phys. Rev. Lett.* **130** 210801
[12] Xie Y M, Lu Y S, Chen Z B, *et al.* 2022 *PRX Quantum* **3** 020315
[13] Zeng P, Zhou H Y, Wu W J and Ma X F 2022 *Nat. Commun.* **13** 3903
[14] Wang Z H, Wang R, Han Z F, *et al.* 2023 *Commun. Phys.* **6** 265
[15] Zhou L, Lin J P, Yuan Z L, *et al.* 2023 *Phys. Rev. Lett.* **130** 250801
[16] Zhu H T, Huang Y Z, Pan J W, *et al.* 2023 *Phys. Rev. Lett.* **130** 030801
[17] Bai J L, Xie Y M, Chen Z B, *et al.* 2023 *Opt. Lett.* **48** 3551
[18] Xie Y M, Bai J L, Chen Z B, *et al.* 2023 *Phys. Rev. Appl.* **19** 054070
[19] Zhang C X, Wu D, An J M, *et al.* 2023 *Chin. Phys. B* **32** 124207
[20] Wang X B 2007 *Phys. Rev. A* **75** 052301
[21] Wang X B, Peng C Z, Pan J W, *et al.* 2008 *Phys. Rev. A* **77** 042311
[22] Wang X B, Peng C Z and Pan J W 2007 *Appl. Phys. Lett.* **90** 031110
[23] Jiang C, Yu Z W and Wang X B 2016 *Phys. Rev. A* **94** 062323
[24] Jiang C, Yu Z W, Hu X L and Wang X B 2023 *Nat. Sci. Rev.* **10** nwac186
[25] Fan-Yuan G J, Wang C, Guo G C, *et al.* 2018 *Phys. Rev. Appl.* **10** 064032
[26] Huang X J, Lu F Y, Han Z F, *et al.* 2022 *Phys. Rev. A* **106** 062607
[27] Wang Z H, Wang S, Han Z F, *et al.* 2022 *Opt. Express* **30** 28534
[28] Curty M, Xu F H, Cui W, *et al.* 2014 *Nat. Commun.* **5** 3732
[29] Xu F H, Curty M, Qi B and Lo H K 2013 *New J. Phys.* **15** 113007
[30] Feng B, Huang H D, Wang Q, *et al.* 2023 *Chin. Phys. B* **32** 030307
[31] Davide R, Alberto B, Hugo Z, *et al.* 2018 *Appl. Phys. Lett.* **112** 171104
[32] Curty M, Xu F H, Cui W, *et al.* 2014 *Nat. Commun.* **5** 3732