





Dependency model for high-performance quantum-key-distribution systems

Xiao-Juan Huang ^{*}, Feng-Yu Lu ^{*}, Shuang Wang [†], Zhen-Qiang Yin [‡], Ze-Hao Wang, Wei Chen, De-Yong He, Guan-Jie Fan-Yuan, Guang-Can Guo, and Zheng-Fu Han

CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China;

CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China;

and Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China



(Received 22 September 2022; revised 5 November 2022; accepted 18 November 2022; published 7 December 2022)

A precise estimation of the detection response is essential for a high-performance and secure quantum-key-distribution (QKD) system. Single-photon avalanche diodes (SPADs) are widely applied to estimate the single-photon yields. However, in the presence of the dead time and afterpulse of the SPADs, the estimations of gains in previous models are biased, which will lead to ill-fitting optimized parameters and greatly degrade the system performance. Here, we develop a dependency model for providing more accurate optimization to achieve higher-performance QKD systems. Moreover, to further improve the system performance, our model guides users to choose proper dead time. Our simulation results indicate that our model plays an important role in the practical application and deployment of QKD systems.

DOI: [10.1103/PhysRevA.106.062607](https://doi.org/10.1103/PhysRevA.106.062607)

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] is a technique to generate and share private keys securely between two remote parties in the presence of eavesdroppers. In theory, the laws of quantum physics guarantee the unconditional security of the QKD [4–7], which has drawn wide attention in the world and achieved significant progress in both theory [8–12] and practice [13–16].

In actuality, weak coherent lasers are used to substitute for perfect single-photon sources. Weak coherent lasers emit highly attenuated laser pulses, each of which may contain more than one photon. They provide an excellent opportunity for eavesdroppers to perform the photon-number-splitting (PNS) attack [17,18], especially when the quantum channel loss is high. To tackle the PNS attack, a notable scheme named the decoy-state method was proposed [8,19,20]. The decoy-state scheme dexterously circumvents the security loophole introduced by multiphoton pulses and channel loss in practical QKD systems.

In decoy-state QKD schemes, parameter optimization is significant for maximizing the system performance. And a lot of works [21–25] have proved that the performance of the optimized system is greatly improved, compared with that of the unoptimized systems. Generally, users simulate the system based on the practical devices and environment, and evaluate the optimal parameters of the system according to the

simulation results. As a result, an accurate model to describe the practical situation is of great concern.

Because of the cost-effective price, high quantum efficiency, and good robustness, single-photon avalanche diodes (SPADs) are widely employed for single-photon detection in practical QKD systems [26]. One of the most important factors that can be used to qualify the performance of SPADs is the afterpulse [27]. The afterpulse is correlated with the previous ignition avalanches, which is called the non-Markovian property [28]. When photons trigger an avalanche, a part of photon carriers will be trapped at a deep energy level due to the material defects of the SPADs. Then the trapped carriers will release over time and may trigger a pseudodetection event if the SPAD is biased above the breakdown voltage. As an intrinsic characteristic of the SPADs, the afterpulse will introduce random detector responses, which increases the quantum bit error rate (QBER) [29,30]. Especially, the afterpulse of the signal state has great contributions to the gain and QBER of decoy states [31].

Particularly, in order to alleviate the influence of the afterpulse, a possible way is to introduce the dead time, a hold-off time during which the SPAD is unable to detect photons after a detection event. In this interval, the gate of the SPAD is on off state, and any photons including light pulses will not produce any amplified signals. After the hold-off time, the SPAD is ready for a new detection cycle. Giving a sufficiently high dead time, the afterpulse effect can be neglected, which will degrade the error performance. However, blindly increasing the dead time leads to a low count rate that will decrease the secret key rate (SKR), and goes against high-speed QKD systems. Therefore, an applicable dead time is crucial. Given that, precisely describing the model based on the dead time and afterpulse is vital for achieving higher-speed and higher-

^{*}These authors contributed equally to this work.

[†]wshuang@ustc.edu.cn

[‡]yinzq@ustc.edu.cn

performance QKD systems. And beyond that, the absence of the afterpulse and dead time description leads to the skewing of simulated gains and QBERs, which results in ill-fitting optimal parameters, thus lower SKR.

Reference [32] proposed an analytical model for the dark counts and dead-time regime on the measured count rate, based on free-running SPADs. But this model does not take the afterpulse effect into account. Reference [33] analyzes effects of dead time and active reset on afterpulse probability of InGaAs/InP single-photon avalanche diodes. In Ref. [33], the authors introduced three models to calculate the afterpulse probability: the simple model, the first-order model, and the second-order model, which are applicable to different situations. The second-order model can provide a more accurate SPD model, but its analytical model is complex so that it can only be found numerically, while our model is of good applicability and can give simple, analytical, and comprehensible estimates of gains.

In our paper, based on gated-mode SPADs, we develop a dead time and afterpulse model, named the “dependency model,” in Sec. II. Our model helps users to estimate the actual gains of each state. In Sec. III, we validate the veracity of our model. The gains estimated by our dependency model and Monte Carlo simulation are both in good agreement with the experimental results. In Sec. IV, we compare our model with the previous model that omits afterpulse and dead time, named the “isolated model,” and our model shows great advantage in implementing higher-performance QKD systems. Last but not least, choosing proper dead time is crucial for further improving the SKR and practical deployment of high-speed QKD systems. A conclusion is provided in Sec. V.

II. MODELS

On account of the low price, high quantum efficiency, and good robustness, SPADs are widely used as single-photon detectors in practical QKD systems. As is shown in Fig. 1(b), the SPAD is working on gated mode. In Fig. 1(c), except for the light pulses in blue rectangles, there are two other factors to trigger the detector responses: dark counts in green rectangles and afterpulse in red rectangles. It should be noticed that users cannot tell which factor causes the detection response and they just record all response events.

As already stated, the afterpulse of SPADs is non-Markovian in nature. After a detection response, the population of the trapped carriers exponentially decays in time [34]. Most of trapped carriers are subsequently released, which leads to high afterpulse rate. As an intrinsic property of the SPADs, the afterpulse will bias the estimated gains and introduce QBERs. Based on this property, the most common method to alleviate the impact on afterpulse is to set the dead time. As is shown in Fig. 1(b) in dashed lines, during the dead time, there are no on-gate states applied to the detector, and whether light pulses, dark counts, or afterpulses, detection responses will occur with a certain probability of zero. As a consequence, we have to evaluate the discarded events in dead time to obtain more accurate gains. However, the previous model simply considers the responses caused by light pulses and dark counts, ignoring the effects of dead time and afterpulses, resulting in incorrect estimates of the true gains

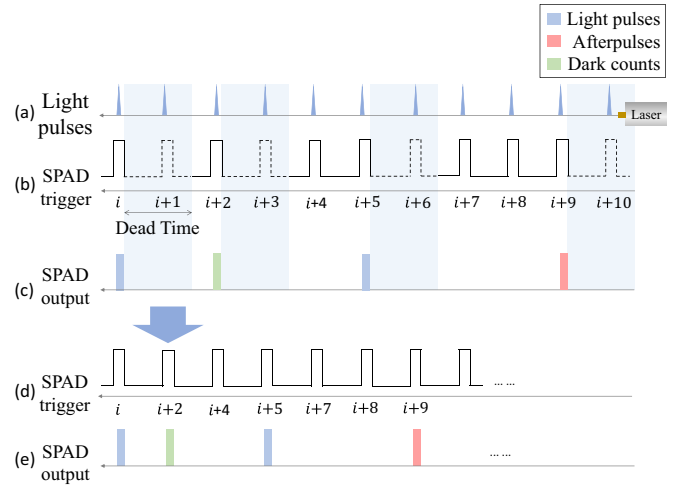


FIG. 1. Schematic illustrations of the response of a SPAD detector. (a) Light pulses sent by Alice, assuming that the gate and the optical pulse have the same frequency. (b) The SPAD operating in the gated mode. After a response event, in any case, the SPAD will not respond during the dead time in dashed lines. (c) Events ignited by light pulses in blue rectangles, afterpulses in red rectangles, and dark counts in green rectangles after setting dead time. The detection responses at detection windows of $(i+5)$, $(i+2)$, and i , which all have impact on the current detection window, and $(i+9)$. The response at the $(i+9)$ th detection window is triggered by afterpulse. (d) and (e) are equivalent to (b) and (c) after setting dead time, respectively. The pulses during dead time are discarded in the equivalent physical scenarios.

and QBERs. Here, we first analyze the previous model. Then we build our model and extend it.

A. Isolated model

In previous works, the gain with intensity μ is often given by

$$D = 1 - e^{-\eta\mu}(1 - Y_0), \quad (1)$$

where η is the detection efficiency and Y_0 is the dark count rate. Equation (1) means the light pulses and dark counts ignite the SPAD responses with probability D . The light pulses and dark counts have nothing to do, and each response is independent. Thus we regard this model as the isolated model.

As is shown in Fig. 2, the red line represents the optimal SKR of the isolated model in three-intensity-decoy-state QKD protocol [35] which is deferred to Appendix A. The pentagrams are the corresponding Monte Carlo simulation results. The Monte Carlo simulation is a method to be used to simulate the real detecting process, and details are presented in Appendix B. In practice, the afterpulse and dead time exist. If using the isolated model to analyze, the gap between theory and practice is wide. The results in Fig. 2 say it all. It reveals that the SKR is seriously overestimated in the isolated model, which will mislead users to analyze the system performance in practice.

This simulated gains are not precise enough to fit the practical situation. In general, the dead time and afterpulse are both the most important factors for SPADs. Because of the

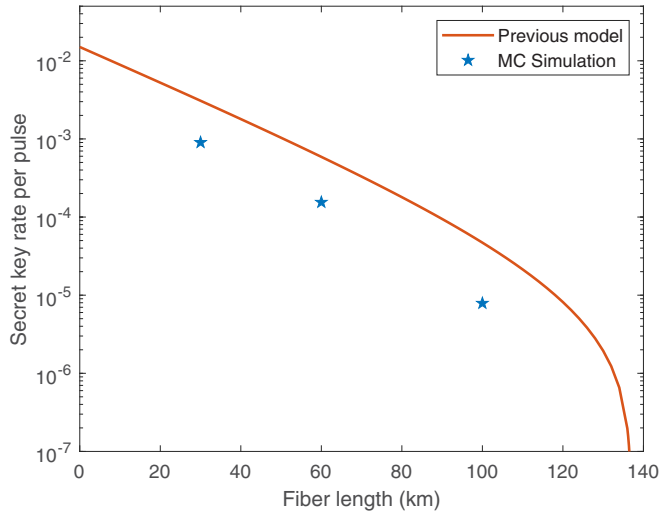


FIG. 2. Secret key rate as a function of fiber length L . The red line is the optimal secret key rate of the isolated model and the pentagrams are the corresponding Monte Carlo simulation results at $L = 30, 60,$ and 100 km.

exponential distribution of the afterpulse rate, after a detection response, afterpulse can ignite another response with a high probability and dead time alleviates this effect. The dead time and afterpulse affect the simulated gains significantly so that both of them cannot be neglected. Thus, we need to paint a more precise physical picture.

B. Dependency model

Actually, due to practical manufacturing processes, the dead time and afterpulse are inevitable. The afterpulse will cause random responses that will introduce QBERs while the dead time can reduce this negative effect. As shown in Figs. 1(b) and 1(c), in the dead-time interval, the pulses will not participate in the detection process. In other terms, these pulses are discarded, as is shown in Fig. 1(d). We can see that the dead time is set depending on former detection response. In the back of this interval, the SPAD continues to work normally in the gated mode. By the way, τ represents the number of gates during each dead-time interval. For instance, in Fig. 1(b), the dead time corresponds to one gate, $\tau = 1$, and for ease of illustration and presentation, we redefine τ as the dead time.

For the sake of understanding, let us discuss the counts and gain of the single state with intensity μ first. As is shown in Fig. 1(d), after setting dead time, the actual number of pulses participating in the detection process decreases, assuming that \hat{n} is the number of detection responses after setting dead time correlated to Fig. 1(e). Thus, there are $\hat{n}\tau$ pulses discarded in the dead-time duration and the remaining pulses, $N - \hat{n}\tau$ pulses, participate in the detection process. We can estimate the total detection responses \hat{n} by

$$\hat{n} \approx D'(N - \hat{n}\tau), \quad (2)$$

where the D' corresponds to response probability triggered by light pulses, dark counts, and afterpulses, and is given by

$$D' = 1 - (1 - D)(1 - P_{AP}), \quad (3)$$

where D is given by Eq. (1) and P_{AP} is the response probability triggered by afterpulse, which is related to all previous response events. More information about the derivation of P_{AP} [31] is given in Appendix C. We can estimate the average afterpulse response probability of system P_{AP} and it is expressed by

$$P_{AP} = \frac{q}{1 - q}D, \quad (4)$$

where

$$q = \sum_{i=\tau+1}^j \hat{p}(i) \quad (5)$$

is the overall afterpulse rate and \hat{p} is the afterpulse rate coefficient. The $\hat{p}(i)$ is a conditional probability and indicates that after a response event, it may cause the afterpulse occurrence with a probability $\hat{p}(i)$ at the i th succeeding detection window. $\hat{p}(i)$ represent the afterpulse contribution caused by one response event. Thus, q reflects the totally afterpulse contribution outside the dead time. That is, Eq. (4) reflects that historical response events contribute to P_{AP} . In the dead-time duration, the afterpulse rate will not contribute to P_{AP} thus setting $\hat{p}(i) = 0$, where $i \in (0, \tau]$. By the way, the \hat{p} is measured experimentally and the details about the measuring method are shown in Appendix D.

Equation (2) is the estimated total number of detection responses triggered by the three factors—light pulses, dark counts, and afterpulse—in the presence of dead time. The D' is the gain that does not consider the dead time, but patches the afterpulse into the total responses events. The $D'(N - \hat{n}\tau)$ is a bit higher than \hat{n} . Here, we ignore the effect of high order of D' and consider them to be approximately equal. And the results in Sec. III will justify making this approximation.

The most important thing is to evaluate the real number of detection responses. After abandoning pulses in the duration of dead time, we can estimate the number of detection responses \hat{n} as

$$\hat{n} = \frac{ND'}{1 + \tau D'}. \quad (6)$$

We find that the detection response \hat{n} is lower than the original estimated gain, $n = ND'$, which confirms that Eq. (6) is consistent with the actual situation that the dead time will decrease the count rate. In actuality, users regard the gain as

$$\hat{D} = \frac{\hat{n}}{N}. \quad (7)$$

Thus, the gain with intensity μ after correcting is expressed by

$$\hat{D} = \frac{D'}{1 + \tau D'}. \quad (8)$$

Different from the isolated model, previous response situations have great impact on latter events and are inextricably linked. Correcting for the isolated model is essential. For this reason, we call our model the “dependency model.” The dependency model can provide more accurate gain simulations and help users to evaluate the practical system performance in theory, especially in the decoy-state scheme.

C. Extension of the dependency model

The decoy-state scheme is proven to be used to estimate the contribution from single-photon signals and is widely applied in practical QKD systems. Usually, people will further optimize the decoy parameters, including the intensity of each state, and the probability choice of intensities and bases, to achieve better performance of QKD systems. Nevertheless, in the decoy-state scheme, since the dead time and the afterpulse will affect other cycles, the error of the previously isolated model will be larger, resulting in worse performance of the system. Thus, our dependency model becomes more significant. Here, we extend our model to the decoy-state scheme. Taking an r -intensity decoy-state scheme as an example, Alice randomly prepares a pulse with intensity μ_i [$\mu_i \in (\mu_1, \mu_2, \mu_3, \dots, \mu_r)$].

Unlike the single intensity situation, we have to figure out discarded pulses with different intensities, assuming that P_{μ_i} is the probability to choose the intensity μ_i . Similarly, we can derive the number of response events of each state:

$$\begin{aligned}\hat{n}_{\mu_1} &\approx NP_{\mu_1}D'_{\mu_1} - \tau \left(\sum_{\mu_i} \hat{n}_{\mu_i} \right) P_{\mu_1}D'_{\mu_1}, \\ \hat{n}_{\mu_2} &\approx NP_{\mu_2}D'_{\mu_2} - \tau \left(\sum_{\mu_i} \hat{n}_{\mu_i} \right) P_{\mu_2}D'_{\mu_2}, \\ \hat{n}_{\mu_3} &\approx NP_{\mu_3}D'_{\mu_3} - \tau \left(\sum_{\mu_i} \hat{n}_{\mu_i} \right) P_{\mu_3}D'_{\mu_3}, \\ &\dots \\ \hat{n}_{\mu_r} &\approx NP_{\mu_r}D'_{\mu_r} - \tau \left(\sum_{\mu_i} \hat{n}_{\mu_i} \right) P_{\mu_r}D'_{\mu_r}.\end{aligned}\quad (9)$$

The $\tau(\sum_{\mu_i} \hat{n}_{\mu_i})$ represent the total number of pulses in the dead time interval and we can estimate the discarded pulses of each state $\tau(\sum_{\mu_i} \hat{n}_{\mu_i})P_{\mu_r}$. The formulas in Eq. (9) are similar to Eq. (2). Adding up these terms,

$$\sum_{\mu_i} \hat{n}_{\mu_i} = N \sum_{\mu_i} P_{\mu_i}D'_{\mu_i} - \tau \left(\sum_{\mu_i} P_{\mu_i}D'_{\mu_i} \right) \left(\sum_{\mu_i} \hat{n}_{\mu_i} \right), \quad (10)$$

we find the total number of detection responses of all states as

$$\sum_{\mu_i} \hat{n}_{\mu_i} = \frac{N(\sum_{\mu_i} P_{\mu_i}D'_{\mu_i})}{1 + \tau \sum_{\mu_i} P_{\mu_i}D'_{\mu_i}}. \quad (11)$$

Substituting Eq. (11) into Eq. (9), and getting the \hat{n}_{μ_i} ,

$$\hat{n}_{\mu_i} = \frac{NP_{\mu_i}D'_{\mu_i}}{1 + \tau(\sum_{\mu_i} P_{\mu_i}D'_{\mu_i})}. \quad (12)$$

After correcting, the gains are given by a general formula:

$$\hat{D}_{\mu_i} = \frac{D'_{\mu_i}}{1 + \tau \sum_{\mu_i} P_{\mu_i}D'_{\mu_i}} \quad (13)$$

where μ_i [$\mu_i \in (\mu_1, \mu_2, \mu_3, \dots, \mu_r)$].

Here, what is worthy to be mentioned is that our model can be extended to realize any QKD protocols with multiple

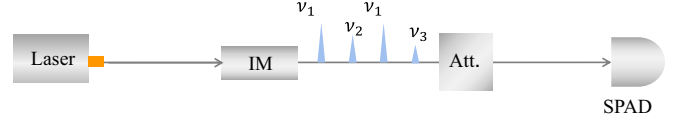


FIG. 3. Experimental setup. IM, intensity modulator; Att., variable optical attenuator; SPAD, detector.

decoy states and shows great compatibility with any single-photon avalanche diode detectors in practice. What is more, our formula is straightforward and comprehensible.

III. EXPERIMENTAL VERIFICATION

In order to make our model more convincing, we used a simple experiment to verify our model. As is shown in Fig. 3, it is our experimental setup. The intensity modulator is used to modulate the ν_1 , ν_2 , and ν_3 intensity. These light pulses pass through an optical attenuator, with which we simulate a transmission loss of $L = 20$ km of optical fiber. Some important experimental parameters are listed in Table I.

We calculate the \hat{D}_{ν_i} of each state in theory, in Monte Carlo simulations and experimentally. \hat{D}_{ν_i} is the gain after correcting the dead time and afterpulse. In theory, the \hat{D}_{ν_i} is given by Eq. (13).

The results are presented in Fig. 4. We introduce three intensities with fixed probabilities, and set the dead time as 5, 10, and 20 gates as examples. Theoretical values are in lines, experimental results are in asterisks, and the Monte Carlo simulation results are in circles. The theoretical values of the gain \hat{D}_{ν_i} provided by our model are in good agreement with the value measured by experiment. It proves that our model is reasonable to accurately describe the dead time and afterpulse, and can estimate the gain of each state precisely. It can provide more precise analytical reference for practical experiment. Also the Monte Carlo simulation results agree with the experimental results. It proves that it is reliable to use Monte Carlo simulation to simulate the real experiment.

IV. RESULTS

In this section, we begin with the Monte Carlo method to simulate the detection process in the three-intensity decoy-state BB84 QKD [35] as an example. The detailed simulation process is given in Appendix B. After Monte Carlo simulation, we can obtain the statistic of detection responses of each state type. It is accessible for us to calculate the actual detection probability, QBER, and other information through statistical results. The results of the numerical simulation are presented and discussed.

TABLE I. Experimental parameters: N is the total number of pulses, Y_0 is the dark count rate, ν_i are the intensities of each state, P_{ν_i} are the corresponding selecting probabilities, and η_D is the detection efficiency of our SPAD.

N	Y_0	ν_i	P_{ν_i}	η_D
10^9	1.6×10^{-5}	0.5 0.3 0.1	0.6 0.1 0.3	0.18

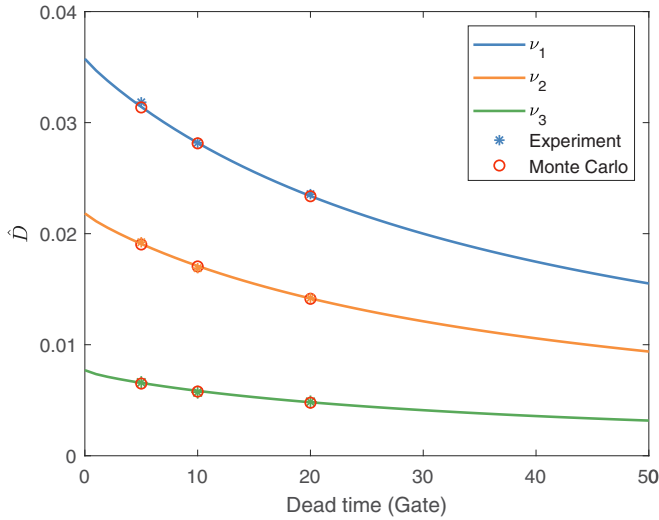


FIG. 4. The comparison between our model, Monte Carlo simulation, and experimental results. From the top down, the three lines correspond to the gains of ν_1 , ν_2 , and ν_3 in theory. Experimental results are in asterisks, and the Monte Carlo simulation results are in circles.

Some other important experimental parameters are listed in Table II. The calculations of the SKR are explained in Ref. [35] and discussed in Appendix A. Moreover, the full parameter optimization is used.

Figure 5 shows the SKRs in different situations. The red line presents the situation that the afterpulse and dead time are both neglected in the isolated model. The optimal parameters are substituted due to the reality that SPADs have inherent dead time and afterpulse properties in practice, as is shown in blue line. The yellow line shows the SKR of our model. To validate the reliability of our model, the optimal parameters of our dependency model and isolated model at $L = 30, 60, 100$ km are substituted into the Monte Carlo simulation in solid circles and squares, respectively. The theoretical results and the Monte Carlo simulation results are highly coincident, which suggests that our model is realistic. Moreover, the solid circles agree with the blue line but are away from the red line, which means that the previous isolated model is skewed far from the practical situation. Moreover, the solid squares almost coincide with the yellow line, which reveals the precision of our dependency model. In a word, our model is practical and necessary.

Comparing the red line and blue line in Fig. 5, it is obvious that the SKR decreases greatly, which means a worse performance of the QKD system. This situation gives a biased

TABLE II. Experimental parameters: N is the total number of pulses sent by Alice, τ is the dead time, e_{mis} is the misalignment-error probability, Y_0 is the dark count rate, f is the error-correction efficiency, and ϵ_{sec} and ϵ_{cor} are the security parameters used in the secret-key-rate formula.

N	τ	e_{mis}	Y_0	f	ϵ_{sec}	ϵ_{cor}
10^9	5	5×10^{-3}	6×10^{-7}	1.16	10^{-9}	10^{-15}

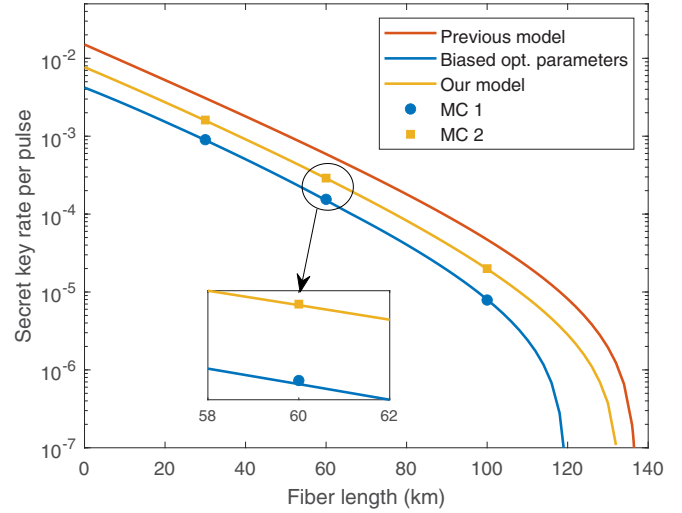


FIG. 5. The secret key rates as the function of fiber length in different cases. The secret key rate of the isolated model after full parameter optimization is in red (upper) line. The optimization parameters in the isolated model are substituted into the reality that exists at dead time and afterpulse, which is in blue (lowest) line. The secret key rate of our dependency model is in yellow (middle) line. Solid circles and squares represent the Monte Carlo simulation results in the dependency model and in the isolated model respectively. The inset is a partial enlargement.

simulated value of gains and results in a skewing optimal parameter reference. It demonstrates that the inaccurate isolated model is a stumbling stone that hinders people from finding an accurate optimal parameter reference for practical application and further theoretical analysis. The isolated model contributes to a worse practical QKD system, failing to perform its full potential.

As is shown in Fig. 5, the SKR of our model in yellow line is lower than that in red line. The reason is that afterpulse introduces QBERs. Meanwhile, though setting dead time will decrease the QBER induced by afterpulse, the count rate decreases at the same time. But it is still higher than the blue line.

To further improve system performance, we analyze the SKR as a function of the dead time in the cases of different values of L , as is shown in Fig. 6. With the increase of dead time, there is a sharp increase when dead time τ is small. Then, a slight rise and a steady decline follow. When $\tau = 0$, the SKRs are low. The reason is that the QBERs induced by afterpulse are high. And because the afterpulse rate decays exponentially in time, after setting dead time, the QBERs decline greatly, which makes the SKRs increase sharply.

As can be seen from Fig. 6, longer dead time is not better. Using our model, the optimal dead time can be obtained according to the actual experimental environment. With the increase of dead time, most of the carriers in traps in a SPAD have released in this interval, especially when the magnitude of the dead time can be equal to or greater than the trap lifetime. The probability of afterpulse becomes very low, thus we have low QBER. However, the increase of dead time means a reduction of count rate, which may lead to a decrease of the SKR. So longer dead time is not always better. When the dead

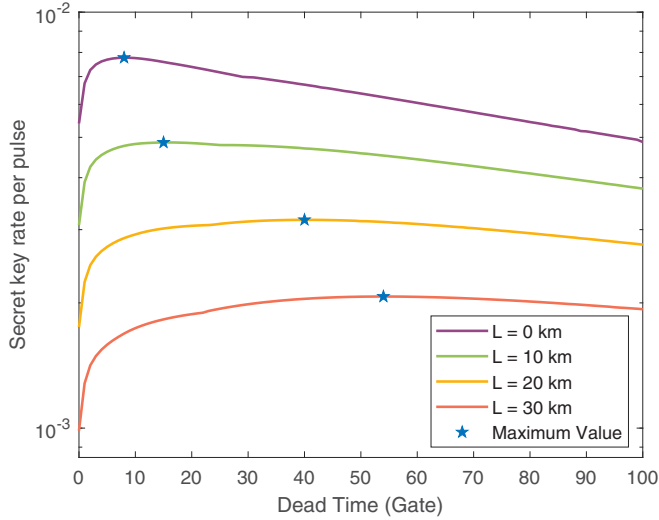


FIG. 6. The secret key rate of our model as a function of the dead time at different transmission distances. The curves from top to bottom represent the secret key rates of $L = 0, 10, 20,$ and 30 km, respectively. To make it clear, the pentagrams are used to represent the optimal values of dead time in different distance regimes.

time is too long, because the afterpulse rate \hat{p} is already very low, further increasing the dead time will not only have little effect on reducing QBER and improving the performance of the system, but will make the system worse because of the reduction of the count rate. Dead time is a parameter that needs to be optimized. Thus, a sound dead time plays an important role in further improving system performance.

As is shown in Fig. 6, we have simulated the optimal dead time in different distance regimes. And we find that the optimal dead time at long distance is longer than that at short distance. The increase in transmission distance will lead to a decrease in the count rate triggered by light pulses. And the light count is randomly distributed, thus the light-count distribution is going to be more dispersed in the longer-distance regime, while the distribution of the afterpulse always tends to be immediately adjacent to the previous response. Therefore, as the transmission distance increases, the influence of the dead time on the light counts will decrease, while the effect on the afterpulse remains almost constant. On the other hand, with the increase of transmission distance, the QBER induced by afterpulse will gradually become dominant in the SKR. So comparing with the case of short transmission distance, the suppression of the afterpulse become more significant, resulting in longer optimal dead time. In different cases, the optimal dead time is different, and our model can help users to choose a proper dead time and analyze the effect on the real QKD system.

According to the results, our model reveals good compatibility to afterpulse and dead time. Although the QBER is introduced by the afterpulse and the count rate decreases due to setting dead time, our dependency model still shows great advantage in balancing the relation between them. Our dependency model help users to evaluate the optimal parameters and provide a better performance of the QKD system. In contrast, the previous isolated model will mislead the simulation and

degrade the practical system performance. Meanwhile, a reasonable dead time is positive for further increasing the SKR and constructive to the application of higher-performance QKD systems.

V. CONCLUSION

In conclusion, we develop an improved dead time and afterpulse model named the “dependency model” to evaluate more accurate gains. Afterpulse ignites the detection responses randomly while the dead time can reduce the negative impact on SKR. In addition, we theoretically analyze and evaluate the gap of the SKRs between the isolated model and our dependency model in the same condition. The performance of the isolated model gets worse while our model is superior, not only in providing optimized parameters accurately, but also in a better system performance. Furthermore, we present the SKRs as a function of the dead time at different fixed distances. The result shows that the SKR first grows and then decreases with the adding of dead time. The dependency model guides people to choose proper dead time to further improve the performance of the QKD systems. Therefore, our model is proven to be compatible with the dead time and afterpulse in practical QKD systems.

First and foremost, high SKR is significant to expand the application of QKD. The SKR can be improved by reducing the QBER and increasing the count rate. The proposed model can reduce the QBER caused by the afterpulse in the method of setting the dead time, and improve the count rate as much as possible by choosing decoy parameters and the dead time reasonably. Our model is readily comprehensible and plays an important role in the practical application and deployment of QKD systems.

ACKNOWLEDGMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grants No. 62271463, No. 61961136004, No. 62171424, and No. 62105318), and China Postdoctoral Science Foundation (2021M693098).

APPENDIX A: CALCULATION OF SECRET KEY RATE

In real-word experiments, to give full play to the best performance of QKD system, users always select a group of optimal parameters including selecting the intensities of states as well as the probability of different intensities and bases, according to the actual experimental environment. The secret key rate R is given by

$$R = \frac{l}{N} \quad (\text{A1})$$

where

$$l = s_{X,0} + s_{X,1}[1 - h(e_{X,1})] - \lambda_{\text{EC}} - 6 \log_2 \frac{21}{\epsilon_{\text{sec}}} - \log_2 \frac{2}{\epsilon_{\text{cor}}} \quad (\text{A2})$$

where $h(x) = -x \log_2 x - (1-x) \log_2(1-x)$ is the binary entropy function. The $s_{X,0}$ and $s_{X,1}$ denote the number of the vacuum events and the number of the single-photon events in the X basis, which are given by

$$s_{X,0} = \tau_0 \frac{\mu_2 F^-(\mu_3, n_{X,\mu_3}) - \mu_3 F^+(\mu_2, n_{X,\mu_2})}{\mu_2 - \mu_3} \quad (\text{A3})$$

and

$$s_{X,1} = \frac{\tau_1 \mu_1}{\mu_1(\mu_2 - \mu_3) - \mu_2^2 + \mu_3^2} \times \left\{ F^-(\nu_1, n_{X,\mu_2}) - F^+(\mu_3, n_{X,\mu_3}) - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left[F^+(\mu_1, n_{X,\mu_1}) - \frac{s_{X,0}}{\tau_0} \right] \right\}, \quad (\text{A4})$$

where $\tau_n = \sum_{\mu_i=\mu_1, \mu_2, \mu_3} e^{-\mu_i} \mu_i^n P_{\mu_i} / n!$ is the probability that Alice sends a n -photon state, and the $n_{X,\alpha}^\pm$ is an intermediate variable corresponding to Hoeffding's inequality that is given by

$$F^\pm(\mu_i, n_{X,\mu_i}) = \frac{e^{\mu_i}}{P_{\mu_i}} \left[n_{X,\mu_i} \pm \sqrt{\frac{n_X}{2} \ln \frac{21}{\epsilon_{\text{sec}}}} \right], \quad (\text{A5})$$

where $n_X = \sum_{\mu_i} n_{X,\mu_i}$. The n_{X,μ_i} is given by Eq. (6). In addition, we also calculate the phase error rate associated with the single-photon events:

$$e_{X,1} = \frac{v_{Z,1}}{s_{Z,1}} + \gamma \left(\epsilon_{\text{sec}}, \frac{v_{Z,1}}{s_{Z,1}}, s_{Z,1}, s_{X,1} \right), \quad (\text{A6})$$

where

$$v_{Z,1} = \tau_1 \frac{F^+(\mu_2, m_{Z,\mu_2}) - F^-(\mu_3, m_{Z,\mu_3})}{\mu_2 - \mu_3} \quad (\text{A7})$$

and

$$\gamma(a, b, c, d) = \sqrt{\frac{(c+d)(1-b)b}{cd \log 2} \log_2 \left(\frac{c+d}{cd(1-b)b} \frac{21^2}{a^2} \right)}. \quad (\text{A8})$$

The $\lambda_{\text{EC}} = n_X f h(E_X)$ is the consumption of the information in error correction, f is the efficiency factor of the error correction, and ϵ_{sec} and ϵ_{cor} are the security parameters.

APPENDIX B: MONTE CARLO SIMULATION

We use Monte Carlo simulation to simulate the detection process to identify the validity of our dependency model. Alice randomly selects different intensities, $\mu_i \in (\mu_1, \mu_2, \mu_3, \dots, \mu_r)$, with its corresponding probability P_{μ_i} , respectively, where $P_{\mu_i} \in (P_{\mu_1}, P_{\mu_2}, P_{\mu_3}, \dots, P_{\mu_r})$, and randomly encodes her qubits in ω basis with the probability of P_ω , where $P_\omega \in (P_X, P_Z)$. Alice sends her qubits to Bob via the optical fibers with an attenuation coefficient of 0.2 dB/km. And the transmittance η_{ch} is expressed by $10^{-0.2L/10}$. Bob uses the detection program to receive the signals and decodes the qubits. If the detector responds, perform dead time operation, otherwise determine whether the afterpulse elicits a response or not based on the previous response situation. In the end, we obtain the statistic of detection responses, and calculate and analyze the information we need. The detailed simulation

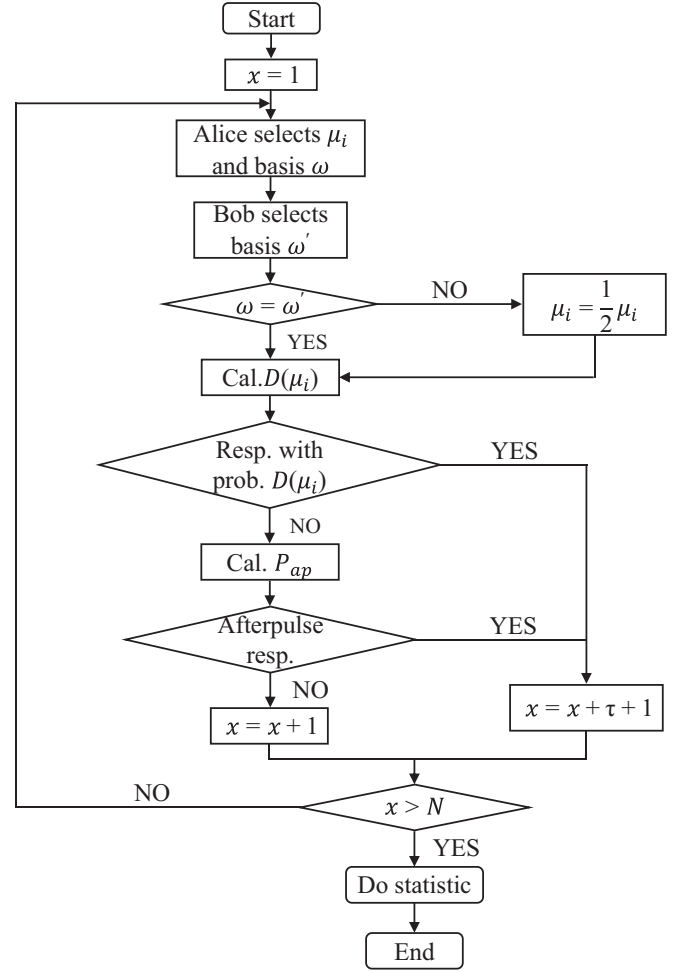


FIG. 7. Pseudocode of Monte Carlo simulation.

process is shown in Fig. 7. The x is the round number, $D(\mu_i)$ corresponds to Eq. (1), and P_{AP} is the afterpulse contribution related to its previous responses.

APPENDIX C: DERIVATION OF AFTERPULSE PROBABILITY

P_{AP} is the response probability triggered by afterpulse, which is related to all previous response events. Because of the non-Markovian property of afterpulse, historical response events will contribute to P_{AP} at the current detection window, thus

$$P_{\text{AP}} = \sum_{i=\tau+1}^k D_i \hat{p}(i) \quad (\text{C1})$$

where D_i is the detector response probability of the i th detection and $\hat{p}(i)$ is the afterpulse rate coefficient. In other words, $\hat{p}(i)$ indicates that after a response event it may cause the afterpulse occurrence with a probability $\hat{p}(i)$ at the i th succeeding detection window. Thus, $D_i \hat{p}(i)$ is the afterpulse contribution from the i th response event. P_{AP} represents the sum of the effects of all previous response events on the afterpulse at the current detection window.

The detection response can be ignited by light pulse, dark count, and afterpulse. The afterpulse ignited by a light pulse or dark count is called the first-order afterpulse. Therefore, the first-order afterpulse probability, $P_{AP}^{(1)}$, is given by

$$P_{AP}^{(1)} = \sum_{i=\tau+1}^k \hat{p}(i) D_i. \quad (C2)$$

D_i is the response probability triggered by the light pulse or dark count:

$$D_i = \tilde{D} = \sum_{\mu} P_{\mu} \tilde{D}_{\mu}, \quad (C3)$$

where \tilde{D}_{μ} is the weighted average of the gain of varying decoy states and is given by

$$\tilde{D}_{\mu} = (P_X^2 + P_Z^2) \left\{ 1 - \left[1 - \frac{1}{2}(1 - e^{-\mu\eta}) \right] (1 - Y_0) \right\} + 2P_X P_Z [1 - e^{-\mu\eta/2} (1 - Y_0)]. \quad (C4)$$

The afterpulse will ignite afterpulse as well, which are collectively called the high-order afterpulse. For accuracy and authenticity, we have to consider these higher-order afterpulses. Therefore,

$$\begin{aligned} P_{AP}^{(2)} &= \sum_{i=\tau+1}^k \hat{p}(i) P_{AP}^{(1)} = q^2 \tilde{D}, \\ P_{AP}^{(3)} &= \sum_{i=\tau+1}^k \hat{p}(i) P_{AP}^{(2)} = q^3 \tilde{D}, \\ &\dots \\ P_{AP}^{(l)} &= \sum_{i=\tau+1}^k \hat{p}(i) P_{AP}^{(l-1)} = q^l \tilde{D}. \end{aligned} \quad (C5)$$

P_{AP} is given by

$$P_{AP} = \sum_{l=1}^{\infty} P_{AP}^{(l)} = \frac{q}{1-q} \tilde{D}, \quad (C6)$$

where

$$q = \sum_{i=\tau+1}^j \hat{p}(i) \quad (C7)$$

is the overall afterpulse rate and meets $q < 1$.

APPENDIX D: MEASUREMENT OF $\hat{p}(i)$

With the development of experimental techniques, there are various methods to measure the afterpulse rate coefficient $\hat{p}(i)$ accurately. Here we use the method in Ref. [36]. In our paper, the data are collected based on the scheme, the setup of which is shown in Fig. 8. The pulsed laser source and the single-photon detector are triggered by clock signals of 1 and 50 MHz, respectively. The pulsed laser generates pulse trains spaced 1 μ s apart, while the SPAD opens its gate every 20 ns. That means only one trigger signal arrives at the detector in every 50 detection windows. By using an attenuator, the mean photon number of a coherent pulse which

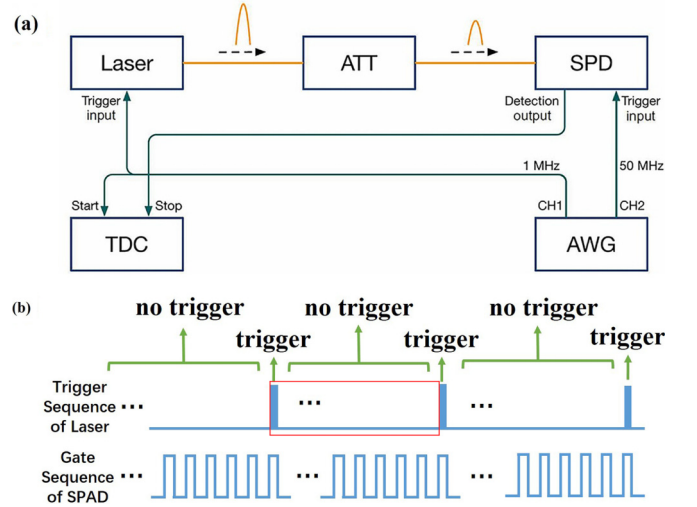


FIG. 8. (a) Schematic diagram of the measurement of the overall afterpulse rate \hat{p}_{AP} . Laser, short-pulse laser source; ATT, attenuator; SPD, single-photon detector; TDC, time-to-digital converter; AWG, arbitrary waveform generator. (b) Schematic diagram of the trigger sequence and detection windows. The repetition frequency of the laser is different from the detector, for example, the pulsed laser source and the single-photon detector are triggered by clock signals of 1 and 50 MHz, respectively. That means only one trigger signal arrives at the detector in every 50 detection windows.

is generated by the laser is attenuated to 0.1. To measure the required data, a time-to-digital converter is started by a clock signal, which is the same as the trigger signal of the laser, and stopped by the response signals of the detector. In each period of start, there is a time tag with a constant delay to the start signal according to pulse-emitting events, as is shown in Fig. 8(b).

Here, we only measure the counts at a time tag as is shown in Fig. 8(b) in the red box. The count, denoted by C_{dd} , contains a successful detection response in a detection window.

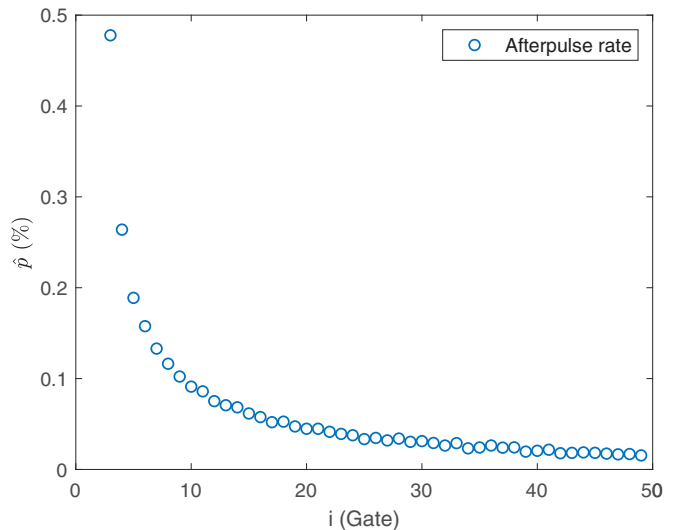


FIG. 9. The measured afterpulse rate at each gate, $p(i)$. The SPAD detector opens its gate every 20 ns.

There are sequent detection windows created by the afterpulse responses and dark counts, the count of which is denoted by $C_{ad}(i)$ at each detection window, because the detector opens its gate without an incident pulse. In addition, the dark counts, C_d , can be obtained by counting the detector responses with the extinct laser source. Then, the afterpulse rate $\hat{p}(i)$ can be derived:

$$\hat{p}(i) = \frac{C_{ad}(i) - \frac{C_d}{50} \times (50 - 1)}{C_{dd}}. \quad (\text{D1})$$

By this method, we can obtain the afterpulse rate coefficient $\hat{p}(i)$ accurately, which is easy to achieve.

The result is shown in Fig. 9. In our simulations, we use the measured \hat{p} to determine the value of the overall afterpulse rate q and afterpulse response probability P_{AP} . And the \hat{p} decays quickly with time (with gates increasing). As an example, when the dead time is set to be five gates, the overall afterpulse rate q is about 2.2%, and when the dead time is set to be 20 gates, the q is about 1.12%. With the increase of dead time, P_{AP} decreases. And the P_{AP} is related to the actual pulse intensity and other parameters, so there will be some differences in different cases, as is shown in Eq. (C6). From the value of q , we can also roughly judge the effect of the afterpulse on the system. Moreover, our model is applicable to any detector type and can be used to estimate the real gains of QKD protocols.

APPENDIX E: EFFECT OF AFTERPULSE IN HIGH-SPEED SYSTEMS

We have simulated the P_{AP} as a function of repetition rate at different transmission distances, as is shown in Fig. 10 in blue lines. At high repetition rate, the afterpulse increases sharply. It will be more prominent in higher-speed systems, especially when the value of P_{AP} is comparable to the gains of decoy states; thus the QBER of the system will greatly increase, which will degrade the QKD system performance.

Due to the nonideality of actual SPADs, the afterpulse and the dark counts are inevitable. In practice, users cannot distinguish what causes the response. Dark counts and afterpulse

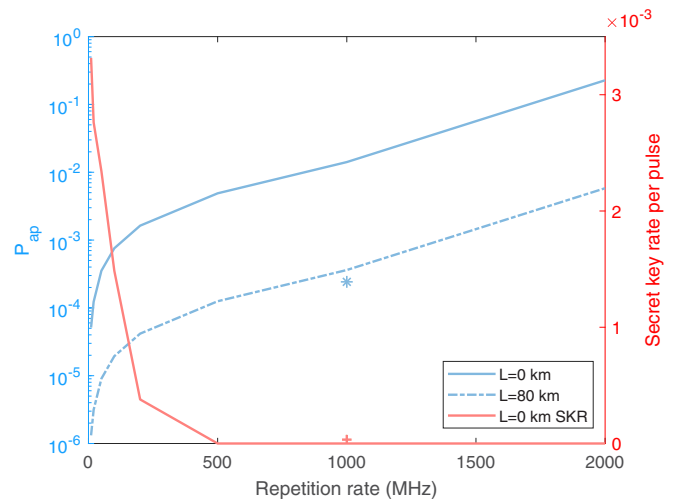


FIG. 10. The afterpulse probability P_{AP} as a function of the repetition rate of the QKD system at different transmission distances in blue lines. The secret key rate as a function of repetition rate of the QKD system at $L = 0$ km. When the dead time of the 1-GHz system is increased to 1000 ns, the P_{AP} and the corresponding SKR are marked by an asterisk and a crisscross, respectively.

will lead to error counts which will degrade the performance of QKD systems, especially the afterpulse effect. Here, we simulate SKR at $L = 0$ km, as is shown in Fig. 10 in red line. Other parameters are the same as in Table I. When the repetition rate is 50 MHz, the SKR is 2.34×10^{-3} per pulse, while at 1 GHz the SKR is zero and the P_{AP} is about 1.41×10^{-2} . In this case, the value of P_{AP} is on the same order of magnitude as the value of the gain of the decoy states. Thus, the error count induced by afterpulse is very high. From that, we find that the afterpulse effect has more influence on high-speed systems. To improve the high-speed system, longer dead time is needed. When dead time in a 1-GHz system is increased to 1000 ns, the P_{AP} is about 2.42×10^{-4} and the corresponding SKR is about 3.33×10^{-5} per pulse, as is shown in Fig. 10 by an asterisk and a crisscross, respectively. In higher-speed systems, longer dead time is needed to mitigate the effect of the afterpulse.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, Piscataway, NJ, 1984), p. 175.
- [2] A. K. Ekert, in *Quantum Measurements in Optics* (Springer, New York, 1992), pp. 413–418.
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [4] H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
- [5] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
- [6] R. Renner, *Int. J. Quantum Inform.* **06**, 1 (2008).
- [7] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, in *Proceedings of the International Symposium on Information Theory, 2004, ISIT 2004* (IEEE, Piscataway, NJ, 2004), p. 136.
- [8] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [9] H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [10] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [11] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, *Phys. Rev. A* **98**, 062323 (2018).
- [12] A. Laing, V. Scarani, J. G. Rarity, and J. L. O’Brien, *Phys. Rev. A* **82**, 012304 (2010).
- [13] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, *Nat. Photonics* **10**, 312 (2016).
- [14] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, *Nature (London)* **549**, 43 (2017).

- [15] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li *et al.*, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [16] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin *et al.*, *Phys. Rev. Lett.* **124**, 070501 (2020).
- [17] G. Brassard, N. L utkenhaus, T. Mor, and B. C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
- [18] N. L utkenhaus, *Phys. Rev. A* **61**, 052304 (2000).
- [19] W.-Y. Hwang, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [20] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Phys. Rev. A* **72**, 012326 (2005).
- [21] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, *Phys. Rev. A* **88**, 062339 (2013).
- [22] X. Ma, C.-H. F. Fung, and M. Razavi, *Phys. Rev. A* **86**, 052305 (2012).
- [23] F. Xu, H. Xu, and H.-K. Lo, *Phys. Rev. A* **89**, 052333 (2014).
- [24] Z. Li and K. Wei, *Quantum Engineering* **2022**, 9717591 (2022).
- [25] C.-M. Zhang, J.-R. Zhu, and Q. Wang, *Phys. Rev. A* **95**, 032309 (2017).
- [26] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, *Light Sci. Appl.* **4**, e286 (2015).
- [27] H. Li, H. Jiang, M. Gao, Z. Ma, C. Ma, and W. Wang, *Phys. Rev. A* **92**, 062344 (2015).
- [28] F.-X. Wang, W. Chen, Y.-P. Li, D.-Y. He, C. Wang, Y.-G. Han, S. Wang, Z.-Q. Yin, and Z.-F. Han, *J. Lightwave Technol.* **34**, 3610 (2016).
- [29] A. Yoshizawa, R. Kaji, and H. Tsuchida, *Opt. Express* **11**, 1303 (2003).
- [30] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, *IEEE J. Sel. Top. Quantum Electron.* **21**, 168 (2014).
- [31] G.-J. Fan-Yuan, C. Wang, S. Wang, Z.-Q. Yin, H. Liu, W. Chen, D.-Y. He, Z.-F. Han, and G.-C. Guo, *Phys. Rev. Appl.* **10**, 064032 (2018).
- [32] H. Georgieva, A. Meda, S. M. Raupach, H. Hofer, M. Gramegna, I. P. Degiovanni, M. Genovese, M. L opez, and S. K uck, *Appl. Phys. Lett.* **118**, 174002 (2021).
- [33] A. V. Losev, V. V. Zavodilenko, A. A. Koziy, A. A. Filyaev, K. I. Khomyakova, Y. V. Kurochkin, and A. A. Gorbatsevich, *IEEE J. Quantum Electron.* **58**, 1 (2022).
- [34] S. Cova, A. Lacaita, and G. Ripamonti, *IEEE Electron Device Lett.* **12**, 685 (1991).
- [35] Charles Ci Wen Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, *Phys. Rev. A* **89**, 022307 (2014).
- [36] G.-J. Fan-Yuan, J. Teng, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, *Phys. Rev. Appl.* **13**, 054027 (2020).