

Afterpulse Analysis for Quantum Key Distribution

Guan-Jie Fan-Yuan,^{1,2,3} Chao Wang,^{1,2,3} Shuang Wang,^{1,2,3,*} Zhen-Qiang Yin,^{1,2,3,†} He Liu,^{4,5}
Wei Chen,^{1,2,3} De-Yong He,^{1,2,3} Zheng-Fu Han,^{1,2,3} and Guang-Can Guo^{1,2,3}


¹*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China*

²*CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

³*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*

⁴*Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*

⁵*University of Chinese Academy of Sciences, Beijing 100049, China*

 (Received 31 May 2018; revised manuscript received 7 November 2018; published 13 December 2018)

The afterpulse effect is an intrinsic characteristic of the single-photon avalanche photodiode that has been widely used in quantum key distribution (QKD). As QKD systems move into the gigahertz regime, the afterpulse effect is no longer ignorable, which will lead to a great deviation compared with the existing analytical model. Here we develop an analytical model to make QKD systems more afterpulse compatible. In addition, we obtain the secure key rate for our model with the analysis of statistical fluctuation using Hoeffding's inequality and Azuma's inequality. Our results show that the optimized parameters of the afterpulse-compatible model can provide a much higher key rate than the optimized parameters of the previous afterpulse-omitted model in the same situation.

DOI: [10.1103/PhysRevApplied.10.064032](https://doi.org/10.1103/PhysRevApplied.10.064032)

I. INTRODUCTON

Quantum key distribution (QKD) [1,2] can share a private key securely between two parties. Unlike classical cryptography, the security of QKD relies on the principles of quantum physics, with any eavesdropping on a quantum channel being detected inevitably by extra signal disturbance. Furthermore, the private key can provide unconditional secure communication combined with the one-time pad [3].

In practice, since the first QKD protocol proposed in 1984 by Bennett and Brassard [1], a great number of QKD experiments [4–10] have been reported and commercial QKD devices [11–14] have been made available. The goals of QKD [15] such as unconditional security and high-speed systems never changed over the past three decades. However, the imperfections of practical devices have blocked the efforts of researchers to achieve their goals [16], such as the afterpulse effect of a single-photon avalanche detector (SPAD) [17–19].

Because of high quantum efficiency, low price, and great robustness, the use of SPADs is the mainstream solution for single-photon detection in practical QKD [20]. One of the most-important effects in SPADs is the afterpulse. Afterpulses come from the release of carriers that

are created by former ignition avalanche and trapped by defects and impurities in the multiplication layer of the SPAD [20]. The afterpulse probability, P_{ap} , is related to the avalanche duration time, hold-off time, lifetime of detrapping carriers, etc. Unfortunately, high-speed QKD systems [10,21] require a high frequency of detection and a short hold-off time; hence P_{ap} will significantly increase with the system working frequency.

The afterpulse effect has considerable impacts on high-speed QKD systems. One of them (the impacts of afterpulse effect on QKD systems) is blinding existing analytical models from reality. The gain and error rate derived from afterpulse-omitted models are far from real values. Especially for the widely used decoy-state method [22–25], the afterpulse of the signal state contributes greatly to the gain and error rate of decoy states. In addition, biased results will mislead further theoretical analysis. Besides, the optimized parameters from the biased model, such as the intensity and selection probability of decoy states, will degrade real system performance. Moreover, if the finite-size effects are taken into account in QKD systems, which focus on practical security in the finite-resource regime, the final secure key rate would also be sensitive to additional detections by the afterpulse effect. Therefore, an accurate model is needed.

In this paper, we develop an afterpulse-compatible model in Sec. II. The afterpulse is patched into the events

*wshuang@ustc.edu.cn

†yinzq@ustc.edu.cn

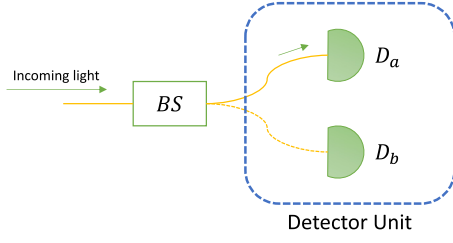


FIG. 1. The dual-detector receiver. A beam splitter (BS) is used to distinguish bit 0 and bit 1 in phase-coding QKD (polarization-coding scheme replaces the BS with a polarizing BS). When Alice and Bob choose the same basis, the light pulse goes to only one detector, which is marked. D_a , detector a; D_b , detector b.

to which the detector responds; therefore, there are three sources of detector responses: light pulse, dark count, and afterpulse. In addition, we use Hoeffding's inequality and Azuma's inequality to bound parameters for fluctuation analysis in Sec. III. Then we present the simulation results and a discussion in Sec. IV, which show that our model is more tolerant of P_{ap} than the afterpulse-omitted model for all approaches. A summary is provided in Sec. V.

II. MODEL

In previous QKD models [23,25], the detection system, regardless of the number of detectors, was considered as a unit. However, the afterpulse behavior of the detector depends only on its own properties, and therefore the detectors must be analyzed independently. Here we take a widely used dual-detector system for complete qubit measurement as the detection unit as shown in Fig. 1.

In the dual-detector system, we call the detector that receives pulses “detector a” and we call the other one “detector b.” Furthermore, the gain and quantum-bit bit error rate (QBER) are given by

$$Q_\mu = p_\mu^a(1 - p_\mu^b) + (1 - p_\mu^a)p_\mu^b, \quad (1)$$

$$E_\mu Q_\mu = e_d p_\mu^a(1 - p_\mu^b) + (1 - e_d)(1 - p_\mu^a)p_\mu^b, \quad (2)$$

where p_μ^a and p_μ^b are response probabilities of detectors a and b, respectively, when the pulses are prepared with intensity μ , and e_d is the misalignment-error probability.

Without the afterpulse effect, p_μ^a and p_μ^b can be written as [26]

$$p_\mu^a = 1 - e^{-\mu\eta}(1 - Y_0), \quad (3)$$

$$p_\mu^b = Y_0, \quad (4)$$

where μ is the intensity of the coherent source, η is the overall transmission of the channel, and Y_0 is the background counting rate. To adapt the model to afterpulses,

we change the expressions for p_μ^a and p_μ^b to

$$p_\mu^a = p_\mu^{a1} + p_\mu^{a2},$$

$$p_\mu^{a1} = 1 - e^{-\mu\eta}(1 - Y_0), \quad (5)$$

$$p_\mu^{a2} = (1 - p_\mu^{a1})P_{\text{ap}},$$

$$p_\mu^b = p_\mu^{b1} + p_\mu^{b2},$$

$$p_\mu^{b1} = Y_0, \quad (6)$$

$$p_\mu^{b2} = (1 - p_\mu^{b1})P_{\text{ap}},$$

where p_μ^{a1} and p_μ^{b1} correspond to original response probabilities, p_μ^a and p_μ^b , that are triggered by pulses and dark counts; p_μ^{a2} and p_μ^{b2} are the patched terms that represent the contribution of the afterpulse; and P_{ap} is the probability of the afterpulse.

Previous work [27] shows that the afterpulse of a SPAD is non-Markovian in nature; that is, historical detector responses contribute to P_{ap} :

$$P_{\text{ap}} = \sum_{j=1}^n \hat{Q}_j \hat{p}_j, \quad (7)$$

where \hat{Q}_j is the detector avalanche probability of the j th detection from this detection window, and \hat{p}_j is the corresponding afterpulse rate coefficient, which represents the probability of the afterpulse ignited by the j th avalanche. Here the detector avalanche can be ignited by the light pulse, dark count, and afterpulse.

For the precision and trustworthiness of the afterpulse model, the order of the afterpulse is introduced.

Definition 1 (kth-order afterpulse).—The first-order afterpulse is the afterpulse that is ignited by a light pulse or dark count. The k th-order afterpulse ($k > 1$) is the afterpulse that is ignited by the $(k - 1)$ th-order afterpulse.

According to Definition 1, the probability of a first-order afterpulse, $P_{\text{ap}}^{(1)}$, is given by

$$P_{\text{ap}}^{(1)} = \sum_{j=1}^n \hat{Q}_j^d \hat{p}_j, \quad (8)$$

where \hat{Q}_j^d is the light-pulse and dark-count part of \hat{Q}_j^d . On average, \hat{Q}_j^d is equal to \hat{Q}^d , a weighted average of the gain of varying decoy states:

$$\hat{Q}_j^d = \hat{Q}^d = \sum_{\alpha=\mu, \nu, \dots} P_\alpha \tilde{Q}_\alpha, \quad (9)$$

$$\tilde{Q}_\alpha = (P_X^2 + P_Z^2) \left\{ 1 - \left[1 - \frac{1}{2}(1 - e^{-\mu\eta}) \right] (1 - Y_0) \right\}$$

$$+ 2P_X P_Z [1 - e^{\mu\eta/2}(1 - Y_0)], \quad (10)$$

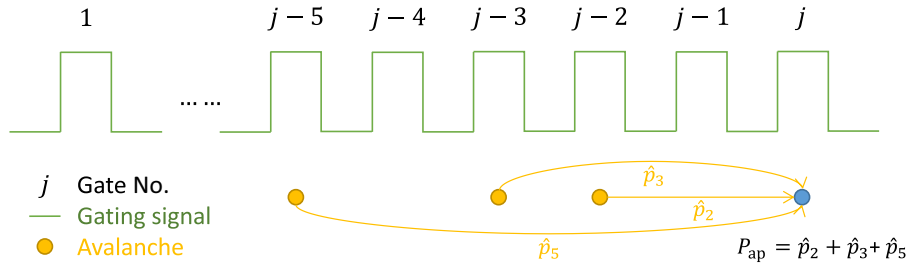


FIG. 2. The non-Markovian property of the afterpulse as an example. Current detection is denoted by j and avalanches are reported in detection windows of $j-2, j-3$, and $j-5$, which are marked as yellow dots. \hat{p}_2, \hat{p}_3 , and \hat{p}_5 are the probability coefficients that represent the former second, third, and fifth avalanche's contribution to current detection. In Eq. (7), avalanches are replaced by their probabilities \hat{Q}_j .

where P_α and \tilde{Q}_α are the selecting probability and response probability of the state of intensity α , respectively, and P_X and P_Z are the probabilities of selecting basis (X and Z) in preparation and measurement. Therefore,

$$P_{\text{ap}}^{(1)} = \sum_{j=1}^n \hat{p}_j \hat{Q}^d = \hat{p} \hat{Q}^d, \quad (11)$$

where $\hat{p} = \sum_{j=1}^n \hat{p}_j$ is the overall afterpulse rate.

Moreover, the probability of the k th-order afterpulse, $P_{\text{ap}}^{(k)}$, is given by the recursion chain

$$\begin{aligned} P_{\text{ap}}^{(2)} &= \sum_{j=1}^n \hat{p}_j P_{\text{ap}}^{(1)} = \hat{p}^2 \hat{Q}^d, \\ P_{\text{ap}}^{(3)} &= \sum_{j=1}^n \hat{p}_j P_{\text{ap}}^{(2)} = \hat{p}^3 \hat{Q}^d, \\ &\dots \\ P_{\text{ap}}^{(k)} &= \sum_{j=1}^n \hat{p}_j P_{\text{ap}}^{(k-1)} = \hat{p}^k \hat{Q}^d. \end{aligned} \quad (12)$$

Then, P_{AP} is given by

$$P_{\text{ap}} = \sum_{k=1}^{\infty} P_{\text{ap}}^{(k)} = \sum_{k=1}^{\infty} \hat{p}^k \hat{Q}^d = \frac{\hat{p}}{1 - \hat{p}} \hat{Q}^d, \quad (13)$$

where $\hat{p} < 1$.

Use of Eqs. (1) and (2) requires independence of the responses of the two detectors. With the help of following theorem, we show that this independence between the responses of two detectors remains valid even when the afterpulse effect is included.

Theorem 1[28]: Let X_1, X_2, \dots, X_n and Y_1, Y_2, \dots, Y_n be independent random variables. Then $Z_1 = g(X_1, X_2, \dots, X_n)$ and $Z_2 = h(Y_1, Y_2, \dots, Y_n)$ are also independent, where g and h are Borel-measurable functions.

According to the previous model, the responses of detectors ignited by a light pulse and dark count are independent. This independence is naturally inherited by our model. We denote those responses as R_1^i and R_2^i , where subscripts 1 and 2 represent detectors 1 and 2, respectively, and superscript i is the sequence number of the detection window.

For the i th detection, the responses can be triggered by a light pulse, dark count, and afterpulse in our model. For detector 1, the contribution of the light pulse and dark count is R_1^i . According to Eq. (8) and the recursive chain equation (12), the contribution of the afterpulse is a function of $R_1^{i-1}, R_1^{i-2}, \dots, R_1^{i-n}$. Therefore, the response of detector 1 is a function of $R_1^i, R_1^{i-1}, \dots, R_1^{i-n}$. Similarly, the response of detector 2 is a function of $R_2^i, R_2^{i-1}, \dots, R_2^{i-n}$. On the basis of Theorem 1, because of the independence between $R_1^i, R_1^{i-1}, \dots, R_1^{i-n}$ and $R_2^i, R_2^{i-1}, \dots, R_2^{i-n}$, the responses of detectors 1 and 2 at the same detection window are independent.

III. CALCULATION OF SECURE KEY RATE

In a real-world experiment, the resources of legitimate users are limited. Statistical fluctuations might enable attacks by an eavesdropper. Therefore, the analysis must be executed in the finite-size regime to ensure security. Specifically, the upper bounds and lower bounds of the gain and error rate must be given to estimate the gain and error rate of single-photon states for evaluation of the final secure key rate [29].

The method to bound the parameters is crucial. The solution must be trustworthy enough for system security and tight enough for high-key-rate performance. In this section, we use two approaches to bound the parameters: one is Hoeffding's inequality [30,31] and the other is Azuma's inequality [32–36]. The results are given in Sec. IV.

With the model presented in the previous sections, the gain and QBER can be obtained by Eqs. (1) and (2). Furthermore, the number of vacuum events s_0 , the number of single-photon events s_1 , and the phase error rate $e_{1,p}$ are

required to calculate the secure key rate R :

$$R = \frac{l_X + l_Z}{N}, \quad (14)$$

where

$$l_\omega = s_0^\omega + s_1^\omega [1 - H_2(e_{1,p}^\omega)] - \lambda_{\text{EC}} - 6 \log_2 \frac{21}{\varepsilon_{\text{sec}}} - \log_2 \frac{2}{\varepsilon_{\text{cor}}}, \quad (15)$$

where N is the total number of pulses (sent by Alice), $\omega \in \{X, Z\}$ represents a basis, $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary Shannon entropy function, $\lambda_{\text{EC}} = n^\omega f_e H_2(E_\omega)$ is the consumption of the information in error correction, f_e is the efficiency factor of the error-correction method used, and ε_{cor} and ε_{sec} are security parameters. All parameters needed can be estimated by analytical formulas [25,31]. For example, the analytical formulas of the three-intensity (μ, ν_1, ν_2) decoy scheme are given by

$$s_0^\omega = \frac{\tau_0}{\nu_1 - \nu_2} \left(\frac{e^{\nu_2} \nu_1 n_{\nu_2}^{\omega+}}{P_{\nu_2}} - \frac{e^{\nu_1} \nu_2 n_{\nu_1}^{\omega-}}{P_{\nu_1}} \right), \quad (16)$$

$$s_1^\omega = \frac{\mu \tau_1}{\mu \nu_1 - \mu \nu_2 - \nu_1^2 + \nu_2^2} \left[\frac{e^{\nu_1} n_{\nu_1}^{\omega-}}{P_{\nu_1}} - \frac{e^{\nu_2} n_{\nu_2}^{\omega+}}{P_{\nu_2}} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left(\frac{e^\mu n_\mu^{\omega+}}{P_\mu} - \frac{s_0^\omega}{\tau_0} \right) \right], \quad (17)$$

$$e_{1,p}^\omega = \frac{\nu_1^{\bar{\omega}}}{s_1^{\bar{\omega}}} + \gamma \left(\varepsilon_{\text{sec}}, \frac{\nu_1^{\bar{\omega}}}{s_1^{\bar{\omega}}}, s_1^{\bar{\omega}}, s_1^\omega \right), \quad (18)$$

where

$$\gamma(a, b, c, d) = \sqrt{\frac{(c+d)(1-b)b}{cd \log 2}} \sqrt{\log_2 \left[\frac{c+d}{cd(1-b)b} \frac{21^2}{a^2} \right]}, \quad (19)$$

$$v_1^\omega = \frac{\tau_1}{\nu_1 - \nu_2} \left(\frac{e^{\nu_1} m_{\nu_1}^{\omega+}}{P_{\nu_1}} - \frac{e^{\nu_2} m_{\nu_2}^{\omega-}}{P_{\nu_2}} \right), \quad (20)$$

ω and $\bar{\omega}$ are different bases (i.e., $\omega = Z$ when $\bar{\omega} = X$ and vice versa), and $n_\alpha^{\omega\pm}$ and $m_\alpha^{\omega\pm}$ are the upper bound and the lower bound of the number of detections and bit error of basis ω and intensity α .

To deal with the correlations between detections introduced by the afterpulse, according to the counterfactual

protocol proposed in Refs. [31,37], the counts and errors can be bounded by Hoeffding's inequality:

$$n_\alpha^{\omega\pm} = n_\alpha^\omega \pm \sqrt{\frac{n^\omega}{2} \ln \frac{21}{\varepsilon_{\text{sec}}}},$$

$$m_\alpha^{\omega\pm} = m_\alpha^\omega \pm \sqrt{\frac{m^\omega}{2} \ln \frac{21}{\varepsilon_{\text{sec}}}}. \quad (21)$$

Furthermore, Azuma's inequality is also able to bound the dependent parameters on the condition that a martingale is constructed by the difference between the sum of detections and its expectation; that is, $n - E(n)$ [34]:

$$n_\alpha^{\omega\pm} = n_\alpha^\omega \pm \sqrt{2n^\omega \ln \frac{21}{\varepsilon_{\text{sec}}}},$$

$$m_\alpha^{\omega\pm} = m_\alpha^\omega \pm \sqrt{2m^\omega \ln \frac{21}{\varepsilon_{\text{sec}}}}, \quad (22)$$

where $n^\omega = \sum_\alpha n_\alpha^\omega$ and $m^\omega = \sum_\alpha m_\alpha^\omega$.

In the numerical simulation, n_α^ω and m_α^ω can be derived by

$$n_\alpha^\omega = NP_\alpha P_\omega Q_\alpha^\omega,$$

$$m_\alpha^\omega = NP_\alpha P_\omega E_\alpha^\omega Q_\alpha^\omega, \quad (23)$$

where $P_\alpha, P_\omega, Q_\alpha^\omega$, and $E_\alpha^\omega Q_\alpha^\omega$ are the ratio of the α state, the selecting probability in the ω basis, the gain of the α state in the ω basis, and the QBER of the α state in the ω basis, respectively.

IV. SIMULATION RESULTS AND DISCUSSION

In this section, we present and discuss the results of the numerical simulation. Here we use the three-intensity-decoy-state protocol in all key-rate calculations. Moreover, full parameter optimization is used. We use experimental parameters similar to those used in Ref. [31] for our numerical simulation. The values of these parameters are listed in Table I. Figure 3 shows the key rate as a function of loss in the case of different values of \hat{p} (0%, 5%) obtained with

TABLE I. Experimental parameters used in the numerical simulations. N is the total number of pulses, f_e is the error-correction efficiency, ε_{sec} and ε_{cor} are the security parameters used in the secure-key-rate formula (e.g., failure probability), Y_0 is the background counting rate, e_d is the misalignment-error probability, and η_{Bob} is the transmittance at Bob's side.

N	f_e	ε_{sec}	ε_{cor}	Y_0	e_d	η_{Bob}
10^9	1.16	10^{-9}	10^{-15}	6×10^{-7}	5×10^{-3}	10%

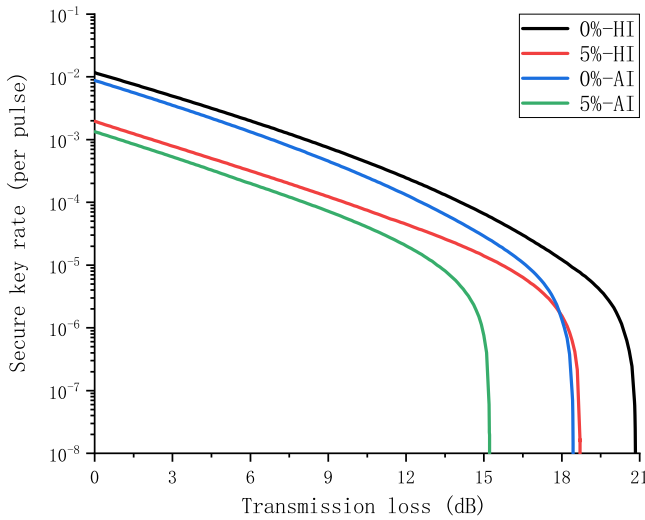


FIG. 3. Optimal secure key rate (per pulse) on a logarithmic scale as a function of transmission loss for different values of \hat{p} obtained with Hoeffding's inequality (HI) and Azuma's inequality (AI).

Hoeffding's inequality and Azuma's inequality (0% corresponds to the afterpulse-omitted model). From no afterpulse to an overall afterpulse rate of 5%, for both bounds of statistical fluctuations, the secure key rates remain the same order of magnitude and the reduction of the limiting secure-communication distance is under 3 dB. Moreover, tighter bounds of Hoeffding's inequality [Eq. (20)] result in a higher secure key rate than Azuma's inequality; the gap widens with increasing transmission loss because the decline in the number of detections amplifies the capability difference between these two concentration inequalities. In summary, despite the afterpulse introducing an additional QBER, the key rate still performs well.

Figure 4, based on fluctuation analysis with Hoeffding's inequality and Azuma's inequality, shows the advantage of our model for secure key rate when the transmission loss and \hat{p} are given. For the parameters that are optimized separately for our afterpulse-compatible model and the previous model, which contains only efficiency and the dark count rate of the detector, the key rate obtained from the former (solid lines) is significantly greater than that obtained from the latter (dashed lines) in the same situation. The gap between them widens with increasing transmission loss for the same high \hat{p} . When the transmission loss is kept constant, the solid lines reveal the growing advantage of the afterpulse-compatible model at higher \hat{p} . Even if \hat{p} is too harsh for the former model's optimal parameters to generate a secure key, the solid line still remains high. Therefore, these gaps imply the susceptibility of a real system to operating parameters and the significance of a vivid analytical model.

In addition, Fig. 5 shows the optimal intensity of the signal state as a function of \hat{p} and reveals the detailed impact

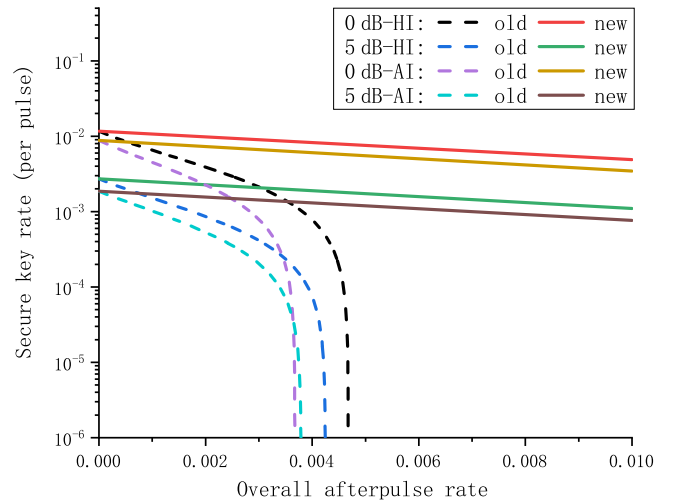


FIG. 4. Comparison between the secure key rates obtained with the optimized parameters of the afterpulse-omitted model (old) and the afterpulse-compatible model (new) as a function of \hat{p} based on the fluctuation analysis with Hoeffding's inequality and Azuma's inequality. The solid red, yellow, green, and brown lines represent the optimal key rates in the afterpulse-compatible model at a channel loss of 0 and 5 dB. The dashed black, violet, blue, and azure lines represent the key rates derived with the optimized parameters of the afterpulse-omitted model in the afterpulse-compatible model at a channel loss of 0 and 5 dB. AI, Azuma's inequality; HI, Hoeffding's inequality.

of the afterpulse on parameter optimization in QKD systems. In the decoy-state protocol, the afterpulse is mainly ignited by the signal state because the gain of decoy states is significantly smaller than the gain of the signal state. Because of the randomness of the afterpulse, the greater the intensity of the signal state, the higher the error rate introduced by the afterpulse. On the other hand, the afterpulse accounts for a significant portion of the gain and QBER of decoy states; therefore, the additional detections can impact the estimations of parameters (e.g., the gain and error rate of single-photon states). Hence, the intensity of the signal state decreases with increasing \hat{p} because of the error rate and the deviation of parameter estimation introduced by the afterpulse.

According to the results, our model can preserve the final secure key rate with the afterpulse effect taken into account, not only for Hoeffding's inequality but also for Azuma's inequality. Although substantial additional error rates are introduced by the afterpulse, the key rate is still satisfactory.

Moreover, for real-world detectors, which are inevitably affected by the afterpulse effect, the reoptimized parameters with our model will provide better performance in practical QKD systems. In contrast, the optimized parameters of the previous model cannot tolerate normal afterpulse probability [38] in all methods of fluctuation analysis.

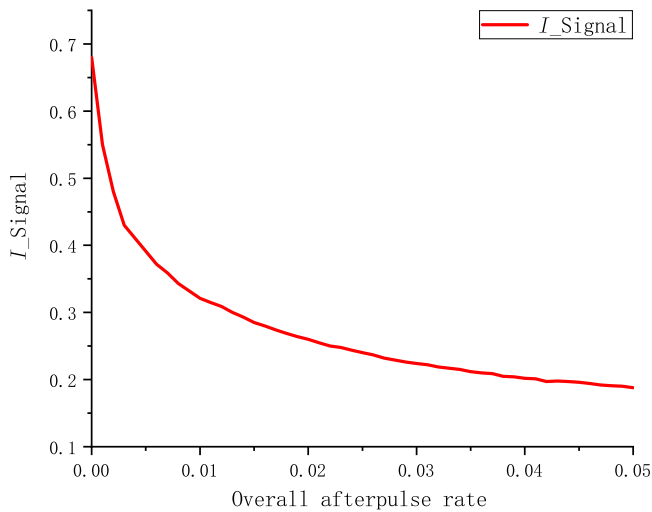


FIG. 5. Intensity of the signal state as a function of \hat{p} .

V. CONCLUSION

In conclusion, we develop an analytical model in a QKD system to obtain its compatibility with an afterpulse. In our model, the afterpulse, which has essential correlation with former detections, is considered as the third source of detector responses after a light pulse and dark count. In addition, we analyze the impact of the afterpulse on the secure key rate with several approaches of fluctuation analysis. Although the afterpulse introduces an additional QBER and more parameters need to be bound, the key rate still performs well in our model. Furthermore, the key rate obtained with the optimized parameters with our afterpulse-compatible model is much higher than that obtained with the optimized parameters of the afterpulse-omitted model in the same situation; therefore, the tolerance against the afterpulse effect can be significantly improved in practical QKD systems.

With the rapid growth of the system working frequency, the impact of the afterpulse effect becomes increasingly severe. Our work provides an effective way to construct an afterpulse-compatible QKD system with security and high key rate preserved. The model is valid for any protocol and is especially suitable for high-speed scenarios.

ACKNOWLEDGMENTS

We thank Charles Ci Wen Lim, H.-X. Li, X.-D. Yang, X.-T. Hou, L. Xiao, and H. Dai. for helpful discussions. We acknowledge S.-P. Ma for constant encouragement, and also thank R.-N. Zhu and B. Liu for critical communication support. This work was supported by the National Key Research And Development Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grants No. 61622506, No. 61575183, 61627820, No. 61475148, and No. 61675189), the Strategic Priority Research Program (B) of the Chinese

Academy of Sciences (Grants No. XDB01030100 and No. XDB01030300), and the Anhui Initiative in Quantum Information Technologies.

- [1] C. H. Bennett, and G. Brassard, in *Conf. on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
- [2] A. K. Ekert, Quantum Cryptography based on Bells Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] G. S. Vernam, Cipher printing telegraph systems, *J. AIEE* **45**, 109 (1926).
- [4] S. K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J. G. Ren, J. Yin, Q. Shen, Y. Cao, and Z. P. Li, *et al.*, Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [5] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W. S. Tam, A. Plevs, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, *Optica* **4**, 163 (2017).
- [6] Y. Liu, T. Y. Chen, J. Wang, W. Q. Cai, X. Wan, L. K. Chen, J. H. Wang, S. B. Liu, H. Liang, and L. Yang, *et al.*, Decoy-state quantum key distribution with polarized photons over 200 km, *Opt. Express* **18**, 8587 (2010).
- [7] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre, *Nat. Photonics* **9**, 163 (2015).
- [8] S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zou, G. C. Guo, and Z. F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, *Nat. Photonics* **9**, 832 (2015).
- [9] C. Wang, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Measurement-device-independent quantum key distribution robust against environmental disturbances, *Optica* **4**, 1016 (2017).
- [10] S. Wang, W. Chen, Z. Q. Yin, D. Y. He, C. Hui, P. L. Hao, G. J. Fan-Yuan, C. Wang, L. J. Zhang, and J. Kuang, *et al.*, Practical gigahertz quantum key distribution robust against channel disturbance, *Opt. Lett.* **43**, 2030 (2018).
- [11] ID Quantique, <https://www.idquantique.com>.
- [12] MagiQ Technologies, <http://www.magiqtech.com>.
- [13] QuintessenceLabs, <https://www.quintessencelabs.com>.
- [14] Qasky, <http://www.qasky.com/en/>.
- [15] H. K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* **8**, 595 (2014).
- [16] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photonics* **4**, 686 (2010).
- [17] R. H. Hadfield, Single-photon detectors for optical quantum information applications, *Nat. Photonics* **3**, 696 (2009).
- [18] D. Y. He, S. Wang, W. Chen, Z. Q. Yin, Y. J. Qian, Z. Zhou, G. C. Guo, and Z. F. Han, Sine-wave gating ingaas/inp single photon detector with ultralow afterpulse, *Appl. Phys. Lett.* **110**, 111104 (2017).
- [19] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, Room temperature single-photon detectors for

- high bit rate quantum key distribution, *Appl. Phys. Lett.* **104**, 021101 (2014).
- [20] J. Zhang, M. A. Itzler, H. Zbinden, and J. W. Pan, Advances in ingaas/inp single-photon detector systems for quantum communication, *Light: Sci. Appl.* **4**, e286 (2015).
- [21] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, and H. Sato, *et al.*, High speed prototype quantum key distribution system and long term field trial, *Opt. Express* **23**, 7583 (2015).
- [22] W. Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [23] X. B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [24] H. K. Lo, X. F. Ma, and K. Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [25] X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* **72**, 012326 (2005).
- [26] Z. W. Yu, Y. H. Zhou, and X. B. Wang, Reexamination of decoy-state quantum key distribution with biased bases, *Phys. Rev. A* **93**, 032307 (2016).
- [27] 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, Non-markovian property of afterpulsing effect in single-photon avalanche detector, *J. Lightwave. Technol.* **34**, 3610 (2016).
- [28] V. K. Rohatgi, and A. K. M. E. Saleh, *An introduction to probability and statistics* (John Wiley & Sons, Hoboken, New Jersey, 2015), p. 120.
- [29] D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings* (Chicago, 2004), p. 136.
- [30] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [31] C. C. W. Lim, M. Curty, N. Walenta, F. H. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, *Phys. Rev. A* **89**, 022307 (2014).
- [32] K. Azuma, Weighted sums of certain dependent random variables, *Tohoku Math. J.* **19**, 357 (1967).
- [33] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, Finite-key security analysis of quantum key distribution with imperfect light sources, *New J. Phys.* **17**, 093011 (2015).
- [34] J. C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Unconditional Security of a Three State Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **94**, 040503 (2005).
- [35] Z. Q. Yin, H. W. Li, W. Chen, Z. F. Han, and G. C. Guo, Security of counterfactual quantum cryptography, *Phys. Rev. A* **82**, 042335 (2010).
- [36] H. X. Li, H. D. Jiang, M. Gao, Z. Ma, C. G. Ma, and W. Wang, Statistical-fluctuation analysis for quantum key distribution with consideration of after-pulse contributions, *Phys. Rev. A* **92**, 062344 (2015).
- [37] M. Curty, F. H. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H. K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 3732 (2014).
- [38] C. Wang, F. X. Wang, H. Chen, S. Wang, W. Chen, Z. Q. Yin, D. Y. He, G. C. Guo, and Z. F. Han, Realistic device imperfections affect the performance of hong-ou-mandel interference with weak coherent states, *J. Lightwave. Technol.* **35**, 4996 (2017).