Estimation of key rate after setting dead time*

Liu Dong(刘 东)[a], Yin Zhen-Qiang(银振强)[a]†, Wang Shuang(王 双)[a]‡, Wang Fen-Mei(王粉梅)[b], Chen Wei(陈 巍)[a] and Han Zheng-Fu(韩正甫)[a]

[a] *Key Laboratory of Quantum Information of the Chinese Academy of Sciences, University of Science and Technology of China, Hefei* 230026, *China*
[b] *Army Officer Academy of PLA, Hefei* 230031, *China*

(Received 5 December 2011; revised manuscript received 27 December 2011)

The estimation of key rate is an important aspect of the quantum key distribution process, especially in the use of dead time. In this paper, we demonstrate a numerical simulation to estimate the average detection probability and the key rate. Using our method, the estimated average detection probability is better than the previous result. Besides, we can easily find the best dead time, especially when considering the impact of after pulse.

Keywords: dead time, key rate, quantum key distribution

PACS: 02.60.Cb **DOI:** 10.1088/1674-1056/21/6/060202

1. Introduction

Quantum key distribution (QKD) allows two parties to share a random sequence which can be used in secure communication. Its unconditional security is guaranteed by the physical principle. The practical system is based on the attenuated laser signal which may contain more than one photon in a pulse. So this may be a weak point for eavesdropping attacks. The security of the practical QKD needs to be considered. Huang[1] proposed the decoy state method, and Lo[2,3] gave the GLLP formula for the secure key rate as follows:

$$R \approx q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}. \quad (1)$$

Here q depends on the protocol [1/2 for the Bennett–Brassard 1984 (BB84) protocol], μ denotes the average photon number of signal states, Q_μ is the detector's response probability caused by signal states at Bob's side, E_μ is the overall bit error rate in QKD system, Q_1 and e_1 are the response probability and bit error rate caused by single photon pulse, and $H_2(x)$ is the binary Shannon information function, with the form

$$H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x). \quad (2)$$

The variables, such as Q_μ and E_μ, can be measured directly from the experiment.

Usually, we need to know the estimated value of the count rate of a particular system before running it. When the devices used in the system are perfect, this estimation will be very easy. Unfortunately, no device is perfect, especially the single photon detector[4,5] which contains dark count and after pulse. When its repetition frequency is high,[6–8] the after pulse occurs more frequently, resulting in a significant increase of bit errors. In order to make QKD work well, a possible way is introducing dead time to reduce the errors and improve the safety rate. During the dead time, no gates are applied to the detector, so after a detection event, the following pulses will be ignored. For a given system with dead time, it is hard to estimate the average detection probability without running the QKD system. The authors of Refs. [9] and [10] used different formulas to estimate the results. The former used a negative exponential term to modify the raw key rate:

$$\mathrm{Raw}_1 = fp\,\mathrm{e}^{(-fp\tau)}. \quad (3)$$

The latter used

$$\mathrm{Raw}_2 = fp\frac{1}{1+fp\tau}. \quad (4)$$

Here, τ denotes the dead time, f is the frequency of gate, p is the detection probability for every gate,

*Project supported by the National High Technology Research and Development Program of China (863 Program) (Grant No. 2009AA01A349).

†Corresponding author. E-mail: yinzheqi@mail.ustc.edu.cn
‡Corresponding author. E-mail: wshuang@ustc.edu.cn

© 2012 Chinese Physical Society and IOP Publishing Ltd

usually assigned to the probability of a pulse from Alice to Bob(p_{ab}).

We found when the dead time is relatively large, the estimated values and the actual results are very different.[11,12] In this paper, we demonstrate estimating detection probability by using the method of numerical simulation. In the demonstration, we use BB84 decoy protocol[13] and assume after pulse obeys a negative exponential probability distribution.[14] We obtained the curve of the average detection probability and the secure key rate. By comparing our values with the formula estimates, it shows a significant difference between them, especially when the dead time is larger.

2. Analysis of the average detection probability

The detector used in the QKD system is commonly employed in gated mode. The detector will respond to pulses arriving in the gate-on time, while the pulses out of the gate will be ignored. Once the gate frequency (f) and detection probability for the gate (p) are given, the raw key can be calculated by the formula: Raw $= fp$.

The laser pulse can be modeled as a weak coherent state and the average photon number of each pulse is μ. The optical pulses from the sender Alice, then translate through the quantum channel to the receiver Bob. Given loss coefficient of the channel α (dB/km) and fiber length L (km), the whole loss of the channel can be expressed as: $10^{-\alpha L/10}$. At Bob's side, the whole loss of the devices is β (dB), the detection efficiency of the detector is $\eta_{\rm D}$, then the probability of a pulse from Alice to Bob being detected is

$$p_{\rm ab} = 1 - {\rm e}^{-(\mu\eta_{\rm D}10^{-(\alpha L+\beta)/10})}. \tag{5}$$

We usually use $p_{\rm ab}$ instead of p in Eqs. (3) and (4), without considering the dark count and after pulse. And when dead time is introduced, the expected average detection probability of the signal photon $Q_{\rm s}$ is given by the following approximate formula

$$Q_{\rm s}^1 = p_{\rm ab}\,{\rm e}^{(-p_{\rm ab}m)}, \tag{6}$$

$$Q_{\rm s}^2 = p_{\rm ab}/(1+p_{\rm ab}m), \tag{7}$$

where $m = f\tau$ is the dead time (pulse). Those formulas just give the theoretical approximation. Its result may be inaccurate for longer dead time. They are obtained under the condition that the after pulse's effect is completely shielded by setting dead time.

In fact, the thermally excited carrier, during the gate-on time, also could be detected, giving a dark count in detection. The dark count, one of the bottleneck limits of the performance of detectors, can be reduced as much as possible, but is inevitable. Let $p_{\rm d}$ denotes the probability of detection caused by dark count. Furthermore, if an emission from one of the trapped carriers is detected during the following gate-on time, this detection event is called after pulse. The after pulse's effect is another bottleneck, according to the results in Ref. [15], the after pulse probability will drop to the dark count level after 5 microseconds. Let $p_{\rm ap}$, a function of interval pulses n, denote the probability that an after pulse is observed after n pulses following a detection event. We can use an exponential distribution function to approximate their results

$$p_{\rm ap}(n) = p_0\,{\rm e}^{-an}. \tag{8}$$

Since the probability of after pulse decays exponentially, introducing a proper dead time in detection, during which no detection event occurs, is an effective way to reduce bit errors.

When we consider the dark count and the after pulse, according to the theory of probability, the detection probability of a pulse is

$$\begin{aligned} p = {} & p_{\rm ab} + p_{\rm ap} + p_{\rm d} - p_{\rm ab}p_{\rm ap} - p_{\rm ap}p_{\rm d} \\ & - p_{\rm d}p_{\rm ab} + p_{\rm ab}p_{\rm ap}p_{\rm d}. \end{aligned} \tag{9}$$

In order to obtain more precise values, we need to take this equation into the modification formula in Refs. [13] and [14]. Because of the use of dead time the probability caused by the after pulse cannot be calculated easily. In order to simplify the calculation, people usually ignore the small terms, just taking the first two terms of Eq. (9) as p, so the average detection probability will be inaccurate, and the results will be far from the actual ones. For example the experimental value of the raw key in Ref. [15] is about 13.5 kHz, while the estimated value using the exponential function is only 8.9 kHz when the dead time is 40 μs. If we can simulate the detection process, we believe it will be a good method to obtain a realistic detection probability. In this paper, we provide a numerical simulation for the QKD detection process, from which we can obtain the bit error rate, the average detection probability, secure key rate, and other parameters.

3. Implementation and results

We use the Monte Carlo method to simulate the detection process. In our simulation, we use BB84 decoy state protocol. A big array is used to store the randomly generated optical pulses. The optical pulses contain a signal state, decoy state, and vacuum state, with the probability 0.6, 0.3, and 0.1, respectively. Thus, each element of the array is a signal state with the probability of sixty percent. We assume the gate and the optical pulse have the same frequency. When a pulse arrives, the detection program first determines the type of state: the signal state, decoy state or vacuum state. Moreover, the pulse intensity will be attenuated through the channel, and during this pulse's gate-on time, the photon, which can cause a detection event, will also include two other types of noise. So for each pulse, it also needs to determine whether it is the after pulse, dark count or optical pulse according to their detection probability. For one detector, similar to the case using wrong detection base, it has 0.5 probability of gaining the right result. All the above judgments are based on the random number. We obtain the statistic of detected pulses for each type. Then it is able to calculate the actual average detection probability, error rate, and other information through statistical results. In our simulation, the fiber length is 50 km and its loss is set to 0.2 dB/km, the whole loss of Bob's system is 3 dB, the detector's detection efficiency is 0.1 and the dark count rate is 10^{-5}. The two parameters of after pulse p_0 and a are set to 0.0317 and 0.00115, respectively.

First we ignore the effect of the after pulse, and using our simulation we can obtain the value of the variables mentioned in the formula (1), such as the average detection probability. Figure 1 shows the average detection probability change with dead time. The solid line with small circle is the obtained simulation value, the dashed line is the value obtained from the fractions modified formula (7), and the solid line with dot is the value obtained from the exponential modified formula (6). When the dead time is small, these three results vary slightly. But with increasing dead time the difference between them increases, and is very obvious when $m * p_{\rm ab} > 1$. The difference between the values of formula (7) and ours is smaller than formula (6) and ours.

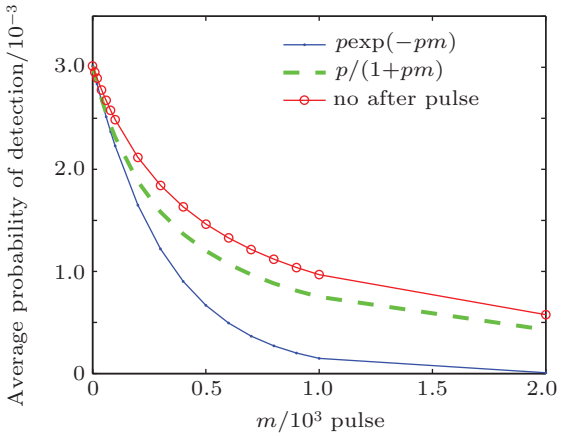


Fig. 1. (colour online) The average detection probability change with dead time, without considering the effect of after pulse.

When the effect of the after pulse is considered the difference will be even greater. Figure 2(a) shows the result with the probability of after pulse satisfying equation (8). The solid line with asterisk shows the average detection probability we obtained. When the dead time is small, the probability of after pulse is bigger, so the average detection probability is

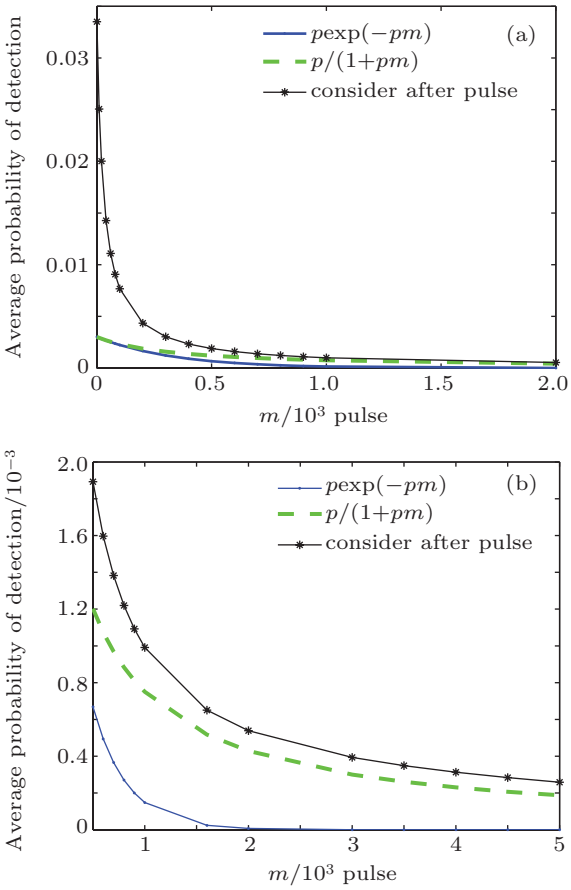


Fig. 2. (colour online) The average detection probability change with dead time considering the influence of after pulse.

particularly bigger than others. Figure 2(b) shows that when the dead time is large enough, satisfying $m * p_{\rm ab} > 1$, the difference between our result and the former is also more obvious.

Figure 3 shows the secure key rate, calculated by formula (1), with and without the effect of after pulse. The values on the solid line with asterisk first increased and then decreased with the increase of dead time. This means that we can easily find the optimum dead time, corresponding to the highest point of this curve.

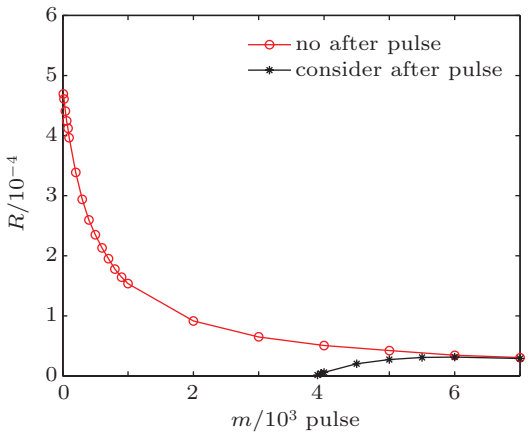


Fig. 3. (colour online) The secure key rate with (solid line) and without (dotted line) after pulse.

4. Conclusion

We demonstrated a new method to estimate the the average detection probability. Using our method, we can obtain a better estimation of the count rate, when the product of dead time (pulse) and $p_{\rm ab}$ is greater than one. Besides, we can easily find the optimum dead time. These results, used as a reference of the system's parameter settings, will be more accurate.

References

[1] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[2] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326
[3] Gottesman D, Lo H K, Norbert L and John P 2004 *Quantum Infor. Comput.* **4** 325
[4] Liu Y, Wu Q L, Han Z F, Dai Y M and Guo G C 2010 *Chin. Phys.* B **19** 080308
[5] Chang J and Wu L A 2003 *Acta Phys. Sin.* **52** 5 (in Chinese)
[6] Stucki D, Ribordy G, Stefanov A, Zbinden H, Rarity J G and Wall T 2011 *J. Mod. Opt.* **48** 1967
[7] Zhang J, Rob T, Claudio B and Hugo Z 2009 *Appl. Phys. Lett.* **95** 091103
[8] Yuan Z L, Sharpe A W, Dynes F, Dixon A R and Shields A J 2010 *Appl. Phys. Lett.* **96** 071101
[9] Eleni D 2006 *S*ecurity and Implementation of Differential Phase Shift Quantum Key Distribution Systems Ph. D. Thesis (California: Stanford University)
[10] Stucki D, Gisin N, Guinnard O, Ribordy G and Binden H 2002 *New J. Phys.* **4** 41
[11] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L and Guo G C 2008 *Chin. Phys. Lett.* **25** 10
[12] Xu F X, Chen W, Wang S, Yin Z Q, Zhang Y, Liu Y, Zhou Z, Zhao Y B, Li H W, Liu D, Han Z F and Guo G C 2009 *Chin. Sci. Bull.* **54** 17
[13] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[14] Feng X X, Huang T, Dong S L, Xiao L T and Jia S T 2008 *Journal of Test and Measurement Technology* **22** No. 6
[15] Yoshizawa A, Kaji R and Tsuchida H 2003 *Opt. Express* **11** 1303