High speed measurement device independent quantum key distribution with finite detector dead time

Ji Yiming, Zhuang Maolu, Zhang Guixin, Chen Aiping, Wang Li, Li Wenqiang

(Air Force Communication NCO Academy, Dalian 116600, China)

Abstract: The detector cannot detect photon successfully when the signal transmission rate exceeds the maximum detector count rate in high speed quantum key distribution scheme. This leads to correlations in the sifted bit string, and the security is compromised. In this paper, the high speed measurement device independent quantum key distribution based on BB84 protocol with finite detector dead time was analyed and the optimal transmission speed was simulated. Simulation result shows that the sifted key rate raised linearly with the increase of photon transmission rate without consideration of the influence of detector′s dead time; with consideration of the influence of detector′s dead time, the sifted key rate is no longer raising with the photon transmission rate infinitely and the curve of sifted key rate is distorted. When the transmission distance is 100 km, the correlation between the sifted key rate and detector dead time is approximate to $2.1/10\tau$, and the correlation between optimal transmission rate and detector dead time is approximate to $3.3\times10^5/\tau$.

Key words: quantum key distribution; single photon detection; measurement device independent; detector dead time; BB84 protocol

CLC number: TN913.7 **Document code:** A **DOI:** 10.3788/IRLA201847.S122001

有限探测死时间的高速测量设备无关-量子密钥分配

姬一鸣,庄茂录,张贵新,陈爱萍,王 丽,李文强

(空军通信士官学校,辽宁 大连 116600)

摘 要: 由于探测器死时间的影响,当信号发送速率超过探测器的最大计数率时,将导致光子到达时不能成功进行探测,造成较高的误码率,影响密钥的安全。文中以 BB84 协议为例,分析了有限探测死时间的高速测量设备无关-量子密钥分配方案的安全性,并对最优传输速率进行了仿真。仿真结果表明:不考虑探测器死时间时,密钥筛选速率随着光子发送速率的增加而线性增加;考虑探测器死时间影响时,密钥筛选速率不再随着光子传输速率的增加而无限增加,筛选密钥曲线发生弯曲。在传输距离为 100 km 时,密钥的筛选速率和探测器死时间的关系接近 $2.1/10\tau$,最优传输速率与探测器死时间的关系接近 $3.3\times10^5/\tau$。

关键词: 量子密钥分发; 单光子探测; 测量设备无关; 探测器死时间; BB84 协议

收稿日期:2018-03-20; **修订日期:**2018-05-11

基金项目:国家自然科学基金(61106068)

作者简介:姬一鸣(1991-),男,助教,硕士,主要从事光纤通信及量子通信方面的研究。Email:ymjr328@163.com

0 Introduction

Measurement Device Independent Quantum Key Distribution(MDI-QKD)[1] was put forward by Lo et al in 2012. It was a new mode of Quantum Key Distribution against the loophole of detector, and can remove all the side channel loophole of all the detectors[2-3]. Based on Decoy State[4-6], the project makes the sharing of quantum key in an absolutely safe environment. Different with the classic mode of quantum key distribution, there is no more single photon detection in Alice and Bob. By transmitting the bytes to an untrusted third party to measure Bell state, it can prove the level of key′s safety [7]. Although the third part is untrusted, there is dead time in the detector τ and the detector has the maximum counting rate $1/\tau$. When the transmitter has a higher transmission rate of photons, it will fail to detect before the photon comes into the detector so that it comes to a higher bit error rate[8]. Rogers has analyzed it in the document[9] because of the effect of detector dead time, if an eavesdropper obtains part of hacking information, it will not fail to come to a higher bit error rate, and the quantum byte of the two measuring base presents a certain probability distribution during the sifting key so that quantum key has no more security. Putting the BB84 protocol[10-12] as an example, this paper analyses the safety of the high speed measurement device independent quantum key distribution with finite detector dead time and simulates the optimal transmitting rate. The simulation indicates that without consideration of the effect of detector dead time, sifted-key rate has a liner rise with the increase of photon transmitting rate; with consideration of the effect of detector dead time, sifted-key rate stops rising with the increase of photon transmitting rate and the curve of the sifted-key rate changes. By calculating the curve, when transmission distance l=100 km, the relation between sifted-key rate and detector dead time is close to $2.1/10\tau$, and the relation between optimal transmitting rate and detector dead time is close to $3.3\times10^5/\tau$.

1 MDI-QKD based on decoy state

In 2013, Sun et al combined decoy state scheme and proposed decoy state MDI QKD scheme[13] and it enhanced the security of the key and the transmission distance was improved. In the scheme, Sun et al used three degree of decoy state scheme (vacuum state v_0, decoy state v_1 and signal state v_2), in the scheme, $v_0\equiv 0$, $v_2>v_1>0$. The scheme had more accurate estimates of the minimum of the single the photon counting rate and the maximum of single photon error rate limit. As is shown in the formula (1) and (2):

$$Y_{11}\geqslant\frac{g_1+g_2+g_3-\mathrm{e}^{\mu_2+\nu_2}Q_{\mu_2\nu_2}+\mathrm{e}^{\mu_1+\nu_1}Q_{\mu_1\nu_1}}{\mu_1\nu_1-\mu_2\nu_2+\alpha\mu_2\nu_1+\alpha\mu_1\nu_2} \tag{1}$$

$$\mathrm{e}_{11\mu\nu}\leqslant\frac{E_{\mu_1\nu_1}Q_{\mu_1\nu_1}\mathrm{e}^{\mu_1+\nu_1}-g_4}{\mu_1\nu_1Y_{11}} \tag{2}$$

In the formulas:

$$\begin{cases} g_1=\mathrm{e}^{\nu_2}Q_{0\nu_2}+\mathrm{e}^{\mu_2}Q_{\mu_2 0}-\mathrm{e}^{\nu_1}Q_{0\nu_1}-\mathrm{e}^{\mu_1}Q_{\mu_1 0} \\ g_2=\alpha(\mathrm{e}^{\mu_2+\nu_1}Q_{\mu_1\nu_2}-\mathrm{e}^{\nu_1}Q_{0\nu_1}-\mathrm{e}^{\mu_2}Q_{\mu_2 0}+Q_{00}) \\ g_3=\alpha(\mathrm{e}^{\mu_1+\nu_2}Q_{\mu_1\nu_2}-\mathrm{e}^{\nu_2}Q_{0\nu_2}-\mathrm{e}^{\mu_1}Q_{\mu_1 0}+Q_{00}) \\ g_4=\mathrm{e}^{\nu_1}Q_{0\nu_1}E_{0\nu_1}+\mathrm{e}^{\mu_1}Q_{\mu_1 0}E_{\mu_1 0}-Q_{00}E_{00} \end{cases} \tag{3}$$

$$\alpha=\min\left(\frac{\mu_1\nu_2^2-\mu_1\nu_1^2}{\mu_1\nu_1^2+\mu_1\nu_2^2},\frac{\mu_2^2\nu_2-\mu_1^2\nu_1}{\mu_2^2\nu_1+\mu_1^2\nu_2},\frac{\mu_2^2\nu_2^2-\mu_1^2\nu_1^2}{\mu_2^2\nu_1^2+\mu_1^2\nu_2^2}\right) \tag{4}$$

It can be obtained by the document[13]:

$$Q_{\mu_2\nu_2}=Q_C+Q_E \tag{5}$$

$$E_{\mu_2\nu_2}Q_{\mu_2\nu_2}=e_dQ_C+(1-e_d)Q_E \tag{6}$$

$$Q_E=2P_d(1-P_d)^2\mathrm{e}^{-\bar{\mu}/2}[I_0(2s)-(1-P_d)\mathrm{e}^{-\bar{\mu}/2}] \tag{7}$$

$$Q_C=2(1-P_d)^2\mathrm{e}^{-\bar{\mu}/2}[1-(1-P_d)\mathrm{e}^{-\eta_a\bar{\mu}/2}]\times[1-(1-P_d)\mathrm{e}^{-\eta_b\bar{\mu}/2}] \tag{8}$$

And the sifted key rate of decoy state MDI-QKD is shown in the formula (9):

$$R\geqslant\mu_2\nu_2\mathrm{e}^{-\mu_2-\nu_2}Y_{11}[1-H(e_{11})]-Q_{\mu_2\nu_2}fH(E_{\mu_2\nu_2}) \tag{9}$$

where f is the error correction inefficiency; $Q_{\mu_2\nu_2}$ is total gain; $E_{\mu_2\nu_2}$ is total error rate; $H(x)$ is the binary Shannon entropy function: $H(x)=-x\log_2(x)-(1-x)\cdot\log_2(1-x)$.

2 High speed MDI-QKD with finite detector dead time

In the MDI-QKD scheme, when analyzing the sifted key generation rate, the influence of detectors′ dead time is generally not considered. However, in an actual system, there is some detectors′ dead time τ, thus detectors have limited maximum count rate $1/\tau$. When photon transmission rate is greater than maximum count rate of detectors, detectors cannot complete successful detection of arrival photon, which results in higher error rate. If an eavesdropper uses part of tapping the way to eavesdrop on the key generation process, in introduction of BER at the same time, the eavesdropper could get some key information, and in the sifted key, the key of two bases presents a certain probability distribution so that the eavesdropper can obtain the key information. Rogers et al. analyzed the process and proposed an idea of efficient detection. The security of high-speed QKD scheme was analyzed, and the sifted key could be obtained when the transmission rate was not higher than $1/2\tau$. In 2010, Viacheslav[14] et al. did a further analysis of the process and proposed that the QKD scheme based on the BB84 protocol had an effective detection to (i.e. it can be successfully used to sifted the key) the probability p with consideration of detectors′ dead time which is shown in formula (10):

$$P_a=\frac{1}{1+0.5(k-1)\eta} \tag{10}$$

where η is the total gain, $\eta=Q_{\mu_2 v_2}$; $k=\rho\tau$, ρ is transmission rate of photon, τ is detector dead time. Combining with detectors′ dead time, we will have

$$R_d \geqslant P_a\cdot(\mu_2 v_2 e^{-\mu_2-v_2} Y_{11}[1-H(e_{11})]-Q_{\mu_2 v_2} f H(E_{\mu_2 v_2})) \tag{11}$$

We set the transmission distance l=100 km, and other parameters as Tab.1.

Tab.1 Main parameters setting[15]

e_0	e_d	P_d	f	η_C	τ/ns
0.5	1.5%	3×10^{-6}	1.16	14.5%	100

This paper had an analysis on the simulation of high-speed MDI-QKD scheme of detectors′ dead time, as shown in Fig.1. It can be seen from the diagram, the sifted key rate raised linearly with the increase of photon transmission rate without consideration of the influence of the detectors′ dead time. However, when we consider the impact of detectors′ dead time, the sifted key generation rate curve (dotted line) is distorted obviously, and the sifted key generation rate is no longer linearly rising with increase of the photon transmission rate. In the simulation, we set detectors′ dead time τ=100 ns, and it can be figured out that the sifted key generation rate curve is distorted not at 10^7 Hz but at 10^{10} Hz. This is because the used optical fiber transmission channel has a loss, when photons which the sending rate is 10^7 Hz come to the transmitting terminal, the rate is far less than 10^7 Hz. In this moment the existence of detectors′ dead time will not have influence in photon detection and the sifted key generation rate rises linearly with the increase of photons transmission rate; when the transmission speed of photon is $\rho \geqslant 10^{10}$ Hz, the rate of photon at transmitting terminal is higher than the highest counts of detectors. At this time the existence of detectors′ dead time has an impact on successful photon detection and the curve of the sifted key generation rate is distorted.

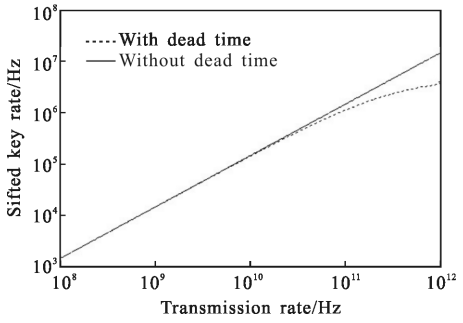

Fig.1 Relationship between transmission rate and sifted key generation rate

Finally, the maximum value of the sifted key generation rate and the photon transmission rate are

simulated and analyzed, as shown in Fig.2. In the simulation process, the transmission distance of the fixed key is described by l=100 km. The influence of dead time of different detectors on the sifted key generation rate is analyzed by setting different the detectors dead time when τ=50, 100, 150 ns. As you can see from the diagram, when the dead time is at τ=50 ns(solid line), the maximum sifted key generation rate is reached at 4.2×10^6 Hz; when the dead time is at τ=100 ns (point, line), the sifted key generation rate is 2.0×10^6 Hz; when the dead time is at τ=150 ns (dotted line), the maximum rate is 1.4×10^6 Hz. The sifted key generation rate increases with the decrease of the detectors′ dead time. By calculation, when l= 100 km, the relation between the sifted key generation rate and the detectors′ dead time is close $2.1/10\tau$ and the relation between optimal transmission rate and the detectors′ dead time is close $3.3\times10^5\frac{1}{\tau}$.

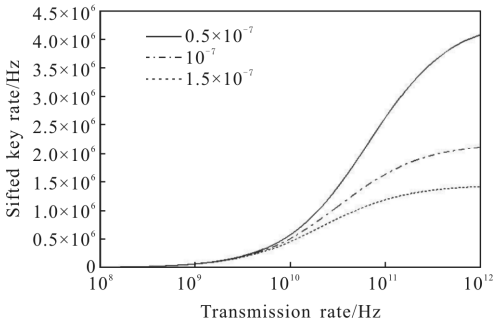

Fig.2 Relationship between sifted key generation rate and transmission rate under different detector dead time

3 Conclusion

In this paper, the high speed MDI-QKD scheme with finite detector dead time is analyzed. When photon arrival rate is greater than maximum count rate of detectors, the detectors can′t successfully detect all photons which results in high bit error rate. By using the effective detection idea proposed by Rogers et al, the relation between the sifted key generation rate of MDI-QKD scheme and the detectors′ dead time is analyzed. As it can be seen from the simulation, in the case that the detectors′ dead time is affected, the sifted key generation rate does not increase indefinitely with the increase of the photon transmission rate. Finally, the maximum sifted key generation rate and the optimal photon transmission rate are simulated under different dead time of detectors conditions, and the optimal photon transmission rate at different dead time is obtained. With the development of detectors, especially the generation of superconductor detectors, the dead time of detectors is decreasing, which can greatly increase the transmission rate of photons and improve the efficiency of key generation.

References:

[1] Lo H K, Curty M, Bin Q. Measurement device independent quantum key distribution [J]. ***Physical Review Letters***, 2012, 108: 130503.

[2] Dong C, Zhao S H, Dong Y, et al. Measurement device independent quantum key distribution for the rotation invariant photonic state [J]. ***Acta Physica Sinica***, 2014, 3 (17): 62-66.

[3] Dong C, Zhao S H, Zhao W H, et al. Analysis of measurement device independent quantum key distribution under an asymmetric channel transmittance efficiency [J]. ***Quantum Information Processing***, 2014, 14(11): 2525-2534.

[4] Tang Z Y, Liao Z F, Lo H K, et al. Experimental demonstration of polarization encoding measurement device independent quantum key distribution [J]. ***Physical Review Letters***, 2014, 112: 190503.

[5] Wang J D, Qin X J, Liu S H, et al. An effective active phase compensation method for quantum key distribution system [J]. ***Acta Phys Sin***, 2010, 59(1): 281.

[6] Ma X F, Qi B, Lo H K, et al. Practical decoy state for quantum key distribution [J]. ***Phys Rev A***, 2005, 5: 03005.

[7] Dong C, Zhao S H, Shi L, et al. Analysis of measurement device independent quantum key distribution with an asymmetric channel transmittance efficiency [J]. ***Acta Phys Sin***, 2014, 63: 030302.

[8] Dixon A R, Dynes J F, Yuan Z L, et al. Continuous operation of high bit rate quantum key distribution [J]. ***Applied Physics Letters***, 2009, 94: 231113.

[9] Daniel J Rogers, Joshua C Bienfang, Anastase Nakassis. Detector dead time effects and paralyzability in high speed

quantum key distribution [J]. ***New J Phys***, 2007, 9: 319.

[10] Charles H. Bennett Gilles Brassard. Quantum cryptography: public key distribution and coin tossing [C]//Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing Bangalore, 1984: 175-179.

[11] Lo H K, Ma X F, Kai C. Decoy state quantum key distribution[J]. ***Physical Review Letters***, 2005, 94: 230504.

[12] Mi J L, Wang F Q, Lin Q Q, et al. Practical non-orthogonal decoy state quantum key distribution with heralded single photon source [J]. ***Chinese Physics B***, 2008: 1674-1056.

[13] Shi-Hai S, Ming G, Chun-Yan L, et al. Practical decoy state measurement device independent quantum key distribution [J]. ***Physical Review A***, 2013, 87: 052329.

[14] Viacheslav B, Bing Q, Ben F, et al. Security of high speed quantum key distribution with finite detector dead time [J]. ***Quantum Physics***, 2010, 1005: 0272v1.

[15] Wang Q, Wang X B. Efficient implementation of the decoy state measurement device independent quantum key distribution with heralded single photon source [J]. ***Phys Rev A***, 2013, 88: 052332.