2015 The 5th International Workshop on Computer Science and Engineering
doi: 10.18178/wcse.2015.04.087

Analysis on the Beam-split Eavesdropping by Eavesdropper with Storage Ability

Yanbo Wang, Min He, Zhiyong Zhang, Yong Zhu, Zhiyong Xu

Institute of Communication Engineering, PLA University of Science and Technology, Nanjing, 210007, china

Keywords: QKD, beam- eavesdropping, beam-split proportion, efficiency of eavesdropping, decoy state

Abstract. Focusing on QKD systems based on the weak-coherent pulse photon source and BB84 protocol, puting forward the beam- eavesdropping projects simulating eavesdropper with storage ability--single base-2APD and single base-4APD projects, and obtaining the efficiency of generating keys in the receiver, the efficiency of eavesdropping in the eavesdropper, eavesdropping-information proportion and formula for beam-split proportion. Based on the practical sample with transmission length 10km and average photon number 0.1~0.9, calculate the eavesdropping-information proportion and get 0.35%~5.79% on account of the beam-split proportion 0.2, 0.3, 0.4 and 0.5. Results show that current QKD systems with average photon number 0.1 are safe for the beam-eavesdropping.

Introduction

The absolute security of quantum key distribution(QKD) is based on the ideal single photon source, channel, detectors, etc. Technology restriction leads to the difference between practical QKD systems and ideal QKD systems. In 2004, Gottesman proved that practical QKD systems were still unconditional security[1][7][8][9][10] on the cost of sacrificing the efficiency of keys transmission and distance.

Practical QKD systems based on optical fibre usually use weak-coherent pulse as photon source. The photon source sends out pulses including single photon pulse, vacuum photon pulse and multi-photon pulse. The existence of multi-photon pulse makes the beam- eavesdropping possible. In 2003, Hwang put forward the decoy state project to resist the photon split attack. It takes advantage of changing intensity (decoy state) of light pulse to detect the existence of the photon split attack. This method can effectively resist the photon split attack and raise the QKD distance from about 30km to 130km[2]~[5].

The beam-split eavesdropping[6] splitting photons in proportion, neither disturbs the quantum coherence, nor affects the photon distribution in pulses, which makes the decoy state impossible to detect the existence of eavesdropping. But the beam- eavesdropping will affect the efficiency of transmission. Therefore, through compensating transmission loss by a suitable method and keeping the efficiency in system, the beam- eavesdropping will avoid the detection of BER, decoy state or efficiency of generating keys. This paper analyzes the beam- eavesdropping by eavesdropper with storage ability in a QKD system based on BB84 protocol and polarization code.

Analysis on the Simulation of A Beam- eavesdropping System with Storage Ability

In order to make the beam- eavesdropping having no influence on the efficiency of generating keys, we use low-loss fibre and devices to replace common fiber and devices in the attacked system to make up the loss of splitting light.

Eve with storage ability means that he shares the same base with Bob's. The point is that the measurement base of Eve is the same as Bob's. In theory, it is possible to simulate the situation above if Eve invades Bob's measurement devices and eavesdrops in the branch of bases after base selection

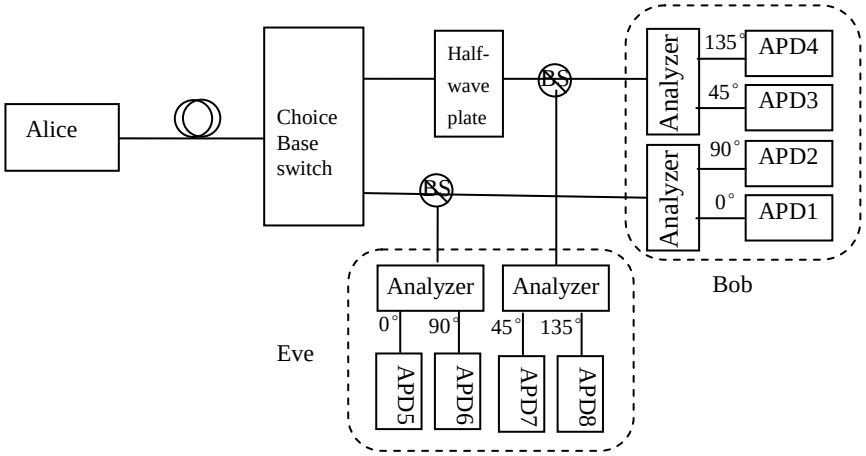


Fig.1: Diagram of eavesdropping system with the same base in Eve and Bob

The essence of the project is eavesdropping single base respectively. To simulate the behavior, Alice could only send states with single base and corresponding results are 50% comparing to double bases. For detectors in theory, Bob and Eve need 2 APD in the single base condition. The single-base-2APD project is used to simulate the beam- eavesdropping in QKD with storage ability and the efficiency of generating keys, efficiency of eavesdropping and eavesdropping-information proportion will be analyzed. For the project of 4APD, the constitution is the same to fig.1, and the rate of key-generating of Bob, the eavesdropping efficiency of Eve and the proportion of eavesdropping information are the same to the project of 2APD. But the number of light quantum is the half of the other project when light arrives at detectors of Bob and Eve.

The project of 2-APD is shown in fig. 2.

Assume the dark-count rate and detection rate of detectors in Bob and Eve are $\varepsilon', \eta', \varepsilon'', \eta''$ respectively. Alice sends a 0°90°polarization pulse with average photon number λ, of which the average photon number attenuates to λ', λ'', after reaching the polarization selector. The average photon number of reaching APD1 and APD2 are λ' and 0, or 0 and λ', while the number of APD5 and APD6 are λ'' and 0, or 0 and λ''.1 and 0 express a photon or not. Sign the photon number reaching Bob and Eve is $i_1 i_2 x_1 x_2$, then:

0000, 1000, 0100, 0010, 0001, 1010, 1001, 0110, 0101.

$P_{i_1 i_2}(\lambda')$, $P_{x_1 x_2}(\lambda'')$, $P_{i_1 i_2 x_1 x_2}(\lambda', \lambda'')$ is the probability of states $i_1 i_2$, $x_1 x_2$, $i_1 i_2 x_1 x_2$, then:

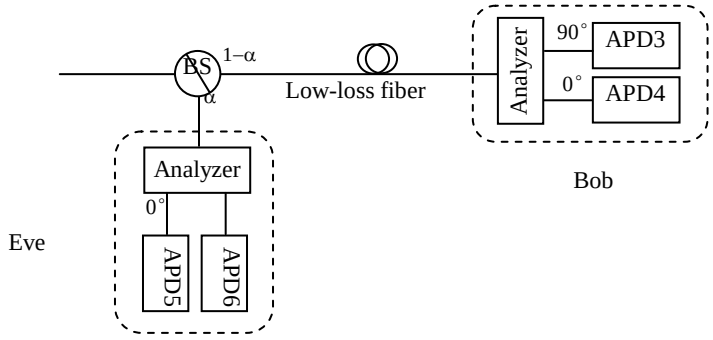


Fig.2: Diagram of single-base-2APD beam- eavesdropping system

$$P_{i_1 i_2 x_1 x_2}(\lambda', \lambda'') = P_{i_1 i_2}(\lambda') P_{x_1 x_2}(\lambda''),$$

$P_{00}(v)=e^{-v}$, $P_{01}(v)=0$, $P_{10}(v)=1-e^{-v}$.

$P_{i_1i_2}$, $P_{x_1x_2}$, $P_{i_1i_2x_1x_2}$ are the probabilities of effective detection of Bob, Eve, Bob & Eve under states i_1i_2, x_1x_2, $i_1i_2x_1x_2$, which means when Alice sends out a 0°polarization light, $P_{i_1i_2}$ is the probability that APD1 responds, $P_{x_1x_2}$ is the probability that APD5 responds, $P_{i_1i_2x_1x_2}$ is the probability that APD1 and that APD5 both responds; when Alice sends 90°polarization light, $P_{i_1i_2}$ is the probability that APD2 responds, $P_{x_1x_2}$ is the probability that APD6 responds, $P_{i_1i_2x_1x_2}$ is the probability that APD2 and APD6 both respond, then:

$P_{i_1i_2x_1x_2}=P_{i_1i_2}P_{x_1x_2}$, $P_{00}=\varepsilon(1-\varepsilon)$, $P_{01}=\varepsilon(1-\eta)$, $P_{10}=\eta(1-\varepsilon)$.

Therefore, when Alice sends out a 0°polarization light, the probability Bob getting an effective detection is: $P_{0^\circ}^{AB}=\sum_{i_1i_2=00}^{10}P_i(\lambda')P_i$.

The probability of Eve getting an effective detection is:

$$P_{0^\circ}^{ABE}=\sum_{i_1i_2=00\sim10}^{x_1x_2=00\sim10}P_{i_1i_2x_1x_2}(\lambda',\lambda'')P_{i_1i_2x_1x_2}=\left(\sum_{i_1i_2=00}^{10}P_{i_1i_2}(\lambda')P_{i_1i_2}\right)\left(\sum_{x_1x_2=00}^{10}P_{x_1x_2}(\lambda'')P_{x_1x_2}\right).$$

Due to $\sum_{i_1i_2=00}^{10}P_{i_1i_2}(v)P_{i_1i_2}=\sum_{x_1x_2=00}^{10}P_{x_1x_2}(v)P_{x_1x_2}=e^{-v}\varepsilon(1-\varepsilon)+(1-e^{-v})\eta(1-\varepsilon)$, then:

$P_{0^\circ}^{AB}=\left[e^{-\lambda'}\varepsilon'+(1-e^{-\lambda'})\eta'\right](1-\varepsilon')$

$P_{0^\circ}^{ABE}=\left[e^{-\lambda'}\varepsilon'+(1-e^{-\lambda'})\eta'\right]\left[e^{-\lambda''}\varepsilon''+(1-e^{-\lambda''})\eta''\right](1-\varepsilon')(1-\varepsilon'')$.

Similarly obtains: $P_{90^\circ}^{AB}=P_{0^\circ}^{AB}$, $P_{90^\circ}^{ABE}=P_{0^\circ}^{ABE}$, then: when Alice sends out a polarization light, the probability of Bob getting an effective detection is:

$$P_{AB}(\lambda,\alpha)=\frac{P_{0^\circ}^{AB}+P_{90^\circ}^{AB}}{2}=\left[e^{-\lambda'}\varepsilon'+(1-e^{-\lambda'})\eta'\right](1-\varepsilon').$$

And the probability of Eve getting an effective eavesdropping is:

$$P_{ABE}(\lambda,\alpha)=\left[e^{-\lambda'}\varepsilon'+(1-e^{-\lambda'})\eta'\right]\left[e^{-\lambda''}\varepsilon''+(1-e^{-\lambda''})\eta''\right](1-\varepsilon')(1-\varepsilon'').$$

The eavesdropping-information proportion is the proportion of the eavesdropping information of Eve and the receiving information of Bob, then:

$$I_{BE}(\lambda,\alpha)=\frac{P_{ABE}(\lambda,\alpha)}{P_{AB}(\lambda,\alpha)}=\left[e^{-\lambda''}\varepsilon''+(1-e^{-\lambda''})\eta''\right](1-\varepsilon''),$$

Obviously, the eavesdropping-information proportion is the detection efficiency of Eve.

Assume the beam-split proportion is α; $\delta'_{\text{fiber-loss}}$, $l'_{\text{fiber-length}}$, $d'_{\text{device-loss}}$, $\delta''_{\text{fiber-loss}}$, $l''_{\text{fiber-length}}$, $d''_{\text{device-loss}}$ are the coefficient of fibre loss, fibre length, and total loss of device in the original system and replaced system respectively. Then obtain: $\lambda'=\lambda(1-\alpha)\beta'$, $\lambda''=\lambda\alpha\beta''$.

$\beta'=10^{-\frac{\delta'_{\text{fiber-loss}}l'_{\text{fiber-length}}+d'_{\text{device-loss}}}{10}}$ is the total loss of the original system, $\beta''=10^{-\frac{\delta''_{\text{fiber-loss}}l''_{\text{fiber-length}}+d''_{\text{device-loss}}}{10}}$ is total loss of the replaced system by eavesdropper.

Calculating on the Available Beam-split Proportion

Assume that replace the devices in the ordinary system with low-loss fibre and high-performance devices to obtain the beam-split proportion using the loss difference of the two light paths, which will keep the efficiency of the generating keys. The replaced fibre length may as well be 10km.

In general, the loss coefficient of the fibre in the ordinary system is $\delta'_{\text{fiber-loss}}$=0.25db/km, and the replaced one is 0.17db/km. Assume the total device loss of the ordinary system in 10km is $d'_{\text{device-loss}}$=5db, while the replaced one is $d'_{\text{device-loss}}$=3db. Assume the attenuation is 0 and $\beta''=1$.

According fig. 2, obtain β'_{ordinary}=0.177828 in the ordinary system and $\beta'_{\text{low-loss}}$=0.338844 in the replaced system.

The loss difference of the two systems is:

$\Delta\beta' = \beta'_{\text{low-loss}} - \beta'_{\text{ordinary}}$=0.338844–0.177828=0.161016

The minimum requirement of a successful beam- eavesdropping is keeping λ' , the average photon number arriving at Bob, unchanged. $\lambda' = \lambda\beta'_{\text{ordinary}}$. And the replaced system satisfies $\lambda' = \lambda\beta'_{\text{low-loss}}$, then:

$$\lambda' = \lambda\beta'_{\text{ordinary}} = \lambda\beta'_{\text{low-}loss}\left(1 - \frac{\Delta\beta'}{\beta'_{\text{low-}loss}}\right) \Rightarrow \alpha = \frac{\Delta\beta'}{\beta'_{\text{low-loss}}} = 0.475192.$$

It is clear the useful beam-split proportion of Eve is near 0.5.

Sample Calculation on the Eavesdropping Efficiency

Data calculation below will help to acquire the information proportion of the beam- eavesdropping.

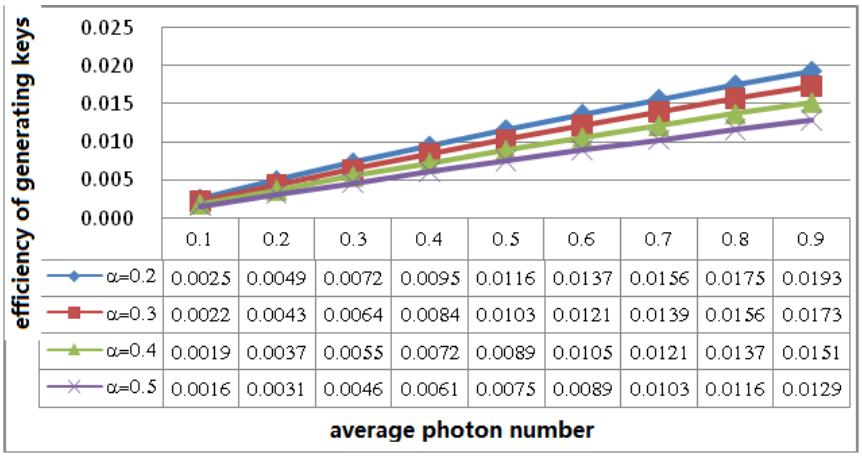
Assume the dark-count efficiency of Bob is $\varepsilon' \approx 10^{-5}$, the detection efficiency is η'=0.1; While the dark-count efficiency of Eve is $\varepsilon'' \approx 5\times10^{-6}$, and the detection efficiency is η''=0.2; the total loss coefficient in the replaced system is $\beta'_{\text{low-loss}}$=0.338844.

Consider the beam-split proportion α=0.2, 0.3, 0.4, 0.5, when λ=0.1~0.9, obtain the efficiency of generating keys in Bob, the eavesdropping efficiency of Eve, and the eavesdropping-information proportion are shown in fig. 3, fig. 4, fig. 5.

Summary

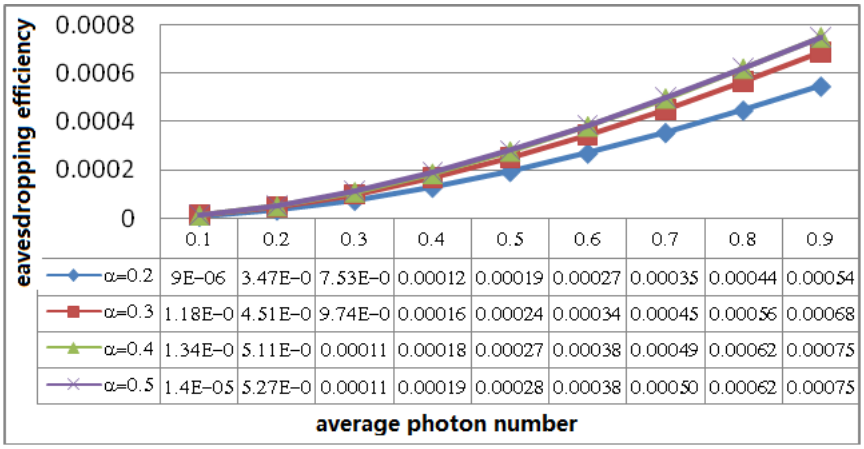
Theory analysis and figure calculation show that the beam- eavesdropping can avoid the detection of photon-number distribution. Replace the ordinary system with high-performance fibre to make up the beam- loss and get the beam-split proportion, which can avoid the detection of the efficiency of generating keys.

Calculations show that replacing 10km fibre can gain near 50% beam-split proportion. When the average photon number is 0.1, the eavesdropping-information proportion is 0.86%, that is the amount of keys Eve obtains through beam- eavesdropping is 0.86% that of Bob. Even the average photon number is 0.9, the eavesdropping-information proportion is only 5.79%. The proportion can be totally eliminated by privacy amplification. The generally accepted average-photon number in current QKD systems is 0.1. Therefore, even if the eavesdroppers obtain the storage ability, the beam-eavesdropping cannot threaten the security of QKD systems.



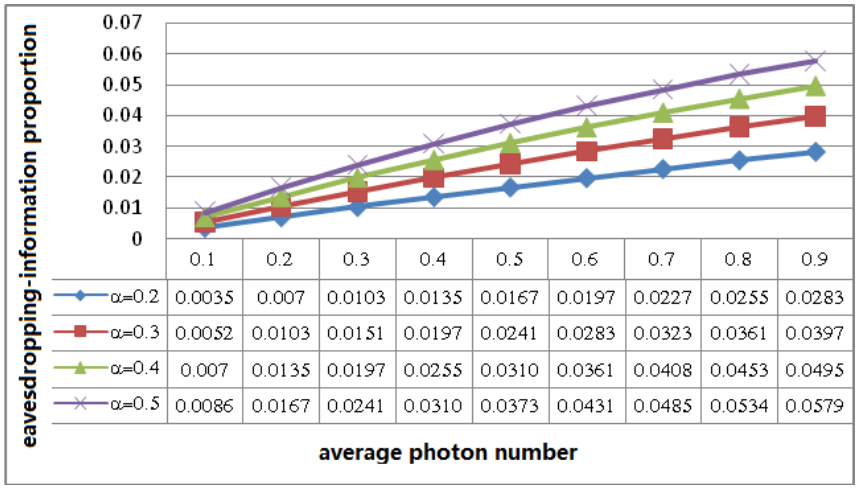
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
α=0.2	0.0025	0.0049	0.0072	0.0095	0.0116	0.0137	0.0156	0.0175	0.0193
α=0.3	0.0022	0.0043	0.0064	0.0084	0.0103	0.0121	0.0139	0.0156	0.0173
α=0.4	0.0019	0.0037	0.0055	0.0072	0.0089	0.0105	0.0121	0.0137	0.0151
α=0.5	0.0016	0.0031	0.0046	0.0061	0.0075	0.0089	0.0103	0.0116	0.0129

Fig.3: The efficiency of generating keys in Bob when α=0.2, 0.3, 0.4, 0.5, λ=0.1~0.9



	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
α=0.2	9E-06	3.47E-0	7.53E-0	0.00012	0.00019	0.00027	0.00035	0.00044	0.00054
α=0.3	1.18E-0	4.51E-0	9.74E-0	0.00016	0.00024	0.00034	0.00045	0.00056	0.00068
α=0.4	1.34E-0	5.11E-0	0.00011	0.00018	0.00027	0.00038	0.00049	0.00062	0.00075
α=0.5	1.4E-05	5.27E-0	0.00011	0.00019	0.00028	0.00038	0.00050	0.00062	0.00075

Fig.4: The eavesdropping efficiency of Eve when α=0.2, 0.3, 0.4, 0.5, λ=0.1~0.9



	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
α=0.2	0.0035	0.007	0.0103	0.0135	0.0167	0.0197	0.0227	0.0255	0.0283
α=0.3	0.0052	0.0103	0.0151	0.0197	0.0241	0.0283	0.0323	0.0361	0.0397
α=0.4	0.007	0.0135	0.0197	0.0255	0.0310	0.0361	0.0408	0.0453	0.0495
α=0.5	0.0086	0.0167	0.0241	0.0310	0.0373	0.0431	0.0485	0.0534	0.0579

Fig.5: The eavesdropping-information proportion when α=0.2, 0.3, 0.4, 0.5, λ=0.1~0.9

References

[1] Gottesman D,Lo H K,Lukenhaus N,et al.Security of quantum key distribution with imperfect devices. Quantum Inf Comput . 2004

[2] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901

[3] Wang X B. Beating the photon-number-splitting attack in pratical quantum cryptography. Phys Rev Lett, 2005, 94: 230503

[4] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 94: 230504

[5] Hu J Z, Wang X B. Quantum key distribution with the decoy-state method (in Chinese). Sci Sin Phys Mech Astron, 2011, 41: 459–465

[6] Chen Yan,Yang Hongyu, Deng Ke. Effects of Photon-Number-Splitting Attacks on the Security of Satellite-to-Ground Quantum Key Distribution Systems(in Chinese).ACTA OPTICA SINICA, 2009,11(in Chinese)

[7] Y. Zhao, C. H. F. Fuang, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A 78, 042333 (2008)

[8] Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, 2002, Rev.Mod. Phys.74, 145.

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, 2009, Rev. Mod. Phys. 81, 1301.

[10]Mayers D. Unconditional security in quantum cryptography. J Assoc Comput Mach, 2001, 48: 351–406