A Solution for Beam Splitter Attack on BB84 Protocol*

Huiyao An[1,2], Dunwei Liu[1†], Tao Yu[1]

[1]School of Software and Microelectronics, Peking University, Beijing 100871, China
[2]School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
† liudunwei@pku.edu.cn

Abstract - In the practical Quantum Key Distribution (QKD) systems, the Fused Biconical Taper (FTP) technology beam splitter (BS) has wavelength dependent property. So Eve will get almost all of the secret information without being discovered in the beam splitter attack. This paper proposes a solution to solve the beam splitter attack. It uses three beam splitters to remove the incredible photons which could have been attacked by Eve. Bob gets a proper three-beam-splitter group, so Eve can't catch any secret information without being found.

Index Terms - beam splitter, quantum key distribution (QKD), quantum bit error rate (QBER).

1. Introduction

It is well known that cryptography whether in military or civilian has played a more and more important role. Whether symmetric cryptosystem or public key cryptosystem in classical cryptography, the fundamental problem is the conflict between security and distribution. People's increasing computing power threatens the classic password security. Quantum key distribution is a useful practical way to solve those problems in information cryptography, many QKD protocols have appeared [1-10]. BB84 protocol is a very important model of them [2]. QKD's two branches are the polarization encoding and the phase encoding, respectively. If the polarization encoding scheme does not have an advantage in high-speed passive modulation, it may has been discarded with birefringence of light destroy in practical experiment. For example, National Institute of Standards and Technology (NIST) achieved 1GHz pulse repetition rate of polarization encoding quantum key distribution experiment and conducted a 1550nm optical network research, and K.J.Gordon and P.D.Townsend made the light pulse repetition rate increased to 3.3 GHz [11-16]. A lot of QKD protocols have been widely proved in theory, however, the imperfect factors in practical photon detector, optical fiber, beam splitter and light source damage the security of QKD's protocols [17-20]. The Fused Biconical Taper (FTP) technology beam splitter is adopted in passive modulation of BB84 protocol. By the way, channels will be identified in Bob's measurement after splitting photons. The FBT technology splitter is widely used in reality. But the beam splitter's coupling ratio is dependent on photons' wavelength. Hong-Wei Li and others use this loophole completed a beam splitter attack [21], so they can control the coupling of the beam to change the measurement basis at the receiving end. The beam splitter scheme presented in this paper solves the beam splitter attack on the passive BB84 protocol. In the passive polarization modulation coding protocol, this scheme has a very good superiority and application prospect.

The rest of this study is organized as follows. BB84 protocol and the beam splitter attack are reviewed briefly, and we will propose our scheme in Sec.2. In Sec.3, security analysis of this study is discussed. Finally, a conclusion is given to this study in Sec.4.

2. Review Beam Splitter Attack and Propose a New Scheme

Let review the BB84 protocol and beam splitter attack first. In the legal channel, Alice prepares a single photon sequence and sends it to Bob. If there is no eavesdropping, Bob uses passive modulation measuring basis to measure the single photons. Bob passively selects the measurement basis by the BS for convenient and high speed modulation. More precisely, the BS just distributes those photons into two output ports, so Bob can randomly choose to measure the photon state either in rectilinear basis if it passes through output port 1, or in diagonal basis if it passes through output port 2. The BS's coupling ratio is 0.5. So when there is an eavesdropper, he doesn't know which basis should be used to measure the photons. Alice and Bob can find the Eve by calculating QBER. But the beam splitter attack changes the perfect security. Because different wavelengths photons have different coupling ratio for beam splitter, eavesdropper can escape from Alice and Bob's awareness and steal information by using a pair of wavelengths (low coupling ratio and high coupling ratio of wavelength) to control the measurement basis.

To solve the beam splitter attack on the passive BB84 protocol, we propose the three-beam-splitter program in following Fig.1.

There are three beam splitters for stacking operation. BS1, BS2 and BS3 for the wavelength of 1370 nm and 1550 nm photons' coupling rates are 0, 1 and 0.5, respectively. Three beam splitters for different wavelength photon coupling rate are described in Fig.2.

* This work is partially supported by the National Natural Science Foundation of China (Grant Nos.61179029).

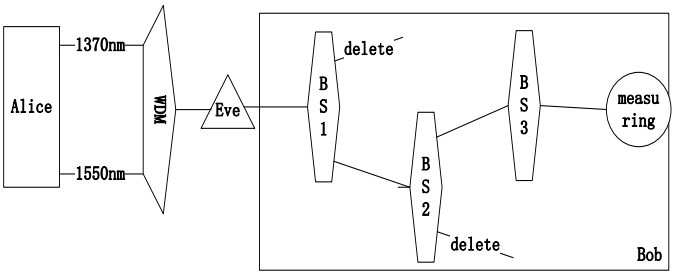

Fig. 1 The three-beam-splitter principle diagram.

In our scheme there will be two different wavelength photons (1370nm and 1550nm) between Alice and Bob, so this method can greatly reduce the QBER from photons interference. The coupling ratios of this two wavelengths are 0.5. If Eve attack wavelength λ1 and λ2 photons, there must have enough photons be used to measure in Bob's end, and QBER should be in a legal range too, otherwise he would be found. To describe the state in photons' transfer process when there is an eavesdropper, two quantum states ($|0^\circ\rangle$ and $|45^\circ\rangle$) are described below. $|90^\circ\rangle$ and $|135^\circ\rangle$ have the same paths respectively in Fig.3 and Fig.4.

If Bob's measurement results meet the requirements of earnings, now he and Alice should delete the different basis ($\{|0\rangle,|1\rangle\}$ or $\{|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2},|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}\}$) between them. Next Bob can calculate the QBER and judge whether the QBER is in the right range. Of course, the communication should be stopped when one of the requirements is not satisfied. Therefore, as long as we set a reasonable income requirement and the QBER (generally, income Y should be at 95% and QBER be at 1%), the eavesdropper cannot hide himself.

3. Security Analysis

We are going to analyze the security of our scheme. Income Y should be more than 95% in the quantum key communication and the noise in environment contributes 1% to QBER.

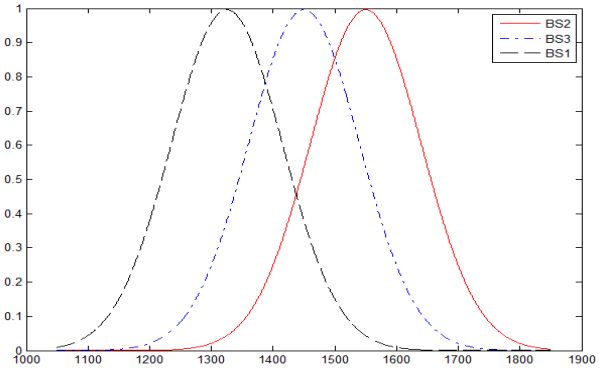

Fig. 2 Three beam splitters' coupling rate with different wavelength photons.

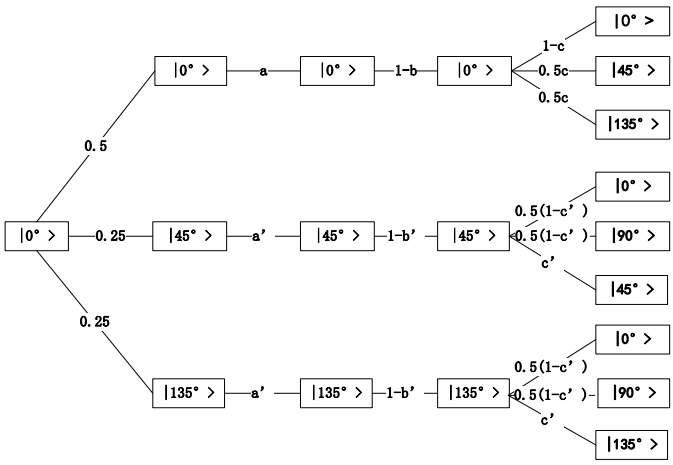

Fig. 3 All possible light path of polarization state $|0^\circ\rangle$. (1-a), (1-b) and c are λ1 photon's coupling ratios, (1-a '), (1-b') and c ' are λ2 photon's coupling ratios of the each beam splitter.

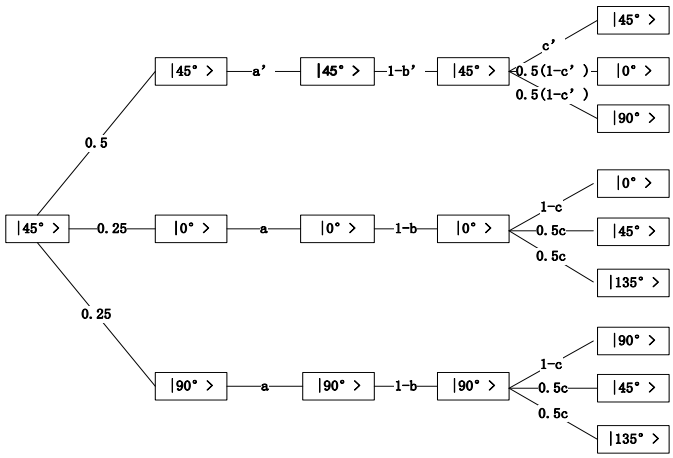

Fig. 4 All possible light path of polarization state $|45^\circ\rangle$.

Eavesdroppers have two possibilities:

①The eavesdropper attacks in 1540 nm to 1570 nm or 1350 nm to 1380 nm range wavelength of the photons. Because only 97% of the wavelength 1540 nm photons can pass BS1, 98% of the photons can pass BS2, so there will be 95.06% of the photons in BS3 that can meet the requirements. Similarly, parameters of 1570 nm photons are 100% , 95% and 95%.So if Eve wants to hack, then he must choose to use photon whose wavelength is from 1540 nm to 1570 nm or from 1350 nm to 1380 nm. By considering intercept-and-resend strategy has been applied by Eve in the quantum channel, the final QBER between Alice and Bob can be given by:

$$E_{BS123}=\frac{1}{2}\left[\frac{0.25a'(1-b')(1-c)}{0.5a'(1-b')(1-c')+0.5a(1-b)(1-c)}+\frac{0.25a(1-b)c}{0.5a(1-b)c+0.5a'(1-b')c'}\right] \quad (1)$$

Income Y is like the following:

$$Y=100a(1-b)\% \quad (2)$$

The income and QBER of the scheme lead to Eve can't get any information to attack without being found. Eve attack 1540 nm to 1540 nm and 1350 nm to 1380 nm range: a, a ', (1 - b') and (1- b) are set up in 0.975 to guarantee profits. When Eve even choose to attack the wavelength of 1540 nm and 1570 nm of photons, c and c 'should be 0.58 and 0.43. So we can get Err = 25.1% and Err ≫ 1% from (1). So even if Eve attacks the legal wavelength, he cannot meet the requirements. And the coupling rate is close to 0.5, by which Eve cannot get useful information.

②Eavesdropper attacks part of the photons. The eavesdropper would naturally choose extreme wavelength for BS3 coupling rate, such as 1150 nm and 1450 nm, or 1750 nm and 1450 nm.1750 nm photons' pass rate in BS1 is 100%, but 15% in BS2. 1450 nm photons' pass rate in BS1 and BS2 are 55% and 40% respectively. We can find that 18.5% of those photons which have been attacked by Eve could reach Bob. So in order to satisfy the yield condition, Eve attacks only 6.13% of the total number of photons. Eve can affect only 1.15% of key information. Finally, it is an ignorable part comparing with Y's requirement of more than 95%.

4. Conclusion

Beam splitter attack rate is based on the coupling wavelength dependence. We just use this factor to fend off beam splitter attack, so our scheme is simple and easy to achieve. There are two kinds of eavesdropping. When the eavesdropper attacks the photon (whose wavelength is from 1540 nm to 1570 nm or from 1350 nm to 1380 nm), income and QBER cannot be satisfied at the same time. So eavesdropper is bound to be found. If eavesdropper attacks a part of the photons, he can just attack 6.13% of the total number of photons and affect 1.15% of key information which is same to the noise effect.

References

[1] Wiesner S. Conjugate coding. SIG A CT News, 1983, 15: 78-88
[2] Bennett C H, Brassard G, India: Ban-galore Press, 1984. 175-179
[3] Ekert A K, Phys. Rev. Lett, 1991, 67: 661-663.
[4] Kim Y H, Kulik S P, Shih Y, Physical Review Letters, 2000, 86: 1370-1373
[5] Cinelli C, Barbieri M, Martini F D, International Journal of Laser Physics, 2005, 15(1): 124-128
[6] Bennett C H, Phys. Rev. Lett, 1992, 68: 3121-3124
[7] C. H. Bennett, et al., Jour of Cryptology, 1992 5(1):3-28.
[8] J. A. Smolin, Phys of Infor., 2004, 48 (1) :47-52.
[9] Bose S, Knight P L, Plenio M B, Physical Review Letters, 1999, 83(9):5158.
[10] Zhou J D, Hou G, Zhang Y D, Physical Review A, 2001, 64:012301.
[11] X. Tang, et al., Proc. of SPIE, 2005 A (1-9): 5893, 58931.
[12] X. Tang, et al., Proc. of SPIE, 2006 P (1-8), 6244.
[13] Mink, X. Tang, et al., Proc. of SPIE, 2006 M (1-7), 6244, 62440
[14] K. J. Gordon, et al., IEEE Journal of Quantum Electronics, 2004 40 (7), 900 – 908
[15] K. J. Gordon, et al., Opt. Express, 2005 13(8), 3015-3020
[16] K. J. Gordon, et al., ECOC European Conference on Optical Communication, 2005 4, 913 – 914
[17] H.Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, Y. Yamamoto, New Journal of Physics - NEW J PHYS , vol. 7, no. 1, pp. 232-232, 2005
[18] ZHANG Ling-fen, Appl opt, 2002, 23(6): 29-31.
[19] ZHAO Su-ying, WANG Xu-lu an, ZH ANG Ning-wei, Infrare, 2007, 28(9): 25-28.
[20] ZHONG Yue-ming, FEMT, 2005, 119: 32- 34.
[21] Hong-Wei Li, Shuang Wang, Jing-Zheng Huang, Wei Chen, Zhen-Qiang Yin, Fang-Yi Li, Zheng Zhou, Dong Liu, Yang Zhang,Guang-Can Guo, Wan-Su Bao, Zheng-Fu Han, Phys. Rev. A.2011