# Analysis of the Performance about Actual Quantum Key Distribution System Based on BB84 Protocol

Huang Kai-guo
Institute of Communication Engineering, PLA University of Science and Technology
Nanjing 210007, China

Wang Yan-bo
Institute of Communication Engineering, PLA University of Science and Technology
Nanjing 210007, China

Zhang Qi-ye
Institute of Communication Engineering, PLA University of Science and Technology
Nanjing 210007, China

Wang Xiao
Faculty of Science, PLA University of Science and Technology,
Nanjing 210007, China

He Min
Faculty of Science, PLA University of Science and Technology,
Nanjing 210007, China

***Abstract*—Analyzed how did the fiber length, the attenuation and the average photon number of the pulse emitted by the single photon source affect the receive efficiency in the fiber channel quantum key distribution system based on the BB84 protocol. A theoretic model relative to the system was represented. It was shown by the emulation that the more average photon number was, the higher efficiency receiver would be, and the final key rate would be higher.**

***Keywords- BB84 protocol; quantum key distribution; photon source frequency; receive efficiency***

## I. INTRODUCTION

Quantum key distribution has drawn highly attention since it was proposed by Bennett and Brassard in 1984[1].It was proved to be an unconditional secure scheme in key distribution which is based on the quantum mechanics. There has been plenty of effort in this area. Reference [2] analyzed the effects of the Breidbart eavesdropping scheme of the extended BB84 quantum key distribution protocol. Reference [3] analyzed the security of practical QKD system, and it calculated the upper limit in QKD protocol. Reference [4] simulated the QKD system based on BB84 protocol in Java language. Reference [5] promoted a principle of polarization feedback which keeps polarization states stable and realized a polarization encoded QKD experiment system. Reference [6] promoted a novel phase modulated QKD scheme with high security and high efficiency. Reference [7] put forward a new QKD protocol based on decoy states. Reference [8] proposed a protocol which based on the heralded single photon source and non-orthogonal decoy state. Reference [9] promoted an advanced BB84 protocol: entangled photon pairs based BB84 protocol and simulated to validate the validity and the security of this protocol. Reference [10] analyzed the BB84 protocol and the SARG04 protocol in theory. Reference [11] analyzed the coefficient of QBER and its influence to the QKD. However, all of them analyzed and researched in a conception way. This paper discussed the practical BB84 system based on the fiber channel and analyzed the performance in theory and calculated it to explore how the performance of the devices affects the system's efficiency.

## II. BB84 PROTOCOL

The BB84 protocol uses four kinds of polarized photon to encode the information. We sign these four kinds of polarized state 0°, 45°, 90°, 135°. X={0°,90°}and Z={45°,135°}form two different orthogonal basis in two dimension Hilbert space. According to the Uncertainty Principle, X can distinguish the 0° and 90° state, Z can distinguish the 45° and 135° state.

The BB84 protocol can be described by four steps:

- Encode and Transmit: The transmitter, Alice chooses a basis in X and Z randomly and encoded the information. Then Alice records the basis;
- Receive and Measure: The receiver Bob chooses a basis in X and Z randomly and measure the state he has received. Then Bob records the basis;
- Compare and Choose: Bob tell Alice which bases he used, Alice reply in which bases they choose the same. Then they discard other bits. In this way, they have shared a key called row key;
- Detect the Eavesdropping: Alice and Bob choose some data randomly in row key and compare it in classical channel. If there are no error bits, we believe the key is safe.

Since the possibility of Alice and Bob choose the same basis is 1/2, so the efficiency is 50%. If there is eavesdropper exists, the eavesdropper measures the state at random basis. The eavesdropper also has 1/2 possibility to choose the right basis. While the eavesdropper chooses the wrong basis, he will change the state. If Bob uses the right basis, he will get a wrong bit. Every time the eavesdropper detects, he has 1/4 possibility to make an error bit. If Alice and Bob choose n bits to detect

eavesdropping, the eavesdropper will be detected in a possibility of $1-(3/4)^n$.

## III. QKD SYSTEM BASED ON BB84 PROTOCOL

Constrained by the technology, there is no ideal single photon source. In practical system, we use attenuated laser pulse, when the average photon number in the pulse is very low, it can simulate the single photon source.

The polarization state of a photon is not so stable; it varies from the time, temperature, the curve of the fiber. In this case, the receiver should correct the polarization state. The polarization controller is a device to achieve this aim. It can convert the input state to the state you want. Firstly, train it to adjust a specific channel. Then it will introduce a phase different to compensate the phase different introduced by the environment. While the environment changes, the controller should be trained again.

The optic-switch can be used to choose the measurement basis. But the loss of the optic-switch is too high relative to the quantum system. It will make the system be complex, so it's not feasible.

For the single photon, the optic-splitter can simulate to choose measurement basis. The advantage of using optic-splitter is keeping the system concise and low loss. But for the pulses which contain multiple photons, optic-splitter may make an invalid measurement, then decreases the efficient of key distribution.

To distinguish the photons whose polarization states are vertical to each other, we can use the polarization beam splitter (PBS). The PBS can be treated as a semi lens. It transmits the 0° photons and reflects 90° photons. We can use APD to detect the photons in the transmission port and reflection port. This is an X-basis detector.

To construct a Z-basis detector, we can add a half wave plate (HWP) before the X-basis detector. The half wave plate can spin the polarization state of the photons in 45°. After the half wave plate, the 45° and 135° state is converted to 0° and 90° state.

According to the analysis of BB84 protocol and the optic devices, we deduce the fiber quantum communication model based on the BB84 protocol as Figure 1.

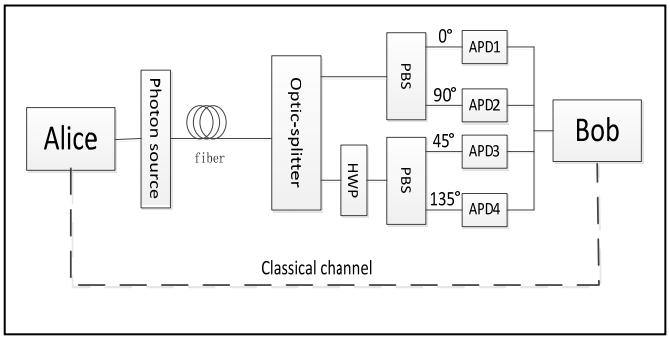


Figure 1. QKD system in fiber channel based on BB84 protocol.

As we can see, the efficiency of practical system is determined by the protocol, photon source, devices and channel loss. But we should take the following aspects into account:

- In the QKD system, it is generally use the APD to detect photons. There are two aspects affect the detect efficiency. One is dark count which means that the count bring by noise rather than photons. Another one is dead time which means that in the time piece after detection the APD cannot detect photons.
- The photon source is heralded single photon source, so there may be multiple photons in a pulse. This will cause an invalid detect. Before Alice and Bob compare their measurement basis, they should filter the data to make sure it is valid.
- The noise in the channel also causes the error bits. Generally, we set a threshold according to the channel. If the bit error rate is higher than the threshold, we believe there is an eavesdropper. If the bit error rate is lower than the threshold, Alice and Bob make the reconciliation to correct error bits. The reconciliation needs to discard some data to make sure the key's security. Different reconciliation protocol has different efficiency. This paper we set the efficiency is 50%.

## IV. SYSTEM MODEL AND SIMULATION

### A. SYSTEM MODEL

The photons will be attenuated by the fiber, optic-splitter, PBS, half wave plate and so on. The loss of these devices is different. The loss of channel (contains the loss of fiber and other utilities such as polarization controller) is signed by $\delta_{channel}$. The light splitting ratio of the optic splitter is $\alpha$: (1- $\alpha$). The loss of the optic-splitter, half wave plate and PBS are signed by $\delta_{splitter}$, $\delta_{hwp}$, $\delta_{pbs}$.

On the assumption that the number of photons emitted by the source obeys the Poisson distribution, the average number is $\lambda$. After attenuated by the channel and get to the $APD_i$, the average number of the photons is $\lambda_i$.

The four APDs photon number state is signed: $(k_1,k_2,k_3,k_4)$, $k_1,k_2,k_3,k_4=0,1,2,\ldots$,

The possibility of the state $(k_1,k_2,k_3,k_4)$ is $P_{k_1}(\lambda_1)P_{k_2}(\lambda_2)P_{k_3}(\lambda_3)P_{k_4}(\lambda_4)$,

which:

$$\lambda_1 = \lambda_2 = \lambda\alpha \cdot 10^{-\frac{\delta_{channel}+\delta_{splitter}+\delta_{pbs}}{10}},$$

$$\lambda_3 = \lambda_4 = \lambda(1-\alpha) \cdot 10^{-\frac{\delta_{channel}+\delta_{splitter}+\delta_{hwp}+\delta_{pbs}}{10}}$$

If there are $k$ photons get to an APD at one time, the possibility of detection is $\eta_k$ ($\eta_0$ means the possibility of dark count). The valid detection means when Alice emits a pulse, there is only one APD response. If the photons number state is $(k_1,k_2,k_3,k_4)$, the possibility of a valid detection is:

$$\eta_{k_1k_2k_3k_4} = \prod_{i=1}^{4}(1-\eta_{k_i})\sum_{j=1}^{4}\frac{\eta_{k_j}}{(1-\eta_{k_j})}$$

$\eta_{k_i}$ means the possibility of $APD_i$ detects the pulse which contains $k_i$ photons. $(1-\eta_{k_i})$ means the possibility of $APD_i$ doesn't detect the pulse which contains $k_i$ photons. For example, Alice transmits the $0^\circ$ state photons, there may be the $APD_3$ or $APD_4$ responses rather than $APD_1$. In this case, we consider it as a valid detection. When Alice and Bob compare their measurement basis, they will correct this error.

For the state $0^\circ$, $90^\circ$, $45^\circ$, $135^\circ$, the possibility of $k_2,k_1,k_4,k_3$ equal 0 is 1. For instance, Alice transmits a $0^\circ$ state, the number of photons get to $APD_2$ must be 0, that is $k_2=0$, $P_0(\lambda_2)=1$.

On the assumption of Alice transmits one of the states in the four states equally. Bob make a valid detection in the possibility of:

$$P_{valid} = \sum_{k_1,k_2,k_3,k_4=0}^{\infty} P_{k_1}(\lambda_1)P_{k_2}(\lambda_2)P_{k_3}(\lambda_3)P_{k_4}(\lambda_4)\eta_{k_1k_2k_3k_4} \quad (1)$$

We sign the speed of the photon source $\mu$. The final key is the key secure enough to encrypt information, and its rate is $\nu$. As we can see in section 1, Alice and Bob will discard 1/2 data to compare their bases, and discard 1/2 data to reconciliation. According to the analysis, it is easy to conclude the relation of $\mu$ and $\nu$:

$$\nu = \frac{\mu \times P_{valid}}{2\times 2}$$

### *B. NUMERICAL SIMULATION*

The parameters of the devices that we generally use are: $\delta_{splitter}$=0.3dB, $\delta_{hwp}$=0.1dB, $\delta_{pbs}$=0.8dB, the detection efficiency of APD, $\eta$=10%, the possibility of dark count, $\eta_0=10^{-5}$, The light splitting ratio is 50:50, that is $\alpha$=0.5.

The loss of standard fiber is 0.2dB/km. Other utilities in the channel has a total loss of 2dB. When the fiber length $l$ is 50km, the loss of the channel is $\delta_{channel}$=12dB, when $l$ is 20km, the loss of the channel is $\delta_{channel}$=6dB.

From the equation (1), we can calculate the relation between the average number of photons in a pulse and the receive efficiency. It is shown as table I.

TABLE I. THE RELATION BETWEEN AVERAGE NUMBER OF PHOTONS AND RECEIVE EFFICIENCY

| Average photon number λ | The receive efficiency when l=50km | The receive efficiency when l=20km |
|---|---|---|
| 0.1 | 0.00049 | 0.00183 |
| 0.2 | 0.00094 | 0.00363 |
| 0.3 | 0.00139 | 0.00542 |
| 0.4 | 0.00184 | 0.00720 |
| 0.5 | 0.00229 | 0.00899 |
| 0.6 | 0.00274 | 0.01077 |
| 0.7 | 0.00319 | 0.01255 |
| 0.8 | 0.00364 | 0.01433 |
| 0.9 | 0.00409 | 0.01610 |

Set the speed of the photon source to be 20MHz, the length of the fiber is 20km and 50km, at this time, the key distribution rate is shown in figure 2 and table II.

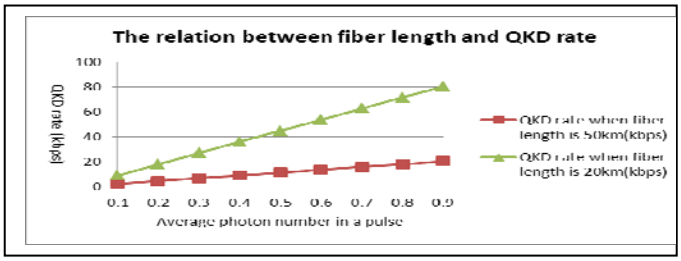


Figure 2. The relation between fiber length and QKD rate.

TABLE II. KEY DISTRIBUTION WHEN THE PHOTON SOURCE SPEED IS 20MHZ

| Average photon number λ | Key distribution rate at fiber length *l*=50km (kbps) | Key distribution rate at fiber length *l*=20km (kbps) |
|---|---|---|
| 0.1 | 2.452 | 9.167 |
| 0.2 | 4.705 | 18.127 |
| 0.3 | 6.957 | 27.079 |
| 0.4 | 9.209 | 36.020 |
| 0.5 | 11.461 | 44.949 |
| 0.6 | 13.712 | 53.862 |
| 0.7 | 15.962 | 62.759 |
| 0.8 | 18.212 | 71.637 |
| 0.9 | 20.462 | 80.495 |

## V. CONCLUSION

This paper studies the practical quantum key distribution system based on BB84 protocol, and it researches the expressions of the efficiency of receiver. But in this paper, there are only take photon source speed, channel loss, dark count into consider. Many other aspects are discarded. In the QKD system, the reconciliation also affects the key rate.

How to increase the key distribution rate when the eavesdropper exists is an important problem in the subsequently research.

## REFERENCES


[1] BENNETT C H, BRASSARD G. Quantum cryptography: public key and coin tossing[C]// Proceedings of the IEEE International Conference on Computer Systems and Signal Processing, New York, 1984:175-179.

[2] Yang Li, Wu Ling-An, Liu Song-Hao. On the Breidbart eavesdropping problem of the extended BB84 QKD protocol [J]. ACTA PHYSICA SINICA, 2002, 51(5):961-965. (Chinese)

[3] Chen Zhixin, Tang Zhilie, Liao Changjun, et al.Pratical Security Problem of Six States QKD Protocol[J].ACTA PHOTONICA SINICA,2005,35(1):126-129. (Chinese).

[4] Ivan C, Tommaso O. Implementation of real time high level protocol software for quantum key distribution[C]//IEEE International Conference on Signal Processing and Communications .Dubai ,United Arab Emirates,2007:24-27.

[5] Chen Jie, Li Yao, Wu Guang, et al. Stable quantum key distribution with polarization control[J].ACTA PHYSICA SINICA,2007,56(9):5243-5247. (Chinese)

[6] Chen Xia, Wang Fa-qiang, Lu Yi-qun, et al. A Differential Phase Shift Key Distribution QKD System Combing with Efficient BB84 Scheme[J]. ACTA PHOTONICA SINICA, 2008,37(5):1052-1056. (Chinese)

[7] Hu J Z, Wang X B. Quantum key distribution with the decoy-state[J]. Sci Sin Phys Mech Astron,2011,41(4):459-465. (Chinese)

[8] Zhou Yuan-yuan, Zhou Xue-jun, Gao Jun. Method of non-orthogonal decoy state quantum key distribution with heralded single photon source[J].Journal of PLA University of Science and Technology(Natural Science Edition),2010, 11(2):216-220. (Chinese)

[9] Shi Rui-juan, Zhu Chang-hua, Chen Nan, et al. Performance Analysis of Entangled Photon Pairs-based BB84 Protocol by Simulation. Computer Simulation. 2008, 25(6):120-123. (Chinese)

[10] S. Ali, M. Wahiddin. Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols[J].The European Physical Journal D.2010,60:405-410.

[11] Zhao Feng, Li Jing-ling, Analysis of the coefficient of QBER and its influence[J].Journal of Optoeletronics· Laser, 2010, 21(9):1383-1385. (Chinese)