A simple control system of quantum key distribution with high visibility*

MA Hai-qiang（马海强）[1,2**], **WANG Long**（汪龙）[1], **LI Shen**（李申）[2], **JIAO Rong-zhen**（焦荣珍）[1], **and WU Ling-an**（吴令安）[2**]

1. School of Sciences, Beijing University of Posts and Telecommunications, Beijing 100876, China

2. Laboratory of Optical Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China

(Received 1 December 2011)

A relatively simple plug-and-play control system of quantum key distribution (QKD) based on PCI7300 card is demonstrated, including mechanism design, key generation and key acquisition. The system works very well at the repetition frequency of 1 MHz, and the key generation rate is 100 k/s. A visibility of better than 95% over 50 km-long fiber at 1.31 μm is obtained, which is stable under ordinary lab conditions for 24 h without any feedback control or adjustment. The presented system is a quite promising candidate to realize the QKD in the future.

Document code: A **Article ID:** 1673-1905(2012)04-0318-3

DOI 10.1007/s11801-012-1145-9

Quantum key distribution (QKD) has been developed for several years, which is used to create absolutely shared secret key between Alice and Bob[1,2]. During the last two decades, all the known practical setups for the QKD are realized with photons, which can be roughly classified into two categories as the one in optical fiber[3-10] and the one in free space[11]. The QKD experiment system can be divided into two parts, known as the optical system and the control system, both of which are important. Generally, commercial devices are most frequently used in the QKD controlling systems, which can not match with each other and can lower the efficiency of the code rate. It raises many challenges to the design of electronics for the QKD controlling systems[12,13]. In this paper, we present a control system including details about mechanism design, key generation and key acquisition.

According to Bennett-Brassard 1984 (BB84) protocol, Alice sends a series of single photons to Bob via the quantum channel. When the photons arrive at Bob's side, Bob uses a series of random figures among 1, 2, 3 and 4 which represent random phase shift ϕ_B to modulate every photon passing through him by his phase modulator (PM) PMB. Later the photons modulated by Bob return to Alice who also uses a series of prepared random phase shift ϕ_A to modulate the photons by her phase modulator PM_A. Since the photons are modulated twice by Alice and Bob, the photons are detected or not in the end depending on the phase shift of $\phi_B-\phi_A$. The photons can be detected by the single photon detector (SPD) which is controlled by Alice's computer.

In our experimental system, the laser device not only generates a series of pulses at repetition frequency of 1 MHz, but also provides the global clock (GC) to the whole system at the same frequency. When a laser pulse is generated, the laser device sends a rising edge to every device in the system to take the proper action. For example, Alice and Bob must give out their random figure to the PM when the photons arrive. The SPD must begin to detect whether there is a photon when the photon ought to arrive. Because of the long distance between Alice and Bob, different clocks are applied on each side for convenience instead of using a unique GC source. The two clocks must be the same, otherwise some calibration is needed. Obviously, precise time delayer is necessary since we must control the times that the photon runs in the fiber and the clock signal runs in the wire. Thus, four delayers in all are required between GC and PM_A, GC and PM_B, GC and SPD_1, GC and SPD_2 to make all devices operate at the proper time when the photon arrives referring to the GC.

The PM is controlled by its input port receiving analog electronic signal, which only works at pulse-state. The computer should output the data at a rate up to 1 MHz, but the

* This work has been supported by the National Natural Science Foundation of China (Nos.61178010 and 10805006), the Fundamental Research Funds for the Central Universities (No.bupt2010zx04), and the China Postdoctoral Science Foundation (No.20100480508).

** E-mails: hqma@bupt.edu.cn; wula@aphy.iphy.ac.cn

parallel port cannot satisfy the demand. The P7300 card developed by ADLink company is applied in the experimental system for this high performance of inputting and outputting data. Between Alice's and Bob's computers and their PMs respectively, two home-made phase modulator mate (PMM) devices are used for converting the digital signal to analog signal, and the devices also satisfy the rule of the PM. It will give a pulse with fixed width, whose amplitude is based on the computer's output data to drive the PM properly.

Considering the high frequency of 1 MHz, computer is expected to output the data at the exact frequency. The data are put into the memory of the P7300 card, through which the card fetches data directly by working in direct memory access (DMA) mode, instead of using some codes to response the rising edge, and it generates some random data saved to disk. To deal with the contradiction that memory is limited but the keys generate continuously, the long prepared series are broken into many blocks which have certain logical size. In other words, the generated keys are one group by one group whose length is 10000 keys. At every interval of the two consecutive groups during the key generation, the computer processes the data of last group and prepares the data of the next group.

How to synchronize Alice and Bob is another challenge of the QKD control system. In our experimental system, Alice and Bob are not peer to peer, but Alice controls the receiving and dispatching of the data only.

When the system is to be started, Bob must enter the "READY" state to wait "GROUP_START" command from Alice. When a group of data transmission is finished, Bob also sends the "GROUP_END" command to Alice to indicate that he has completed the data outputting and has prepared the data of next group. When Alice receives this command, she can start a new group by sending "GROUP_START" again.

The application of delayers in the system ensures that the PMs can modulate the nearest photon accurately. Since the photon travels a long distance between Alice and Bob and the repetition frequency of the laser pulses is high, there are several photon pulses running in the fiber at the same time. Then PM_A and PM_B modulate different photons at the same time. If we cannot know how many photon pulses are there in the fiber, we also cannot decide which pulse is modulated through the random data by Alice and Bob. The GC works forever, so there are photons in the fibers forever. When the "GRO UP_ START" command is issued, the data acquisition must start at once without waiting for the first photon which is modulated, since we cannot recognize it from the photons which are not modulated before the group begins. In the experiment, a series of test data are designed for Alice and Bob to get the distance between Alice and Bob and the location of the first modulated photon in the acquisition data array. As is shown in Tab.1, A_1, A_2, A_3, A_4,⋯, A_M is the array of random data for Alice, B_1, B_2, B_3, B_4,⋯, B_M is another array for Bob, and Z_1, Z_2, Z_3, Z_4,⋯, $Z_{M+\varepsilon}$ is the acquisition data array which means the detection probability. Since the photon transmission takes time, the length of $\boldsymbol{Z}$ array is a little larger than those of $\boldsymbol{A}_M$ and $\boldsymbol{B}_M$.

Tab.1 Detection probability of the detector for different values of phase shifts chosen by Alice and Bob

M	1	2	3	4 ……	M	$M+\varepsilon$
$\boldsymbol{A}_M$	0	1	0	1 ……	0	×
$\boldsymbol{B}_M$	0	0	1	1 ……	0	×
$\boldsymbol{Z}_M$	0	1	1	0 ……	0	0

We postulate the following for example. First, we let B_i= 0(i = 1, 2, ⋯, M), A_i= 0(i = 1, 2, ⋯, p − 1, p + 1, ⋯, M), where p is an appropriate location, and A_p=2. The column $\boldsymbol{Z}$ is expected that there is only one "1". We can find the location of the only one "1" from the acquisition result in the column $\boldsymbol{Z}$, and let the location be l_{Alice}. Using the same method, we can find l_{Bob}, too. From above discussion, the distance between Alice and Bob can be decided by $|l_{\mathrm{Alice}}- l_{\mathrm{Bob}}|$, and the location of the first modulated photon can also be decided by l_{Alice}.

In fact, the laser pulse is strongly attenuated, so the average number of photons in each pulse is of the order of 0.1. The SPD has the quantum efficiency of less than 20%, and it cannot detect every photon. Some dark counts may take place. The test process may need to repeat several times to get the final result.

The long term stability of this scheme is tested at 1.31 μm by using the PiLas laser (made by Advanced Laser Diode Systems) with a repetition rate of 1 MHz and a pulse width of 18 ps[14]. Two SPDs are developed in-house using InGaAs/

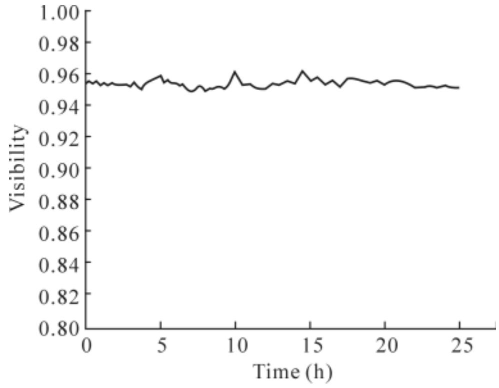

Fig.1 Visibility of our experimental setup as a function of time over more than 24 h

InP avalanche photodiodes (EPM239BA). At the temperature of -62.5 °C, a dark count of about 1×10^{-6} ns^{-1} could be achieved with a quantum efficiency of 18%. A gate width of 20 ns is used for the detectors which are synchronized with the laser at repetition rate of 1 MHz using an external clock trigger. A 50 km-long trunk fiber is applied to connect Alice and Bob. Without any feedback control or adjustment to the system, the visibility is better than 95% for more than 24 h continuous operation, which can be seen from Fig.1.

The control system of quantum key distribution works very well at the repetition frequency of 1 MHz when the distance between Alice and Bob is up to 50 km. The key generation rate is 100 k/s, and the visibility is better than 95% for more than 24 h continuous operation, which makes it a quite promising candidate to realize the QKD in the future.

References

[1] C. H. Bennett and G. Brassard, Quantum Cryptography:Public Key Distribution and Coin, IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 175 (1984).

[2] ZHAO Feng and LI Jing-ling, Journal of Optoelectronics • Laser **21**, 1383 (2010). (in Chinese)

[3] QUAN Dong-xiao, ZHAO Nan, PEI Chang-xing, ZHU Chang-hua and LIU Dan, Journal of Optoelectronics • Laser **22**, 71 (2011). (in Chinese)

[4] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, New Journal of Physics **4**, 41 (2002).

[5] C. Y. Zhou and H. P. Zeng, Applied Physics Letters **82**, 832 (2003).

[6] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka and K. Nakamura, Japanese Journal of Applied Physics **43**, 1217 (2004).

[7] P A Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller and J. E. Nordholt, New Journal of Physics **8**, 193 (2006).

[8] X. F. Mo, B. Zhu, Z. F. Han and G. C. Guo, Optics Letters **30**, 2632 (2005).

[9] Z. Q. Yin, H. W. Li, W. Chen, Z. F. Han and G. C. Guo, Physics Review A **82**, 042335 (2010).

[10] S. H. Sun, H. Q. Ma, J. J. Han, L. M. Liang and C. Z. Li, Optics Letters **35**, 1203 (2010).

[11] Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, C. Y. Lu, C. Z. Peng, T. Yang and J. W. Pan, Physics Review Letters **95**, 200502.1 (2005).

[12] WANG Jian, ZHANG Hong-fei, WAN Xu, GAO Yuan, CUI Ke, CAI Wenqi, CHEN Teng-yun, LIANG Hao and JIN Ge, Journal of Optoelectronics • Laser **21**, 861 (2010). (in Chinese)

[13] ZHAO Nan, PEI Chang-xing, QUAN Dong-xiao and SUN Xiao-nan, Journal of Optoelectronics • Laser **22**, 1411 (2011). (in Chinese)

[14] H. Q. Ma and L. A. Wu, 5th Asia Pacific Conference on Quantum Information Science, Taiyuan, 59 (2010).