Polarization recovery and auto-compensation in Quantum Key Distribution network[1]

Lijun Ma[a], Hai Xu[a,b], Xiao Tang[a]

[a] *National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899*
[b] *University Maryland Baltimore County, Baltimore, MD 21250*
lijun.ma@nist.gov, xiao.tang@nist.gov

ABSTRACT

A Quantum Key Distribution (QKD) network can allow multi-user communication via secure key. Moreover, by actively switching communication nodes, one can achieve high key transmission rate for the selected nodes. However, the polarization properties of different fiber path are different and these properties also randomly drift over time. Therefore, polarization recovery after the switching and auto-compensation during key transmission are critical for the QKD network. In this work, we use programmable polarization controllers to implement polarization recovery and auto-compensation in the QKD network. We will also discuss its time limitation and future improvement.

Keywords: Quantum Key Distribution, Polarization recovery, Polarization auto-compensation.

1. INTRODUCTION

For polarization encoding fiber-based quantum-key distribution (QKD) networks, one major limitation to practical application is that different fiber paths have different polarization properties [1]. Due to perturbation from the ambient environment and other mechanical sources, such polarization properties also drift randomly over time. Consequently, it is important to auto-recover the polarization state of the signal after each switching event and to auto-compensate the temporal drift of the polarization state during the key transmission to a given node [2]. An active polarization alignment sub-system based on the feedback from photodiodes is the most straightforward approach to automatically recover the polarization state as the fiber drifts. Although this approach was first implemented in 1995 in point-to-point QKD system [3], it has not been pursued since then and has not been reported to be implemented in QKD network [1].

In this work, we have developed two active polarization recovery and auto-compensation (PRAC) sub-systems and applied them to a fiber-based polarization encoding QKD system [4]. One is based on liquid crystal retarders and the other is based on 3-axis piezo polarization controllers. For the first time to our knowledge, we demonstrate that the PRAC stabilizes the advanced QKD network. Moreover, we discuss the limitations of operation time and propose approaches for further improvements.

2. SYSTEM CONFIGURATION

We previously reported a polarization encoding QKD system with two nodes connected by 1 km of optical fiber [4-6], and based on this system, we built a 3-node QKD secured network controlled by optical switches [7]. As shown in Fig.

[1] The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Polarization recovery and auto-compensation in Quantum Key Distribution network	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Institute of Standards and Technology,100 Bureau Dr,Gaithersburg,MD,20899**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Proc. SPIE Vol. 6305, 630513 (August 2006)

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

1, the optical switch at Alice controls the destination, Bob1 or Bob2. Once the quantum channel has been established between Alice and Bob1 (or Bob2), Alice and Bob1 (or Bob2) generate and share secured quantum keys enabling subsequent communication with each other via an unsecured commercial internet network. This structure can be extended to a one-to-any network or an any-to-any network. The focus of this work is the polarization auto-recovery after switching and polarization auto-compensation during the key generation and sharing between Alice and one Bob.

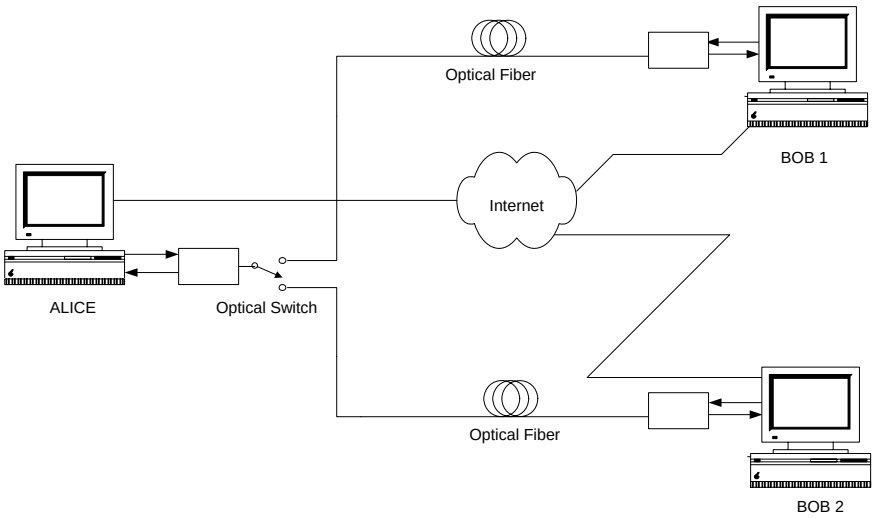

Figure 1. Schematic diagram of a QKD network with one Alice and two Bobs

The quantum channel between Alice and Bob1 is shown in Fig. 2, the channel between Alice and Bob2 is similar. At Alice, laser pulses are generated by vertical cavity surface emitting lasers (VCSELs) and attenuated into single photon level. The polarization states of photons are set by polarizers according to corresponding protocol (B92 or BB84). Then photons are combined and sent into a fiber through a non-polarizing beam splitter (NPBS). The polarizers Pol. 0A, 0B, 1A, and 1B are oriented to 0°, 90°, +45°, and -45° respectively. Only two channels, 0A and 1A, are used for B92, while all four channels are used for BB84. At Bob, polarization controllers recover the polarization state of photons to their original state at Alice. The 3-dB coupler randomly chooses the detection base and the polarization beam splitter (PBS) helps to determine the key value. Finally the photons are detected by single photon detectors (APDs). Two APDs, 0A and 1A, are used for B92, while four APDs are all used for BB84.

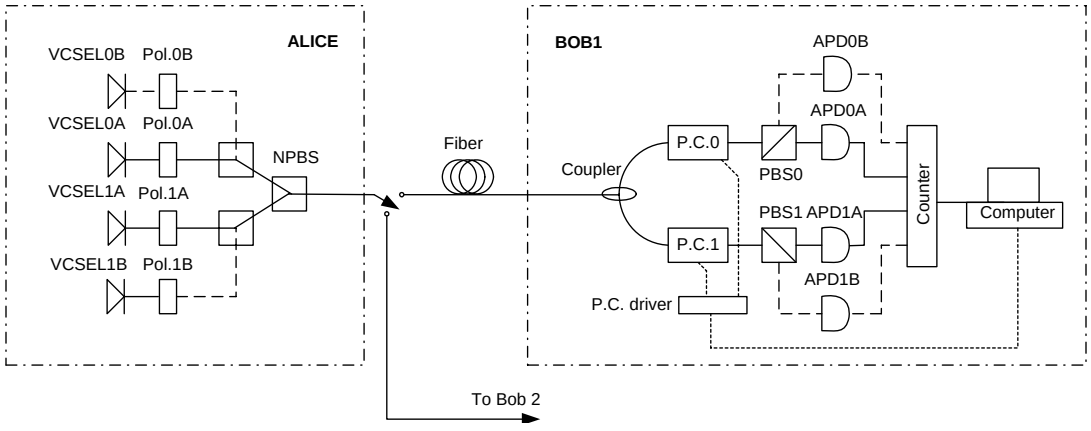

Figure 2. Schematic diagram of the QKD system with PRAC sub-systems. VCSEL: Vertical Cavity Surface Emitting Laser ; Pol.: Polarizer; NPBS: Non-Polarizing beam splitter; P.C.: Polarization Controller; PBS: Polarizing beam splitter; APD: Silicon avalanche photodiode.

By replacing manually adjusted polarization controllers with computer programmable controllers and sampling the counts from APDs as feedback signal, we developed two different active PRAC sub-systems at Bob1 and Bob2 to automatically recover and maintain the polarization state of arriving photons.

3. POLARIZATION RECOVERY AND AUTO-COMPENSATION

Two pairs of liquid crystal retarders (LCR) are used in the PRAC at Bob1. Each pair forms a polarization controller for one of two output arms of the 3-dB coupler. The axes of the LCRs in the pair are pre-aligned with the PBS, as shown in Fig. 3(a), and their phases are controlled by a computer. The slow axes of the two LCRs are aligned to the passing axis of PBS by 0° and 45° respectively, while PBS splits the 0°-component of the signal to output port 1 and 90°-component to output port 2 (+/- 45° for the other basis). The retardance (α, β) of the LCRs is determined by the applied voltage, which is controlled by the same computer. In Eq. (1) we show the transformation of the Jones vectors of the whole PRAC. With proper applied voltages, and thus the phase retardance of LC, ideally we can rotate received signals at arbitrary polarization states to realize the BB84 or B92 protocol.

$$\begin{cases} E_{out1} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \cos(\beta/2) & i\sin(\beta/2) \\ i\sin(\beta/2) & \cos(\beta/2) \end{bmatrix} \begin{bmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{bmatrix} E_{in} \\ E_{out2} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \cos(\beta/2) & i\sin(\beta/2) \\ i\sin(\beta/2) & \cos(\beta/2) \end{bmatrix} \begin{bmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{bmatrix} E_{in} \end{cases} \quad (1)$$

Two in-line polarization controllers are equipped in the PRAC at Bob2. Each consists of three Piezo-driving phase retarders and their axes are independently controlled by 3 piezo drivers. The phase retardances of the three retarders are fixed at π/4, π/2, and π/4 respectively. We can realize arbitrary polarization transformations by setting the axis of each phase retarder. The structure of the PRAC at Bob2 is shown in Figure 3(b). In comparison, the LC-based PRAC has to be aligned with PBS while the piezo one does not since it can realize arbitrary transformations. On the other hand, the piezo PRAC is fiber based with virtually no insertion loss, though it may drift slowly.

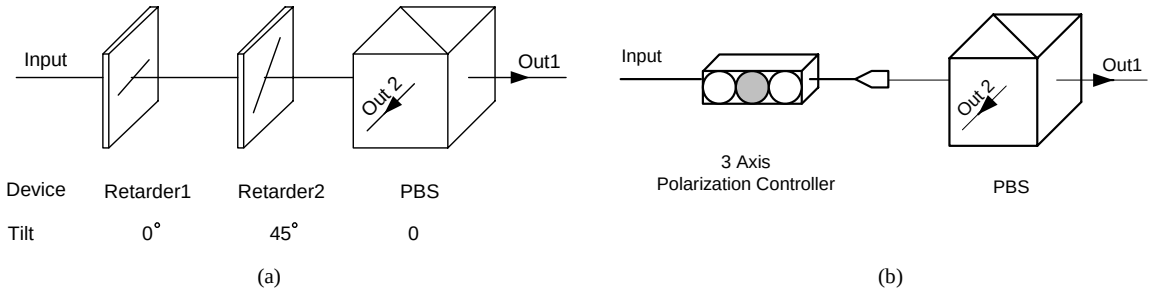

Figure 3. Two kinds of PRAC setting: Liquid Crystal Retardance (a) and Piezo Polarization Controllers (b)

The extinction ratio (ER) in polarization encoding QKD systems is defined as the ratio of the correct counts to the incorrect counts in compatible protocol bases in BB84, for example, the ratio between the photon counts of the two output ports of the PBS for a given basis once photons at a given key value at the same basis were repeatedly sent. In B92, the ER is the ratio of the counts in compatible detection bases to the counts in incompatible detection bases, for example, the ratio between the counts of the output port 1 of two PBS once a given key value is sent. Polarization drift in the transmission fiber induces fluctuation of the ER, which directly influences the quantum bit error rate (QBER). The extinction ratio can be measured by turning on/off corresponding VCSELs and comparing the counts from APDs. As a result, ER is a suitable feedback signal for PRAC.

A computer at Bob is used to request the turning on/off of VCSELs at Alice, to sample the counts from the APDs, to set the polarization controllers, and thus to realize the polarization auto-recovery and auto-compensation (PRAC). In auto-recovery mode, we set different applied voltages for the polarization controllers, measure the ER in each setting, and finally choose the optimal setting voltage. The whole procedure contains two stages: First a coarse-step search is performed to find the optimal area and then a fine-step search to find the optimal points. During the key transmission between Alice and a given Bob, every 15 minutes we halt the key transmission and send predetermined keys with predetermined bases to measure the ER. We first check the ER at current settings. When the fiber has drifted so significantly since the last PRAC operations that ER decreases below 20 dB, we will restart auto-recovery mode process. Otherwise, we start the auto-compensation mode process. We first check points near the current setting. If the transmission fiber drifts insignificantly so that the current setting remains optimal, we resume key transmission without any change to the setting. Otherwise, we change the current setting to the nearby one that gives the highest ER and start another search step. We repeat above steps until the current setting gives the optimal ER. Then we resume the key transmission.

4. RESULTS AND DISCUSSION

In our experiment in the laboratory, we studied both types of PRAC. In order to guarantee the QBER induced by polarization leakage to be less than 1%, the ER should be larger than 20 dB. With both of the PRACs we find that the ER is above 21 dB after auto-recovery mode and is maintained beyond 20 dB with auto-compensation. The curves in Figure 4 show the ER over a period of 24 hours with and without PRAC. As shown in the figure, with manual adjustment of the polarization controller, the extinction ratio is adjusted to 21 dB at the beginning, but it degrades gradually due to the polarization drift. With the PRACs, the extinction ratio is kept above 20 dB for 24 hours under our laboratory environment. Due to the finite searching steps and slight fluctuation in VCSEL, the ER does not reach the maximal value of 22 dB after every auto-compensation operation.

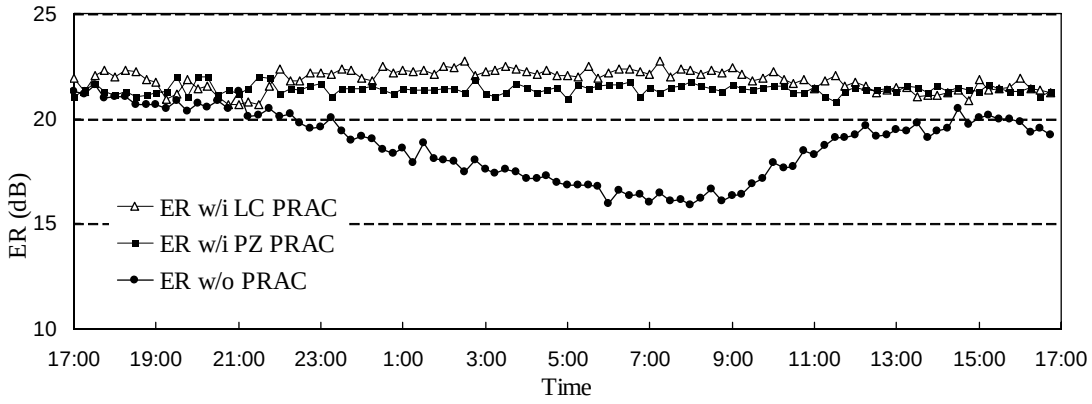

Figure 4. The extinction ratio with/without PRAC sub-system. With PRAC, the ER is collected immediately after each PRAC tracking operation, which is performed every 15 minutes over 24 hours. Without PRAC, the ER is measured every 15 minutes but the system is untouched during the whole 24 hours.

It is important to reduce the operation time of PRAC. This time of is determined by

$$\begin{aligned} T_{op} &= n \times (t_{PC} + t_{COL}) && auto\text{-}recovery \\ T_{op} &= n \times m \times (t_{PC} + t_{COL}) && auto\text{-}compensation \end{aligned} \tag{2}$$

where T_{op} is the operation time, n is the number of search steps, and m is the number of nearby settings compared in each step in the auto-compensation mode. In this experiment we set $m = 9$. The time period t_{PC} is the responding time of polarization controllers, and t_{COL} is the time needed to collect a sufficient number of photons in ER measurements.

The number of search steps (n) is about 2500 in auto-recovery mode and varies in auto-compensation mode depending on the degree of polarization drift during two PRAC operations. In this experiment, the fiber length between Alice and Bobs is 1 km and the mean photon number is set to 0.1. Under these settings, the collect time t_{COL} is set to 50 ms to guarantee sufficient counts in the ER measurement. In a LC PRAC the communication time of the USB port is negligible in comparison with the liquid crystal response time, which is about 100 ms [8]. The response time of the piezo polarization controller is about 30 μs [9], which is much faster than that of liquid crystal. However, the communication speed of the RS232 interface between the piezo controllers' driver and the PC is greatly limited, therefore its response time becomes as long as 150 ms.

According to Eq. (2) and the above discussion, the operation time in the auto-recovery mode is around 6 minutes in the LC PRAC and 8 minutes in the piezo PRAC), which is in agreement with the experiment result. For the auto-compensation mode, the number of search steps in each PRAC operation is show in fig. 5. Because the amount of polarization drift in each 15-minute interval varies, each PRAC operation needs different searching loops to find the optimal applied voltage under which the ER is maximized. As a result, T_{op} differs in each operation. The PRACs were tested in a laboratory environment for 24 hours with the operation taking action every 15 minutes. The operation time for the LC PRAC is 15 second (10 loops) with a searching step length of 0.01V (the full range is 0-10 V). The operation time for the PZ PRAC is 36 second (20 loops) with a searching step length of 0.15 V (the full range is 0-150V). Note that applying a search step in LC PRAC is to shift the phase of the phase retarder, while in PZ PRAC it is to change axis orientation of the phase retarder, so their operation time can not be compared directly. Our future improvements for the PRAC will balance the search precision and operation time to reach the shortest operation time with the required precision.

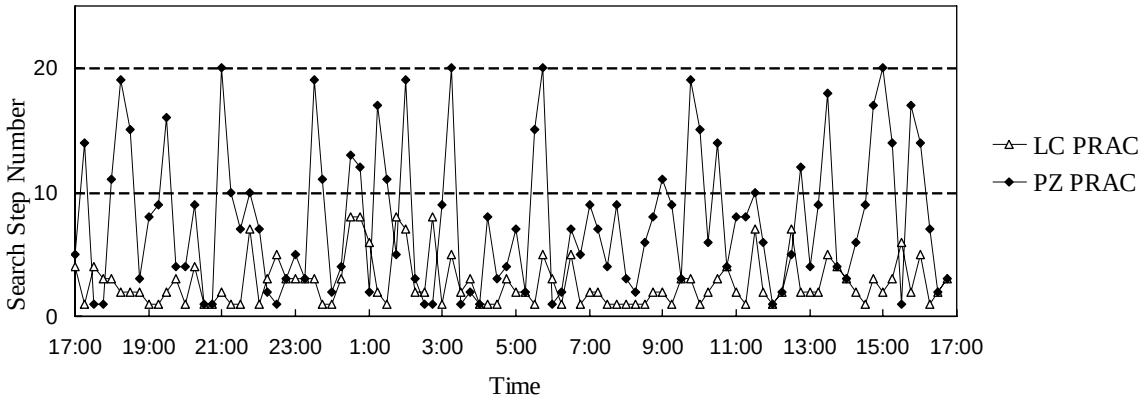

Figure 5. The number of search steps in every PRAC instance.

The operation time of the current PRACs is possibly still too long for QKD systems operating in the field. There fiber may drift significantly in 6-8 minutes and thus fail the auto-recovery. Moreover, due to the fast fiber drift, one must perform auto-compensation more frequently, for example, once per minute. If the auto-compensation time is still 15 seconds, the effective key transmission rate is thus reduced by one fourth. We can shorten the PRAC operation time by reducing the response time of polarization controllers t_{PC} and the collection time t_{COL}. However, the t_{PC} for a LC PRAC can not be further reduced due to the long response time of the liquid crystal itself. On the other hand, it is possible to reduce the t_{PC} of a PZ PRAC, since its limitation is due to the driver's interface to the computer instead of the piezo controller itself. Currently, a new piezo driver with a fast computer interface is under development. With the new driver, we expect to reduce t_{PC} of the PZ PRAC to the same level of piezo controller itself (tens of micro seconds). In order to reduce the collection time t_{COL} a potential solution is to increase the photon number during the PRAC operation. With a higher mean photon number, it is possible to reduce t_{COL} to less than 1 ms. In this approach, fast optical switches could be added at Alice and synchronized with the PRAC at Bob to bypass the attenuators. This

research is also underway. With the approaches mentioned above, we expect a reduced searching step time of about 1ms. Then T_{op}, the operation time for auto-recovery mode may be reduced to several seconds, and the T_{op}, operation time for auto-compensation mode may be reduced to less than 100 ms.

As mentioned earlier, current the auto-compensation mode process requires the suspension of key transmission and therefore reduces the effective key transmission rate. One could also implement a real-time PRAC scheme in which the polarization drift is monitored and compensated during the key transmission. By this means continuous key transmission may be achieved. In such a scheme, the ER cannot be used as the feedback because one VCSEL at Alice must be turned off in the ER measurement. Currently we are investigating a PRAC scheme in which the QBER is used as feedback. One difficulty in using the QBER is that one needs to identify whether the fast dynamic fluctuation of the QBER is induced only by the polarization drift.

5. CONCLUSION

We have developed polarization auto-recovery and auto-compensation sub-systems for QKD networks based on liquid crystal retarders and piezo polarization controllers. Both sub-systems have been integrated in a 3-node QKD network demonstration. The operation time is still the main obstacle for the sub-system to be practical for field application. In order to reduce its operation time, we are going to optimize the search step length, select faster PC-controllable polarization controllers, and increase the photon number during PRAC to reduce the sampling time in the further work.

ACKNOWLEDGEMENT

This work was supported in part by the Defense Advanced Research Projects Agency under the DARPA QuIST program.

REFERENCES

1. N. Gisin G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, Rev. Mod. Phys. 74, 145-195 (2002).
2. K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, “A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System,” IEEE J. of Quantum Electron, Vol. 40, 900-908 (2004)
3. J.D. Franson and B.C. Jacobs,” Operational system for quantum cryptography” Electronics Letters Vol. 31, No. 3, 232-234 (1995)
4. Xiao Tang, Lijun Ma, Alan Mink, Anastase. Nakassis, Barry Hershman, Joshua Bienfang, Ronald F. Boisvert, Charles Clark, and Carl Williams, “High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding,” in Optics and Photonics 2005: Quantum Communications and Quantum Imaging III, Proc. SPIE 5893, 1A-1-1A-9 (2005).
5. Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Hai Xu, Barry Hershman, Joshua Bienfang, David Su, Ronald F. Boisvert, Charles Clark, and Carl. Williams, “Quantum Key Distribution system operating at sifted key-rate over 4Mbit/s”, Defense and Security 06, Proc. SPIE 6244, 62440P-1~ 62440P-8(2006)
6. Xiao Tang**,** Lijun Ma, Alan Mink, Anastase Nakassis, Hai Xu, Barry Hershman, Joshua Bienfang, David Su, Ronald F. Boisvert, Carles Clark, and Carl Williams, “Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s”, Optics Express, Vol. 14 (6): 2062-2070 (2006)
7. Xiao Tang**,** Lijun Ma, Alan Mink, Anastase Nakassis, Hai Xu, Barry Hershman, Joshua Bienfang, David Su, Ronald F. Boisvert, Carles Clark, and Carl Williams, “Demonstration of Active Quantum Key Distribution Network,” in Optics and Photonics 2006, San Diego, Aug.13~17
8. Meadowlark optics catalog: liquid crystals section, http://www.meadowlark.com/catalog/LiquidCrystals.pdf
9. General Photonics product catalog: http://www.generalphotonics.com/PolariteII.htm