High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding[1]

Xiao Tang[2], Lijun Ma, Alan Mink[3], Anastase Nakassis, Barry Hershman, Joshua Bienfang,
Ronald F. Boisvert, Charles Clark and Carl Williams
National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899

ABSTRACT

We have implemented a quantum key distribution (QKD) system with polarization encoding at 850 nm over 1 km of optical fiber. The high-speed management of the bit-stream, generation of random numbers and processing of the sifting algorithm are all handled by a pair of custom data handling circuit boards. As a complete system using a clock rate of 1.25 Gbit/s, it produces sifted keys at a rate of 1.1 Mb/s with an error rate lower than 1.3% while operating at a transmission rate of 312.5 Mbit/s and a mean photon number $\mu = 0.1$. With a number of proposed improvements this system has a potential for a higher key rate without an elevated error rate.

Keywords: Quantum key distribution, polarization encoding, BB84, B92, cryptography, one-time pad.

1. INTRODUCTION

A Quantum Key Distribution (QKD) system can create a shared, secret cryptographic key over unsecured optical links between two users. In 1984 Bennett and Brassard [1] proposed their quantum key distribution protocol, BB84. A simplified version, B92, was published in 1992 [2]. Since then, a number of groups have developed experimental QKD systems, which were described in a comprehensive review article [3]. These QKD systems were either operating in free-space [4,5] or over optical fiber [6,7]. The first study of fiber based QKD at 810 nm wavelength was reported in 1994 [8]. The security of the shared secret key afforded by QKD is guaranteed by the fundamental quantum properties of single photons. The generation of secret key at high speed and in real time would enable the use of one-time pad cryptography, which provides provable security.

Effective detection of single photons is a critical issue in QKD development. Currently Ge or InGaAs based avalanche photo diodes (APDs) are used to detect single photons at telecom wavelengths (1550 and 1310 nm). But their detection efficiency is low and their operating speed is seriously limited by after-pulsing and a long recovery time (dead time) in the APD after an avalanche process. Silicon based APDs have much better performance but they can only detect photons at visible or near IR wavelengths shorter than about 1000 nm. At these shorter wavelengths, a single mode telecom fiber has high loss and becomes multimodal, thus limiting the potential transmission distance. However, these Si-APDs may be used in QKD systems integrated into local area networks (LANs). Gordon et al [9] have reported a detailed study on an experimental polarization encoding QKD system at 850 nm with Si-APD using standard telecom fiber. The longest fiber length they reported was about 11 km.

---

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

[2] xiao.tang@nist.gov; phone 301-975-2503; www.nist.gov
[3] alan.mink@nist.gov; phone 301-975-5681; www.nist.gov

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding	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
Proceedings of SPIE Vol. 5893, Optics and Photonics Conference, San Diego, CA, Jul 31-Aug 4, 2005.

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	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**9**	

At NIST, a free-space polarization encoding QKD system operating over a 730 m link was developed in 2004 [4]. Using the infrastructure from that free-space system, we implemented a fiber-based polarization encoding QKD system operating over 1 km of optical fiber with a synchronized clock rate of 1.25 GHz. This fiber-based system uses 850 nm VCSELs as the light source and Si-APDs for the single photon detectors. Like the free-space system, the fiber-based system is designed to implement the four-state BB84 protocol with linear-polarization states, but our initial demonstration is based on B92. The sifted key rate of our QKD system is expected to double once upgraded to the BB84 protocol. Executing the B92 protocol and operating at a data transmission rate of 312.5 Mbit/s and an average photon number $\mu = 0.1$, a sifted key rate of 1.1 Mbit/s is achieved with an error rate lower than 1.3%. After error correction and privacy amplification secure keys are generated. In this paper, we discuss the design and performance analysis of this fiber-based polarization encoding QKD system.

2. SYSTEM CONFIGURATION

The NIST fiber-based polarization encoding QKD system is similar to the NIST free space system [4]. The experimental configuration is shown in figure 1. Alice and Bob are PC-based commercial off the shelf computers using a Linux operating system. A pair of custom high-speed data handling circuit boards were designed and implemented at NIST. The boards communicate with Alice and Bob via their PCI bus. On each board, there is a field-programmable gate array (FPGA) and gigabit Ethernet serializers/deserializers (SerDes): one for the classical channel and four for the quantum channel. A 1.25 Gbit/s CWDM transceiver at each end of 1 km of SMF-28 fiber is used to form the bi-directional classical channel at 1510 nm and 1590 nm. Alice's board generates classical and quantum data-streams at a synchronized 1.25 GHz. Bob's board recovers and synchronizes to that clock from the received classical channel data-stream, which uses a standard 8B/10B encoding scheme.

Alice and Bob are also connected via a unidirectional quantum channel that is parallel to the classical channel. In order to take advantages of the high speed 10 Gbit/s multimode VCSELs and the high speed, high detection efficiency of Si-APDs, a wavelength of 850 nm is used for the quantum channel. When executing the B92 protocol, Alice randomly fires pulsed light polarized at +45 degree in path 0 and vertical in path 1, see figure 1. In each path the light from the VCSELs is coupled into a multimode fiber and then attenuated by a variable optical attenuator (VOA). The attenuation is carefully adjusted to yield a mean photon number $\mu = 0.1$ at Alice's output. The attenuated light is then coupled into a single mode 850 nm fiber patchcord and collimated into free-space. After one beam passes through a vertically (V) oriented polarizer and the other through a +45 degree oriented polarizer, they are combined via a non-polarizing beam-splitting cube (NPBS) and then coupled into a single mode fiber (Corning HI780, 1 km). After attenuation, this results, on average, in only one photon in every 10 pulses that leaves from Alice. At the receiver, Bob, a 1 x 2 non-polarizing single mode fiber coupler performs a random choice of measuring polarization states: either horizontal or -45 degree, which corresponds to bit values of "0" or "1". A fiber polarization controller (P.C.) is installed in each branch (path 0 and path 1) of the fiber coupler to recover the photon's polarization state. In each path, single photons are measured by a polarizing beam-splitting cube (PBS). After the PBS an interference filter (I.F.) is used to remove noise at other wavelengths. Finally, the photons are coupled into a 62.5 μm multimode fiber and then focused on to the surface of the Si-APD for detection.

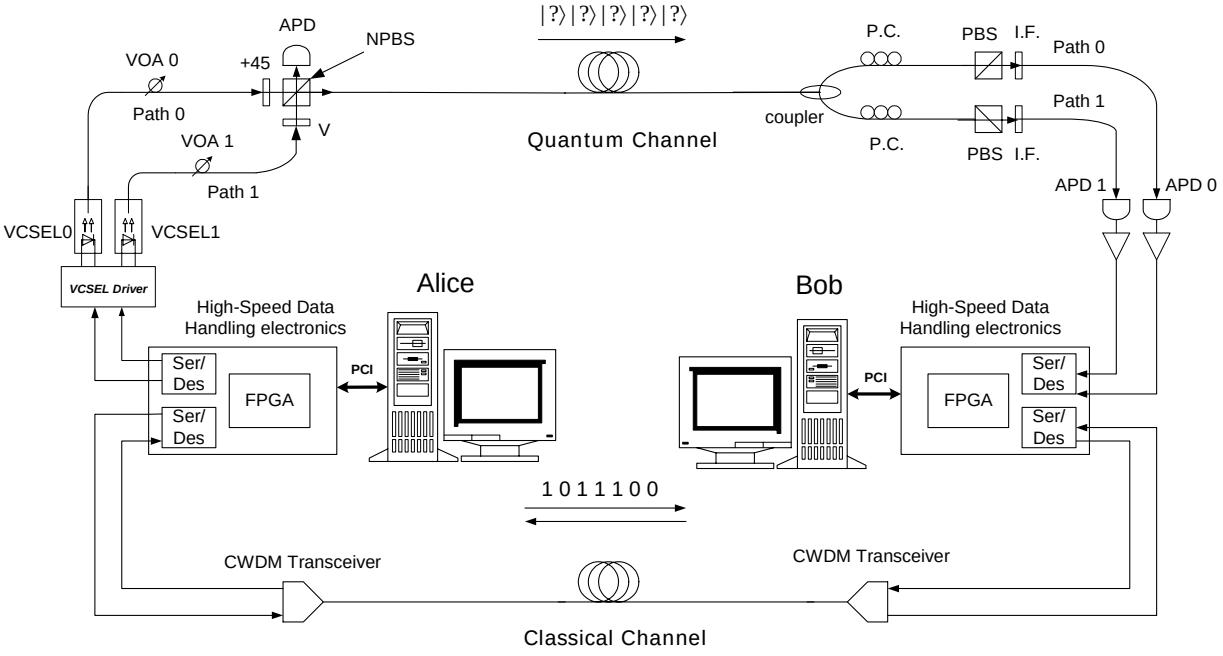
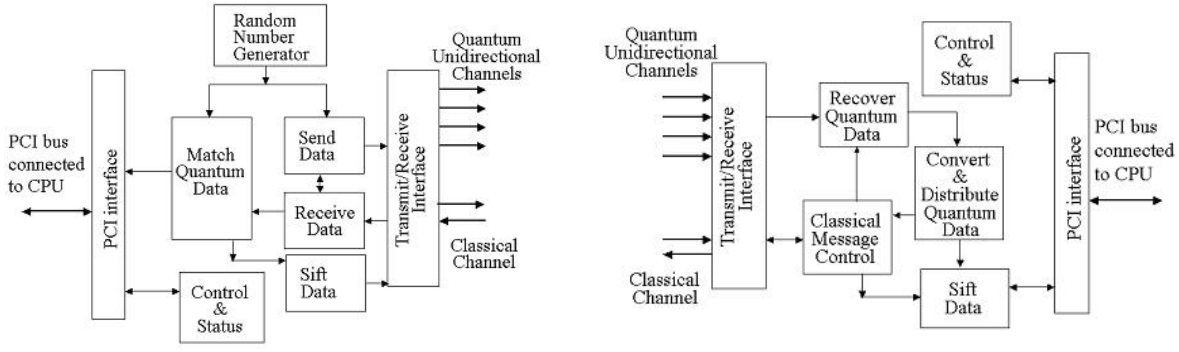


Figure 1. Experimental setup

The FPGA on Alice's board, see figure 2(a), generates and stores a bit-stream of pseudo random data at up to 1.25 Gbit/s. Every 2048 bits are grouped in a packet, where the 0's trigger VCSEL0 to produce a 45 degree polarization and the 1's trigger VCSEL1 to produce a vertical polarization. The data rates used in our measurements correspond to a photon pulse repetition rate at 312.5 or 156.25 Mbit/s (1/4 or 1/8 of the clock rate). Alice sends a synchronizing message to Bob on the classical channel at the beginning of each quantum packet. Bob's FPGA, see figure 2(b), searches for the rising edge of detected photon signals from the APDs. For each detection event, the packet number and bit position within the packet (and basis value for BB84), but not the bit value, of the detected photons are returned to Alice over the classical channel. Alice's FPGA matches each detection event with the corresponding event of the stored bit-stream. The matched results, again without the bit values, are sent back to Bob to confirm reception and then both Bob and Alice send the bit values to their CPUs for reconciliation and privacy amplification [10] to generate their shared secret keys. The quantum error rate can be measured in real time from the raw data before reconciliation.



(a) Alice (b) Bob

Figure 2. Block diagram of the high-speed data handling printed circuit boards at Alice and Bob

3. EXPERIMENTAL RESULTS AND ANALYSIS

3.1 **Polarization Recovery**

In a polarization encoding QKD system the polarization state of a photon carries quantum key information. When a photon travels in free space its polarization state does not change, if air turbulence is negligible. However, when a photon travels in an optical fiber its polarization state is subjected to changes. There are three main causes for problems with polarization encoding in fiber-based systems [11]: first, transporting a vector (polarization) along a curve (fiber); second, changes in mechanical stress that cause birefringence; and third, polarization dependent losses in optical components used in the system. If the fiber link is well secured and stable, the first problem may be eliminated. Birefringence in fiber is due to three main sources: (1) birefringence introduced in the manufacturing process (such as shape and inner strain), (2) elastic birefringence introduced by mechanical force (such as bending, lateral stress and torsion) and (3) electric and magnetic birefringence [12]. The birefringence change is usually caused by the change of mechanical stress in the fiber due to environmental variation such as of temperature or vibration, depending on the mechanical and thermal stability of the environment. Temperature changes are usually quite slow, on the order of tens of minutes. Vibration changes can occur more frequently, possibly on the order of seconds. Another effect of the birefringence is the polarization mode dispersion (PMD). PMD limits the minimal usable pulse length of the laser; however, this problem can be avoided if a laser with a coherence time longer than the polarization mode delay is used [11]. We can avoid the third problem by choosing suitable optical components or compensating for the error as long as we know the polarization characteristics of the optical components used.

Although the polarization state changes when photons pass through a fiber, the relation between the two non-orthogonal polarizations is not changed after they traveled in the same path. At the fiber output, when a polarization controller recovers one of the two non-orthogonal polarizations the other is also transformed to a state that has the same relation with respect to the PBS as they were at the fiber input. Manual polarization controllers are used in our QKD system to recover the polarization state for each path in the quantum channel independently at the output of the fiber.

In the system, when linearly polarized light with a high degree of polarization (DOP, the ratio of polarized light to non-polarized light) at Alice travels through the fiber to Bob its polarization orientation is changed and the DOP may also deteriorate as well. A polarization extinction ratio (in decibel) for the system is defined as the minimum counts divided by the maximum counts of orthogonal polarized photons detected by the APD when the polarization controller is properly adjusted. A poor extinction ratio will yield high crosstalk and therefore a high error rate. Based on the B92 protocol, the polarization state of the PBS is set to be non-conjugated to the polarization state of the photons from its own path (45 degree), and to be conjugated to the polarization state of the photons from the other path to block the crosstalk. Considering the detection probability of the non-conjugated quantum is 0.5, the probability of the conjugated quantum should be less than 0.005 in order to reduce the extinction ratio-related error rate to 1%. In that case, the extinction ratio of the system should be better than 23 dB.

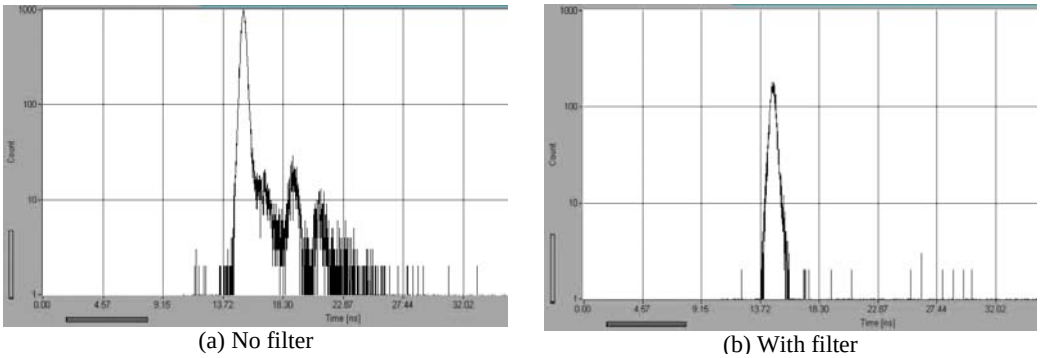
The system extinction ratio is determined by the extinction ratio of polarizing components in the system (polarizers at Alice and PBSs at Bob) and the depolarization in the photon-traveling path (fiber and other optical components such as NPBS). However, the 50/50 NPBS cube distorts the polarization state, especially for the reflected beam. Though the NPBS cube balances the power of p and s light components, it does not fully maintain their phases. We measured the extinction ratio of a light beam linearly polarized at 45 degree and reflected in an NPBS to be just 17 dB. So, we configured the 45 degree polarized light to pass straight through the NPBS cube and the vertically polarized light to be reflected by the cube. Bob's polarization controllers not only compensate for the polarization changes in the fiber, but also the phase distortion in the NPBS. The system extinction ratio can reach as high as 30 dB, which approaches the limitation of the value for the polarizing components themselves. This result shows the fiber and optical components in the system can be chosen to have a negligible effect on the degree of polarization.

Our experiments in the lab show that the extinction ratio can be kept above 23 dB for as long as 2-3 hours after the initial setup. However, for field application or longer distance, the extinction ratio will deteriorate faster. In this case an auto-compensation system is necessary. We continue to investigate auto-compensation schemes.

3.2 Noise reduction

Some minor noise pulses appear along with each data pulse when the transmission distance increases in the quantum channel. Figure 3(a) shows the main data pulse followed by some noise pulses after 1 km transmission in the QKD system. Please note that the word "pulse" used in this section is actually a histogram of accumulated photon counts. The "pulse width" corresponds to system timing jitter. In the polarization recovery adjustment process, we find that the polarization states of these noise pulses are different from the main pulse and different from each other. The amplitude of the largest noise pulse is about 2 orders of magnitude smaller than the main pulse.

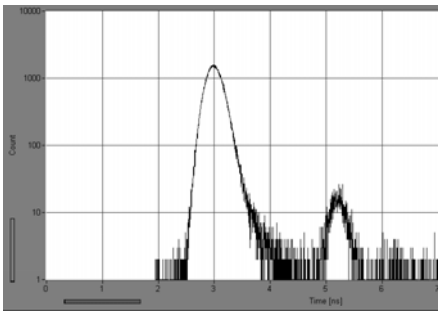
The noise pulses deteriorate the performance of the system because they have different polarization states and they broaden the pulse width, therefore the crosstalk and jitter are increased. We found the wavelength of these noise pulses is different from that of the main pulse. These noise pulses can be removed completely by inserting an interference filter (bandwidth of 5 nm centered at 850 nm) when HI780 fiber is used, see figure 3(b). More detailed study is needed to identify the cause of these noise pulses.



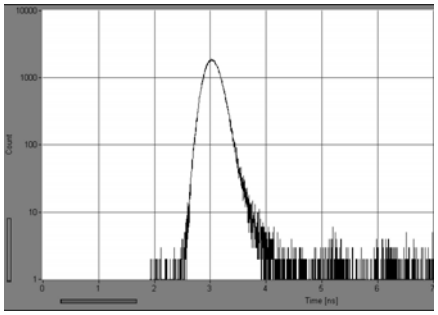
(a) No filter (b) With filter

Figure 3. The response pulses via 1 km 850nm single-mode fiber

To make QKD systems more practical, the fiber should be compatible with fibers commonly used in standard telecommunication networks. We experimented with 1 km of SMF-28 fiber for the quantum transmission at 850 nm. Since the cutoff wavelength of the fiber is much longer than 850 nm, some higher order transverse modes exists in the fiber, see Figure 4(a). The higher order mode travels slightly slower than the fundamental mode (2.3 ns delay in our case). Also its polarization state is different from that of the fundamental mode. The amplitude of the higher order mode could be higher than the minimal amplitude of the fundamental mode. The pulse of the higher order mode becomes a lower limit on the system extinction ratio. This pulse could be counted in an adjacent time window when the transmission data rate is high enough. These effects increase the error rate. With the SMF-28 fiber being fusion spliced to a piece of HI780 fiber, which functions as a spatial filter, the higher order mode is greatly suppressed, see Figure 4(b). Other groups also reported similar approaches to filter the noise from higher modes [9, 13]. After removing the noise pulse from the higher order mode, the classical channel and the quantum channel are able to share a single standard telecom fiber by using 850/1550 nm WDMs.



(a) Pulses of fundamental and higher order modes



(b) The higher order mode is greatly suppressed

Figure 4. The response pulses via 1 km 1550 nm single-mode fiber

3.3 Transmission data rate

Transmission data rate is an important performance parameter for a QKD system, since higher transmission data rates can yield more encryption keys and enhance the communication capacity. Our custom high-speed data handling boards on both Alice and Bob provide sifted data directly to the CPU for error correction and privacy amplification, which can then be used by application-level data encryption. Hence, we use the sifted key rate from the boards as one of our quantum performance metrics. The sifted key rate can be estimated by the following equation:

$$R = \mu \cdot L_f \cdot L_c \cdot L_d \cdot Pd \cdot L_o \cdot \nu \tag{1}$$

Where R is the sifted key rate, μ is the mean photon number per pulse at the output of Alice. This parameter is set to 0.1 (10 dB) as is common in the literature. In this case, 9% of the pulses contain a single photon, less than 1% contains more than one photon, and the rest of the pulses are negligible according to Poisson statistics. A higher mean photon number leads to a higher sifted key rate but more pulses will contain more than a single photon and will require a higher degree of privacy amplification. A lower μ reduces the sifted key rate. When the sifted key rate is too low the dark counts of the APD will cause high error rates. L_f is the optical loss of the fiber. We use 1 km HI780 fiber and its nominal loss at 850 nm is about 2.3 dB/km. The actual measured value is about 3 dB, including the losses due to three connectors and other losses, such as bending. L_c and L_d are the losses in the 50/50 coupler and the transmission loss at PBS. The Pd is the photon detection efficiency of the APDs. According to the specifications, this value is about 45% (3.5 dB) at 850 nm. Other losses, $L_{o,}$ in the system are about 2 dB. ν is the quantum data repetition rate.

Table 1. Photon budget

	Value (dB)	Comments
Mean photon number (μ)	10	0.1 photon per pulse
Loss in fiber (L_f)	3	2.3 dB/km and loss on connectors and bending
Loss in coupler (L_c)	3	1x2 50/50 non-polarizing coupler
Loss on detection (L_d)	3	Transmission possibility for a photon polarized at 45 degree
Efficiency of APD (Pd)	3.5	45% of APD detection efficiency at 850 nm
Other loss (L_o)	2	Other loss in the system, such as filters
Total	24.5	

The values of these losses in our system are shown in Table 1, which yield a total loss of about 24.5 dB. When Alice sends quantum data at a repetition rate, ν, of 312.5 Mb/s and 156.25 Mb/s to Bob, we achieve 1.1 Mb/s and 0.6 Mb/s sifted key rate, respectively, which correlates well with equation (1).

3.4 Quantum Error Rate

The quantum channel error rate, also called quantum bit error rate (QBER), is defined as the ratio of incorrect counts to total counts that are recorded at Bob's APDs. The quantum errors are mainly caused by the following factors: (1) The dark count rate of the APD and light leakage into the system, (2) Cross-talk caused by an imperfect polarization extinction ratio of the system, (3) Temporal jitter of the system.

The first factor is caused by a thermo-initiated avalanche process in the APD and some unexpected photon detections. It is independent from the system clock and the data rate. The dark counts of the APD used in our system are at the order of 10^2 per second. With proper light sealing and filtering, the counts due to light leakage are only a few tens per second. When compared to our Mbit/s data rates, this first factor is negligible.

The second factor is caused by the imperfect polarization extinction ratio of the PBS, the polarization recovery unit and an unstable condition of the fiber. The extinction ratio of the PBS is about 30 dB. In the best case, the manual polarization controllers can be adjusted to get a system extinction ratio of 30 dB, however, the system extinction ratio was measured to be between 23-28 dB during our experiments. So this factor contributes about 1% of error to the QKD system. It is also independent from the system clock and data rate.

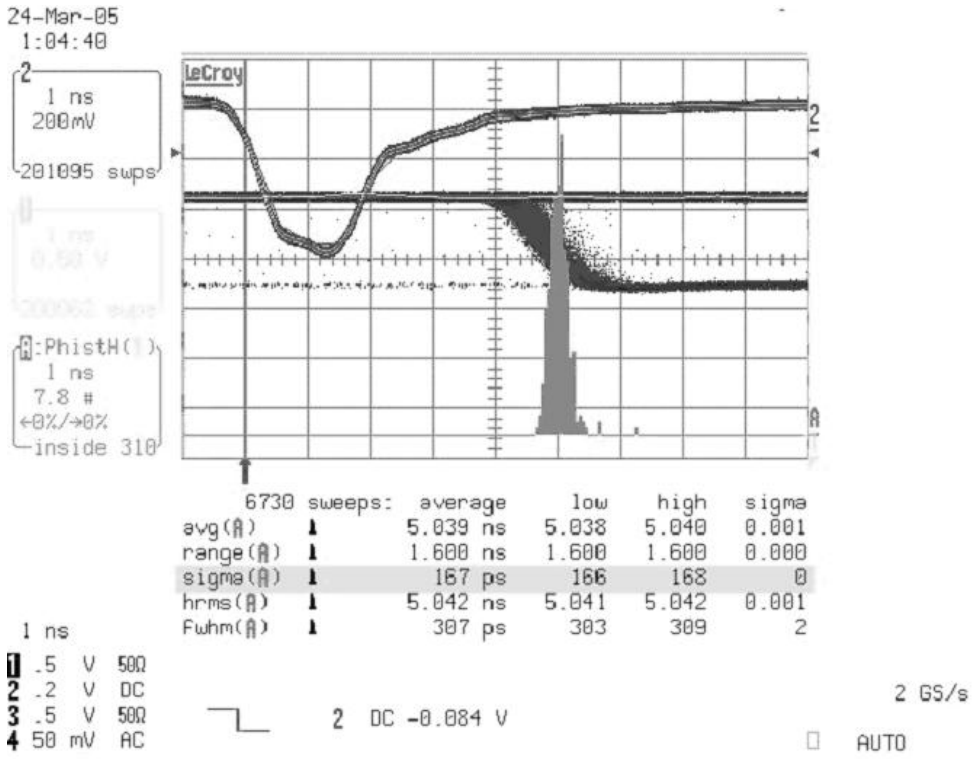


Figure 5. Jitter in the quantum channel

The jitter in the classical channel is mostly caused by electronic elements in the circuit boards and the CWDM transceivers. The jitter in the quantum channel is mainly from VCSELs and their drivers as well as the APDs. Figure 5 shows the jitter in the quantum channel, measured with a repetitive data stream, is about 167 ps (standard deviation), which is small enough to guarantee the pulse can be contained within an 800 ps clock period. However, the observed pulses are spread over two clock periods (1.6 ns). We believe this is caused by a timing misalignment between the classical channel and the quantum channel since we can currently only align the timing with an accuracy of 800 ps. A finer timing adjustment is needed to ensure the data pulse can be kept within a detection time window of 800 ps. For this reason our QKD system was operated with a data repetition rate of 312.5 or 156.25 Mbit/s to ensure the pulses will not be skewed to the adjacent pulse spaces. This results in an error rate of about 1.2-1.3%. If the jitter is much smaller than the photon pulse period, the error rate is mainly caused by an imperfect polarization extinction ratio. With improvements to the jitter, the system should be able to run at a higher data repetition rate without an elevated error rate.

4. CONCLUSION

We have implemented a polarization encoding quantum key distribution system over 1 km of optical fiber. To our knowledge, as a complete system, the NIST fiber based polarization encoding QKD testbed currently runs at the highest sifted key rate, more than 1 Mbit/s over 1 km with $\mu = 0.1$ and an error rate lower than 1.3%. When the photon pulse and its tail are kept well within the detection time window the quantum error rate is mainly caused by an imperfect system extinction ratio. An automatic polarization control unit is necessary to maintain a high enough extinction ratio for practical applications. An interference filter removes noise at other wavelengths while the spatial filtering procedure removes noises due to higher order modes generated in standard telecom fiber. That means standard telecom fiber can be used to transmit single photons at 850 nm for a polarization encoding QKD system. The overall system jitter limits the maximum data rate, thereby limiting the sifted key rate. An improved VCSEL triggering unit and APD detection module with less jitter will increase the sifted key rate. At these higher speeds, with these proposed improvements, integration of QKD and standard telecom systems may become practical. These are the research directions we plan to pursue.

ACKNOWLEDGEMENT

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

REFERENCES

1. C. H. Bennet and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing” in Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing, pp. 175-179, Bangalore, India, December 10-12, (1984).
2. C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett., 68, 3121-3124 (1992).
3. N.Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography” Rev. Mod. Phys. Vol. 74, 145~195 (2002).
4. J.C. Bienfang, A. J. Gross, A. Mink, et al. “Quantum key distribution with 1.25 Gbps clock synchronization”, Optics Express. Vol. 7 (9), 2011 (2004).
5. J. G. Parity, P. R. Tapster and P. M. Gorman, “ Secure Free-space key-exchange to 1.9 km and beyond”, Journal of Modern Optics, vol. 48, 1887-1901 (2001).
6. Gobby C., Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber”, Applied Physics Letters, Vol. 84, 3762-3764 (2004).
7. D. S. Bethune, M. Navarro and W. P. Risk “Enhanced autocompensating quantum cryptography system”, Applied Optics, Vol. 41, 1640-1648 (2002).

8. J. Breguet, A. Muller and N. Gisin, “Quantum cryptography with polarized photons in optical fibers, experiment and practical limits”, Journal of Modern Optics, vol. 41, 2405-2412 (1994).
9. Karen J. Gordon, Veronica Fernandez, Paul D. Townsend, and Gerald S. Buller, “A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System”, IEEE J. of Quantum Electronics, Vol. 40, 900-908 (2004).
10. A. Nakassis, J. Bienfang, and C. Williams, “Expeditious reconciliation for practical quantum key distribution,” to appear in Quantum Information and Computation II, Proc. SPIE 5436 (2004).
11. Hoi-Kwong Lo, Sandu Popescu and Tim Spiller (editors), *Introduction to Quantum Computation and Information*, P122, World Scientific (1998).
12. Serge Huard, *Polarization of Light*, John Wiley & Sons, Masson (1997).
13. Paul D. Townsend, “Experimental Investigation of the Performance Limits for First Telecommunications-window Quantum cryptography Systems”, IEEE Photonics Technology Letters, Vol. 10, No.7, 1048-1050 (1998).