High-Speed Quantum Key Distribution Systems for Optical Fiber networks in campus and metro areas[1]

Xiao Tang, Lijun Ma, Alan Mink, Tiejun Chang, Hai Xu, Oliver Slattery, Anastase Nakassis, Barry Hershman, David Su, and Ronald F. Boisvert

Information Technology Laboratory
National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899
xiao.tang@nist.gov

ABSTRACT

Complete high-speed quantum key distribution (QKD) systems over fiber networks for campus and metro areas have been developed at NIST. The systems include an 850-nm QKD system for a campus network, a 1310-nm QKD system for metro networks, and a 3-user QKD network and network manager. In this paper we describe the key techniques used to implement these systems, including polarization recovery, noise reduction, frequency up-conversion detection based on PPLN waveguide, custom high-speed data handling and network management. A QKD-secured video surveillance system has been used to experimentally demonstrate these systems.

Keywords: Quantum Key Distribution, Detection time bin shift, Single photon detector, optical fiber communication.

1. INTRODUCTION

Since 1984 when the idea of quantum key distribution (QKD) [1] was invented, a number of groups have successfully demonstrated experimental QKD systems. Many of these were described in a comprehensive review article [2]. Laboratory high-speed QKD technology has become sophisticated, and integrating them into existing networks is the next and crucial step for commercial application of QKD technology.

Networks are commonly divided into three categories, (i) local area networks (LAN); (ii) metropolitan area networks (MAN) and (iii) wide area networks (WAN). The LAN, sometimes referred to as a campus area network, is a short distance network (usually <5 km) typically using a star/hub topology. For this type of network, mass produced hardware is deployed since low-cost is a significant consideration. MANs are geographically larger than LANs and usually cover a city area (<50 km). MANs are usually based on a ring or mesh network topology implemented with Wavelength Division Multiplexing (WDM) technology. A WAN, sometimes called a core network or long-haul network, covers a broad area linking metropolitan areas and crossing national boundaries (e.g., several hundreds km or longer). This type of network usually uses a mesh network topology and Dense WDM (DWDM) technology. Long distance and high throughput are the main requirements for this kind of network.

We have developed several technologies to integrate QKD into these networks. For LANs, an 850-nm system is a good choice, since low-cost vertical cavity surface emitting lasers (VCSELs) and silicon-based avalanche photodiodes (APDs) work at this wavelength very well. Our 850-nm QKD system produces a key rate of more than 1 Mbit/s over 4 km of standard telecom fiber [3, 4]. To further reduce the cost and improve the security, we implemented a detection-time-bin-

---

shift (DTBS) scheme in our QKD system [5, 6].   For the longer distances encountered in MANs, telecom wavelengths (1550 or 1310 nm) must be used.   We developed an up-conversion technique based on a periodically poled lithium niobate (PPLN) waveguide to convert 1310-nm photons into photons detectable by silicon-APDs [7, 8].   With this technique, we realized about 1 Mbps sifted-key rate over 10 km with a low error rate.   We are developing an entangled photon source at 1310 and 895-nm to link LANs via a MAN QKD system.   For a WAN, there is no suitable QKD technology with a faint laser source, since photons will be attenuated below the noise level over such long distances and photons can not be copied or amplified.   One potential solution for QKD over a WAN is a quantum repeater with an entangled-photon-pair source, and our 1310/895-nm entangled-photon pair source may provide a basis for this application.   To support a complete high-speed QKD system, we also designed and implemented high-speed data handling printed circuit boards, which continuously generate and process the gigabit per second data streams necessary to produce megabit per second secure key rates [9, 10].   To demonstrate a quantum network, we implemented a 3-node QKD network using a MEMS-based optical switch, and developed a network manager to coordinate all activities in the quantum network [11-13].   Using this 3-node network, we have demonstrated a switched video surveillance application secured by QKD and a one-time pad cipher.

In this paper, we present our high-speed QKD systems for LANs and MANs, including our techniques for automatic polarization and timing alignment, high-speed data handling, time-shared APDs, up-conversion detector and noise reduction, as well as network management.   We also discuss entangled photon sources and their use in integrating QKD systems into WAN.

2.   HIGH SPEED CAMPUS AREA QKD SYSTEM

For LANs, QKD systems at 850-nm are a good choice, since silicon avalanche photo diodes (Si-APDs [14]) operate well at this wavelength and the attenuation in optical fiber is acceptable over such short distances. Si-APDs can operate in free-running mode and the jitter response is about several hundred ps, which allows the 850-nm QKD system to operate at clock rates in excess of 1 Gb/s.   Using Si-APDs and 850-nm VCSELs, we implemented a high-speed QKD system over a short distance.

Figure 1 shows schematically our fiber-based QKD system using the BB84 protocol. It uses a pair of custom printed circuit boards designed and implemented at NIST. Each board uses a field programmable gate array (FPGA). One board is installed in the Alice computer and the other in the Bob computer. Each board communicates with the processor via their PCI bus interface. The boards exchange information between Alice and Bob through the classical channel and manage all aspects of high-speed data generation and processing [9] needed to create a shared sifted key according to the BB84 protocol [1].

In this system, 850-nm is used for the quantum channel, 1510 and 1590-nm are used for the bi-directional classical channel. Alice generates pseudo-random data to encode the photon polarization in two non-orthogonal bases (horizontal/vertical and +/- 45 degree), and then sends them to Bob through the quantum channel. To compensate for the change of polarization state during transmission, Bob, cooperating with Alice, does polarization compensation to recover the photon polarization state.   Bob recovers Alice's clock from the classical channel, allowing it to synchronize data and time with Alice. In addition, since the data paths for quantum and classical channels are different, Alice and Bob also need to align the timing between the quantum channel and the classical channel.   Bob's board then receives detection event signals from the APDs when photons arrive, and sends their bit positions and their measuring bases, but not their bit values, back to Alice over the classical channel.   After matching each detection event with the corresponding event of the stored quantum bit-stream, Alice tells Bob which detection events are valid (i.e., measuring basis matches encoding basis) via the classical channel.   At this point, Alice and Bob share a "sifted key". Alice and Bob then send their sifted keys to their own computers for subsequent error reconciliation and privacy amplification necessary to generate shared secret keys [15].   The sifted-key rate and the quantum bit error rate (QBER), two important metrics for QKD systems, can be measured in real time from the raw data before reconciliation in our system.

For polarization encoding QKD systems, one major limitation to practical application is that different fiber paths have different polarization properties. Due to perturbations from the ambient environment and other mechanical sources, such polarization properties also drift randomly over time. Consequently, it is necessary to auto-recover the polarization state of the signal and to auto-compensate the temporal drift of the polarization state during photon transmission. We have developed polarization auto-recovery and auto-compensation sub-systems for our QKD systems based on piezo polarization controllers. This polarization recovery and compensation process takes less than 1 minute.
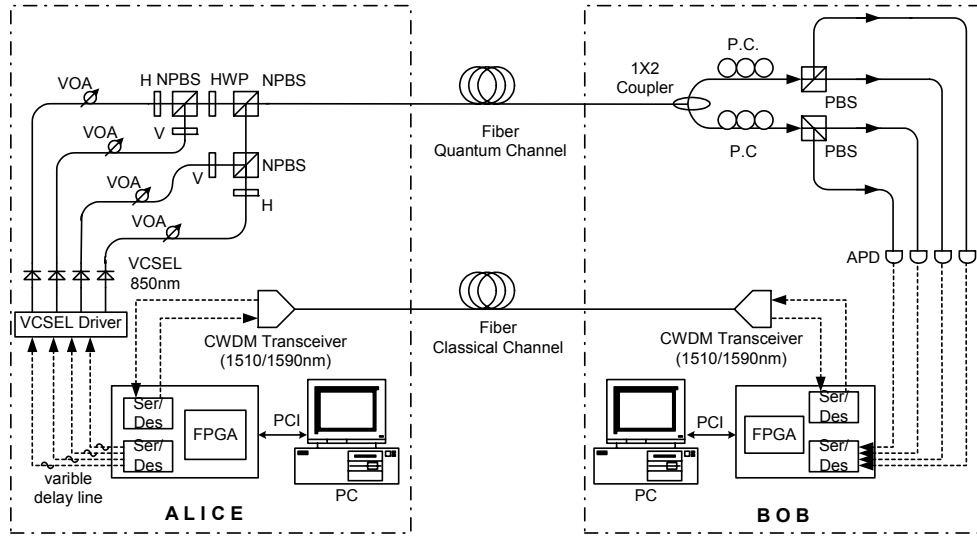

Figure 1. Schematic diagram of the BB84 QKD system; VCSEL: Vertical-Cavity Surface-Emitting Lasers; HWP; Half-wave plate; VOA: Variable Optical Attenuator; NPBS, Non-polarizing Beam Splitter; P.C.: Polarization Controller; FPGA: Custom printed circuit board controlled by a field-programmable gate array; PCI: PCI bus; PBS: Polarizing Beam Splitter; Solid line: Optical fiber; Dotted line: electric cable.

In a high speed QKD system, the sifted-key rate R can be estimated by the following equation if the influence of the APD's dead time is ignored:

$$R = \mu \cdot L_f \cdot L_o \cdot Pd \cdot L_p \cdot \nu \qquad (1)$$

Here the mean photon number μ is set to 0.1. L_f is the loss in the transmission fiber. L_o represents other losses such as bending, coupling and connection losses in the quantum channel. Pd is the APD's detection efficiency. L_p is the protocol related loss. ν denotes the quantum channel transmission rate. The calculated and measured sifted-key rates for two different clock rates for fiber lengths of 1 and 4 km are shown in Fig. 2. The solid mark points represent the measured data and the lines represent the calculated data using equation 1 at clock rates of 625 and 312.5 Mbit/s. The measured sifted-key rate is in compliance with the calculated data. From the experimental results, the sifted key rate of this system can provide more than 4 Mbit/s over 1 km distance with a mean photon number of 0.1. At such high-speed, secured video transmission encrypted by quantum keys with a one-time-pad cipher is possible. However, due to the relatively high attenuation of optical fibers at 850-nm, the sifted key rate reduces quickly over distance. The sifted key rate is just about 1Mbit/s at 4 km distance. Therefore, the 850-nm QKD system is suitable only for LANs.
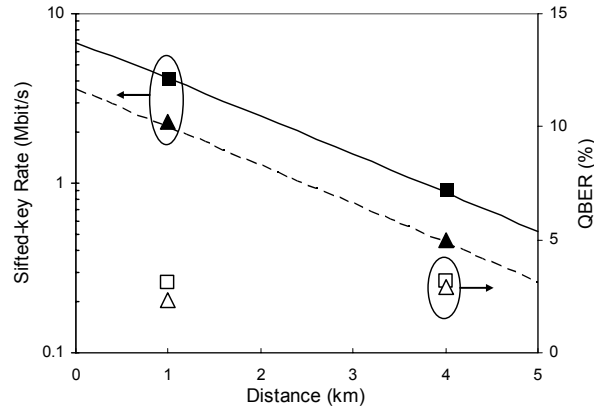
Figure 2. The system performance of the QKD system with BB84 protocol.   Solid and dashed lines are the calculated sifted-key rate at clock rates of 625 MHz and 312.5 MHz.   Solid and hollow squares are the measured sifted key rate and QBER of the clock rate 625MHz.   Solid and hollow triangles are the measured sifted key rate and QBER at the clock rate 312.5MHz.

Randomly selecting detection bases is a required function for the receiver (Bob) in a QKD system. Active selection of detection bases in a high speed QKD system requires a high-speed active switch and an additional random data source, which results in a complex and costly system. To reduce this complexity, a scheme with a passive coupler (a non-polarizing beam splitter for a free-space system or a passive fiber coupler for a fiber system) is more commonly used in current QKD systems. However, the passive scheme uses twice the number of single photon detectors as an active scheme, 4 detectors for the BB84 protocol and 2 for the B92 protocol, as shown in Fig. 3(a).   To further reduce the cost of this QKD system, we proposed and implemented an improved detection-time-bin-shift (DTBS) scheme that only needs one detector rather than the two in conventional scheme.   Because single photon detectors are the most expensive elements used in QKD systems, this could significantly reduce the cost of QKD systems.   The concept of the DTBS scheme is to project the measurement bases and/or measured photon values into different detection time-bins and then to time-division-multiplex (TDM) one detector to detect them. The scheme was first introduced in Ref. [16] and applied to B92 [17] protocol. We improved on the original DTBS scheme to avoid an extra 50% photon loss, and also extended the DTBS scheme to the BB84 protocol. By projecting into time-bins, the DTBS scheme just needs one detector for B92 (Fig. 3 (b)) and BB84 (Fig. 3 (c)).   The trade-off for using fewer detectors is that the single photon transmission rate must be reduced to half (B92) or a quarter (BB84) to allow for the required number of detector time bins (DTBs) and the sifted-key rate is reduced as a result.
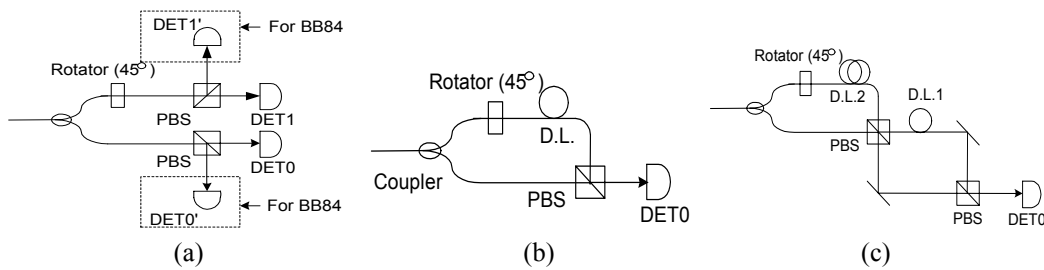

Figure 3. (a) Bob side of a conventional QKD for BB 84 and B92; (b) Bob side of a DTBS QKD for B92; (c) Bob side of a DTBS QKD for BB84. Rotator (45°): half wave plate; DET: single photon detector; PBS: polarizing beam splitter; D.L.: delay line, the delay time for D.L.2 is twice as for D.L.1.

Security is always the highest priority for QKD systems. Although in theory the security of QKD is guaranteed by the physics of the quantum channel, the actual security might be limited in practice by imperfect properties of physical devices. The security of a QKD system requires the keys be a true random sequence.   Even if the Alice sends Bob a

true randomly encoded photon sequence, the keys might lose their randomness because of the imperfect properties of single photon detectors, which would degrade the security of the QKD system. Three crucial security issues are: self-correlation caused by the dead-time of single photon detectors [18,19], key value imbalance, and the measurement basis imbalance caused by unbalanced detection efficiency of detectors. In our DTBS QKD systems, these security concerns are intrinsically avoided.

We implemented a DTBS QKD system based on a fiber-based QKD system that we developed previously. The structure of the system is similar to the one shown in Fig. 4. The B-92 protocol used here is only to demonstrate the scheme's feasibility; the scheme also can be used with the BB84 protocol. In comparison with conventional QKD systems, the DTBS scheme saves one APD and an electrical channel at Bob's side. It further reduces the system cost and simplifies the system structure.
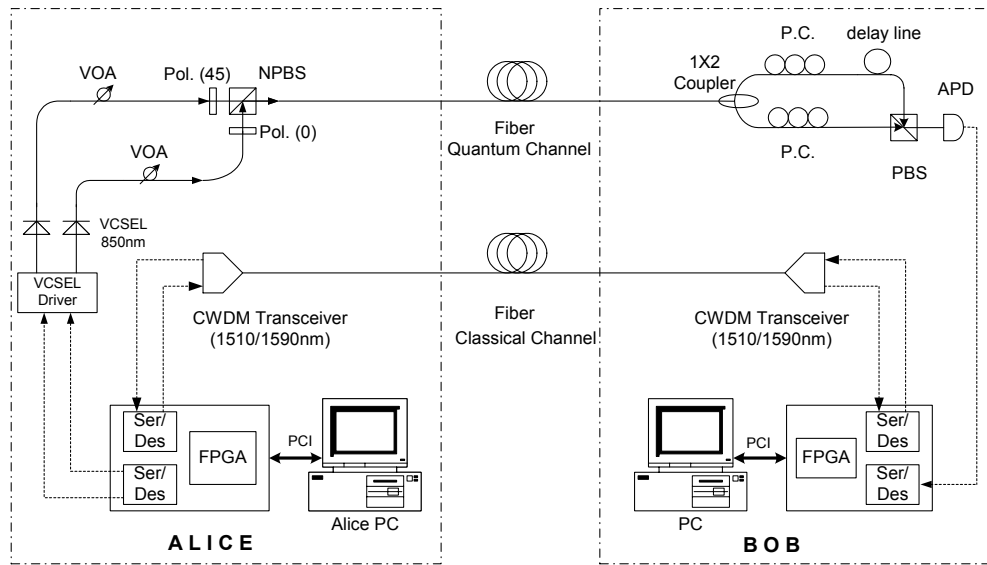

Figure 4. Schematic diagram of our B92 DTBS-QKD system; VCSEL: Vertical-Cavity Surface-Emitting Lasers; Pol.: Polarizer; VOA: Variable Optical Attenuator; NPBS, Non-polarizing Beam Splitter; P.C.: Polarization Controller; FPGA: Custom printed circuit board controlled by a field-programmable gate array; PCI: PCI bus; PBS: Polarizing Beam Splitter; Solid line: Optical fiber; Dotted line: electric cable.

The sifted key rate and QBER of the DTBS QKD system are shown in Fig. 5(a). Operating at 312.5 MHz, our DTBS QKD system produces sifted-keys at a rate more than 1 Mbit/s at a mean photon number 0.1 over 1.1 km of fiber, which is about half the rate of our conventional QKD system operating at 625 MHz. This is the expected trade-off between using two APDs vs. one. The QBER (about 2%) remains about the same as our conventional system. Self-correlation becomes a problem in conventional QKD systems, as shown in Fig. 5(b), when data rates are high relative to the detector dead-time. However, DTBS QKD systems avoid this problem and the probability that two neighboring bits are different remains at 0.5 as required.
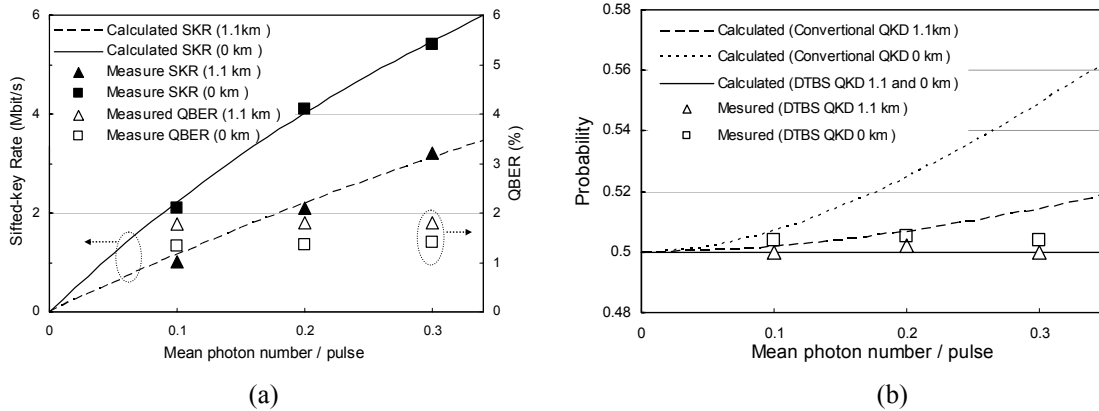
Figure 5. The system performance of the B92 DTBS QKD system at 0 km (back-to-back) and over 1.1 km. (a) Calculated and measured sifted key rate (SKR) and QBER.   (b) Calculated and measured probability that neighboring two bits are different.

3. HIGH SPEED METRO AREA QKD SYSTEM

For QKD over a MAN, the wavelength of the quantum signal should be in the 1310-nm or 1550-nm bands, where telecom fibers experience the lowest loss.   WDM and erbium-doped fiber amplifier (EDFA) technologies, widely used in MANs, result in noise over single photon level throughout the 1550-nm band caused by the Raman scattering of strong optical communication signals and the amplified spontaneous emission (ASE) of EDFAs.   Hence the best choice of wavelength for WDM of QKD systems in a MAN is in the 1310-nm band to co-exist with standard telecom using the 1550-nm band.

The available detectors that operate in this wavelength are InGaAs avalanche photodiodes (APD) [20] and superconducting single-photon detectors [21]. InGaAs APDs must be operated in a gated mode (Geiger mode) and the system clock rate is limited by the available gating frequency of the device, typically several MHz [20]. As a result, the sifted-key rate is also limited [22]. Superconducting single-photon detectors (SSPDs) can be operated in a free-running mode and their time response is usually less than 100 ps. However, SSPDs are expensive and complicated to use because they need to be operated at a very low temperature (4 K). By contrast silicon APDs are low cost, operate un-gated at relatively high data rates and don't require cooling. The peak detection efficiency of silicon APDs is around 70% near 650 nm, which is the highest among these single-photon detectors. The limitation of the Si-APD is that its detection efficiency decreases rapidly at wavelengths longer than 1000-nm. To continue to use silicon APDs, we have implemented an up-conversion detector using a pump wavelength at 1550 nm to convert photons at 1310 nm to 710 nm.

The structure of a pair of our up-conversion detectors is shown in Fig. 6. The key element is a waveguide made of periodically poled lithium niobate (PPLN, HCP Photonics). A 1557-nm CW laser is modulated to a pulse train and then is amplified using an EDFA. An optical filter FLT_0 with the full width half maximum (FWHM) of 7 nm is used to suppress the noise of the EDFA. We will show later that this filter is important for noise reduction because the optical noise between 1000 nm and 1300 nm can induce a large amount of dark counts and the wavelength-division multiplexer (WDM) before the PPLN may not be sufficient to suppress this noise. After the FLT_0, the 1550-nm pulse is split into two by a 50:50 coupler and used to pump two 1306-nm signals. These two 1306-nm signals, for example, could be from the two outputs of an interferometer in a phase-based QKD or they could be from the two outputs of a 3-dB coupler in a polarization-based QKD. After polarization control, the 1306-nm signal and the 1557-nm pump are combined by the WDMs and then are sent to PPLNs. Each 710-nm output of the PPLNs is then further filtered and finally detected by a Si-APD [8]. We claim that a 1310-nm QKD system with a 1550-nm pump up-conversion detector could yield better system performance, particularly when the system is designed to oprate at a high secure-key rate over relatively short distances. We studied various aspects of the 1550-nm pump up-conversion detector. It has high polarization sensitivity

with a polarization extinction ratio larger than 25 dB. The pulsed pump light helps to reduce the dark count rate and the internal conversion efficiency remains at approximately 100% as long as the pump pulse is sufficiently wider than the signal pulse. The detection efficiency of the up-conversion detectors is listed in Table 1.
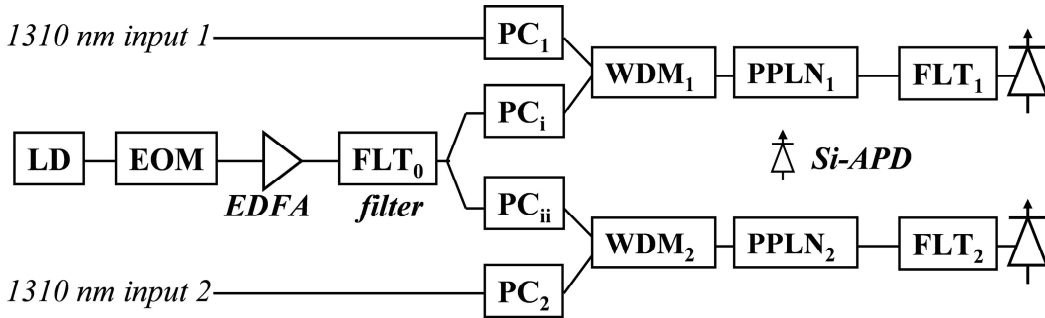

Figure 6. Configuration of the 1550-nm pumped up-conversion detectors. LD: Laser diode; EOM: Electric-optic modulator (LiNbO$_3$); EDFA: Erbium-doped fiber amplifier; FLT: Optical filter; PC: Polarization controller; WDM: Wavelength-division multiplexer for 1310 nm and 1550 nm; PPLN: Periodically-poled LiNbO$_3$ waveguide module.

Table 1. Transmittance of the components used and overall detection efficiencies of the 1550-nm pumped up-conversion detectors

	PPLN1	PPLN2
PC and WDM at 1310 nm	70%	74%
Input coupling of PPLN at 1550 nm*	52%	71%
Input coupling of PPLN at 1310 nm*	44%	59%
Output coupling of PPLN at 710 nm*	92%	77%
Filter before APD*	75%	88%
APD efficiency at 710 nm*	70%	70%
Overall efficiency	15%	20%

* These parameters are provided by the manufactures. Others are measured.

We applied the 1550 nm pumped up-conversion detectors to our B92 polarization encoding QKD system at 1310 nm as shown in Fig. 7. To polarization-encode the quantum channel, we start by modulating a 1306-nm CW light into a 625 MHz pulse train with a FWHM of 220 ps and evenly splitting it into two polarization channels. Each pulse train is further modulated by one of the 625 Mbit/s quantum channel data streams. The two complementary quantum streams are passed through their polarizers and then combined by a 45-degree polarization maintaining combiner with their polarization states being separated by 45 degrees in the Jones space. The combined 1306-nm quantum stream is attenuated to a mean photon number of 0.1 per bit and then multiplexed with the 1510-nm classical channel via a WDM and transmitted over one standard single-mode fiber.

At Bob, another WDM is used to demultiplex the quantum and the classical channels. The 625 MHz clock is extracted from the classical data stream and is used to generate the pump pulse train with a FWHM of 620 ps. A 3 dB fiber coupler splits the quantum signal evenly, which will be detected by a 1557 nm pumped detector. As shown in Fig. 6, the polarization decoding is performed using PCs for polarization compensation of the fiber transmission and PPLNs as polarizers.
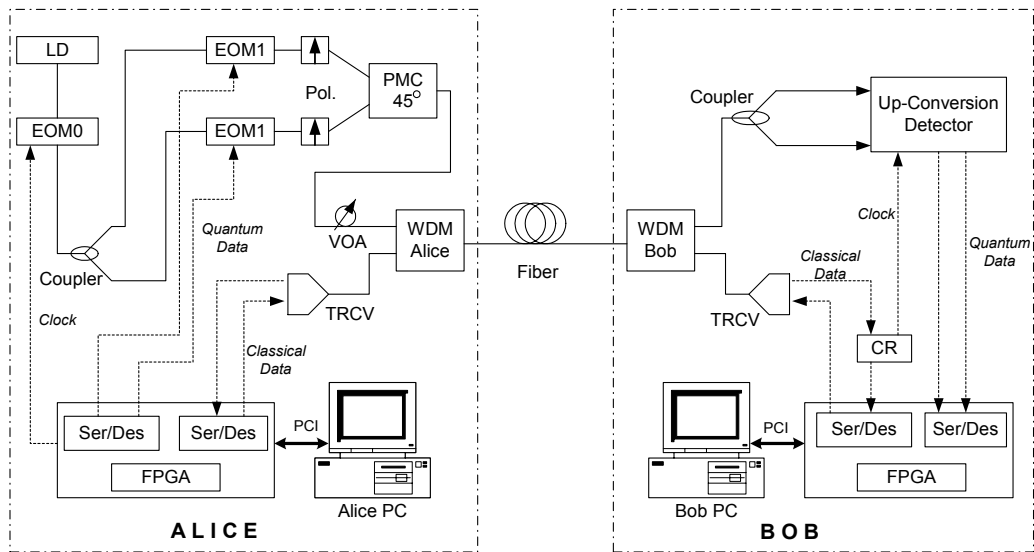
Figure 7. The B92 polarization coding QKD system at 1310 nm. LD: Laser diode; EOM: Electric-optic modulator (LiNbO₃); PC: Polarization controller; PMC-45º: Polarization maintaining combiner that combines two light signals that are separated by 45 degrees; VOA: Variable optical attenuator; WDM: Wavelength-division multiplexer; SMF: Standard single-mode fiber; TRCV: Optical transceiver; CR: Clock recovery module; FPGA: Custom printed circuit board controlled by a field-programmable gate array; PCI: PCI connection; Up-conversion detector: See Fig. 2; Dotted line: Electric cable; Solid line: Optical fiber.

The PPLN up-conversion detector is well known to be polarization sensitive. In Fig. 8(a) we show the dependence of the conversion efficiency on the deviation angle of the 1310-nm input polarization state in PPLN1. Similar results were obtained for PPLN2. The deviation angle is the angle (in Jones space) between the given input polarization state and the state at which the conversion efficiency is maximized. Divided by the maximum value, the conversion efficiency is normalized to 1. As shown in the figure, the polarization extinction ratio of PPLN is more than 25 dB. We also compared the measurement results with the polarization sensitivity of an optical polarizer, whose transmittance T is a function of deviation angle θ, shown as $T \sim \cos^2(\theta)$. The PPLN plays a role of an ideal polarizer in the polarization encoding QKD system.

The system performance is shown in Fig. 8(b). During the measurements, the pump power is fixed at 40 mW. The sifted-key rate is 2.5 Mbit/s with a back-to-back connection (0 km), 1 Mbit/s at 10 km, and 60 Kbit/s at 50 km. The error rate is approximately 3% for back-to-back, remains below 4% up to 20 km, and reaches 8% at 50 km. The finite extinction ratio of the modulator and the timing jitter of the system induce a background error rate ER0 of approximately 2.5% and the remaining portion of the error rate is from dark counts induced from both the pump light and the classical channel. We were able to generate secure keys in real time and used them as a one-time-pad for a continuous 200-Kbit/s encrypted video transmission over 10 km.
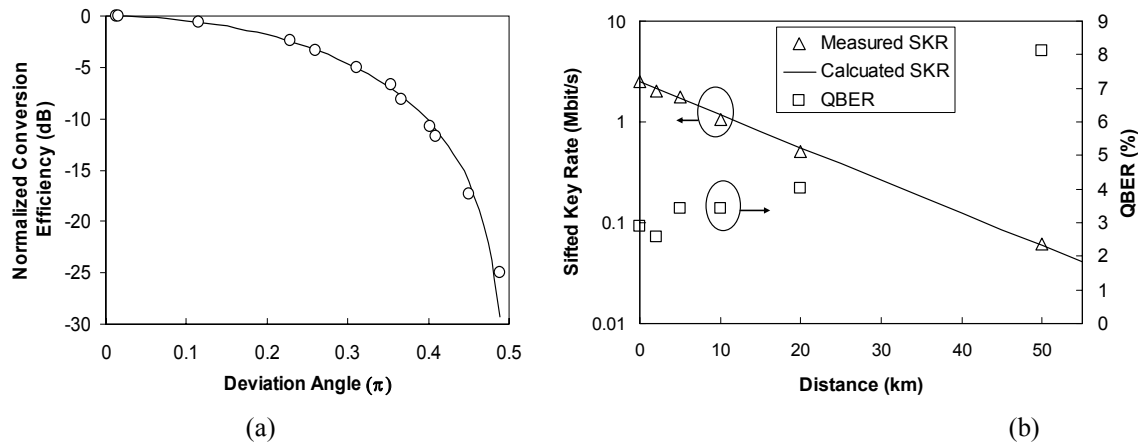
(a)　　　　　　　　　　　　　　　　　　　　(b)

Figure 8. (a) Normalized conversion efficiency as a function of deviation angle of the input 1306-nm signal of the PPLN1. The *x*-axis shows the deviation angle in unit of π-rad. Open circle: Measurement results; Solid line: $\cos^2$ curve. The PPLN$_2$ detector exhibits similar behaviors. (b) System performance of the B92 polarization-based QKD system with the 1557-nm pumped up-conversion detector. The solid line (to the left): calculated sifted-key rate; The triangles: sifted-key rate measured in the experiment; The squares (to the right): error rate measured in the experiment.

4. QKD NETWORKING

We have developed several high-speed and long-distance point-to-point QKD systems.   However, speed and distance are not the only objectives of our QKD systems. Integrating QKD systems into existing commercial networks that support secure communication between interconnected users is necessary for evaluating possible issues in the practical deployment of such systems.

A QKD network is a sub-network within a standard communication network. A QKD network only exchanges secure keys, it does not send secure messages. Secure messages are sent over the standard communication network, using the secure keys established by the QKD network. The first step is to extend the current point-to-point QKD systems into a QKD network. There are two schemes for a QKD network, passive and active. The passive scheme uses passive optical components, for example, the optical coupler, to implement multi-user connectivity. In this scheme, one can realize multi-terminal communications simultaneously, that is "broadcast" from one node to multiple nodes. Several groups have successfully demonstrated a QKD network based on this scheme [23~25]. However, in passive communication networks, the photons (and hence the bits that they represent) are split by couplers according to their coupling ratio and distributed proportionally to each node, resulting in a greatly reduced key rate between each node. The second scheme adopts active optical components such as optical switches, to dynamically control the communication path. This scheme is similar to and compatible with current optical networks, and establishes a reconfigurable QKD network. The system switching time and the influence of the active optical devices on the QKD system are the main factors used to evaluate this type of network.

The system configuration of our active 3-node polarization encoding QKD network is shown schematically in Fig. 9. One Alice node and two Bob nodes use the same technology as our point-to-point QKD system we developed previously, but we added two MEMS optical switches at the Alice side to control the communication route of the quantum channel and the classical channel. A network manager program was developed to coordinate these nodes, operate the optical switches and provide independent synchronized secret key streams to application programs.
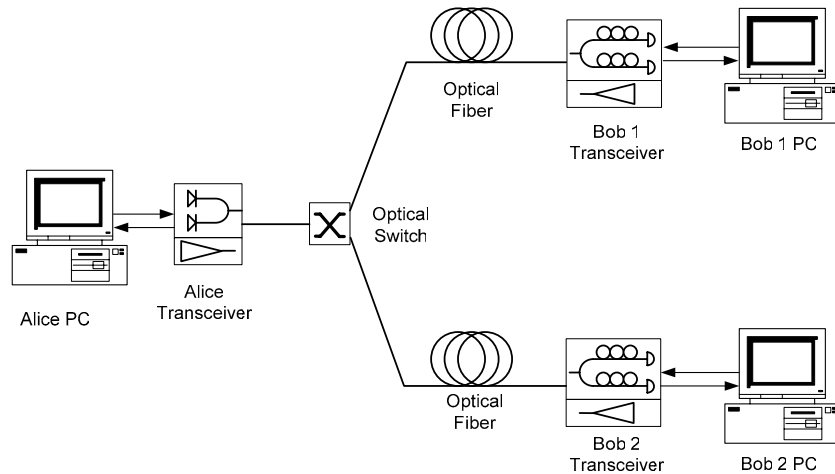
Figure 9. Configuration of the active 3-node QKD network. Two optical fibers are used for quantum and classical channels separately in each link.

For an active QKD network, it is important to achieve a short system switching time, i.e., the time used to establish the connection between Alice and one of the Bobs.   In our 3-node network, the sifted key rate is similar to that in our point-to-point link, even though optical switches are installed.   If the optical switches are installed in the transmission path, the insertion loss of an optical switch causes additional loss of photons and indeed reduces the sifted-key rate. However, we install the optical switch inside Alice, where its insertion loss can therefore be considered as internal attenuation, and hence the sifted-key rate is the same as that of a point-to-point system.   This is an important distinction since, for example, 2 Alice's and 1 Bob can implement a 3-node QKD system also, but the insertion loss of the optical switches inevitably reduces the sifted key-rate. In general QKD network, such as N-Alices by M-Bobs, some optical switches must be installed in the transmission links, and therefore, their insertion loss will reduce the key rate. However, the QBER measurement results verify that the error rate does not change significantly when the switch is added. Therefore, the switch can be regarded as transparent and the polarization-encoding QKD system can be implemented through a reconfigurable network with this kind of transparent optical switch without significantly adding to the error rate.

In an active QKD network, we define a system switching time as the time taken to establish a secure key transmission after the switching signal is received. The system switching time is an important factor for active networks.   The system switching time includes the times of four component operations. First, the optical switch must close the previous link and open the new link, an operation whose efficiency depends on the switching time of the optical switch. Then, Alice and Bob need to perform three other operations: polarization recovery, time alignment and software initialization, before the connected nodes can generate secret keys.   The switching time of optical switches is relatively short, less than 1ms. The time requirement for polarization recovery, on the other hand, is relatively long and the most significant part in system switching time. In polarization recovery, photons are collected in different detectors and are then used as feedback to adjust the piezo-driving polarization controller. Although the response time of the polarization controllers is as small as 100 μs, the time required to collect enough photons for each feedback point is about 50 ms. Moreover, the recovery time varies in each operation, depending on the number of feedback points needed before the optimum settings are found.   In our experiment, the polarization recovery time ranges from several seconds up to 50 seconds.

Timing alignment is needed to compensate for different delays between the classical channel and each of the quantum channels. An automatic timing alignment procedure is conducted on the system after the polarization recovery.   The timing alignment takes approximately 3-5 second per quantum channel, but only needs to be done once for any given switch setting. Software initialization includes raw key sifting, error reconciliation and privacy amplification, and needs enough time to accumulate a number of Mbits of initial secure key. This depends on the speed of both Alice's and Bob's computers as well as the key rate. In this experiment, software initialization time is approximately 40 seconds. The

system switching time in this network is therefore approximately 1-2 minutes.   Fig. 10 shows the system switching time of the experimental network measured every hour over a 48 hour period. The average system switching time in the experiment is approximately 69 seconds.
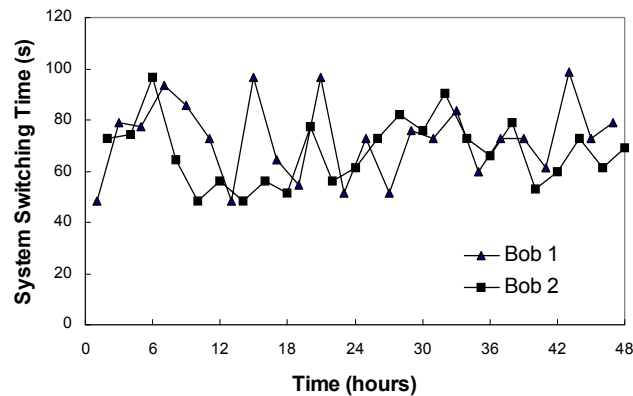

Figure 10. Measured system switching time. The switching time is measured after each switch operation, which is performed every 1 hour over 48 hours

The second step in developing a quantum network is to integrate a QKD sub-network with the security applications running on a standard communication network. We developed such a manager for our QKD network. A quantum network manager needs to set the switch as directed, complete all QKD start-up procedures, start the QKD protocols to enable the secret key flow, and then stop the protocols to disable the flow when switching is requested. It must also supply an interface for existing network security applications (e.g., IPsec, TLS, etc.) that will provide synchronized secure key streams between two cooperating processes. The manager consists of a set of application program interfaces (APIs) or commands that request operations including link switching, establishing an independent synchronized secure key stream, accessing bits from that key stream, suspending that key stream, and closing that key stream, etc. The QKD managers, one at each QKD node, communicate over the standard IP channels of the communications network. With the network manager, the QKD network can automatically reconfigure the transmission links and implement multi-node quantum key distribution without any manual control and tuning.

The quantum network manager, depicted in Fig. 11(a), consists of a main loop that spawns a number of threads as well as our QKD protocol stack as a separate process. The coordination manager thread controls various network elements such as the switch, the polarization compensation module and the manager at the other end of QKD network link. The first in, first out (FIFO) multiplex manager synchronizes the key flow from the secret key store of our QKD protocol stack, see Fig. 11(b), into the various application FIFOs, as illustrated in Fig. 11(c). It uses a separate socket to exchange information about which keys to be added to each FIFO with its cooperating counterpart at the other end of the quantum network link. For each FIFO, the manager spawns a FIFO interface thread, which provides the user interface between the application and the FIFO.

The associated QKD protocol stack is shown in Fig. 11(b). The raw key stream generation and management along with the sifting algorithm are implemented in hardware via a custom printed circuit board (PCB). This hardware allows us to send photons at Gb/s rates, resulting in Mb/s of sifted key, which is a more manageable rate for the remainder of our protocol stack that is implemented in software. Our enhanced software versions of the Cascade reconciliation algorithm and the privacy amplification algorithm have the capacity to yield a few Mb/s of secret key. Planned enhancements to our custom PCB will allow us to migrate these software algorithms to hardware, improving our throughput to between 10 and 20 Mb/s of secret key.
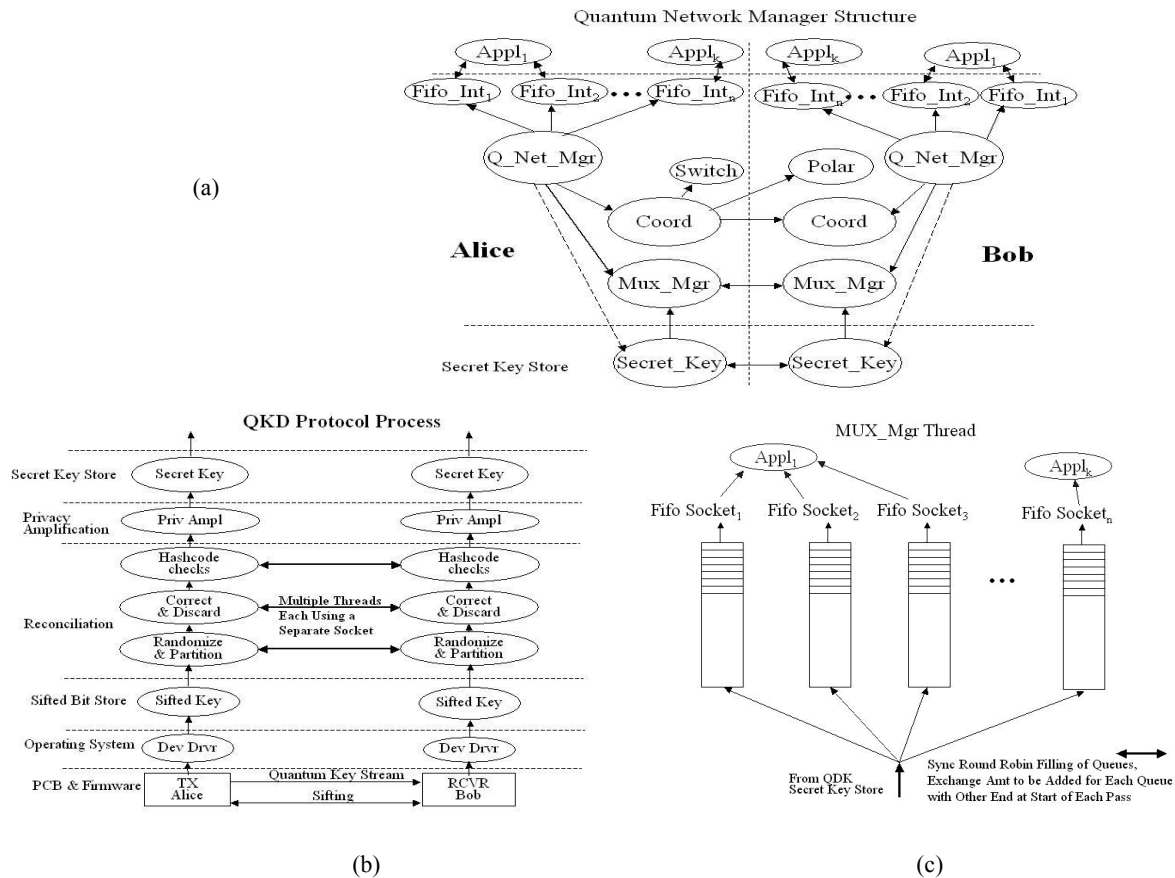
Figure 11. (a) Structure of the network manager; (b) The QKD infrastructure protocol stack, (c) The MUX_Mgr synchronizes keys entering all FIFOs

A high-speed QKD network can support a wide range of potential applications in Local Area Networks (LANs). One high-speed example application is a QKD secured video surveillance network. A video surveillance system secured by our three-node QKD network (shown in Fig. 12) has been demonstrated The two Bob nodes at two different locations are each equipped with a video camera, while Alice is installed at the surveillance station. A set of QKD network managers, one on each QKD node, cooperate to control the optical switches and the initial link connection. Once the secure quantum keys are generated between the selected pair of nodes, the video content from the camera at the selected Bob node is encrypted using the one-time pad cipher with the secure keys and sent to Alice over an unsecured public network, which, in this experiment, is the Internet. Alice then decrypts the transmitted data and displays the video. The speed of our system enables real-time one-time pad encryption and decryption of streaming video.
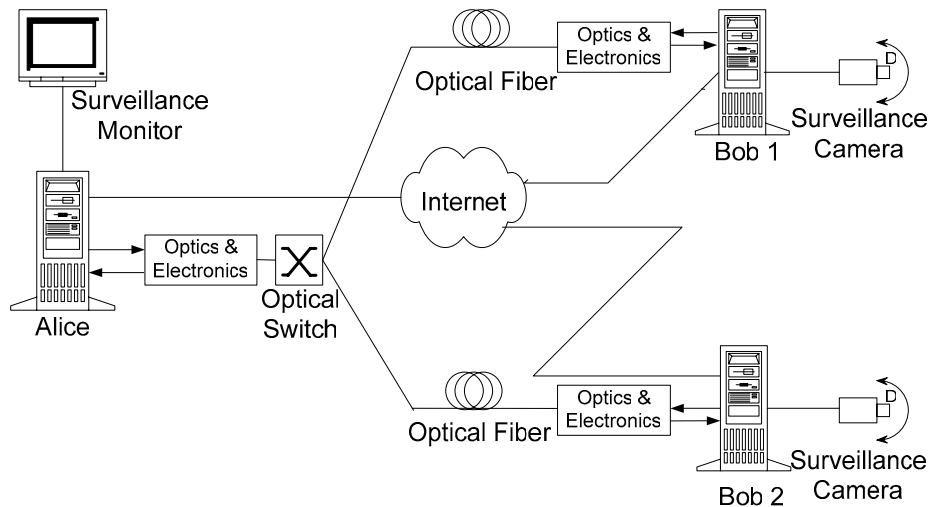
Figure 12. QKD secured network application: secured surveillance system

5. FUTURE QKD NETWORK

We have implemented fiber-based QKD systems for optical networks using 850-nm for LANs and 1310-nm wavelengths for MANs, and developed a network manager to manage the QKD network and interface to security applications.   To fully integrate QKD in networks, we are now focusing on the following tasks.

First, we need to study the integration of QKD technology into existing network security protocols. We are now investigating the issues and feasibility of doing this. QKD is a provably secure method of generating and distributing secure cryptographic keys that can than be used to encrypt and decrypt messages. Existing security protocols, such as IPsec and TLS, currently rely on public key exchange methods to distribute secure keys. When quantum computers are available such key exchange mechanisms will be broken. Furthermore, a breakthrough algorithm for factoring or computing discrete logarithms may also threaten such key exchange mechanisms at any time. Transitioning to future technologies, such as QKD, must be done well before such threats become reality, because past secrets will also be vulnerable.

Second, we are developing a 1310/895-nm high repetition rate entangled photon source using a PPKTP waveguide. The source will be used for studies of entanglement-based QKD networks. Entangled photon source, a core element for quantum information, provides a novel horizon for QKD technology.   With such a source, QKD, in theory, can break through the current distance limitation and support many new applications. Our entangled photon source can be used to connect QKD networks at different levels. For example, the 1310/895-nm entangled photon source can connect separate LANs (850-nm system) via a MAN (1310nm system). Also it can be used to connect a fiber-based QKD system (1310-nm) and a free-space QKD system (895-nm). Moreover, our proposed entangled photon source may be used in studies of quantum memory and quantum repeaters.

6. CONCLUSION

Complete high-speed quantum key distribution systems over fiber networks suitable for LANs and MANs have been developed at NIST. The systems include a high-speed point-to-point system and a low-cost point-to-point system at 850-nm for LANs, a point-to-point system at 1310-nm with up-conversion detectors for MANs, a 3-node quantum network using MEMS optical switches that is controlled by a set of network manager programs.   A QKD secured video surveillance application has been used to demonstrate the use of these systems.   We are currently working on the

integrating QKD technology into existing network security protocols, and developing entangled photon source based QKD systems, each of which will contribute to a fully functional QKD system in commercial optical networks.

ACKNOWLEDGEMENT

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. of the IEEE Int. Conf. on Computers, Systems & Signal, 175-179 (1984).
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography" Rev. Mod. Phys. 74, 145-195, (2002).
3. X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. Bienfang, D. Su, R. Boisvert, C. Clark, and C. Williams, "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s", Optics Express, 14 (6), 2062-2070 (2006).
4. X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. Bienfang, D. Su, R. Boisvert, C. Clark, and C. 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).
5. L. Ma, T. Chang, X. Tang, "Detection-Time-Bin-Shift Polarization Encoding Quantum Key Distribution System,", CLEO/QELS Technical Digest 08 , QWB4 (2008).
6. L. Ma, T. Chang, A. Mink, O. Slattery, B. Hershman and X. Tang "Experimental Demonstration of a Detection-time-bin-shift Polarization Encoding Quantum Key Distribution System", IEEE Communications Letters, 12(6), 459-461, (2008).
7. H. Xu, L. Ma, A. Mink, B. Hershman, and X. Tang, "1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm," Optics Express, 15(12), 7247-7260 (2007).
8. H Xu, L. Ma, X. Tang, "Low noise PPLN-based single photon detector," Optics East 07, Proc. SPIE. 6780, 67800U-1 (2007).
9. A. Mink, "Custom hardware to eliminate bottlenecks in QKD throughput performance," Optics East 07, Proc. SPIE. 6780, 678014-1 (2007).
10. A. Mink, X. Tang, L. Ma, A. Nakassis, B. Hershman, J. Bienfang, D. Su, R. F. Boisvert, C. Clark, and C. Williams, "High Speed Quantum Key Distribution System Supports One-Time Pad Encryption of Real-Time Video", Defense and Security 06, Proc. SPIE 6244, 62440M-1~62440M-7 (2006).
11. L. Ma, A. Mink, H. Xu, O. Slattery and X. Tang, "Experimental Demonstration of an Active Quantum Key Distribution Network with Over Gbps Clock Synchronization", IEEE Communication Letters, 11(12), 1019~1021 (2007).
12. A. Mink, L. Ma, T. Nakassis, H. Xu, O. Slattery, B. Hershman, X. Tang, "A Quantum Network Manager that Supports a One-Time Pad Stream," Second International Conference on Quantum, Nano and Micro Technologies , ICQNM, 16-21, (2008).
13. X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. Bienfang, D. Su, R. Boisvert, C. Clark, and C. Williams, "Demonstration of active quantum key distribution network.", Optics and Photonics 06, Proc. SPIE 6305, 630506 (2006).
14. PerkinElmer Product Catalog: http://optoelectronics.perkinelmer.com/catalog/Product.aspx?ProductID=SPCM-AQR-14.

15. 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).
16. J. Breguet, A. Muller and N. Gisin, "Quantum Cryptography with Polarized Photons in Optical Fibres Experiment and Practical Limits" Journal of Modern Optics, 41(12), 2405-2412 (1994).
17. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., 68, 3121-3124 (1992).
18. H. Xu, L. Ma, J. Bienfang, and X. Tang, "Influence of the dead time of avalanche photodiode on high-speed quantum-key distribution system", CLEO/QELS 06, CLEO digest JTuH3, (2006).
19. D. J. Rogers, J.C. Bienfang, A. Nakassis, H. Xu and C. W. Clark, " Detector dead-time effects and paralyzability in high-speed quantum key distribution" New Journal of Physics, 9, 319 (2007).
20. http://www.idquantique.com.
21. R. H. Hadfield, J. L. Habif, J. Schlafer, L. Ma, A. Mink, X. Tang, S. Nam, "Quantum key distribution with high-speed superconducting single-photon detectors," submitted to CLEO/QELs 2007.
22. C. Gobby, Z. L. Yuan, and A. J. Shields, "Unconditionally secure key distribution over 50 km of standard telecom fiber," Electron. Lett., 40, 1603- 1605, (2004)
23. S.Phoenix, S. Barnett, P. Townsend, and K. Blow, "Multi-user quantum cryptography on optical networks", Journal of modern optics, 72 (6), 1155-1163 (1995).
24. P. Townsend, S. Phonenix, K. Blow, and S. Barnett, "Design of quantum cryptography systems for passive optical networks", Electronics Letters, 30(22), 1875-1877 (1994).
25. V. Fernandez, R.J. Collins, K.J. Gordon, P.D. Paul, and G.S. Buller, "Passive Optical Network Approach to GigaHertz-Clocked Multiuser Quantum Key Distribution", J. Quantum Electronics, 43(2), 1~9, (2007).