Experimental Demonstration of an Active Quantum Key Distribution Network with Over Gbps Clock Synchronization

Lijun Ma, *Senior Member, IEEE,* Alan Mink, Hai Xu, *Member, IEEE,* Oliver Slattery, and Xiao Tang

***Abstract*— We demonstrate a three-node QKD network that allows multiple users to share secure keys. This QKD network operates on the 850 nm and 1550 nm wavelengths at 1.25 Gbps clock rate. The communication route is controlled by MEMS optical switches. In this paper, we report the network structure and experimental results including the performance of the optical switch, polarization recovery, and timing alignment technology during switching. This demonstration experimentally shows that QKD can be extended to active multi-node networks.**

***Index Terms*— Optical fiber communication, data security, quantum cryptography, quantum network, quantum key distribution.**

I. Introduction

SECURITY has become a critical issue for current data communication systems and networks, which demand provably secure encryption techniques. Quantum Key Distribution (QKD) is one approach that can provide unconditional security of communication and is based on the fundamental laws of physics rather than mathematical or algorithmic computational complexity. Although speed and distance are important objectives of QKD systems, integrating a QKD system into a network that supports security for a number of interconnected users is also crucial for evaluating the practicality of deployment of such a system into commercial infrastructures.

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, or ”broadcast” from one node to multiple nodes. Several groups have successfully demonstrated a QKD network based on this scheme [1] . 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. Optical switches have been investigated in QKD systems [2], but it has not been reported on a complete active QKD network.

We demonstrate a complete 3-node active QKD system controlled by commercial Micro-Electro-Mechanical Systems (MEMS) optical switches. In this paper, we introduce the system configuration and present the performance results of the network. We also developed a high-level QKD network management system, by which we successfully achieve a video surveillance system secured by a QKD generated one-time pad transmitted over the commercial internet.

II. System Configuration

Our system is a 3-node fiber-based polarization encoding QKD network operating at 1.25 Gbps clock rate, which is shown schematically in Figure 1. At Alice, two vertical-cavity surface-emitting lasers (VCSEL) generate 850-nm optical pulse trains, which are complementarily modulated by pseudo-random data generated by a custom high speed data handling circuit board in Alice’s computer. The two pulse trains are attenuated down to single photon level. Their polarization orientations are set at 45 and 90 degrees respectively and they are then combined into a single fiber, forming the quantum channel. The classical channel is generated by a wavelength division multiplexer (WDM) transceiver, which transmits a 1510 nm signal and receives a 1590 nm signal. The communication routine of the quantum channel and the classical channel are controlled by two MEMS optical switches independently. For the link between Alice and Bob 1, we use 1 km of standard telecom fiber (SMF28) with a short length (∼20 cm) of HI780 fiber fusion spliced to the end of the SMF28 fiber. This HI780 fiber provides fundamental-mode propagation at 850 nm and is used to remove the higher order mode components generated in the SMF28. For the link between Alice and Bob 2, a 1 km 850 SM Fiber (HI780) is used as quantum channel. The classical channels between Alice and the two Bobs both use standard telecom fiber (SMF28). At each Bob, the arriving photons are randomly selected by a 50/50 coupler into different detection bases. After the polarization state is automatically recovered by polarization controllers, these photons are detected by silicon avalanche photodiodes (APDs). For the classical channel, another WDM transceiver receives the 1510 nm signal and transmits a 1590 nm signal.

High-speed data handling boards, designed and implemented at NIST, are installed in both the Alice and Bobs’ computers. The board at Alice generates pseudo-random data streams to fire corresponding lasers in accordance with the QKD protocol. The board at each Bob collects the detection events and communicates with Alice through the classical channel to perform the sifting algorithm. Alice and Bob’s boards then send the sifted bit values to their own com-

Manuscript received September 4, 2007. The associate editor coordinating the review of this letter and approving it for publication was Costas Georghiades. This work was supported in part by the Defense Advanced Research Projects Agency under the DARPA QuIST program. The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology.

The authors are with Advanced Network Technologies Division, the National Institute of Standards and Technology, Gaithersburg, MD 20878 USA(e-mail: xiao.tang@.nist.gov).

Digital Object Identifier 10.1109/LCOMM.2007.071477.

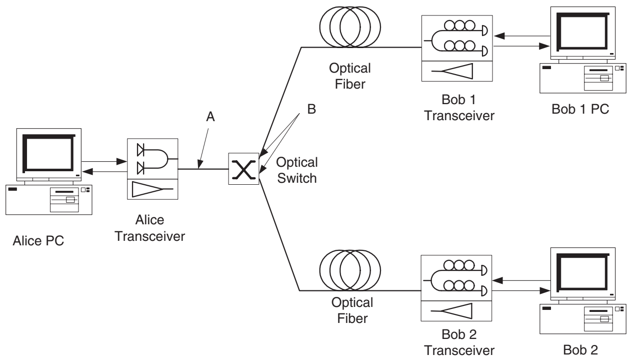

Fig. 1. Configuration of active 3-node QKD secured network. Two optical fibers are used for quantum and classical channels separately in each link.

puters for the subsequent error reconciliation and privacy amplification, performed over the classical channel, necessary to generate shared secret keys. The computers of Alice and Bob then use the shared secret keys for application-level data encryption as necessary to implement secure communications through an unsecured network.

The system can perform either the BB84 or B92 protocol. Though not as secure as the protocol BB84 and vulnerable to the ”intercept-resend” attack, the B92 protocol is relatively simple to implement at a lower cost, and it is widely used in laboratory studies of the physical-layer of QKD systems. Therefore, the following experiments described in this paper were conducted using the B92 protocol. It should be noted, however, that our system can be converted to the BB84 protocol by adding additional APDs and faint laser sources.

III. Results and Discussion

The sifted-key rate and quantum bit error rate (QBER) are widely used as the criteria of QKD system performance. For an active QKD network, it is also important to achieve a short system switching time, the time used to establish the connection between Alice and one of the Bobs. We measure and discuss these parameters next.

The point-to-point QKD sifted-key rate is determined by the mean photon number, μ , at Alice's output; the loss in the transmission fiber, including fiber attenuation, bending, coupling and connectors; the protocol related loss; and the detection efficiency of the APD. These factors remain the principle influence to the sifted-key rate in network QKD systems. Besides these factors, the insertion loss in the optical switch should be taken into account.

The 3-node QKD network is configured as follows. The mean photon number, μ , at Alice is set to 0.1. The loss in the transmission fiber is measured to be 2.3 dB/km at 850 nm, while other losses such as bending, coupling and connection losses in the quantum channel amount to approximately 3 dB. The silicon APD's detection efficiency is approximately 45% at 850 nm. Protocol B92 has 6 dB protocol loss because all polarization-incompatible photons and half of the polarization-compatible photons are blocked before entering the detector.

We measured the sifted key rate based on three settings. In setting 1, the mean photon number, μ , is set to 0.1 before the optical switches (at point A in Fig. 1); in setting 2, μ is set to 0.1 after the optical switches (at point B in Fig. 1); and in setting 3, μ is set to 0.1 at the output of Alice in the point-to-point links (bypass switches). The sifted key rates of the two links in the network are measured based on the three settings and the results are shown in Table I. Comparing the results of setting 1 with the results of setting 3, the sifted-key rate in the network is approximately 1dB lower due to loss from the insertion of the optical switches. When the optical switch is located inside Alice (setting 2), it is shown from the data that the sifted-key rate is comparable with the point-to-point link (setting 3). In other words, if the optical switches are installed in the transmission path, the insertion loss of optical switch causes additional loss of photons and reduces the sifted-key rate, however, when the optical switches are installed inside Alice, where its insertion loss can therefore be considered as internal attenuation, the sifted-rate is the same as that of a point-to-point system. Therefore, in the configuration of our QKD network, it is advantageous on the sifted-key rate to install optical switches at Alice. 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.

TABLE I
Measured Sifted-Key Rate

	Setting 1	Setting 2	Setting 3
Alice to Bob 1	1.57 Mbps	1.96 Mbps	1.98 Mbps
Alice to Bob 2	1.73 Mbps	2.14 Mbps	2.14 Mbps

TABLE II
Measured PER, Timing Jitter and QBER

	Bypass Switch	Through Switch
PER at Bob 1	22.1 dB	22.0 dB
PER at Bob 2	22.7 dB	22.9 dB
Timing Jitter at Bob 1(FWHM)	295 ps	295 ps
Timing Jitter at Bob 2(FWHM)	298 ps	304 ps
QBER at Bob 1	2.3%	2.4%
QBER at Bob 2	2.2%	2.2%

Our results also show that the links to Bob 1, in which the standard 1550 nm single-mode fiber SMF-28 is used, induce more photon loss. This is due to the fact that SMF-28 cannot provide single mode transmission at 850 nm and those photons in the higher mode are filtered off by the short length of HI710. By comparison, the link to Bob 2 uses HI710 throughout and there is no photon loss due to the filtering of higher-mode photons. For a 1 km of transmission length, the photon loss due to the higher mode transmission and subsequent filtering is less than 1dB, as shown in Table I.

We measured the polarization extinction ratio (PER), timing jitter and QBER in the two links, with and without the optical switch as shown in Table II. The results indicate 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

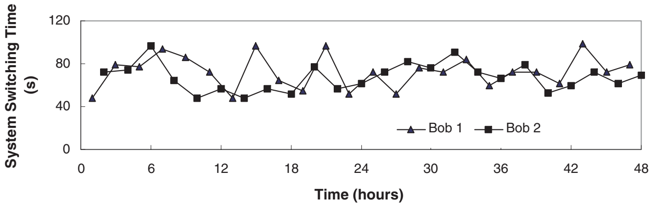

Fig. 2. Measured system switching time.

optical switches without significantly adding to the error rate.

In an active QKD network, we define 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 subsequent operations. First, the optical switch must close the previous link and open the required link, which depends on the switching time of optical switches. Then, Alice and Bob need to perform the other three operations: polarization recovery, time alignment and software initialization, so that the two nodes can generate secret keys. The switching time of optical switches is relatively short, less than 1 ms. The time requirement for polarization recovery, on the other hand, is the relatively long 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 the feedback is about 50 ms. Moreover, the recovery time varies in each operation, which depends on the number of recovery iterations before the optimum points are found. The detailed method and algorithm of polarization recovery at this network have been described elsewhere [3]. In our experiment, the polarization recovery time ranges from several seconds up to 50 seconds. To compensate for different delays between classical channels and quantum channels, an automatic timing alignment is conducted on the system after the polarization recovery. The timing alignment takes approximately 3∼5 seconds. The software initialization includes raw key sifting, error reconciliation and privacy amplification, and needs enough time to accumulate a few Mbits of an initial secure key, and so it depends on the speed of both Alice's and Bob's computers as well as the key rate. In this experiment, the software initialization time is approximately 40 seconds. The system switching time in this network is therefore approximately 1∼2 minutes. Figure 2 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.

IV. Network Management and Secured Surveillance System

We developed a management system that coordinates operations of all nodes in the network. The manager consists of a set of commands that request operations including link switching, polarization recovery, key sifting, error reconciliation, and privacy amplification functions, etc. These commands are sent through the internet. 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. A high-speed QKD network can provide a wide range of potential applications in Local Area Networks (LANs). One important application is a QKD secured video surveillance network. A video surveillance system secured by the three-node QKD network is demonstrated as shown in Figure 3. The two Bobs at two different locations are each equipped with a monitoring video camera, while Alice is installed at the surveillance station. A network management computer controls the optical switches and the initial link connection. Once the secret quantum keys are generated between the two nodes, the video content from the monitoring camera at Bob is encrypted with the secret key bits and sent to Alice over an unsecured public network, which, in this experiment, is the Internet. Alice can then decrypt the transmitted data and display the video. The speed of our system enables real-time one-time pad encryption and decryption of streaming video.

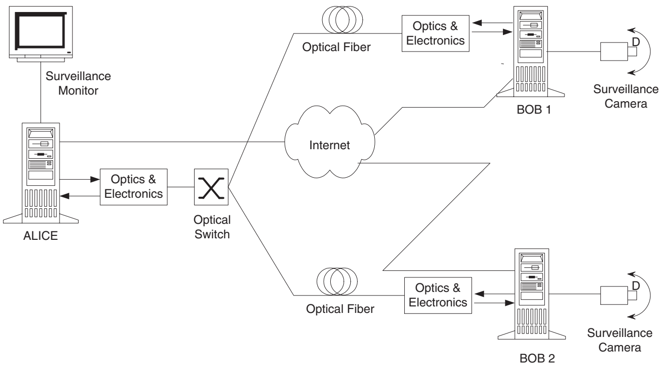

Fig. 3. QKD secured network application: secured surveillance system.

V. Conclusion

We have demonstrated, for the first time to our knowledge, a complete active three-node QKD secured network, which operates at 1.25 Gbps clock rate and is controlled by optical switches. Using this network, a QKD secured video surveillance system has been successfully demonstrated.

References

[1] V. Fernandez, *et al.*, "Passive optical network approach to gigahertz-clocked multiuser quantum key distribution," *J. Quantum Electron.*, vol. 43, no. 2, pp. 1-9, 2007.

[2] P. Toliver, *et al.*, "Experimental investigation of quantum key distribution through transpenrent optical switch elements," PTL, vol. 15, no. 11, pp. 1669-1671, 2003.

[3] L. Ma, *et al.*, "Polarization recovery and auto-compensation in quantum key distribution network," *Optics and Photonics*, Proc. SPIE 6305, 630513-1-6 (2006)