Experimental Demonstration of a Detection-Time-Bin-Shift Polarization Encoding Quantum Key Distribution System

Lijun Ma, *Senior Member, IEEE,* Tiejun Chang, Alan Mink, *Member, IEEE,* Oliver Slattery, Barry Hershman, and Xiao Tang

***Abstract*— Detection-time-bin-shift (DTBS) is a scheme that uses time division multiplexing of a single photon detector between two photon bases in a quantum key distribution (QKD) system. This scheme can simplify the structure of a QKD system, reduce its cost and overcome the security problems caused by the dead-time induced self-correlation and the unbalanced characteristics of detectors. In this paper, we introduce an improved DTBS scheme and implement it based on our previously developed conventional fiber-based QKD system using the B92 protocol. Our DTBS QKD system generates sifted keys at a rate of more than 1 Mbit/s with a quantum bit error rate (QBER) lower than 2% over 1.1 km of fiber.**

***Index Terms*— Quantum cryptography, quantum key distribution, detection-time-bin-shift.**

I. Introduction

QUANTUM key distribution (QKD) is a technique for developing a secure encryption key over unsecured communication channels that is guaranteed by the fundamental quantum properties of single photons. At present, high cost is one of the challenges for QKD technology to be widely used in commercial applications. Single photon detectors are the most expensive elements used in QKD systems. The detection-time-bin-shift (DTBS) scheme [1] uses half as many single photon detectors as in a conventional QKD system, and therefore, significantly reduces the cost. We propose an improved DTBS scheme and have implemented a fiber-based DTBS QKD system using the B92 protocol [2] based on our system developed earlier [3]. This scheme can also be used in the BB84 protocol [4] for higher security and reduced cost. In our DTBS QKD system, only one silicon avalanche photodiode (Si-APD) and two vertical cavity surface emitting lasers (VCSELs) at 850 nm are used along with a number of off-the-shelf optical parts and standard telecom fibers for the optical links. Operating at 312.5 MHz, our DTBS QKD system produces sifted keys at a rate exceeding 1 Mbit/s with an error rate lower than 2% over 1.1 km of fiber. Since only one APD is used, this system intrinsically avoids security concerns due to the detector dead-time and the unbalanced detection efficiency.

Manuscript received February 15, 2008. The associate editor coordinating the review of this letter and approving it for publication was M. Ma . This work was supported by the NIST quantum information initiative program. This work is an extension of the QuIST program supported in part by the Defense Advanced Research Projects Agency (DARPA). 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 the Advanced Network Technologies Division, Information Technology Laboratory, the National Institute of Standards and Technology, Gaithersburg, MD 20878 USA (e-mail: xiao.tang@nist.gov).

Digital Object Identifier 10.1109/LCOMM.2008.080237.

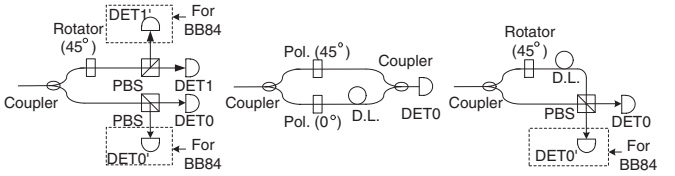

Fig. 1. Schematic diagram of the Bob's side of a QKD system. (a) Conventional QKD system. (b) DTBS QKD system proposed in ref. [1]. (c) Improved DTBS QKD system. Coupler: Passive Fiber Coupler; D.L.: Delay Line; PBS: Polarizing Beam Splitter; DET: Single Photon Detector.

In this paper, we discuss our improved DTBS scheme and present performance results from an experimental implementation of our improved DTBS scheme in our QKD system.

II. Improved DTBS Scheme

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 the 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 than an active scheme, 4 detectors for the BB84 protocol and 2 for the B92 protocol, as shown in Fig. 1(a).

To reduce the number of detectors in the passive scheme, Ref. [1] proposed the DTBS scheme, which time division multiplexes a single photon detector between two photon bases. The trade-off for using fewer detectors is that the single photon transmission rate must be reduced by half to allow for the two detector time bins (DTBs) and the sifted-key rate is reduced as a result. This scheme is shown in Fig. 1(b). However, the second coupler in the scheme causes an additional 3dB loss and it can't be extended to the BB84 protocol. We propose an improved DTBS scheme shown in Fig. 1(c). This scheme has a simpler structure, avoids the additional loss and can be extended to BB84 by adding another detector.

In the improved scheme, a passive coupler performs a random choice of measuring polarization bases and projects the results of the different bases onto a short or long (delay) path resulting in the photon arriving in one of two adjacent DTBs. In the short path, the polarization state of the photon is unchanged. In the long path, the photon is delayed by a

1089-7798/08$25.00 © 2008 IEEE

DTB and the polarization state of the photon is rotated by 45°. The photons on these two paths are combined using a polarizing beam-splitter (PBS) and then fed to the detector. One (for B92) or two (for BB84) single photon detectors are used to sense the photons. Photons that take the short path are measured at 0° basis (B92) or 0°/90° basis (BB84) and detected in the first DTB. Photons that take the long path are measured at 45° basis (B92) or +/-45° basis (BB84) and detected in the second DTB. The data handling algorithms of our QKD system are reconfigured to interpret events occurring in alternating DTBs as data from different bases but occurring in the same transmission time bin. Exposure of the individual DTBs is the same as exposing the values detected and will compromise the security of the QKD system.

In addition, the DTBS scheme improves security for the B92 protocol. All single photon detectors have a dead time, the recovery time following each detection event. For example, the Si-APD used in our QKD system has a 50 ns dead-time. In a B92 system, two detectors are used to detect ”0” and ”1”, respectively. Once one detector has been fired by a photon, it becomes unavailable for its dead time period. There is a high probability that in a high repetition rate system the other detector will be fired before the first detector recovers, which results in strings of 1010.... Runs of such strings reduce the randomness of the keys and degrade the security of the QKD system. This dead-time induced self-correlation problem was discussed previously [5] [6] along with schemes for prevention, such as actively disabling detectors or adding different propagation delays depending on the state. In the B92 DTBS scheme, this problem is intrinsically solved, since no photons will be detected until the single detector recovers independent of whether they are ”0” or ”1”. This ensures the next key bit is truly chosen with a probability of 0.5. Furthermore, the B92 DTBS scheme also avoids security concerns due to differences of detection efficiency between multiple detectors.

III. System Configuration

We modified our existing fiber-based QKD system [3] to incorporate DTBS using the B92 protocol, as shown in Fig. 2. Our QKD system uses a pair of custom printed circuit boards with a field programmable gate array (FPGA) for communications and to control the system and process the data at a continuous high data rate. The pair of boards is installed in both the Alice and Bob computers and communicates with their processor via a PCI bus. Alice’s board generates a random data stream for the two quantum channels and sends an 800-ps electrical pulse (FWHM) every 3.2 ns (312.5 MHz) on a randomly selected channel. These electrical pulses directly modulate two vertical-cavity surface-emitting lasers (VCSELs) at 850 nm and generate optical pulse trains. These two optical pulse trains then are attenuated down to a single photon level. Their polarization orientations are set at 0° and 45°, respectively, and they are then combined into a standard telecom fiber (SMF28).

At Bob’s side, the arriving photons are randomly selected by a 50/50 passive fiber coupler into long and short paths. Polarization controllers are used to recover the polarization state of photons and add another 45° polarization rotation in the long path. The delay between the long and the short optical paths is 1.6 ns, or one DTB. All photons are reflected by or passed through a PBS and are then detected by a Si-APD (PerkinElmer SPCM-AQR-14). For each transmission clock period (3.2 ns), the ”0” photons arrive at the detector in the first DTB and the ”1” photons arrive at the detector in the second DTB. The detection signals are sent to the custom printed circuit board in Bob’s PC for processing.

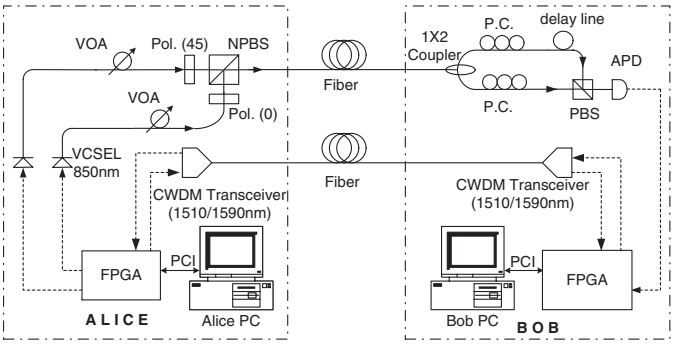

Fig. 2. Schematic diagram of our B92 DTBS-QKD system; VCSEL: Vertical-Cavity Surface-Emitting Lasers; Pol.: Polarizer; VOA: Variable Optical Attenuator; NPBS, Non-polarizing Beam Splitter; P.C.: Polarization Controller; FPGA: Custom Printed Circuit Board; PCI: PCI bus; PBS: Polarizing Beam Splitter; Solid line: Optical fiber; Dotted line: Electric cable.

Two 1.25 GHz coarse wavelength division multiplexing transceivers form the bi-directional classical communication channel operating at 1510 nm and 1590 nm. Bob recovers Alice’s clock from the classical channel, allowing it to synchronize data with Alice. Since the data paths for quantum and classical channels may be slightly different, Alice and Bob first need to align the timing between each quantum channel and the classical channel. There are two alignment controls. One is a sub-bit timing control (40 ps increments), as the data enters the board, to align the data with the local clock edge. The other is a multiple bit delay, located within the FPGA, to align the quantum data with the corresponding classical data. For our DTBS implementation, only one quantum channels needs to be aligned, rather than two, since the two quantum channels are engineered to be aligned with each other. Once the timing alignment is finished, Bob and Alice can begin the QKD protocol. Bob tells Alice the transmission clock time bin of detected events, but not the DTB, over the public classical channel, and then Alice and Bob can perform the sifting, error reconciliation and privacy amplification algorithms, resulting in shared secure keys. The sifted-key rate and the QBER, two important performance metrics for QKD systems, can be measured in real time from the raw data before reconciliation in our system.

IV. Results and Discussion

Two configurations of the DTBS QKD system are used in our measurements: (1) a back-to-back configuration, which uses one 2-meter SMF28 fiber for the classical channel and another 2-meter HI-780 fiber for the quantum channels and (2) a 1.1 km configuration, which uses two 1.1 km SMF28 fibers for both classical and quantum channels. The end of the 1.1 km quantum channel fiber is fusion-spliced to a 40 cm HI-780 fiber connecting to Bob.

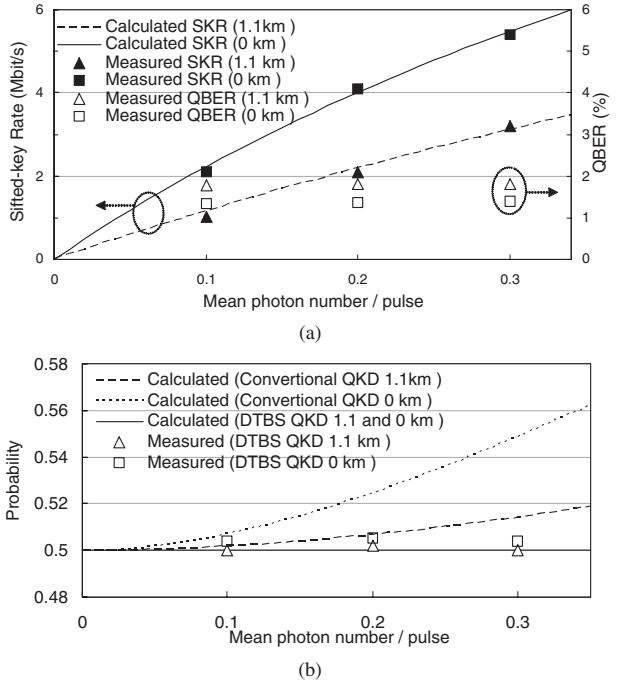

Fig. 3. The system performance of the B92 DTBS QKD system at 0 km (back-to-back) and over 1.1 km. (a) Sifted Key Rate (SKR) and QBER (b) Probability that neighboring two bits are different.

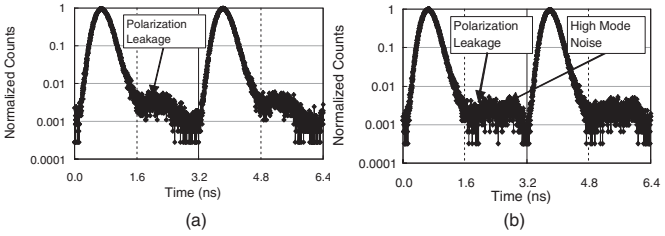

Fig. 4. Histogram of the output at APD for a repetitive pattern of 0101 (count numbers are normalized). (a) The back-to-back setting; (b) The 1.1 km setting.

For each configuration, we measured the sifted-key rate and the QBER. In Fig. 3(a) we plotted the measured data as a function of the mean photon number, along with the theoretically calculated sifted-key rates [3], and we see that the measured data agrees well with the calculated results. Our conventional QKD system achieves more than 2 Mbit/s sifted key rate, while the DTBS QKD system achieves more than 1 Mbit/s sifted key rates at $\mu = 0.1$ over 1.1 km of fiber. This is the expected trade-off between using two APDs vs. one. Also, from Fig. 3, we can see that the QBER doesn't change as μ increases, but is lower for the back-to-back configuration than for the 1.1 km configuration as expected, since the longer the distance the higher the QBER.

For QKD systems to be secure, their components must operate close to their theoretical specifications. An important theoretical specification is that each key bit is random (i.e., the probability of its value is 0.5). Fig.3(b) shows the calculated probability [5] [6] that two neighboring bits are different in traditional QKD and DTBS QKD systems and the measured results from our DTBS QKD system. In conventional QKD systems, the next bit probability may not be 0.5 at high data rates due to the dead-time induced self-correlation. However, in DTBS QKD systems the probability remains at 0.5 as required by the protocol.

As QBER increases, secure key rates decrease. QBER is mainly due to dark counts, polarization leakage and timing jitter. The dark counts are caused by the intrinsic dark counts of the APDs and system light leakage. Polarization leakage is caused by the imperfect polarization extinction ratio of the PBS and the polarization recovery unit. Timing jitter is caused by the transmission optical pulse width and the jitter of the APDs. The dark-counts of the system are measured at a few hundred per second, so its contribution to QBER is negligible in our high-speed QKD system. Polarization leakage and timing jitter are our two main factors of QBER. In the back-to-back configuration, Fig. 4(a) shows that polarization leakage (the small peak in the second DTB) and timing jitter (the tail in the second DTB) are reduced by more than 20 dB, resulting in a QBER of about 1.3%, Fig. 3(a). Photons at 850 nm have a higher order mode in transmission over a standard telecom fiber, and residual noise of the higher mode after the spatial filter with a spliced 850 nm SM fiber contributes to QBER too. In Fig. 4(b), another small peak in the second DTB is caused by this high-order noise, though the noise is reduced by more than 20 dB after the spatial filter. Due to the noise, the QBER measured in the 1.1 km setting is about 1.8%.

V. Conclusion

An experimental fiber-based DTBS QKD system has been demonstrated. It has a simplified structure in comparison with conventional QKD systems and uses only one Si-APD for the B92 protocol. The system uses low-cost commercial 850 nm VCSELs and standard telecom fiber, which further reduces the system cost. The DTBS QKD system operates at a 312.5 MHz transmission clock rate and generates more than 1 Mbit/s sifted-key rate over 1.1 km of fiber with a quantum bit error rate less than 2%. Furthermore, the system avoids security concerns related to dead-time induced self-correlation and unbalanced characteristics of detectors. The only trade-off for the DTBS QKD system is that the key rate is reduced in half from the conventional QKD system. Such a system is most suitable for short distance, low-cost, high-speed QKD networks.

References

[1] J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibres experiment and practical limits," *J. Modern Optics*, vol. 41, no. 12, pp. 2405–2412, 1994.

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, 1992.

[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*, vol. 14, no. 6, pp. 2062–2070.

[4] C. H. Bennet and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[5] 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, May 2006.

[6] 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*, vol. 9, pp. 319, 2007.