Detection-time-bin-shift Schemes for Polarization Encoding Quantum Key Distribution System[1]

Lijun Ma, Tiejun Chang, Alan Mink, Oliver Slattery, Barry Hershman, Xiao Tang

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

ABSTRACT

Detection-time-bin-shift (DTBS) is a scheme that projects the measurement bases or measured photon values into detection time-bins and then time division multiplexes a single photon detector 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 introduced self-correlation and the unbalanced characteristics of detectors. In this paper, we present several DTBS schemes for QKD systems based on attenuated laser pulses and entangled photon sources. We study the security issues of these DTBS schemes, especially the time-bin-shift intercept-resend attack and its countermeasures. A fiber-based DTBS QKD system has been developed and its results are presented in this paper.

Keywords: quantum key distribution, detection time bin shift, optical fiber communication.

1. INTRODUCTION

Quantum key distribution (QKD) is a technique for generating secure encryption keys over unsecured communication channels that is guaranteed by the fundamental quantum properties of single photons. Although the development of QKD systems is technologically advanced, only few QKD systems are commercially available. High cost is one of the challenges for QKD technology to be widely used in commercial applications. The detection-time-bin-shift (DTBS) schemes can reduce the number of single photon detectors, the most expensive device in QKD systems, by projecting the measurement bases or measured photon value into detection time-bins, and, therefore, significantly reduces the cost.

The DTBS scheme was first presented in Ref. [1], for a polarization-encoding QKD system based on the B92 protocol [2]. We improved on the initial scheme by avoiding extra photon loss and extended it to the BB84 protocol [3] and the E91 protocol (the entangled photon pair based QKD) [4]. With this improved DTBS schemes, not only is the system cost reduced, but security concerns caused by detector dead-time and unbalanced detection efficiency are solved as well. However, when gated mode photon detectors are used in DTBS schemes, a time-bin-shift (TBS) intercept-resend attack might undermine the security of the QKD system and countermeasures should be adopted in the system.

We implemented a fiber-based DTBS QKD system using the B92 protocol [5, 6] with our improved DTBS scheme. The B92 protocol used here is only for a demonstration of the scheme's feasibility. This DTBS scheme also can be used in the BB84 protocol or the E91 protocol. 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 few off-the-shelf optical parts and standard telecom fibers for the optical links. Operating at 312.5MHz, our DTBS QKD system produces sifted keys at a

---

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

Quantum Communications and Quantum Imaging VI, edited by Ronald E. Meyers, Yanhua Shih,
Keith S. Deacon, Proc. of SPIE Vol. 7092, 709206, (2008) · 0277-786X/08/$18 · doi: 10.1117/12.793722

rate over 1 Mbit/s with an error rate lower than 2% over 1.1 km of fiber. Since only one APD is operating in free-running mode, this system intrinsically avoids security concerns due to the detector dead-time and unbalanced detection efficiency, and avoids the TBS intercept-resend attack.

In this paper, we present several DTBS schemes for QKD systems based on attenuated laser pulses and entangled photon-pair sources. We study the security issues of these DTBS schemes, especially the TBS intercept-resend attack and its countermeasures. A fiber-based DTBS QKD system has been developed and its experimental results will be presented in this paper.

2. DTBS SCHEMES

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. In practice, 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), or 8 detectors for E91 protocol, as shown in Fig. 1(b).

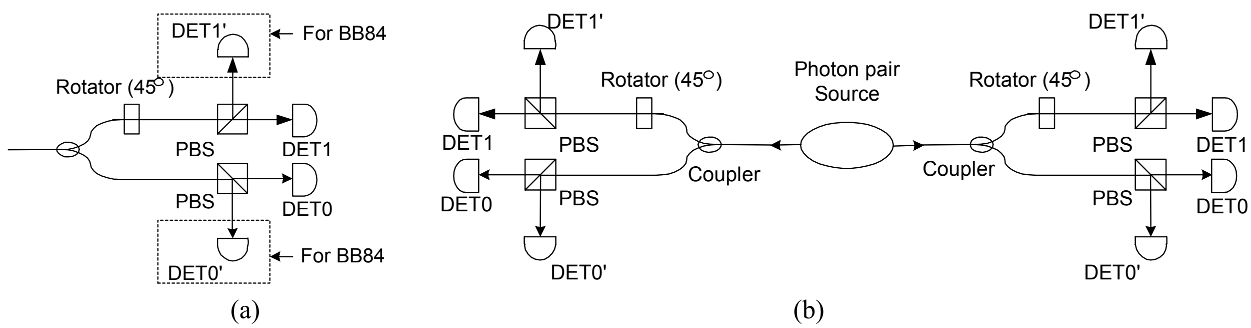


Fig.1. Schematic diagram of conventional schemes for polarization-encoding QKD system. (a) The bob side of BB84 and B92 protocol, (b) The E91 protocol. Coupler: Passive Fiber Coupler; D.L.: Delay Line; PBS: Polarizing Beam Splitter; DET: Single Photon Detector.

2.1 DTBS schemes for B92 protocol

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 DTBs and the sifted-key rate is reduced as a result. This scheme is shown in Fig. 2(a). However, the second coupler in the scheme causes an additional 3dB loss and it can't be extended to the BB84 protocol. We proposed an improved DTBS scheme [5], shown in Fig. 2(b). This scheme has a simpler structure and avoids the additional loss.

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 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 single photon detector is used to sense the photons. Photons that take the short path are measured at 0° basis and recorded in the first DTB. Photons that take the long path are measured at 45° basis and recorded in the second DTB. The PBS works as a polarization measurement and combiner, and thus there is no extra photon loss in this configuration.

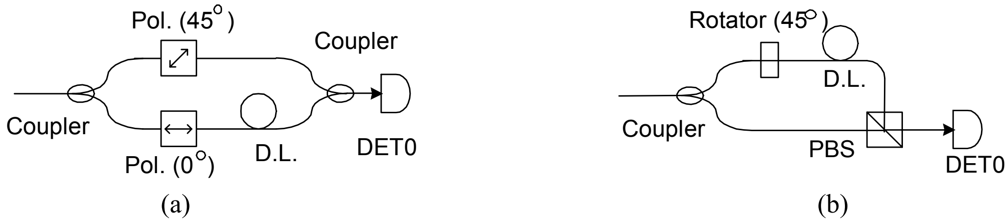


Fig.2. Schematic diagram of DTBS-QKD system for B92. Coupler: Passive Fiber Coupler; D.L.: Delay Line; PBS: Polarizing Beam Splitter; DET: Single Photon Detector.

2.2 DTBS schemes for BB84 protocol

In the BB84 protocol, there are two photon values for each measurement basis, therefore, there are more options to implement DTBS schemes in this protocol, (I) project the measurement bases into DTBs; (II) project the photon values into DTBs; and (III) project both measurement bases and photon values into DTBs.

For the type I BB84 DTBS scheme, the structure is shown in Fig. 3(a) and detection photon values are shown in Table I. After projecting the measurement bases into DTBs in this type of DTBS scheme, the photons measured by V/H basis arrive at the 1st DTB and the photons measured by +/-45° basis arrive at the 2nd DTB. The photon detectors are used to distinguish the photon values. This type of DTBS scheme is quite simply accomplished by just adding one more photon detector to the improved B92 DTBS QKD system, and each transmission clock period needs two DTBs.

The type II BB84 DTBS scheme, whose structure is shown in Fig. 3(b) and detection photon values are shown in Table II, projects the photon values into DTB. All photons measured by +/-45° basis are detected by Detector 0 and those measured by V/H basis are detected by detector 1, and the different photon value arrive at different DTBs, that is "0" is in 1st DTB and "1" is in 2nd DTB. Similar to type I, this type uses two photon detectors and each transmission clock period needs two DTBs.

For the type III BB84 DTBS scheme, we project both measurement bases and photon values into DTBs and use only one detector. Its structure is shown in Fig. 3(c) and the detection photon values are shown in Table III. The measurement bases and photon values are distinguished only by DTBs. The photons measured by the V/H basis arrive in the 1st and 2nd DTBs according to their values and the photons measured by +/- 45° basis arrive in the 3rd and 4th DTB according to their values. All the photons are detected by one detector and each transmission clock period needs four DTBs.

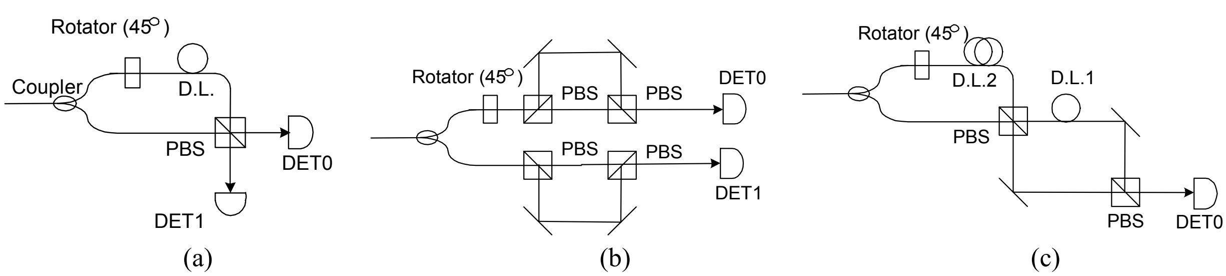


Fig.3. Schematic diagram of DTBS QKD system for BB 84. Coupler: Passive Fiber Coupler; D.L.1: single time-bin Delay Line; D.L. 2: double time-bin Delay Line; PBS: Polarizing Beam Splitter; DET: Single Photon Detector.

Table 1 detection values of type I DTBS BB84 scheme.

	1st DTB	2nd DTB
DET 0	'0' (V/H basis)	'0' (+/-45 basis)
DET 1	'1' (V/H basis)	'1' (+/-45 basis)

Table 2 detection values of type II DTBS BB84 scheme.

	1st DTB	2nd DTB
DET 0	'0' (+/-45 basis)	'1' (+/-45 basis)
DET 1	'0' (V/H basis)	'1' (V/H basis)

Table 3 detection values of type III DTBS BB84 scheme.

	1st DTB	2nd DTB	3rd DTB	4th DTB
DET 0	'0' (V/H basis)	'1' (V/H basis)	'0' (+/-45 basis)	'1' (+/-45 basis)

2.3 DTBS schemes for E91 protocol

For entangled photon-pair based (E91 protocol) QKD systems, the two receivers are the same as the BB84 protocol, so all three BB84 DTBS schemes can be used. Fig. 4 shows a DTBS schemes for E91 protocol with the type III scheme. This scheme just needs two single photon detectors, compared to 8 in the conventional scheme, resulting in a significant cost reduction.

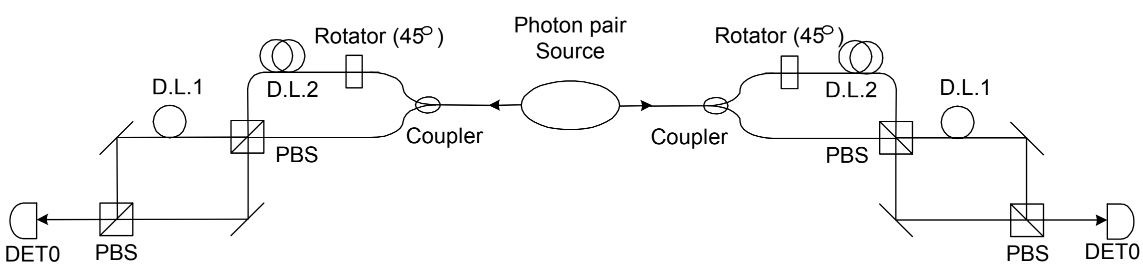


Fig.4. Schematic diagram of DTBS QKD system for E91; Coupler: Passive Fiber Coupler; D.L.1: single time-bin Delay Line; D.L. 2: double time-bin Delay Line; PBS: Polarizing Beam Splitter; DET: Single Photon Detector.

Along with the reduction in hardware described above, the quantum transmission and event detection algorithms in the QKD system need to be changed also. The transmission clock rate should be reduced by half (B92 and BB84 type I and II) or a quarter (BB84 type III), because each transmission clock period contains two or four DTBs in these DTBS schemes. The event detection algorithms must be revised to classify a detection based on a combination of the detector and the DTB in which it was received. The sifting, reconciliation and private amplification algorithms require no modification. Thus the DTBS schemes offer a time vs. cost (hardware) trade-off.

3. SECURITY ANALYSIS IN DTBS SCHEMES

Security is always the highest priority for QKD systems. Although in theory the security of QKD is guaranteed by the fundamental principles of quantum physics, in practice it might be limited by the imperfect properties of actual devices. For example, detector dead-time and unbalanced detection efficiency may cause sifted keys to lose their randomness, and the gated-mode single photon detectors might be vulnerable to the TBS attack. We will discuss the security of DTBS schemes in this section.

3.1 Advantages of DTBS schemes in security issue

The security of a QKD system requires that the keys must be random, measured randomly from two non-orthogonal bases. Even if Alice sends a series of randomly encoded photons to Bob, they may 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, key value and measurement basis imbalance, caused by unbalanced detection efficiency of detectors.

Self-correlation caused by the dead-time of single photon detectors

All single photon detectors have a dead-time, which is the recovery time following each detection event. The dead time for a silicon avalanche photodiode (Si-APD) is usually 50-70 ns. During the dead time, the bias voltage of the detector is below the breakdown level and no photon can be detected [7]. In a high transmission rate QKD system, some photons will arrive before the detectors recover, so there is a high probability that same detector sequence will repeatedly click, which results in self-correlation. For example, in a conventional 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. In a high repetition rate system there is a high probability that the other detector will fire 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. BB84 systems suffer from the same problem using conventional detection schemes. This dead-time induced self-correlation problem was discussed previously along with potential solutions [8, 9].

In B92 DTBS scheme and BB84 DTBS scheme type II and III, the "0" and "1" values are detected by the same photon detectors, therefore photons will be detected until the single detector recovers independent of whether they are "0" or "1". The self-correlation is intrinsically solved. The type I BB84 DTBS scheme still suffers from this problem.

Key value imbalance caused by unbalanced detection efficiency of detector

The randomness of keys means that each value, "0" and "1", has the same 50% probability. However, in conventional systems, different photon detectors are used to detect different photon values (0 or 1) and it is difficult to build all photon detectors with identical detection efficiency. The unbalance characteristics of detectors can cause key value imbalance. A detector with higher efficiency would detect more photons with a given value (such as 0) than the other detector (1 in this case) with a lower efficiency. The imbalance undermines the randomness of keys and the security of a QKD system.

The B92 DTBS scheme and type II and III BB84 DTBS schemes avoid this security concern due to differences of detection efficiency, since they use same photon detectors to detect the both values of photons. Type I of BB84 DTBS scheme still suffers from this problem.

Measurement basis imbalance caused by unbalanced detection efficiency of detector

Random selection of the non-orthogonal measurement bases is crucial for the security of distributed keys. Although a passive coupler can realize a random selection, the unbalance detection efficiency of detectors might make the final keys coming from certain measurement basis more likely than those from the other measurement basis in conventional schemes. If the detection efficiency for different measurement bases have large differences, more keys will come from a certain measurement basis, and the security of QKD system is undermined.

The B92 DTBS scheme and BB84 DTBS type I and III schemes intrinsically avoid this problem since they use the same detectors to detect the photon going through both non-orthogonal measurement bases. Type II of BB84 DTBS scheme still suffers from the problem.

Table 4 summarizes these security concerns caused by the dead-time introduced self-correlation and unbalanced characteristics of detectors. The conventional schemes suffer from all these security concerns. The table shows the B92 DTBS scheme and type III of BB84 DTBS scheme avoid all these security problems. Type I and type II of BB84 DTBS schemes can suppress some security problems. For example, when the self-correlation is the main concern and the unbalanced detection efficiency is not significant, the type II is a good choice.

Table 4 Security concerns in conventional and DTBS schemes of QKD system.

	Conventional scheme (BB84 and B92)	DTBS scheme (B92)	DTBS scheme (BB84 Type I)	DTBS scheme (BB84 Type II)	DTBS scheme (BB84 Type III)
Self-correlation	X	O	X	O	O
Value imbalance	X	O	X	O	O
Basis imbalance	X	O	O	X	O

X: suffering form this security concern; O: this security concern tolerant.

3.2 TBS intercept-resend attack and its countermeasures

Although some of the DTBS schemes overcome the security loss caused by self-correlation and unbalanced detectors, they may be subject to the TBS intercept-resend attack when using single photon detectors that work in gated mode. The properties of the detector gating along with the DTBs enable this attack. Some single photon detectors, such as InGaAs APD, only work in gated mode, in which the detectors can detect photons only in certain time windows.

The TBS intercept-resend attack occurs when Eve intercepts a photon, measures the photon in the basis used for the longer path, and then sends another photon to Bob encoded with the measured value but in the basis of the shorter path, and delays its expected arrival at Bob by one DTB (for B92 or the type I or II BB84) or two DTBs (for the type III BB84). If Bob receives and measures the photon in the basis that Eve uses to measure, it would occur in the DTB with the same measure basis Eve uses (2^{nd} DTB for B92 or the type I and II BB84, or the 3^{rd} and 4^{th} DTB in the type III BB84), in which Eve has the same measured value with that in Bob. Eve would know this by watching the sifting messages between Alice and Bob. If Bob receives the photon incorrectly in the wrong basis, then it would be forced into the non-active DTB, out of the detection window, and never be detected due to the detector gating. Thus Eve would know the value of every photon received by Bob. Bob and Alice may get suspicious if all the detection events occur in only one measurement basis. So Eve can use the other basis just as easily by sending that photon to Bob one DTB early, rather than one DTB late. The concept is to have Eve send what it intercepts to Bob in such a way that if Bob measures it in the wrong basis, that event will occur in an inactive DTB and be ignored, so only those photons measures in the correct basis will be detected.

We use the type I BB84 DTBS QKD scheme as an example. If the detection window is set as two DTBs, as shown in Fig.5(a), and the detector is gated so that at least one DTB before the 1^{st} DTB and one after the 2^{nd} DTB are inactive and unmonitored, it is subject to the TBS intercept-resend attack. Eve intercepts a photon, measures it with the H/V basis used by the 1^{st} DTB, and then sends a new photon based on the measured value at the +/-45° basis advanced by one time bin. After the photon arrives at Bob, if the photon is measured in the H/V basis it will occur in the inactive DTB prior to the 1^{st} DTB and not be detected. If the photon is measured in the +/-45° basis it will follow the longer detector path and occur in the 1^{st} DTB, as shown in Fig. 5(b). Since the photon was measured in the basis that Eve sent, it value will be measured correctly also. By monitoring the sifting messages between Bob and Alice, Eve knows which photons Bob received from Eve and by implication their value. By monitoring the sifting messages between Alice and Bob, Eve knows which photons were sifted out by Alice. As a result Eve knows the sifted key value. By the same procedure, Eve can use the other basis and send a new photon delayed by one DTB, as shown Fig. 5(c). In this way, Eve can randomly select the measurement basis and advance or delay sending the new photon to accomplish the attack. Both Alice and Bob don't know there is an Eve in the system because the error rate doesn't increase and the key values are not unbalanced.

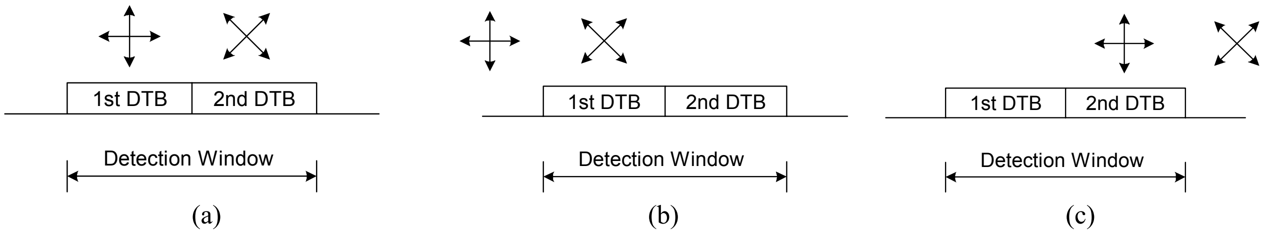


Fig.5. Time-shifting attack to DTBS system with gated photon detectors. (a) without time-shit (b) one time-bin advanced shift (b) one time-bin delayed shift.

The reason that the DTBS QKD system with gated-mode single photon detectors is vulnerable to the TBS intercept-resend attack is because it is missing the photon counting outside the detection window. Therefore, there are two countermeasures to avoid the TBS intercept-resend attack: one is using redundant DTBs and the other is a single DTB per clock. We are still using the type I of BB84 DTBS scheme as an example. The redundant DTB method, as shown in Fig 6(a), adds two additional active redundant DTBs (R-DTB) that are in the detection window.. These two redundant DTBs are monitored to see if any abnormal counts occur, which would imply a TBS attack. The drawback of this countermeasure is that detector dark counts would increase as the detection window broadens. The second countermeasure is to use one DTB per clock, equal to the gated detection window, and the delay being equal to a clock period, as shown in Fig 6(b). This eliminates the possibility of Eve being able to change the timing of received photons such that DTBS will map a detection event out of the active detection window. Using this method, there is no increase in the dark counts, but the transmission clock rate is reduced by half..

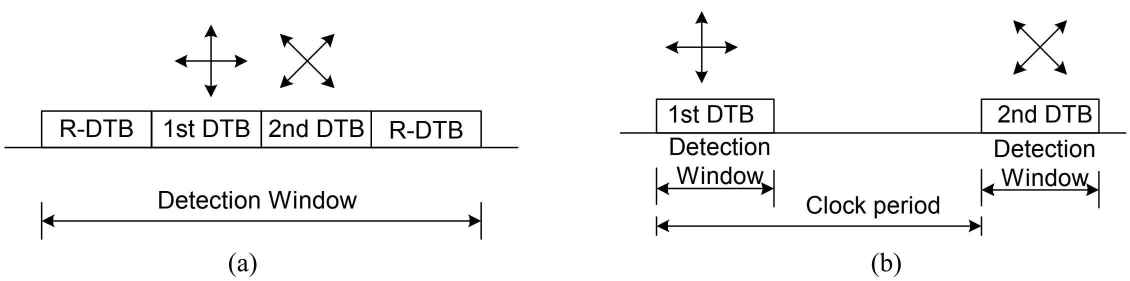


Fig.6. Countermeasures for TBS intercept-resend attack. (a) Redundant DTB setting; (b) one DTB setting. DTB: Detection time bin. R-DTB: Redundant detection time bin.

4. EXPERIMENTAL DEMONTRATION OF DTBS QKD SYSTEM

To demonstrate the DTBS QKD scheme's feasibility, we implemented a DTBS QKD system based on a fiber-based QKD system that we developed previously [10]. The Schematic diagram of the DTBS QKD system is shown in fig 7. The 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. 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. Alice's board generates a random data stream for the two quantum channels and sends an 800 ps electrical pulse (FWHM) every 3200 ps (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 are then attenuated down to single photon levels. 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 after photons traveled in the fiber and add another 45° polarization rotation in the long path. The optical delay between the long and the short paths is 1.6 ns, or one DTB. All photons are reflected by or pass 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 in the second DTB. The detection signals are sent to the custom printed circuit board in Bob's PC for processing.

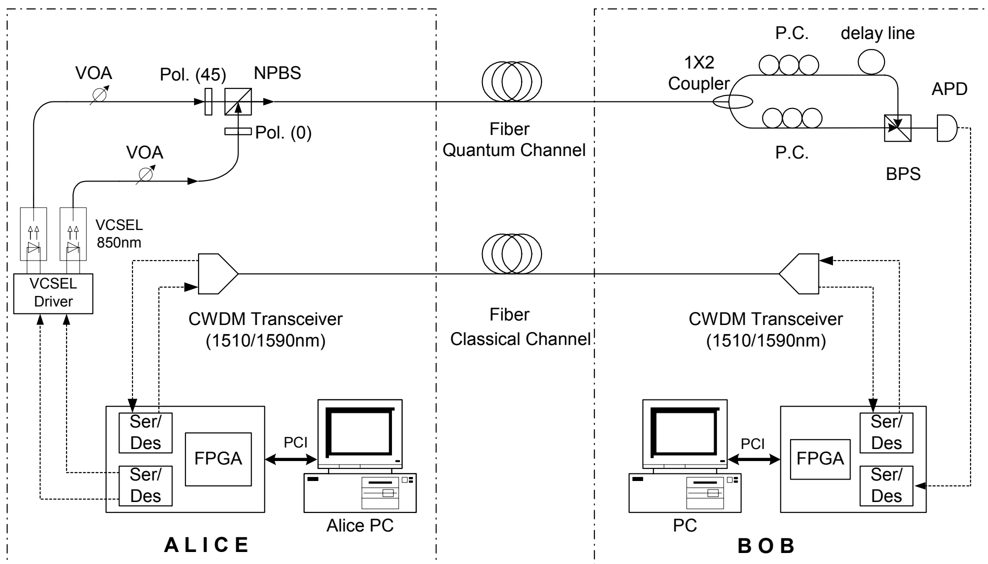
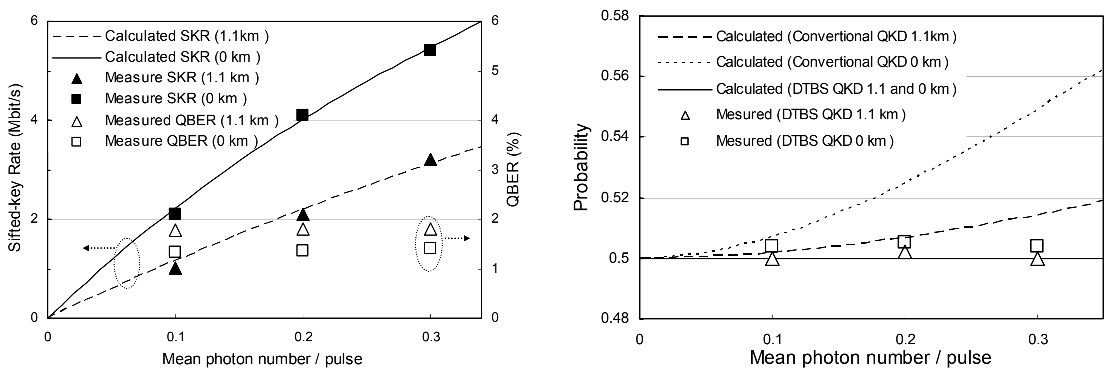


Fig. 7. Schematic diagram of our B92 DTBS-QKD system; VCSEL: Vertical-Cavity Surface-Emitting Lasers; Pol.: Polarizer; VOA: Variable Optical Attenuator; NPBS, Non-polarizing Beam Splitter; P.C.: Polarization Controller; FPGA: Custom printed circuit board controlled by a field-programmable gate array; PCI: PCI bus; PBS: Polarizing Beam Splitter; Solid line: Optical fiber; Dotted line: electric cable.

Two 1.25 GHz CWDM 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 are 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 channel needs to be aligned, rather than two, since the two quantum channels are configured to be aligned with each other. Once the timing alignment is finished, Bob can receive data sent from Alice. 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.

Two configurations of the DTBS QKD system are used in our measurements: (1) a back-to-back configuration, which uses one 2-meter patch-cord of SMF28 fiber for the classical channel and one 2-meter patch-cord of 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 quantum channel is fusion-spliced with a 40-cm segment of HI-780 fiber before connecting to Bob.

For each configuration, we measured the sifted-key rate and the QBER, two important performance metrics for QKD systems. In Fig 8(a) we plotted the measured data as a function of the mean photon number μ, along with the theoretically calculated sifted-key rates [10], and we see that the measured data agrees well with the calculated results. Our conventional QKD system achieves more than 2Mbit/s sifted key rate, while the DTBS QKD system achieves more than 1Mbit/s sifted key rates at $\mu = 0.1$ over 1.1 km of fiber. This is the expected trade-off in DTBS QKD scheme because the clock rate has been reduced by half. QBER is another important metric for QKD systems. 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 our 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 contributing to QBER. In the back-to-back configuration, polarization leakage and timing jitter is reduced by more than 20 dB, resulting in a QBER of about 1.3%. Since 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 (HI-780) contributes to QBER too. Although the noise is reduced by more than 20 dB after the spatial filter, the residual noise still makes the QBER increase to 1.8%. In comparison to conventional QKD systems, DTBS QKD systems do not cause any extra error in the key distribution.



(a) (b)

Fig. 8. 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.

We use the probability that two neighboring bits are different as a metric for the randomness of keys. For random keys, the probability is 0.5. Fig. 8(b) shows the calculated probability in traditional QKD and DTBS QKD systems [8, 9] 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 introduced self correlation, while in DTBS QKD systems the probability remain at 0.5 as required by the protocol. Because only one APD is used in the system, the imbalanced key value or measurement bases caused by unbalanced detection efficiency is avoided. Furthermore, the APD used in the system operates in free-running mode; therefore, the system does not suffer from the TBS intercept-resend attack.

5. CONCLUSION

Detection-time-bin-shift (DTBS) is a scheme that projects the measurement bases or measured photon value into detection time-bins and then time division multiplexes a single photon detector in a quantum key distribution (QKD) system. DTBS schemes can be implemented in the receiver side of B92, BB84 and E91 QKD systems. DTBS simplifies the structure of a QKD system and reduces its cost. Furthermore, DTBS can overcome the security problems caused by imperfect properties of single photon detectors, such as a detector's dead-time and unbalanced detection efficiency. The time-bin-shift intercept-resend attack against DTBS QKD systems using gated-mode detectors is discussed and countermeasures are presented. To show the feasibility of DTBS, a fiber-based DTBS QKD system has been demonstrated. The system only uses one Si-APD and avoids the security concerns caused by the imperfect properties of single photon detectors.

ACKNOWLEDGEMENT

The authors are grateful for the support of the NIST quantum information initiative.

REFERENCES

1. 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).
2. C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett., 68, 3121-3124 (1992).
3. C. H. Bennet and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,1984, 175-179 (1984)
4. A. K Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. 67, 661–663.(1991)
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. M. Ghioni, A. Giudicem S. Cova, and F. Zappa, “High-rate quantum key distribution at short wavelength: performance analysis and evaluation of silicon single photon avalanche diodes,” J. Mod. Opt. 50, 2251-2269 (2003)
8. 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 Technical Digest06, JTuH3 (2006).
9. 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)
10. 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).