Detection-time-bin-shift Polarization Encoding Quantum Key Distribution System

Lijun Ma, Tiejun Chang and Xiao Tang
Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899
xiao.tang@nist.gov

Abstract: A detection-time-bin-shift scheme for polarization encoding QKD is proposed. This scheme reduces cost and overcomes the security loss caused by dead-time and unbalanced characteristics of detectors. This scheme is experimentally demonstrated with the B92 protocol.

OCIS codes: (270. 5568) Quantum Cryptography; (270.5565) Quantum Communication

1. Introduction

Polarization encoding quantum key distribution (QKD) is one of the most practical techniques for providing high-speed secure quantum encryption in communications. Several groups have reported over Mbps sifted-key rate system at short distances. However, polarization encoding QKD systems have several limitations for practical applications. The cost of polarization encoding QKD is relatively high due to the use of expensive single photon detectors, four detectors for the BB84 protocol [1] and two for the B92 protocol [2]. Furthermore, security losses caused by the dead time of these detectors also limits high-speed QKD systems, especially when avalanche photo diodes (APDs) are used. When one detector detects a photon and goes into hold-off mode, the other detectors are likely to detect photons before the first detector recovers, and thus the neighboring two sifted keys are likely to be different from each other [3]. Besides, the difference in detector quantum efficiency causes an imbalance in the "1" and "0" keys and therefore reduces security. To overcome these problems, we propose a scheme that uses detection-time-bin-shift (DTBS) for polarization encoding keys and reduces the number of single photon detectors. In this scheme, one detector is required for the B92 polarization encoding QKD system. If applied to BB84 system, just two detectors instead of the typical four are used. For the B92 system, this scheme can avoid the security loss caused by the detector's dead-time and unbalanced detection efficiency. The only trade-off for lower cost and higher security is the reduction of the system clock rate, since each clock period contains two detection time bins in this scheme.

2. Scheme and discussion

The main idea for this DTBS scheme is to project the detection bases into time-bin and then use the same detector to detect the photons from different detection bases in different time bins. In this system, Alice (transmitter) has no change from a typical set-up, and the main modification is in Bob (receiver) as shown in Figure 1. At Bob side, an unbalanced Mach-Zehnder interferometer performs a random choice of polarization measuring bases and projects the results of the different bases into different detection time bins (DTB) that is half of the system clock time bin. In the interferometer, a non-polarizing beam-splitter (NPBS) randomly selects the optical path for each photon. In the short path, the polarization states of the photons are unchanged. In the long path, the time is delayed by a DTB, relative to the short path and the polarization states of photons are rotated by 45°. The photons of these two paths are combined using a polarizing beam-splitter (PBS) and then detected. One (for B92) or two (for BB84) single photon detectors are used to count the photons.

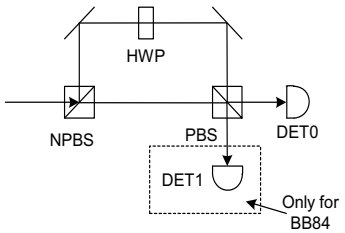


Fig. 1. Schematic diagram of the Bob's side of the DTBS-QKD system; NPBS, Non-polarizing Beam Splitter; HWP, Half-wave Plate; PBS, Polarizing Beam Splitter; DET, Single Photon Detector.

Table 1: Detection events in DTBS QKD with BB84

Pol. angle	Optical path	1st DTB	2nd DTB
0° or 90°	Long	none	?
	Short	"0" or "1"	none
45° or 135°	Long	none	"0" or "1"
	Short	?	none

Table 2: Detection events in DTBS QKD with B92

Pol. angle	Optical path	1st DTB	2nd DTB
0°	Long	none	50% detected
	Short	none	none
45°	Long	none	none
	Short	50% detected	none

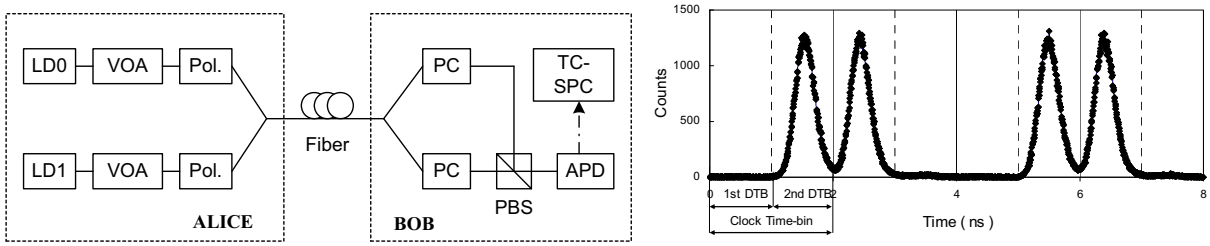
Table 1 and Table 2 show the detection results of protocols BB84 and B92 in DTBS scheme. For the BB84 protocol, photons with polarization 0° or 90° are counted by detector 0 or detector 1 respectively in the first DTB when these

978-1-55752-859-9/08/$25.00 ©2008 IEEE

photons go through the short path, while they are counted by both detectors with 50% possibility in second DTB if going through the long path. Likewise, photons with 45° or 135° are counted with certainty in the second DTB, but with uncertainty in the first DTB. Therefore, the first DTB is the compatible measurement basis for 0° and 90° photons and second is the compatible basis for 45° and 135° photons. In the B92 protocol, the first DTB is a compatible measurement basis for 45° photons and the second one is compatible for 0° photons. When the two detection time-bins are considered as the polarization measurement bases, the DTBS scheme has the same algorithm as the traditional QKD scheme, but it uses only half of the number of detectors. In addition, the scheme improves the security in the B92 protocol. Currently, most single photon counters have a dead time – the hold-off time following each detection event. For example, Si-APD has about tens nanoseconds dead time (50 ns for PerkinElmer SPCM and 70ns for MPD PCDM). In a high repetition rate B92 system, two detectors are used to detect "0" and "1" respectively and thus the neighboring two keys are most likely to be different, i.e., the key is likely to be 1010..., because of the dead time of detectors. The reduction of the randomness of the keys greatly degrades the security of the system. With the proposed DTBS scheme, a B92 system only uses one detector to count all photons. With this scheme, whether "0" or "1" photons will not be detected until the detector recovers, which ensures the neighboring keys being different remains at 0.5 and the security is maintained. Besides, the scheme with one detector also avoids the security loss caused by the unbalanced detection efficiency of different detectors. One trade-off with this scheme is the reduction of system clock rate, since the DTB, instead of clock time bin, should be larger than the timing jitter of pulses to avoid high error rate. The clock rate should be reduced to half of the traditional scheme, and the sifted-key rate is reduced as well.

3. System setup and experiment results

Based on our previous fiber-based QKD system [4], a DTBS QKD system with B92 protocol has been experimentally demonstrated, as shown in figure 2 (a). At Alice's side, two vertical-cavity surface-emitting lasers generate 850-nm optical pulse trains (400 ps FWHM), which are complementarily modulated by random data, and these two pulse trains are attenuated down to single photon level. Their polarization orientations are set at 45° and 90° respectively and they are then combined into a single fiber. At Bob's side, the arriving photons are randomly selected by a 50/50 coupler into long and short paths. Polarization controllers are used to recover polarization state and add another 45° polarization rotation in the long path. All photons are then passed or reflected by a PBS and are detected by a Si-APD (PerkinElmer SPCM-AQR-14). Figure 2 (b) shows the detection results with a repetitive pattern 1010. The photons with "0" are detected in the 1st DTB and those with "1" are detected in 2nd DTB. Therefore, when Bob tells Alice the clock time bin, but not the DTB, of each detected photon though public channel, Alice and Bob can perform the sifting algorithm, error reconciliation and privacy amplification, and then share the secured quantum keys. When the mean photon number per pulse at the output of Alice is set to 0.1 and the transmission fiber length is 1 km, 2.1Mbit/s sifted key rate with about 2.4% quantum bit error rate has been accomplished. Since the system has more than 23-dB polarization extinction ratio, the error rate is dominated by the timing jitter of the APD. The experiment results show that the system has very good balance of two channels and randomness of keys.



(a) (b)

Fig. 2. (a) Schematic diagram of the DTBS-QKD system. (b) Histogram of detected events for a repetitive pattern 1010. In (a): LD, Laser Diode; VOA, Variable Optical Attenuator; Pol., Polarizer; PC, polarization controller; PBS, Polarizing Beam Splitter; APD, Avalanche Photo Diode. TC-SPC: time-correlated single photon counting. In (b), the clock time bin is 2 ns and is indicated by solid lines; the detection time bin is 1 ns and it is indicated by dash lines.

4. References

1. C. H. Bennet and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Institute of Electrical and Electronics Engineers, Bangalore, India,1984), pp. 175-179.
2. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., 68, 3121-3124 (1992)
3. H. Xu, L. Ma, J. Biengang, 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
4. 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 (6): 2062-2070