Polarization Shift Keying for free space QKD

Effect of noise on reliability of the QKD protocols

Ram Soorat and Ashok Vudayagiri
Email: avsp@uohyd.ernet.in
School of Physics, University of Hyderabad
Hyderabad, 500046 India

Abstract: A practical scheme for measurement-device-independent polarization shift keying using two state polarization encoding is presented. Most of the previous work on optical free space laser communications through the atmosphere was concentrated on intensity modulated systems. However, polarization modulated systems may be more appropriate for such communication links, because the polarization seems to be the most stable characteristic of a laser beam while propagating through the atmosphere. Thus, a detailed comparison between intensity and polarization modulated systems is of big interest. The system used the big and powerful LabVIEW handling data and showing function to carry out a real-time processing, analysis and display. When two computers run LabVIEW at the same time, real-time date send and receive between computers by the interface of Virtual instrument, which can realize multi-machine wireless data transmission and reading, in order to complete remote data.

Introduction:

Quantum key distribution (QKD) enables two remote parties to securely exchange cryptographic keys [1, 2]. The security of QKD protocols has been proven in literature [3–5]. Meanwhile, a lot of efforts have been made to achieve the security of QKD with realistic devices [6]. Various device imperfections should be examined before security proofs can be applied to practical scenarios. Our interest is working on bb84 protocol that requires four state polarizations. Here we did two state of polarization based communication.

In principle QKD protocols can be achieved with any pairs of parameters which can be represented by two sets of non-orthogonal basis sets. Although the original BB84 protocol was described in terms of polarization states of photons, in practice a range of properties such as phase, amplitude, frequency etc. are utilized for the protocol [7]. While polarization based schemes would not work in situations such as fiber based communications, where polarizations are not maintained, they are still useful in free space communications. We are building a prototype system which uses an all optical free space communication module which uses polarization based protocol not only for the actual QKD part but also for the parts involving standard communication part such as authentication, handshaking and basis comparison and key reconciliation.

However the success of QKD protocols depend upon the success of the underlying communication method, at least as far as noise is concerned, and this is immaterial whether the protocol uses modulations of polarization, amplitude, phase or photon numbers - or any other quantity. Since noise in the modulation scheme will reduce the fidelity of the key sequence. Therefore we undertook to study the characteristics of a basic polarization shift keying (POLSK) and the effect of its noise on the BB84 protocol. Digital signal transmission using POLSK follows a simple scheme - the 0 and 1 of the signal are mapped to any two orthogonal states of polarization. Atmospheric effects lead to two major noise manifestations (a) bit loss and (b) change in polarization state [8]. Though bit loss is not strictly a `noise', it is treated here as a parameter which affects communication, particularly in QKD protocols where faint lasers pulses

or single photons are used. The change in polarization state can happen either because of scattering by atmospheric particles or due to the inefficiency of polarizers used. VCSEL's which are increasingly being used for their ability of high modulation rate have an inherent competition between two lasing modes, which are orthogonally polarized. This competition gets affected by feedbacks [9]. Our study aims towards a clear understanding of these effects and how each noise source affects the final performance. Many technical issues involves, such as optimum synchronization of the transmitter and detector which improves the bit loss situation as well as polarisation noise.

Virtual instrument development tools LabVIEW is a graphical programming language that easy to read and understand. Lab VIEW has two basic windows: front panel and rear panel. Front panel is a interactive windows that displays input and output of program. Program running results can be seen on the front panel. Rear panel is the graphical source code window, and each input and output controls in front panel has its corresponding icon in rear panel. You can see how the results in front panel to be achieved in the rear panel. Otherwise, the same as manipulate traditional instruments with their hands, we can manipulate the virtual instrument with mouse. Using its signal processing functions and scope chart, we can observe the treatment results of before and after signal processing in the form of time-domain waveform or frequency-domain spectrum chart. Lab VIEW is an ideal tool for CAI(computer assisted instruction)[l0]. There are many simulation software for communication system design. They can be divided into software simulation and hardware simulation. The software simulation is a virtual simulation, like MATLAB/Simulink, System View, etc. [11, 12]. The hardware simulation is the simulation of the actual circuit from the perspective of hardware implementation of the system, like EWBlMultisim, PSpice, Protel, Quartus II , ADS, and so on[13,14,15,]. Network experimental platform of virtual instrumentation can design a variety of virtual instruments according to experiments require of various classes. It not only can replace traditional instruments to achieve the laboratory network, but also reduce the cost of laboratory equipment, improve the experimental teaching conditions and achieve resource sharing. The LabVIEW which represents the graphical development environment is not only powerful, but also can effectively reduce the cost of development applications [16]. With the development of network technology and applications, Achieving network applications, which is based on the virtual instrument technology based on the LabVIEW is a researched focus in the current domestic. International virtual instrument application development[17-19]. Hardware devices use data acquisition card and interface board. The labVIEW platform realized data acquisition and data transmission. The results of these studies will be presented in the conference.

Experimental setup:

Our setup consists of two VCSEL's and their emission is mixed into a single channel using a polarizing beam splitter, so that each VCSEL represents on bit of the signal. The receiver consists of another PBS and two detectors. A third laser helps as an external clock pulse to which both transmitter lasers and detectors can be synchronized. Heterodyne measurement is also investigated using this laser. A random set of zeros and ones are transmitted using this system using a computer and a DAQ card and the signals are received by another computer. A polarization randomizer (rotating disk, liquid crystal, suspension of polystyrene beads) introduces random polarization changes in the system.

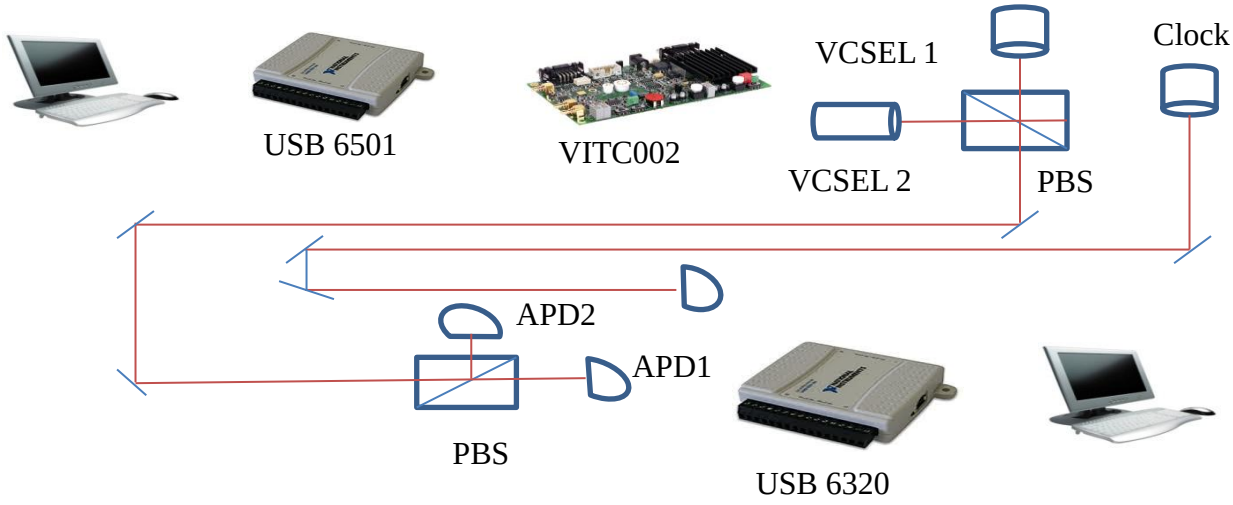


Fig 1: Experimental setup

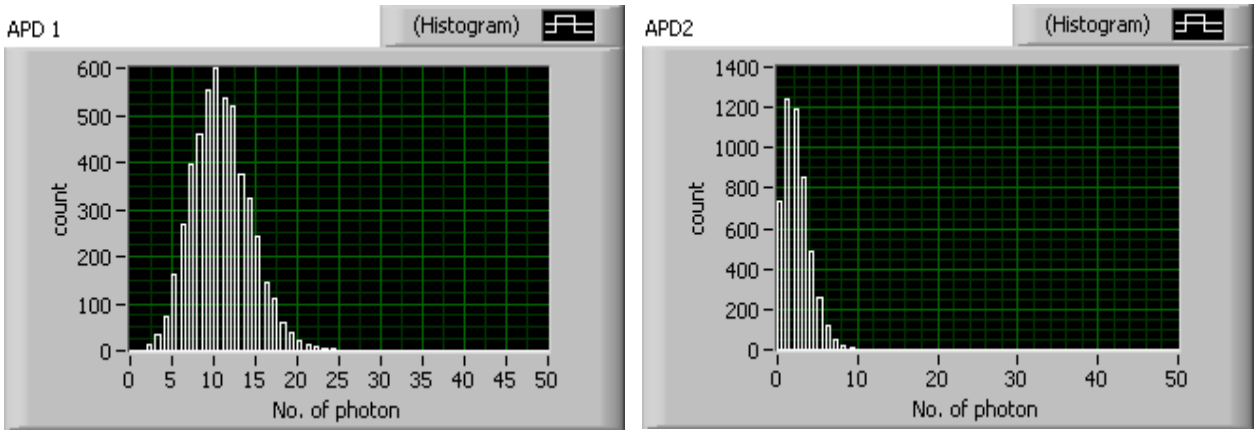
Transmitter:
The Labview part of transmitter consists of code to control lasers L1, L2 and the clock laser L3. Appropriate digital signal, which is an eight bit word as 0000 00xyz, where x, y and z correspond to on/off state of L1, L2 and clock respectively. This eight bit word is sent to the digital port of a DAQ card (USB 6501), which in turn is sent to the laser diode controller VITC002. This ensures that the lasers are switched on and off as required.

Receiver:
The SenSL APD units generate TTL pulses for every photon that is incident upon them. Therefore, we connect the outputs of APD units to the counter pins of the DAQ card (6320 oem). The Labview program counts only those pulses that come within the gated time corresponding to the clock pulse being on. Output of the photodiode which is monitoring the clock pulse is fed to the analogue input of the same DAQ card and is thus monitored. The Labview program also generates histograms of these counts and displays them accordingly.

Result:
First is to characterize the physical system. To achieve this the experiment is done in three stages. At first both L1 and L2 are switched off and the APD counts are measured synchronized to the clock pulse. This gives the background counts. Plotting the distribution of these background counts show the nature of signal to noise ratio our system may have. Then only L1 is pulsed, in synchronization with the clock and corresponding counts on both APD1 and APD 2 are measured. In an ideal system, only APD1 should show any counts for this and APD2 should show only background counts. But due to imperfections, both in PBS as well as the state of polarizations APD 2 will show some counts. Then only L2 is pulsed while keeping L1 off. This will give counts on APD2 and some imperfection counts on APD1. Based on these counts a Degree of Polarization (DOP) is defined as DOP=(APD1-APD2)/(APD1+APD2). This definition, which gives the normalized difference between APD1 and APD2, will also account for any fluctuations. The histograms of the counts indicate the statistical spread of measured quantities. Fig 2 a and b show histograms of background counts for 10 Hz clock frequency and fig 3 a and b show histograms of background counts for 50 Hz clock frequency. Two characteristics can immediately be noticed. Maximum background count of APD1 happens at 10 counts per pulse at 10 Hz clock frequency while it is almost 5 counts per pulse for 50 Hz frequency. This is understandable since the counts are integrated for a shorter time at 50 Hz clock rate as compared to 10 Hz. Similarly the APD2 counts show a maximum at 5 counts and 1

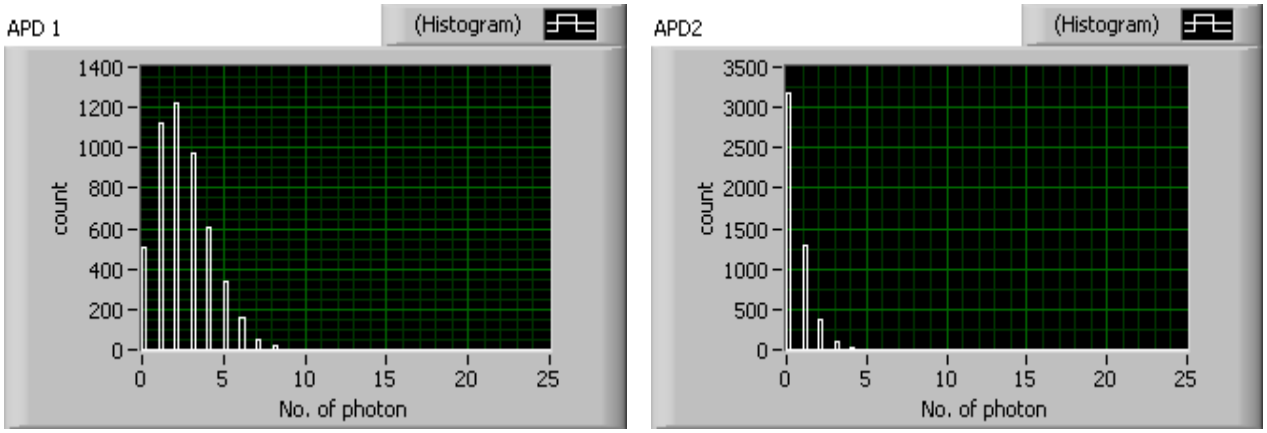
counts respectively per pulse for different clock rates. But the two APD's do show different background counts. APD 1 counts more than APD2. This could be due to positioning of the APD's due to which more stray light falls on APD1 Or due to an inherent difference in the sensitivity of the two detectors. However, we want to show next that this does not affect the performance of the system.

Similarly, the counts on the APD's when the L1 or L2 is pulsed also shows a distribution, which is shown respectively in figures 4 and 5. In case of figure 4, APD1 shows about 100 counts per pulse corresponding to L1. APD2 shows almost close to background counts. On the other hand, when L2 is pulsed, APD2 shows high counts (about 300 counts per pulse), while APD1 also shows about 100 counts per pulse. This is due to the fact that some light reaches APD1 despite the polarizing beamsplitter.



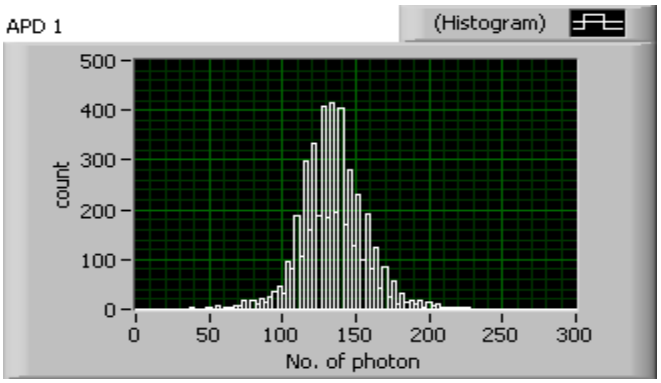
(a)Histogram APD1 back ground noise *(b) Histogram APD2 background noise*

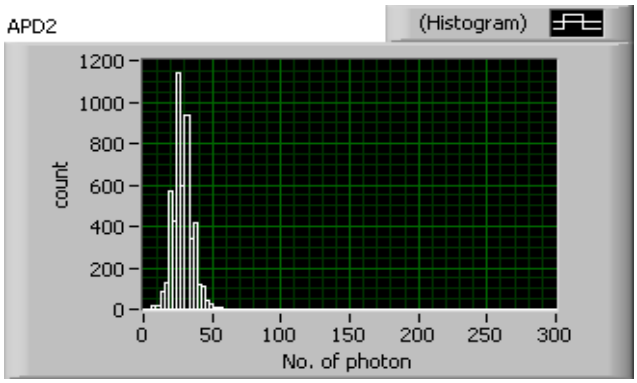
Fig 2: Background noise at frequency 10Hz, number of bit 5000



(a)Histogram APD1 background noise *(b) Histogram APD2 background noise*

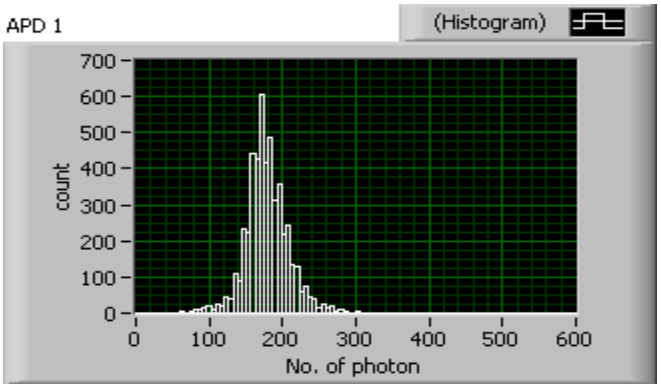
Fig 3: Background noise at frequency 50Hz, number of bit 500

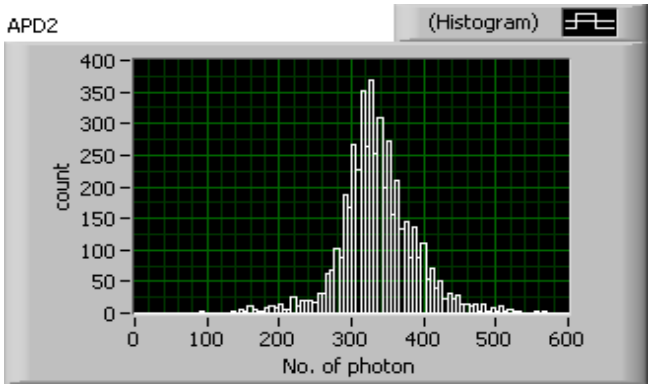




(a) Histogram APD1 actual signal *(b) Histogram APD2 due to leakage*

Fig 4:Laser1on, Laser2off, frequency 50Hz.

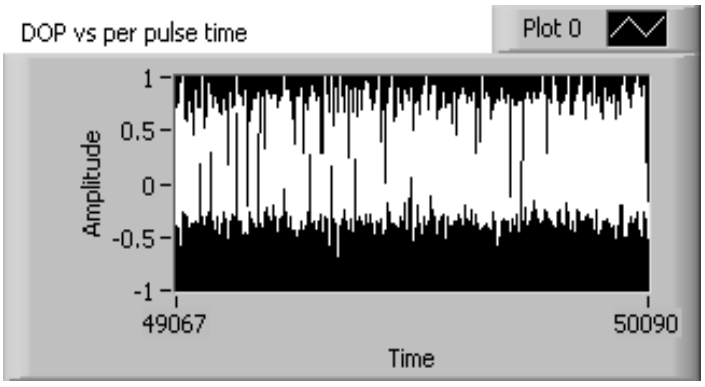


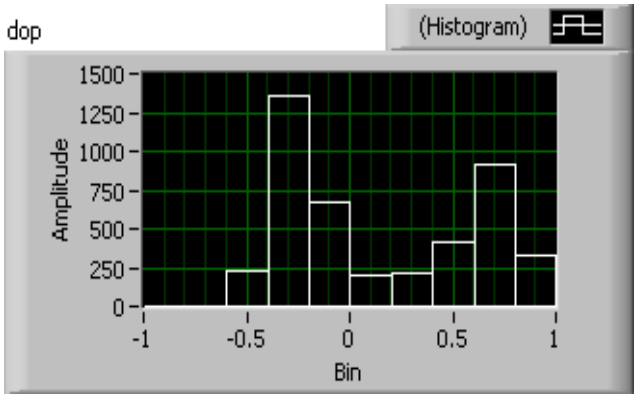


(a) Histogram APD1 leakage signal *(b) Histogram APD2 actual signal*

Fig 5: Laser1off, Laser2on, frequency 50Hz

Degree of polarization(DOP):





(a)wave form DOP vs frequency *(b)Histogram DOP vs bin size*

Fig 6: degree of polarization based on random pulses, frequency 500Hz

Conclusion: This paper has outlined the noise analysis for an FSO (free space optical communication) link employing PSK . For best coding on a quantum state should carry its information in the distribution of single photons. For a single bit, the polarization state is ideal. We have analyzed the possibility of realizing noise in transmission system through the use free space and of the polarization of propagating light. We are quantifying back ground noise and imperfection of PBS noise. We will show this noise will not affect in our optical communication system for QKD.

References

[1] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, Bangalore, India, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).

[3] D. Mayers, Journal of the ACM (JACM) 48, 351 (2001).

[4] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).

[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).

[6] M. Koashi and J. Preskill, Phys. Rev. Lett. 90, 057902 (2003).

[7] Gisin N. Gregoire Ribordy, , Rev. Mod. Phy, 74, 145 (2002)

[8] Grosinger J, "Investigation of polarization modulation in optical free space communication through atmosphere', Masters thesis, Technical University of Vienna, unpublished (2008

[9] S. Bandyopadhyay, Y. Hong, P. S. Spencer, and K. A. Shore, J. Lightwave Tech. 21, 2395 (2003

[10]Yi Wu, Ruixia Yang. Control and Automation Publication Group, 2007,23 (4-1) :259-261

[11].Tiecheng Song, Journal of Electrical & Electronic Education, 2003,25 (5) :95-97.

[12] Wenxin Chen,Weidong Chen, Journal of Ningbo University of Technology,2007,19(4):88-90.

[13] Shibing Zhang,Guoan Zhang. Journal of Electrical & Electronic Education, 2006,28 (4): 10-13.

[14] Jiafu Zhu,Journal of Western Chongqing University(Social Sciences), 2008,27 (3) :88-90.

[15] Chao Chen,Experimental Technology and Management, 2007,24 (5) :92-93.

[16]YANG Le-ping, LI Hai-tao, ZHAO Yong.,Tshing Hua University Publishing House,2003.

[17] F J, Jime nez, J,De Frutos. Computer Standards & Interfaces, 2005(27), pp. 213–216.

[18] Li Ren-fa, Acta Simulata Systematica Sinica, 2002, 14 (3), pp. 359–362.

[19] NIE Chun-yan, Journal Changchun University, 2004(6).