Compensating Birefringence Effects in Optical Fibre for Polarisation Encoded QKD

S Pillay[1], A R Mirza[1, 2], T B Gibbon[3]and F Petruccione[1, 2, 4]

[1] Quantum Research Group, School of Physics, University of KwaZulu-Natal, Private Bag X54001, Durban 4000, South Africa
[2]QZN Technology, Innovation Centre, Howard College Campus, University of KwaZulu-Natal, South Africa
[3]Department of Physics, Nelson Mandela Metropolitan University (NMMU), Port Elizabeth, South Africa
[4]National Institute for Theoretical Physics, South Africa

E-mail: 206507614@ukzn.ac.za

Abstract. Fibre optic cables provide a convenient channel to implement QKD. In order to implement any polarisation encoded protocols, the state of polarisation of photons must be maintained within the fibre channel. Birefringence due to impurities in the fibre or environmental stresses causes the polarisation of light to be altered when passed through a fibre. If the fibre is fixed and the environment is unchanged, the environmental stresses result in a unique and constant change of polarisation. This can be compensated by rotating the polarisation of each photon appropriately before being measured. If the fibre is subjected to variable conditions, the change in the state of polarisation of photons must be monitored and adjustments must be made at suitable time intervals. These changes can be observed using a test signal and the effects may be compensated with the use of a polarisation controller. While orthogonal states are corrected, protocols such as BB84 and B92 use non-orthogonal basis sets, hence two compensators must be used. However, we propose that by using an appropriate search algorithm, the polarisation controller can isolate the plane on the Poincaré sphere that passes through both bases, thus compensating non-orthogonal states with one device.

1. Introduction

With the increase in global data traffic in recent years, secure communications has become essential. Cryptography ensures the security of such data by using cryptographic protocols to generate a unique and secret key to encode the data during transmission. Conventional methods of encryption rely on the complexity of a mathematical algorithm to secure the key [1].While currently effective, advancements in mathematics and computing may compromise some aspects of conventional cryptography. Quantum Key Distribution (QKD) relies on the laws of physics, and not the complexity of a numerical algorithm, to ensure the security of the key, therefore it is not vulnerable to technological advances [2]. In order to gain unauthorized information about the cryptographic key the eavesdropper will have to measure or copy a part of the signal. These processes violate the laws of quantum mechanics, in particular the Heisenberg Uncertainty principle [3] and the ‘No Cloning’ theorem [4]. These two laws ensure that any interception by an eavesdropper will result in a noticeably high error rate in the transmission of the key. The mutual information between the sender and the eavesdropper may increase due to limitations in the implementation of QKD as a result of background noise and imperfections in the apparatus. This sets an upper bound for the quantum bit error rate of the system. If the error rate is found to be above this threshold, an eavesdropper is assumed and the key is discarded [5].

The data transferred between the transmitter and receiver is in the form of a quantum two-level system (qubit). The qubit state is shown as a linear superposition of two basis states, denoted by $|0\rangle$ and$|1\rangle$. This paper will focus on polarization encoded QKD schemes. In this case, the basis states are implemented as states of polarization (SOP), e.g.$|0\rangle$ may represent a vertically polarised state and$|1\rangle$ may represent a horizontally polarised state [6]. QKD protocols such as BB84 [6] and B92 [7] can be implemented through polarization encoding. These protocols utilise two non-orthogonal polarisation bases, e.g. the rectilinear basis and the diagonal basis. For this example, the resulting qubits are the four available States of Polarisation (SOP): vertical, horizontal, right diagonal and left diagonal. In the case of the B92 protocol, only one state from each basis is needed.

2. A fibre quantum channel

QKD protocols can be easily implemented over a fibre optic link. Light propagates through fibre by means of the processes of total internal reflection and waveguide refraction [8], hence it has the advantage of being independent of a line of sight connection between the transmitter and receiver. A fibre link for QKD is however, not suitable for distances longer than 200 km [9, 10]. This would require a quantum amplifier, which is not yet developed. Impurities and manufacturing errors in the fibre absorb photons which causes a minimum loss of 0.2 dBm per km. Therefore, the qubits become too weak to measure after long distances [11]. Coupling a fibre channel to a free space channel would allow for greater transmission distances since free space has a lower attenuation. It would also allow for various mediums of communication to be used in one meshed network. In order to implement such a setup, it is necessary to establish an untrusted interface between the fibre network and the free space network. It is easier to implement polarization encoding over a free space channel since the atmosphere is not birefringent, therefore, polarization encoding must also be implemented through fibre. This poses a problem since a standard single mode fibre optic cable is not able to maintain the SOP of light that is transmitted through it due to birefringence [12]. Birefringence refers to the refractive differences between orthogonal components of the SOP of light. This causes the SOP of light to be rotated as it is transmitted through fibre and this effect must be compensated in order to accurately measure the transmitted qubits. Additionally, any changes in the surrounding environment will alter the birefringence of the fibre, so compensation of the SOPs must be done in real time [13].

3. Compensating for the changes in SOP

In order to compensate for the changes in SOP caused by the fibre channel, the SOP of each photon at the transmission wavelength must be rotated back to its original state. This is done by passing the photons through a polarisation controller. The fibre squeezers of the polarisation controller simultaneously bend the fibre to induce a ‘reverse rotation’ of the SOP of each photon. Since each photon in the quantum signal has a unique SOP, the polarisation controller will have to adjust each one separately. This, however, poses two concerns. Firstly, the polarisation controller must be able to compensate each photon without prior knowledge of what each respective SOP is. This is necessary in order to maintain the security of the QKD protocol being utilised. Secondly, polarisation controllers must not measure the SOP of any photons, since this will destroy the encoded information before Bob can receive it. This means that the polarisation controller cannot measure the current SOP and then make adjustments to it accordingly. Instead, the setting for the polarisation controller must be independently determined prior to the QKD transmission and any adjustments made to the SOPs of photons must be done passively. In order to determine the correct polarisation controller setting, test pulses must be deployed into the system using either time division multiplexing or wavelength division multiplexing. The polarisation controller must be adjusted to compensate the test pulses and thereby passively compensate the quantum signal.

A good example of this implementation is found in [11]. This setup requires four SOPs however, two polarisation controllers are utilised to compensate these four states. This is because the compensation of one state will automatically correct its orthogonal state. This is shown by applying the Jones matrix that represents one of the phase retarders in a polarisation controller to the Jones vector of a chosen SOP [8]. As an example, equation (1) shows the Jones matrix of a quarter wave plate with its fast axis aligned vertically applied to a quarter wave plate.

$$e^{i\frac{\pi}{4}}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = e^{i\frac{\pi}{4}}\begin{bmatrix}0\\ -i\end{bmatrix} \qquad (1)$$

Equation (2) shows the same calculation done with a horizontal SOP.

$$e^{i\frac{\pi}{4}}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = e^{i\frac{\pi}{4}}\begin{bmatrix}1\\ 0\end{bmatrix} \qquad (2)$$

The resulting vectors in equations (1) and (2) are orthogonal and similar results can be obtained using other sets of orthogonal SOPs. This shows that when two orthogonal SOPs undergo the same transformation using a phase retarder, the resulting vectors will also be orthogonal. Therefore, if a polarisation controller is set to correct for the vertical SOP, the horizontal SOP will undergo the same changes and will also be compensated. Therefore, only one polarisation controller is required per basis.

4. Using one polarisation controller to compensate for both bases

In the proposed scheme, shown in Figure 1, only one polarisation controller is required. In this case, the polarisation controller is in the form of a polarisation locker. The polarisation locker includes many internal piezoelectric polarisation controllers which are driven by an in-line polarimeter and digital signal processor which form an internal feedback loop as shown in Figure 2 [14]. The locker can be pre-programmed so that all output SOPs are fixed. The internal polarimeter will measure the output SOPs and communicate the adjustments that need to be made to the polarisation controller via the feedback loop. Using this method, the polarisation locker is able to ‘lock’ onto a specified SOP. Alternatively, the user can manually increment the value of the SOP along a grid superimposed onto the Poincaré sphere to a specific value.

The locker is used to isolate one point on the Poincaré sphere and fix all incoming light to that SOP. In this setup, the locker is used in a time division multiplexed scheme and a test signal is used to achieve the settings for the locker. The quantum signal is periodically stopped to allow the test signal through the quantum channel. The test signal must have only one SOP e.g. vertical. The SOP locker is then used to return the SOP back to vertical after it undergoes changes in the quantum channel. This would compensate the horizontal SOP as well. Since only one SOP locker is used in this setup, the locker must also compensate the diagonal SOPs. This can only be done if the locker is used to isolate the plane on the Poincaré sphere that passes through all four SOPs being used in the QKD transmission [15]. This is shown in Figure 3. A step search must be used on the locker to correctly identify the plane on which all four SOPs exist. Usually, the locker fixes on one point on the Poincaré sphere, but this point can lie on any path. If the path is specified as the equatorial plane of the sphere, all four SOPs will be correctly compensated. Thus, allowing for polarisation compensation with just one polarisation controller. This method has been implemented manually and has shown successful results. The single photon detection rates measured in this setup corresponded well to the initial SOPs set by the transmitter. The detector measuring the initial SOP obtained a maximum detection rate and the detector measuring the orthogonal SOP obtained only dark counts which correspond to a zero reading.

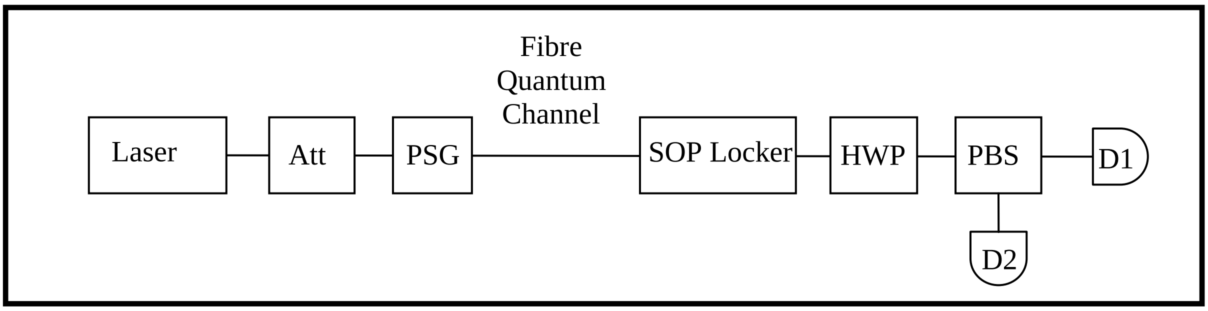

Figure 1: The proposed setup for a polarization encoded QKD scheme. The laser pulses are first passed through an optical attenuator (Att) which creates pseudo-single photons. Each photon is then assigned an SOP with the polarization state generator (PSG) and is transmitted through the quantum channel to the receiver. The receiver then uses the SOP locker to compensate for changes in polarization. A half wave plate (HWP) is used to select the basis in which the receiver will measure each photon and finally, the photons are separated at a polarization beam splitter (PBS) to be measured at one of two detectors.

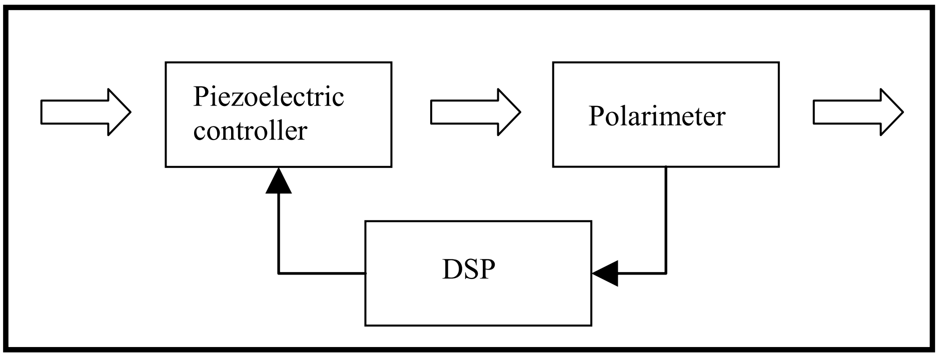

Figure 2: The internal loop of an SOP locker.

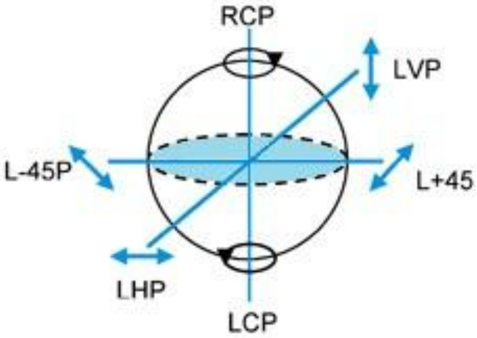

Figure 3 : A diagram of the Poincaré sphere highlighting the equatorial plane which passes through the four linear SOPs. The SOP locker is used to isolate this plane and rotate all SOPs back to their original form.

5. Conclusion

In order to effectively implement polarisation encoded quantum key distribution in fibre optic cables, the birefringence effects of fibre must first be overcome. In order to correct for birefringence, the changes in SOP caused by fibre must first be monitored. A time division multiplexed scheme can be used to test the changes in SOP and polarisation controllers can be used to compensate these changes. In order to use just one polarisation controller, a polarisation locker can be used to isolate the plane on the Poincaré sphere on which both the non-orthogonal bases are located. By using an appropriate search algorithm, the SOP locker can locate this plane and effectively compensate both bases. Future work will focus on automating the search algorithm and integrating it into the QKD system so that polarisation encoded QKD can be implemented in fibre.

Acknowledgements

This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

References

[1] Diffie W and Hellman M E 1976New Directions in Cryptography *IEEE Trans. on Info. Theory* **IT-22** 644-654

[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum Cryptography *Review of Modern Physics* **74**, 145

[3] Krane K 1996 *Modern Physics* (New York: John Wiley& Sons)

[4] Wootters W K and Zurek W H 1982 A Single Quantum Cannot Be Cloned *Nature* **299** 802-803

[5] Capraro I 2008 Advanced Techniques in Free Space Quantum Communication PhD Thesis University of Padua 33-34

[6] Bennet C and Brassard G1984 Quantum cryptography:Public Key Distribution and Coin Tossing*Proc. of IEEE International Conference on Computers Systems and Signal Processing* 175-179

[7] Bennet C 1992 Quantum Cryptography Using Two Nonorthogonal States *Physical Review Letters* **68** 3121-3124

[8] Hecht E 2001 *Optics* (Reading, MA: Addison-Wesley)

[9] Hubel H, Vanner M R, Lederer T, Blauensteiner B, Lorunser T, Poppe A and Zeilinger A 2007 High-fidelity Transmission of Polarization Encoded Qubits from an Entangled Source over 100 km of Fiber *Optics Express* **15** 7853-62

[10] Hughes R J, Morgan G L and Peterson C G, 2000 Quantum Key Distribution Over a 48 km Optical Fibre Network *Journal of Modern Optics* **47** 533-547

[11] Xavier G B, Walenta N, Vilela de Faria G, Temporo G P, Gisin N, Zbinden H and von der Weid J P 2009 Experimental Polarization Encoded Quantum Key Distribution over Optical Fibres with Real-time Continuous Birefringence Compensation *New Journal of Physics* **11** 045015

[12] [Online]www.lunatechnologies.com/files/22pmdweb.pdf

[13] Xavier GB, Vilela de Faria G, Temporo G P and von der Weid J P 2008 Full polarization control for fiber optical quantum communication systems using polarization encoding *Optics Exress* **16** 1867-1873

[14] [Online] http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=1769

[15] [Online] spie.org/x32375.xml