Advancement of quantum communication through entanglement

Y. Ismail[1], A. Mirza[1], A. Forbes[1,2] and F. Petruccione[1,3]

[1]Quantum Research Group, University of KwaZulu-Natal, Private Bag X54001, Durban 4000
[2]CSIR-National Laser Centre, PO Box 365, Pretoria, 0001
[3]National Institute of Theoretical Physics, South Africa

205513117@stu.ukzn.ac.za

Abstract. Quantum communication exploits some of the fundamental features of the quantum world. One of the most advanced quantum information related application aspects at present is Quantum Key Distribution (QKD) which is a process that involves transmitting a secure key between two individuals. The most vital characteristic of such a method is that the secrecy of the generated key is guaranteed by the laws of nature. QKD systems, although capable of producing provably secure keys, must in themselves be trusted. Entanglement provides a basis for an additional layer of security. In this paper, we will outline an optical system used to generate entanglement. The aim of this paper is to characterise the entanglement system. The correlation of entangled pairs was quantified by measuring by the visibility of the rectilinear and diagonal bases. Within the system studied entanglement was verified by violation of the CHSH inequality which was determined to be 2.71 ± 0.03. Furthermore, we touch-on exploiting QKD together with entanglement to shape a quantum network.

1. Introduction

Quantum information science is based on the notion that the manipulation of information is governed only by the laws of physics. Hence, information can be characterized, quantified and processed as a physical entity using the basic properties of quantum mechanics by exploiting some of the fundamental features of the quantum world, i.e. the superposition principle and the Heisenberg uncertainty relation.

Quantum information encapsulates two major disciplines, quantum computing and quantum communication. Ultimately, the security of information lies in the development of quantum communication [1]. At present in classical computers, although capable of utilising mathematical algorithms to uphold the security of information, communication may be threatened by the rapid development of more powerful systems. It is feared that even the key distribution process of the one time pad, which is the most secure method of encryption to date, could reach a point where it could be rendered breakable.

The classical computer may store information as binary logic however with quantum computing it is possible to compute information as a superposition of bits of 0's and 1's known as qubits. While some classical algorithms require exponential processing time, the time frame for the corresponding quantum algorithms is reduced to polynomial time. [2].

Currently one of the inefficiencies experienced by quantum computers is invoking entanglement on demand however immense research is being carried out in this field to further develop this branch of technology. When this becomes a reality, it would be mandatory to consider quantum communication, in particular QKD, to maintain the security of information. Entanglement occurs when two particles interact physically and thereafter separate while maintaining some mutual correlations, the knowledge about one particle can be obtained by observing its entangled partner. The fact that this knowledge of the remote particle is obtained in the absence of any physical interaction with the particle, is significant. This is applicable to all sub-atomic particles such as photons, electrons and molecules.

In this paper we will give an overview of entanglement which will be discussed in Section 2. Section 3 deals with the key distribution process based on the successful implementation of an appropriate protocol. The realisation, generation and verification of entangled states will be dealt with in Section 4. The concluding remarks will be discussed in Section 5 and furthermore we will touch on the advancement of quantum communication through entanglement.

2. Entanglement

Entanglement is the core of quantum information science since it is applicable to the development of both quantum communication and quantum computing. Photons which are entangled are considered indistinguishable and are therefore represented as a single state. This means that there exists a strong mutual correlation between maximally entangled photon pairs independent of the distance between them. This condition implies that quantum entanglement contradicts the concept of locality [3]. A concrete test of the conflict between local realism and quantum mechanics was later verified [4] and consists of a set of inequalities which must be satisfied by any local and realistic theory. Furthermore, quantum mechanics predicts the violation of these so-called Bell's inequalities for measurements on specific quantum-entangled systems. An experimental realisation of the so called Bell's inequalities was later presented by Clauser, Horne, Shimony and Holt (CHSH), which demonstrated a classical argument that bounds the correlation of two particles [5].

Photons can be entangled via phase or polarisation. For the purpose of this study we will concentrate on a polarisation based entanglement source. A photon pair which is entangled via polarisation can be represented either by the rectilinear (horizontal and vertical) or the diagonal (± 45 degrees) basis denoted as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|V\rangle_s|V\rangle_i + e^{i\phi}|H\rangle_s|H\rangle_i\right], \quad (1)$$

where $|V\rangle$ and $|H\rangle$ are the vertical and horizontal states respectively and s and i denote the signal and idler.

Prior to testing for entanglement by the violation of the CHSH inequality, a test of visibility is used to determine the correlation of the entangled photon pairs. The visibility is measured in both bases by considering the maximum and minimum coincidence according to the following condition:

$$V = \frac{C_{max} - C_{min}}{C_{max} + C_{min}}, \quad (2)$$

where V corresponds to the visibility for a given bases and C_{max} and C_{min} are the maximum and minimum coincidence rates respectively.

The verification of entanglement however, lies in the violation of the CHSH inequality which states that in local realistic theories the absolute value of a particular combination of correlations between two particles is bounded by 2, such that the violation is represented as follows:

$$S(\alpha, \alpha', \beta, \beta') = E[\alpha, \beta] - E[\alpha, \beta'] + E[\alpha', \beta] + E[\alpha', \beta'] \leq 2, \quad (3)$$

where α and α' and β and β' denotes the local measurement settings of the two observers, each receiving one of the particles. The normalised expectation value $E[\alpha, \beta]$ is given by:

$$E[\alpha, \beta] = \frac{C(\alpha,\beta) - C(\alpha_\perp,\beta) - C(\alpha,\beta_\perp) + C(\alpha_\perp,\beta_\perp)}{C(\alpha,\beta) + C(\alpha,\beta_\perp) + C(\alpha_\perp,\beta) + C(\alpha_\perp,\beta_\perp)}, \quad (4)$$

where $C(\alpha, \beta)$ denotes the coincidence count rate obtained for the combination of polariser settings and $\alpha_\perp$ and $\beta_\perp$ are the perpendicular polarisation orientations.

Quantum Key Distribution

QKD is a process of sharing a secure key between two authorised parties, the transmitter and the receiver. Communication between QKD systems, to date, has focused on phase-encoded fibre-based solutions. This is due to the ease of implementation. However of recent much investigation has focussed on free-space QKD solutions. This provides further versatility for quantum communication solutions. The key distribution process is achievable by manipulating the quantum state of polarisation of single photons to obtain a secure key. This process makes uses of two channels, a quantum channel in which the encoded single photons are transmitted to initiate a raw key and the classical channel which is used for the post-processing to determine a secure key. QKD is realised by the implementation of the appropriate protocol. There are mainly three types of QKD schemes. One is the prepare-and-measure scheme, such as BB84 [6] and B92 [7], the other are the entanglement based QKD, such as E91 [8] and BBM92 [9] and the continuous variable scheme [10]. For the purpose of this study the BB84, B92 and E91 will be discussed.

BB84

The BB84 protocol was the first QKD protocol. It was proposed by Bennet and Brassard [6]. This is a four state protocol which makes use of two non-orthogonal polarisation bases namely the rectilinear and the diagonal basis. Implementation of the BB84 protocol lies in the encoding of single photons with either the vertical, horizontal or the $\pm 45^o$ state of polarisation. The process entails transmitting a train of encoded single photons to the receiver. The receiver randomly chooses to measure each of the photons in the rectilinear or diagonal bases. This procedure is carried out on the quantum channel. The classical channel is used by the receiver to announce the basis used for each measurement. A sifted key is then produced from the combination of the quantum and classical communication. Single photons with a mismatch in the prepare and measure bases will be discarded. The remainder of the single photons are kept for the continuation of the post-processing procedure.

B92

This is a two-state protocol, similar to the BB84 protocol, except in this case instead of the measurement bases being announced on the classical channel during the post-processing, the detector that clicked is publicized. This protocol entails pre-assigning a bit value to each detector. The single

photons are transmitted as per the BB84 protocol. A classical channel is used to determine the sifted key from the raw key. The authorised parties would be able to distinguish the sifted key by the click of the detector. This process is less efficient than the BB84 protocol however there is greater secrecy during the post-processing of the single photons [7].

E91

The E91 protocol is also similar to the BB84 protocol except it makes use of entanglement. A pair of entangled photons is emitted from a single source such that one photon is directed towards the receiver while the other is sent to the transmitter. Both authorised parties will carry out a measurement independent of each other by randomly choosing between the rectilinear or the diagonal bases. Since these photons are entangled, if the receiver is the first carry out a measurement, the transmitter will automatically measure the anti-correlated state. By one of the authorised parties inverting their string of bits received, a raw key can be produced [8]. The post-processing is carried out as per the BB84 protocol from which a sifted key is obtained.

2. Generation of entangled photon pairs

Experimentally, one implementation of entangled photon pair is generated by a process known as spontaneous parametric down conversion (SPDC),whereby photons of an intense laser pump beam spontaneously are converted by a non-linear crystal into photons of lower frequency. The entangled photon pair that is generated is separated into a signal photon and an idler photon. During this process, the conservation of momentum and energy are obeyed such that the additive energy of the signal and idler is equal to the energy of the pump photon and similarly for the momentum.

A simple optical system scheme was engineered to generate single photon pairs within a polarisation based entanglement system. Within this scheme a UV laser (λ= 404 nm) with an output power of 20 mW was used to pump the nonlinear crystal. The most important component was the type-I Beta Barium Borate (BBO) crystal which is the optical element utilised to initiate the SPDC process. A half wave plate, cylindrical lens and birefringent crystal were used to compensate for additional alignment concerns within the system. Polarisers were placed in both arms to vary the bases (rectilinear or diagonal) and carry out measurements on the entangled photon pairs. Single photon detectors were used to measure the single photon counts, which are the measure of entanglement, used to determine the coincidence count rates. The optical system described is represented schematically and as constructed in the lab in Figure 1(a) and Figure 1(b) respectively. To determine if the system was entangled, a visibility test and the violation of the CHSH inequality were determined and will be discussed in the section that follows.

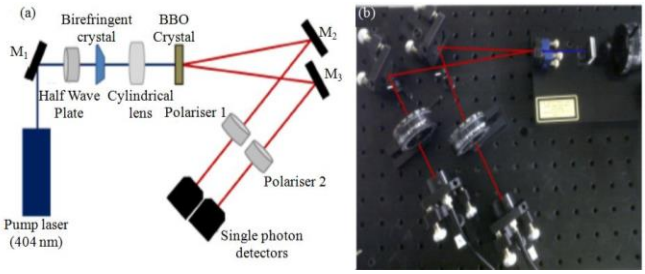

Figure 1: Optical system engineered to generate and verify entanglement: A schematic of an entanglement source (a) and as seen in the laboratory (b).

2.1. Verification of entanglement

The simplest test to verify entanglement of photon pairs would be to carry out a measurement of the correlation curves in two non-orthogonal complementary bases. This is accomplished by fixing the orientation α of one of the polarisers represented in Figure 1(a) and continuously varying the orientation of β of the other. The results obtained are illustrated in Figure 2 where α was set at 0^{o} and 45^{o} for the rectilinear and diagonal basis respectively.

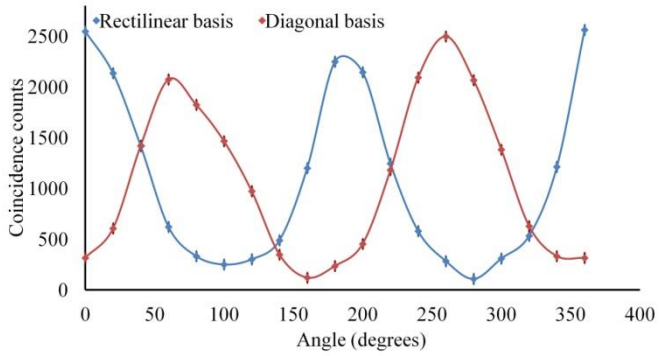

Figure 2: Plot representing the correlation of the rectilinear and diagonal bases.

The recorded coincidence count rates for the above chosen setting showed a $\cos^2(\alpha-\beta)$ dependence. To quantify the quality of the polarization correlations, the visibility, V, of the measured curve was directly estimated by Equation 2. From the above mentioned analysis the visibility in the horizontal/vertical and diagonal basis were determined to be 91.00 ± 0.76 % and 91.00 ± 0.82 % respectively.

To measure the violation of the CHSH inequality the coincidence counts were determined by varying the angles of the polarizer in both arms of the source. To test for the violation the following set of orientation are chosen, $\alpha = 0^{o}$, $\alpha' = 45^{o}$, $\beta = 22.5^{o}$ and $\beta' = 67.5^{o}$. Four separate experimental runs were conducted corresponding to the four terms $E[\alpha, \beta]$ in the definition of S expressed in Equation 3. Each of the terms, $E[\alpha, \beta]$, were calculated from four coincidence counts making it 16 count rates in total as represented in Table 1. The coincidence counts measured resulted in an S-value of 2.71 ±0.03, evaluated using Equation 3 and Equation 4, which indicated a violation of the CHSH inequality and hence verified entanglement.

Table 1: Data collected for the experimental runs to verify entanglement

Expectation value when α is 0 and β is 22.5 deg								
α	β	$\alpha_\perp$	$\beta_\perp$	C(α, β)	C($\alpha_\perp$, β)	C(α , $\beta_\perp$)	C($\alpha_\perp$, $\beta_\perp$)	E(α , β)
0	22.5	90	112.5	8557	1838	1886	8939	0.649
Expectation value when α' is 45 and β is 22.5 deg								
α'	β	$\alpha'_\perp$	$\beta_\perp$	C(α', β)	C($\alpha'_\perp$, β)	C(α', $\beta_\perp$)	C($\alpha'_\perp$, $\beta_\perp$)	E(α', β)
45	22.5	135	112.5	11296	2253	1041	10442	0.737
Expectation value when α is 0 and β' is 67.5 deg								
α	β'	$\alpha_\perp$	$\beta'_\perp$	C(α , β')	C($\alpha_\perp$, β')	C(α , $\beta'_\perp$)	C($\alpha_\perp$ $\beta'_\perp$)	E(α , β')
0	67.5	90	15.5	2950	10707	7238	1642	-0.592
Expectation value when α' is 45 and β' is 67.5 deg								
α'	β'	$\alpha'_\perp$	$\beta'_\perp$	C(α', β')	C($\alpha'_\perp$, β')	C(α', $\beta'_\perp$)	C($\alpha'_\perp$, $\beta'_\perp$)	E(α', β')
45	67.5	135	157.5	13180	1697	2070	11211	0.732

3. Concluding remarks

We have thus shown that it is possible to generate polarisation based entangled photon pairs and characterise them by measuring the visibility of the correlation curves of the rectilinear and diagonal bases. We also proved that our system is entangled since we were able to violate the CHSH inequality. Upon characterising the system, entanglement can be utilised for the advancement of QKD. This is due to the bond that entangled photons share. This instantaneous relationship is a platform for quantum teleportation experiments making QKD the optimal technology for the further development of quantum communication. It has already been shown that ground to ground communication is possible using entanglement [11], being able expand this technology to ground to satellite communication would hopefully result in creating a global quantum network.

References

[1] Buchmann B and Dahmen, eds. 2009 Post-Quantum Cryptography Springer,

[2] Rieffel E 2000 An Introduction to Quantum Computing for Non-Physicists arxiv:quant-ph/9809016v2

[3] Einstein A, Podolsky B and Rosen N 1935 Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. vol.47 (10) 777–780

[4] Bell J S 1964 On the Einstein-Podolski-Rosen Paradox Physics (Long Island City, New York) 403-408

[5] Clauser J, Holt R, Horne M and Shimony A 1969 Proposed Experiment to Test Local Hidden-Variable Theories Phys. Rev. Lett. vol.23 (15) 880-884

[6] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. of IEEE International Conference on Computers, Systems and Signal Processing 175-179.

[7] Bennett C H 1992 Quantum cryptography using any two non-orthogonal states. Phys. Rev. Lett. 68 3121-3124

[8] Ekert A 1991 Quantum Cryptography Based on Bell's Theorem Phys. Rev. Lett. vol. 67 (6) 661-663

[9] Bennett C H, Brassard G and Mermaid N D 1992 Quantum Cryptography without Bell's Theorem Phys Rev. Lett. vol.68 (5) 557-559

[10] Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88(5) 057902-1-4

[11] Ursin *et al* 2007 Entanglement-based quantum communication over 144km Nature vol. 3 481-486