Preparation of quantum state *(review)*

N Ali[1,2,4*], *N. R.* Yusof[1,2], *S* Soekardjo[5], *S.* Saharudin[3] and *R.* Endut[4]

[1]School of Microelectronics Engineering, Universiti Malaysia Perlis (UniMAP), 02600 Arau, Perlis, Malaysia
[2]Semiconductor Photonics & Integrated Lightwave Systems (SPILS), School of Microelectronic Engineering, Universiti Malaysia Perlis, Pauh Putra Main Campus, 02600 Arau, Perlis, Malaysia
[3]Nano Photonics and Nano Electronics, Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur
[4]Advanced Communication Engineering, Centre of Excellence-School of Computer and Communication Engineering, Universiti Malaysia Perlis
[5]Department of Physics, Kulliyyah of Science, International Islamic University Malaysia, Jalan Sultan Ahmad Shah, Bandar Indera Mahkota 25200 Kuantan, Pahang.

Abstract. We reviewed experimental results and publications prepared by the Quantum Laboratory, Mimos Berhad. The complexity of the setups lies mainly in preparing the quantum states. Optics is chosen as the medium of this quantum system. The two methods - fiber based and free space systems are different from each other in terms of experimental setups, components configuration, and selections.

1 Introduction

The communications today are secured by the public key cryptography which is based on the mathematical complexity. As the computer performance improves through technology development, the length of the encryption key has to be increased in order to maintain confidentiality and security of the encrypted massages as it transfers to the other party. On the other hand, the speed of the computer can overcome the mathematical complexity of the encryption system [7], [8]. The main threat of this encryption system is the invention of the quantum computer, which potentially has the computing power billions of times faster than the current technology to process and calculate any digital information [1].

Quantum Computer works in quantum bits (qubits) [9] value as opposed to the current computer that uses binary bits. Quantum mechanic's law is different with the classical computer. A qubit can exist in a normal classical bit and it also can exist in the superposition state which can be both values at the same time. Thus, a computer working in qubit rather than standard bits can make a calculation using both values simultaneously. There is also the term qubyte which is a group of eight qubits. A quantum computer can have power beyond today's classical supercomputer and can just resolve calculation as fast as 1 billion times faster than Pentium III PC [2].

As a preventive measure, people try to maintain the security of messages by securing the encryption key which is breakable very fast by a quantum computer for current public key cryptography. Symmetric key cryptography will assure the messages sent are secured since the keys are only shared by the sender and receiver. On the other hand, the system is difficult to be implemented since it is difficult to send the key securely into the other place via a public communication channel. A trusted party is needed to transfer the key to the other end securely. By introducing Quantum Key Distribution (QKD) the key can be shared between two parties securely via a normal communication link. The security of this system lies in the quantum mechanical principles and will result in securely encrypted messages.

In the experimental implementation of a QKD system, there are two mainly used techniques for the optical quantum system which are the free space system and the fiber based system. In the free space system, the quantum information is sent via polarization of photon since the polarization states are stable in the free space region, even at the quantum level. This is one of the advantages of transmission in the free space region, but the limited line-of-sight limits the expected range of transmission. The second technique is the fiber based system whereby the photon is transmitted through the optical fiber. In the fiber based system, the photon cannot be coded using the state of polarization because it is susceptible in the fiber. Due to this limitation, the system use phase coding method in the fiber which can be retained throughout the transmission.

In this paper, we will go through a theoretical review of the protocol that was used for both setups (fiber based and free space). Then we will explain the experimental setup on the fiber based followed by the free space. After that, this paper will discuss the experimental setup which will explain how the preparation of quantum state affect the experimental setup, and lastly conclusion.

* Corresponding author: norshamsuri@unimap.edu.my

2 Theoretical review

The system is working based on BB84 protocol. In this protocol, the key is transmitted in one of four states and decoded by two bases. The important part is that the protocol uses two conjugate bases. The sender (Alice) encodes the key by two orthogonal states of the quantum system. She will randomly change the two orthogonal states that refer to each basis. This means that, for each encoded key, she will choose the state from the two conjugate bases. The state of this protocol can be any quantum state, but for this explanation, we will use polarization state as an example. One basis consists of two polarization states i.e |H⟩ and |V⟩, or |45⟩ and |135⟩. Where |H⟩ is a horizontal state, |V⟩ is a vertical state. Both states are in rectilinear basis. |45⟩ is diagonal state and can be represented as |D⟩ and |135⟩ represents anti diagonal state and also can be represented as |A⟩. Both states are in diagonal basis. The protocol encoded as below:

Horizontal basis

$|H\rangle \Rightarrow$"0" (1)

$|V\rangle \Rightarrow$"1" (2)

Diagonal basis

$|D\rangle \Rightarrow$"0" (3)

$|A\rangle \Rightarrow$"1" (4)

$$|D\rangle = \frac{1}{\sqrt{2}}(|V\rangle + |H\rangle) \quad (5)$$

$$|A\rangle = \frac{1}{\sqrt{2}}(|V\rangle - |H\rangle) \quad (6)$$

These four states satisfy the following relationship;

$$\langle H|V\rangle = \langle A|D\rangle = 0 \quad (7)$$

$$\langle H|H\rangle = \langle A|A\rangle = \langle D|D\rangle = \langle V|V\rangle = 1 \quad (8)$$

$$[\langle H|A\rangle]^2 = [\langle H|D\rangle]^2 = [\langle A|V\rangle]^2 = [\langle D|V\rangle]^2 = \frac{1}{2} \quad (9)$$

A deterministic result will be produced only when the measurement performed in the basis is identical to the preparation basis. Any measurement in the rectilinear basis on a photon prepared in the diagonal basis will yield an outcome with equal probabilities and vice versa for diagonal basis. This measurement should be initiated by pre agreeing on the key (0 or 1) carried by respective photon states as shown in equation (1) - (4) above. Since Alice is the sender, she will send random polarization |H⟩, |V⟩, |D⟩, or |A⟩ to Bob and Bob will decode the key by randomly and independently chooses either diagonal basis or rectangular basis. Statistically, Bob will only have 50% probability of measuring the photon with the same bases as Alice prepared i.e. 50% chance of deterministic measurements by Bob. He will only know if his outcomes are deterministic when he compares his measurement basis with Alice's through a normal (classical) communication channel. Whenever the basis is identical, Bob will keep the bit and whenever it is not identical he will discard the measured bit. This classical channel can be intercepted by an eavesdropper but she can only know the basis sent, not the information on the code.

In this experiment, the quality of the interference pattern is measured by measuring the visibility. The ratio of the size or amplitude of oscillations to the sum of the powers of the individual waves is defined as the visibility. The sum of the intensities (or powers) of the two interfering waves equals the average of the fringes and can be written as,

$$Visibility_{Real} = \frac{amplitude}{average} \quad (10)$$

Alternatively, the above equation can be written as follows;

$$Visibility_{Real} = \frac{max - min}{max + min}$$

where max- the maximum of the oscillations
min- the minimum of the oscillations

When the two waves/particles have the same polarization, then the predicted visibility will be;

$$Visibility_{ideal} = \frac{2\sqrt{I_1 I_2}}{I_1 + I_2}$$

where I_1, I_2 - Intensities of the optical waves

3 Experimental setup

3.1. Fibre Based QKD

The set-up for the experiment is shown in Figure 1. It represents one interferometer in a complete plug and plays QKD scheme (Alice and Bob's setups will produce only one interferometer). In this setup, the idea is to modulate in the phase of the photon since the state of polarization is scrambled throughout the fiber distance. The light pulse from the LD is guided out at the common port to the bi-directional optical ratio coupler (ORC). The optical pulse will then take the path of either one of the ORC arm. One part of the ORC arm is connected to a phase modulator (PM) while the other (shorter in length) is connected to a polarization maintaining optical fiber with a length of approximately 2 meters. The longer arm has 8 meters extra length from the shorter arm. In this setup, all fiber is polarization maintaining fiber (PM fiber) which all the polarization state is maintained. Because the
PM is a polarization dependent device; the connection of our rotation polarization is after a pass through the phase modulator in order to ensure only the pulse with correct polarization state enters the PM. The light pulses from both arms are then recombined using a polarization beam coupler/splitter (PBCS) where the output is connected to a 10 km optical fiber link. Due to the unbalanced nature

of the interferometer used, the two superposition optical pulses that recombined and left the PBS will be delayed about 40 ns apart. The optical power (intensity) of the two pulses is attenuated (to an average power of -108.93 dBm) by the VOA to achieve a low number of photons per pulse. In optical fiber QKD scheme, 'single photon' is approximated by light pulses with Poisson photon-number distributions characterized by small values of μ, the mean number of photons/pulse. This action is achieved by attenuating the optical pulses such that the μ value is in the range of 0.1 to 1.

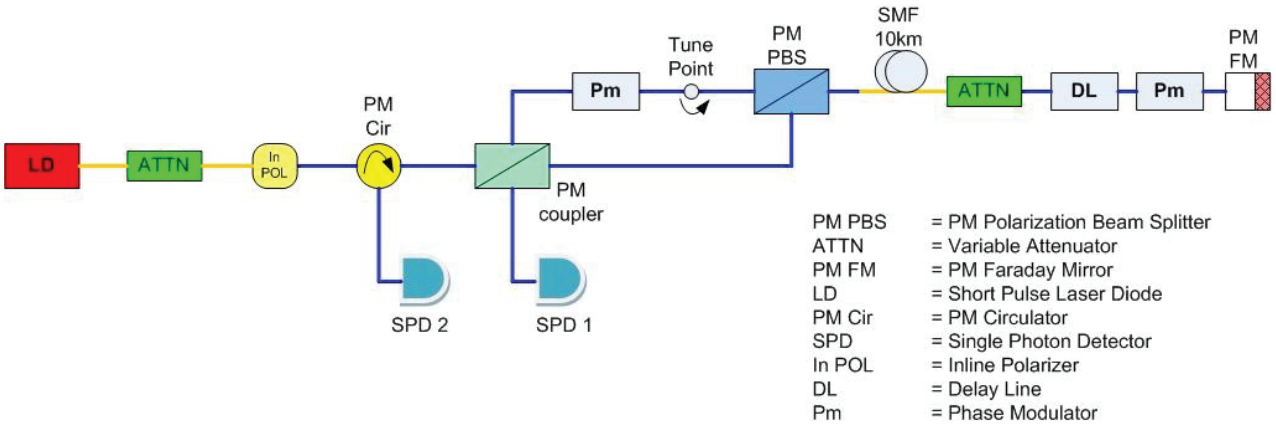

Fig. 1. Schematic of the experimental setup used for Plug and Play configuration QKD interferometer.

The attenuated optical pulse then travels through a standard 10 km telecommunication grade optical fiber (SMF) before it reaches Alice. At Alice, the pulses have to go through the variable attenuator (ATTN) again in order to make sure that the light that reflects back to Bob has a μ value between 0.1 to 1.0. Then the pulses are delayed by a few meter of single mode fiber before being modulated at Alice's modulator. Then the modulated pulses are reflected back by a Faraday mirror (FM) and sent back to Bob. The two pulses will go to the PBS and they will take opposing routes as they come since the polarization of both pulses is already flipped by the FM. Bob will modulate the basis at Bob's modulator, which is placed in the long arm. The interference of the two pulses will determine the readings on the detectors.

3.2 Free sSpace QKD

The cascaded type-I BBO crystal (B2) was placed at the waist position of the sequence femto second pulse collimated by lenses L2 and L3. Each crystal was designed in certain cut-angle to achieve phase matching condition for non-collinear frequency degenerate down conversion. The crystal is rotated with respect to other in such a way that horizontally polarized pump light generates a pair of vertically polarized photon in the first crystal, and vertically polarized pump light generate pairs of a horizontally polarized photon in the second crystal [3]. In order to generate a pair of polarized entangled photon $|\psi\rangle \propto |VV\rangle + |HH\rangle$ we used pump beam polarized at 45o with respect to the crystal axis. By neglecting losses from passing through the first crystal, this polarized pump photon will be equally likely to down-convert in either crystal. Nevertheless, because of the combined effects of group velocity dispersion and birefringence in the two crystals, the space-time components of the two-photon state $|VV\rangle$ associated with the polarized states and $|HH\rangle$ is expected to be temporally displaced after the crystals. As a result, information about "which-polarization" the emitted photon pair has, as well as "which crystal" each pair originated from, may be available from the arrival time of the photon at the detector. On the other hand, the effective polarization entanglement requires the suppression of any distinguishing information in the other degrees of freedom that can provide potential information about the emitted pair.

To eliminate this distinguishing space-time information, a polarization dependent optical delay line for the pump was inserted before the crystal, which is denoted as the delay compensator (DC) in Figure 2. The delay compensator was used as the pre-compensator for group velocity mismatch between ordinary and extraordinary rays in the BBO crystal so that the state associated with $|HH\rangle$ created in the first crystal relative to the state associated with $|VV\rangle$ created in second crystal overlapped with them temporally. As the result, a two-photon Bell state $|VV\rangle + |HH\rangle$ can be directly created.

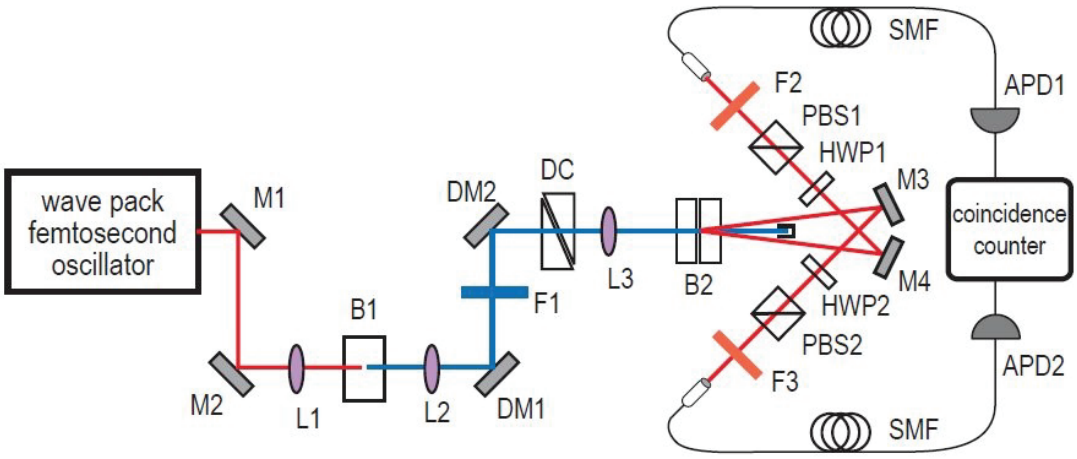

Fig. 2. Plot of coincidence rate as a function of idler polarization analyzer angle θ_1. (a) Signal polarisation analyzer was set at $\theta_1 = 0^o$ and the visibility achieved is V = 98:7%. (b) Coincidence rate for the signal at polarisation analyzer at $\theta_2 = 22.5^o$, with the visibility of 90%

To experimentally demonstrate the polarization entanglement of the collected photon pairs, their polarization correlations in two conjugate bases were measured. This was done by directing the down-converted light into adjustable polarization analyzers, each consisting of a polarizing beam-splitter cube (PBS) preceded by a rotatable half-wave plate (HWP). The residual violet light coming from the first BBO crystal was blocked using long-pass filters. After passing through the analyzers, the photons were coupled into single-mode fibers by using the aspheric coupling lenses with focal length of f= 7.5 mm, the desired spectral bandwidth and the numerical aperture of the optical fiber, and then detected with passively quenched silicon avalanche photon diodes (Si-APDs). The detectors were linked to a time-to-amplitude converter for a record of coincidence counts. To keep the experimental setup compact, two mirrors (M3 and M4) were used to fold the paths of the fluorescence beams.

4 Discussion

4.1. Fibre based QKD

Since the light pulse is phase modulated, the setup should be able to translate between phase and codes according to BB84 protocol. The setup should correctly translate the protocol when Alice codes into the system while the coded message should be correctly translated when Bob is doing the measurement. In order to translate the data in phase, there should be a reference pulse that can interfere with the other pulse that has been phase code. The interference results will depend on the phase difference between the two pulses. The interferometer is used in order to locate the interference and the interference should occur at the Bob setup since Bob will collect the decoded data. In order to have the reference pulses for interference, the unbalanced interferometer is built, and then the pulses will travel by superposition of the two pulses.

The problem is, when the pulses arrived at the Bob setup there will be two pulses that will not interfere with any pulses. They are the pulses that travel through both setups through the short path (SS) and pulses that travel in both setups through the long path (LL). Due to this problem, the interference becomes worsen since there are lost due to the unbalanced interferometer. In addition, the best interference result occurs when the pulses are in the similar polarization state. Due to this limitation, the polarization of the light is used as the compensation method to make sure that the traveling pulses between the setup only pass through the interferometer by these two paths either long-short(LS) arms or short-long(SL) arms. The pulses have to travel from Bob barely without any modulation and then reflected by Faraday mirror purposely to swap the two pulses' polarization states so that these two pulses will follow one of the two paths, LS or SL. The signal is modulated and attenuated into single photon level only after the reflection at Alice. Then, the pulses will go through the Bob setup where Bob will insert the bases phase modulation in order to know which state was sent by Alice. The preparation of the QKD state actually reflected the design of optical setup that needs to be used.

3.2 Free space QKD

Spontaneous parametric down conversion (SPDC) process in nonlinear optical materials is utilized in order to create one of the four Bell states which are maximally entangled. The states can mathematically be written as follows:

$$|\Phi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1 \otimes |V\rangle_2 \pm |V\rangle_1 \otimes |H\rangle_2),$$
$$|\Psi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1 \otimes |H\rangle_2 \pm |V\rangle_1 \otimes |V\rangle_2),$$

$|H\rangle$ ($|V\rangle$) denotes Horizontal (Vertical) polarisation of the photons. We use the notation $\otimes$, as a tensor product describing a composite system of two spatially separated photons. Since the medium is free space the polarisation states are used as the coding method. SPDC process will be able to produce the entangled photon in polarisation state. The value of the measurement can only be revealed by measuring the signal state. This is an ideal random generator for QKD system where both Alice and Bob only know what they are measuring by comparing the bases that they used.

In the QKD system, the entangled photon source of this system needs to be placed somewhere between Alice and

Bob. This means that it is also possible to locate it near (next) to Alice's setup. Alice will measure one of the detector arms by setting the azimuth angle of HWP in path-2 θ_2 to be rectilinear or diagonal bases which correspond to the state of $|V\rangle$, $|D\rangle$, $|H\rangle$ or $|A\rangle$ that Alice measured. In Bob's measurement, while the azimuth angle of HWP in path-2 θ_2 was set to Alice measurement bases, the azimuth angle of HWP in path-1 was rotated to the respective bases. This setup corresponds to the projection measurement onto $|L\rangle \otimes |\theta\rangle$ or $|R\rangle \otimes |\theta\rangle$ where $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$, $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$, and $|\theta\rangle = \cos\theta\,|H\rangle + i\sin\theta|V\rangle$. Since the density matrix of the states approximately described by $\hat{\rho} = p|\Psi^+\rangle\langle\Psi^+| + q|\Psi^-\rangle\langle\Psi^-|$, where p and q are probabilities of finding our system in the state $|\Psi^+\rangle$ and $|\Psi^-\rangle$, respectively. The state should exhibit interference in coincidence rates for the two detector in proportion to $R_C(\theta_1, \theta_2) \propto \cos^2(\theta_1 - \theta_2)$.

5 Conclusion

The preparation of the photon state is the main characteristic that determines experimental setup of the QKD system. The preparation is not only to address the issue of how to produce the state but also how to measure the state so that it can translate the key from one end to another end while maintaining the quantum properties. The visibilities of the interference pattern actually the main important characteristic since it will translate to a good data coding, decoding, and reduced errors during preparation and measurement. Both two setups presented produced good visibilities (90%~98%) which come from good optical setup preparation and configuration.

References

1. Quantum Computer Could Solve Problems In A Few Months That Would Take Conventional Computers Millions Of Years (http://www:sciencedaily:com=releases=2001=09=010913074828:htm), Accessed on 24th March 2010
2. Beyond the PC: Atomic QC Quantum computers could be a billion times faster than Pentium III(http://www:amd1:com=quantum computers:html) Accessed on 14 January 2010Luigi T. De Luca, *Propulsion physics*, EDP Sciences, Les Ulis, (2009)
3. P.G. Kwiat, E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard, Phys. Rev. A 60, R773 (1999).
4. Norshamsuri Ali, Hafzulfika, Salim Ali Al-Kathiri, Abdulla Al-Attas, Suhairi Saharudin, and Mohamed Ridza Wahiddin, *International Conference on Cryptography, Coding and Information Security*, (2008).
5. Norshamsuri Ali, Hafizulfika, and Salim Ali Al-Kathiri, The NCTT-MCP, (2008).
6. Suryadi, Norshamsuri Ali, Suhairi Saharudin, and Mohamed Ridza Wahiddin, MIMOS R&D Symposium, (2006).
7. Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds (http://eprint.iacr.org/2009/374.pdf)
8. Alex Biryukov and Dmitry Khovratovich, Related key Cryptanalysis of the Full AES-192 and AES-256 (https://cryptolux.org/mediawiki/uploads/1/1a/Aes-192-256.pdf)
9. C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Demonstration of a Fundamental Quantum Logic Gate (http://tf.nist.gov/general/pdf/140.pdf)